Department of Computer Science,
University of Otago

Technical Report OUCS-2003-05

The enumeration of simple permutations

M.H.Albert, M.D.Atkinson
Department of Computer Science, University of Otago
M.Klazar
Department of Applied Mathematics and Institute for Theoretical
Computer Science, Charles University, Prague, Czech Republic

Status: Submitted to Journal of Integer Sequences

Department of Computer Science,
University of Otago, PO Box 56, Dunedin, Otago, New Zealand

http://www.cs.otago.ac.nz/trseries/

The enumeration of simple permutations

M.H. Albert[*] M.D. Atkinson[†] M. Klazar[‡]

Abstract

A *simple permutation* is one which maps no proper non-singleton interval onto an interval. We consider the enumeration of simple permutations from several aspects. Our results include a straightforward relationship between the ordinary generating function for simple permutations and that for all permutations, that the coefficients of this series are not P-recursive, an asymptotic expansion for these coefficients, and a number of congruence results.

Keywords: Permutation, P-recursiveness, asymptotic enumeration.
AMS Subject Classification: 05A05, 05A15, 05A16, 11A07

1 Introduction and definitions

The permutation 2647513 maps the interval 2..5 onto the interval 4..7. In other words, it has a *segment* (set of consecutive positions) whose values form a *range* (set of consecutive values). Such a segment is called a *block* of the permutation. Every permutation has singleton blocks, together with the block $1..n$. If these are the only blocks the permutation is called *simple*. For

[*] Department of Computer Science, University of Otago, Dunedin, New Zealand. malbert@cs.otago.ac.nz

[†] Department of Computer Science, University of Otago, Dunedin, New Zealand. mike@cs.otago.ac.nz

[‡] Department of Applied Mathematics (KAM) and Institute for Theoretical Computer Science (ITI), Charles University, Malostranské náměstí 25, 118 00 Praha, Czech Republic. ITI is supported by the project LN00A056 of the Ministry of Education of the Czech Republic. klazar@kam.mff.cuni.cz

example, 58317462 is simple and the simple permutations of length up to 5 are as follows:.

Length	Simple permutations
1	1
2	12, 21
3	None
4	2413, 3142
5	24153, 25314, 31524, 35142, 41352, 42513

Simple permutations have recently had important applications in the study of pattern closed classes of permutations [1].

Let s_n denote the number of simple permutations of length n. We shall be concerned with properties of the sequence (s_n). Consider the ordinary generating functions:

$$\begin{aligned} F(x) &= \sum_{k=1}^{\infty} k! x^k; \\ S(x) &= \sum_{k=4}^{\infty} s_k x^k. \end{aligned}$$

We start $S(x)$ from x^4 because simple permutations of length 1 and 2 need special treatment. Later in this section we will see that the coefficients of S differ from those of $-F^{\langle -1 \rangle}$ (functional inverse, not reciprocal) alternately by 2 and -2. The coefficients of $F^{\langle -1 \rangle}(x)$ were considered by Comtet [4, p. 171] without any combinatorial interpretation. The sequence of absolute values of these coefficients appears as sequence A059372 of [12], and the first few terms are:

$$1, 2, 2, 4, 4, 48, 336, 2928, 28144, 298528, 3454432, 43286528.$$

So we shall see that the numbers s_n are:

$$1, 2, 0, 2, 6, 46, 338, 2926, 28146, 298526, 3454434, 43286526.$$

In section 2 we shall prove that (s_n) is not P-recursive (it cannot be defined by a linear recurrence with polynomial coefficients). In section 3 we derive

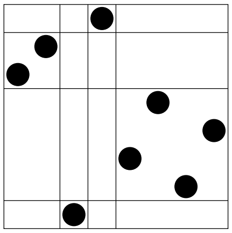

Figure 1: A block decomposition of 67183524. The pattern of the block decomposition is the permutation whose graph is defined by the occupied cells, namely 3142. Within each occupied cell, the individual blocks also define permutations namely 12, 1, 1, and 2413.

the asymptotic behaviour of s_n (the main term is $n!/\mathrm{e}^2$) and section 4 gives various congruences satisfied by the numbers s_n.

In the remainder of this section we derive a structure theorem that shows how arbitrary permutations are built from simple ones, and read off from it equations satisfied by generating functions. We begin with some terminology and notation that will be used throughout.

A *block decomposition* of a permutation σ is a partition of σ into blocks. Of course, if σ is simple there will only be the two trivial block decompositions. An example of a non-trivial decomposition is $\sigma = 67183524$ with blocks (67)(1)(8)(3524).

Given a block decomposition of σ, its *pattern* is the permutation defined by the relative order of the blocks. In the example above, the pattern of the block decomposition (67)(1)(8)(3524) is 3142. We may think of the permutation 67183524 as being constructed from the permutation 3142 by *inflating* each of the elements into a block, in this case the blocks 12, 1, 1, and 2413 (we view each block as a permutation in its own right). We write:

$$67183524 = (3142)[12, 1, 1, 2413].$$

This example is further illustrated in Figure 1. The inflation procedure is an instance of the wreath product for permutations [2].

A permutation which cannot be written in the form $(12)[\alpha, \beta]$ is called *plus indecomposable*, and one which cannot be written in the form $(21)[\alpha, \beta]$ is called *minus indecomposable.* Let i_n denote the number of plus indecomposable permutations of length n. The number of minus indecomposable permutations of length n is also i_n as is easily seen by considering the bijection on permutations of length n which sends π to π' where $\pi'(t) = n + 1 - \pi(t)$.

Theorem 1 *For every non-singleton permutation π there exists a unique simple non-singleton permutation σ, and permutations $\alpha_1, \alpha_2, \ldots, \alpha_k$ such that*

$$\pi = \sigma[\alpha_1, \alpha_2, \ldots, \alpha_k].$$

Moreover, if $\sigma \neq 12, 21$ then $\alpha_1, \alpha_2, \ldots, \alpha_k$ are also uniquely determined. If $\sigma = 12$ (respectively 21) then α_1 and α_2 are uniquely determined subject to the additional condition that α_1 be plus (respectively minus) indecomposable.

The caveat added for the case where $\sigma = 12$ (or 21) is necessary, as is easily seen by considering $\pi = 123$. This can be decomposed as $(12)[1, 12]$ or as $(12)[12, 1]$. However, only the former decomposition has a plus indecomposable first part.

Proof: We first of all suppose that π has two distinct maximal proper blocks A and B that have a non-empty intersection. Then, as the union of intersecting segments is a segment and the union of intersecting ranges is a range, $A \cup B$ is a block. Because of the maximality, $A \cup B = [n]$. But it is also clear that A cannot be an interior segment of $[n]$ nor can it define an interior range. In other words we have

$$\pi = \sigma[\alpha, \beta]$$

where $\sigma = 12$ or $\sigma = 21$. These two possibilities are obviously mutually exclusive. In either case consider all decompositions of π as $\sigma[\gamma, \delta]$. The intersection of their γ parts is also the γ part of a decomposition of this type. So there is a unique such decomposition with smallest γ part. Clearly, this part is plus indecomposable in the case $\sigma = 12$ and minus indecomposable if $\sigma = 21$.

We next suppose that every pair of distinct maximal blocks has empty intersection. Obviously, then the maximal blocks form a block decomposition of π and this decomposition must be coarser than every other block decomposition of π. It follows that this decomposition is the only one whose pattern σ is simple and so we obtain the unique representation claimed for π. ■

We shall shortly see that this theorem gives relations between the following three generating functions:

$$\begin{aligned} F(x) &= \sum_{k=1}^{\infty} k! x^k; \\ I(x) &= \sum_{k=1}^{\infty} i_k x^k; \\ S(x) &= \sum_{k=4}^{\infty} s_k x^k. \end{aligned}$$

Note that our generating functions are all taken to have zero constant term. This slightly unconventional choice turns out to be algebraically convenient at several points.

From Theorem 1 it is easy to see that there is a one to one correspondence between the collection of all permutations with length at least 2 and the collection of sequences:

$$(\sigma,\ \alpha_1, \alpha_2, \ldots, \alpha_k).$$

Here σ may be any simple permutation of length $k \geq 2$, and if $\sigma \neq 12, 21$ then α_1 through α_k are arbitrary permutations, while if $\sigma = 12$ (respectively 21), α_1 is plus-indecomposable (respectively minus indecomposable) and α_2 is arbitrary.

This correspondence, together with the earlier observation that the numbers of plus and minus indecomposable permutations of length n are the same, translates naturally into the following equation:

$$F(x) = x + 2I(x)F(x) + (S \circ F)(x). \tag{1}$$

However, since a plus indecomposable permutation cannot correspond to a sequence beginning with 12, while all other sequences do represent plus indecomposables, it is also clear from the correspondence that

$$I(x) = x + I(x)F(x) + (S \circ F)(x).$$

Solving this latter equation for I, and then substituting in equation (1) before solving for $S \circ F$ gives:

$$(S \circ F)(x) = \frac{F(x) - F(x)^2}{1 + F(x)} - x.$$

Now letting $t = F(x)$ we obtain:

$$S(t) = t - \frac{2t^2}{1+t} - F^{\langle -1 \rangle}(t). \tag{2}$$

We can also obtain an equation for the ordinary generating function of plus indecomposable permutations through the observation that every permutation decomposes into a sequence of plus indecomposable permutations so

$$F(x) = \frac{I(x)}{1 - I(x)}$$

or equivalently

$$I(x) = \frac{F(x)}{1 + F(x)}. \tag{3}$$

Denoting the coefficient of t^n in $F^{\langle -1 \rangle}(t)$ by Com_n (in reference to Comtet who initiated the consideration of this sequence) we obtain directly from equation (2) the simple relationship that for $n \geq 4$:

$$s_n = -\mathrm{Com}_n + (-1)^{n+1} \cdot 2.$$

2 Non P-recursiveness

A sequence of numbers (a_n) is called P-recursive if it satisfies a linear recurrence with polynomial coefficients. A power series is called D-finite if it satisfies a linear differential equation with polynomial coefficients. A sequence (a_n) is P-recursive if and only if its ordinary generating function $A(x) = \sum_n a_n x^n$ is D-finite. More information on D-finiteness and P-recursiveness can be found in Stanley [13, Chapter 6]. If $a_n = n!$ then $a_n - n a_{n-1} = 0$, and thus the sequence $(n!)$ is P-recursive. We show that on the other hand neither sequence (i_n) nor (s_n) is P-recursive. By (2), instead of the latter sequence we can work with (Com_n).

Proposition 2 *The power series $I(x)$ and $C(x) = F^{\langle -1 \rangle}(x) = \sum_{k=1}^{\infty} \mathrm{Com}_k x^k$ satisfy the differential equations*

$$\begin{aligned} I' &= -x^{-2} I^2 + (x^{-2} + x^{-1}) I - x^{-1}; \\ C' &= \frac{C^2}{x - (1+x)C}. \end{aligned}$$

Proof: It follows from the recurrence for $n!$ that $F(x)$ satisfies $x + xF + x^2F' = F$. Thus $F' = ((1-x)F - x)/x^2$. Combining this with $F = I/(1-I)$ we obtain the differential equation for $I(x)$. Similarly, $C' = 1/F'(C) = C^2/((1-C)x - C)$ which is the differential equation for $C(x)$. ■

Klazar [8] used the following method to show that a sequence (a_n) is not P-recursive. Suppose that the ordinary generating function $A(x)$ is non-analytic and satisfies a first order differential equation $A' = R(x, A)$ where R is some expression. Differentiating this relationship and replacing A' by $R(x, A)$, the derivatives of A are expressed as $A^{(k)} = R_k(x, A)$; $R_0(x, A) = A$ and $R_1(x, A) = R(x, A)$. Substituting $R_k(x, A)$ in the equation of D-finiteness

$$b_0A + b_1A' + b_2A'' + \cdots + b_sA^{(s)} = 0,$$

where $s \geq 1$, $b_i \in \mathbf{C}(x)$ and $b_s \neq 0$, we get a non-differential equation $\sum_{k=0}^{s} b_kR_k(x, A) = 0$. If R is such that the expressions $R_0, R_1, R_2, \ldots$ are (i) analytic or even algebraic and (ii) linearly independent over $\mathbf{C}(x)$, we have a nontrivial analytic equation for A. This implies that A is analytic (see Klazar's paper [8] for more details) which is a contradiction. So A cannot be D-finite and the sequence of its coefficients cannot be P-recursive.

To state the result of [8] precisely, we remind the reader that a power series $R(x, y) \in \mathbf{C}[[x, y]]$ is analytic if it absolutely converges in a neighborhood of the origin and that $R(x, y) \in \mathbf{C}((x, y))$ is an analytic Laurent series if, for some positive integer k, $(xy)^kR(x, y) \in \mathbf{C}[[x, y]]$ is analytic. Theorem 1 of [8] says that if $A \in \mathbf{C}[[x]]$ is non-analytic, $R(x, y) \in \mathbf{C}((x, y))$ is analytic, $A' = R(x, A)$, and R contains at least one monomial ax^iy^j, $a \neq 0$, with $j < 0$, then A is not D-finite. This result applies directly neither to $I(x)$ nor $C(x)$ (see Proposition 2) because in the case of $I(x)$ the last condition on R is not satisfied and in the case of $C(x)$ the right hand side R even cannot be expanded as a Laurent series.

However, the substitution $x - (1 + x)C(x) = \theta(x)$ transforms the second differential equation of Proposition 2 into

$$\theta' = -\frac{x^2}{1+x} \cdot \frac{1}{\theta} + \frac{1+2x}{1+x}.$$

Now all conditions are satisfied ($F(x)$ is clearly non-analytic which implies that $C(x)$ and $\theta(x)$ are non-analytic) and thus $\theta(x)$ is not D-finite by Theorem 1 of [8]. The dependence of $C(x)$ and $S(x)$ on $\theta(x)$ and the fact that D-finite power series form a $\mathbf{C}(x)$-algebra ([13, Theorem 6.4.9]) shows that neither $C(x)$ nor $S(x)$ is D-finite.

In order to deal with the case of $I(x)$, we use this opportunity to complement Theorem 1 of [8] in which $R \in \mathbf{C}((x, y))$ by the following theorem which treats the case $R \in \mathbf{C}(x, y)$. Neither of the theorems subsumes the other because not every rational function in x and y can be represented by an element of $\mathbf{C}((x, y))$ (as we have seen) and, of course, not every Laurent series sums up to a rational function. However, the next theorem seems to be more useful because in both examples in [8] and both examples here the right hand side $R(x, y)$ is, in fact, a rational function.

Theorem 3 *Let $P, Q \in \mathbf{C}[x, y]$ be two nonzero coprime polynomials and $A \in \mathbf{C}[[x]]$ be a non-analytic power series which satisfies the differential equation*

$$A' = \frac{P(x, A)}{Q(x, A)}.$$

If $\deg_y Q = 0$ and $\deg_y P \leq 1$ then A is, trivially, D-finite. In all remaining cases A is not D-finite.

Proof: The first claim is clear. If $\deg_y Q = 0$ and $r = \deg_y P \geq 2$ then $A' = a_0 + a_1 A + \cdots + a_r A^r$ where $a_i \in \mathbf{C}(x)$, $r \geq 2$, and $a_r \neq 0$. Differentiation by x gives

$$A^{(k)} = R_k(x, A) = a_{0,k} + a_{1,k} A + \cdots + a_{kr-k+1,k} A^{kr-k+1}$$

where $a_{i,j} \in \mathbf{C}(x)$ and

$$a_{kr-k+1,k} = r(2r-1)(3r-2)\ldots((k-1)r-k+2)a_r^k \neq 0.$$

Thus $R_k(x, y) \in \mathbf{C}(x)[y]$ have y-degrees $kr - k + 1$, $k = 0, 1, 2, \ldots$, which is for $r \geq 2$ a strictly increasing sequence. Therefore $R_0, R_1, R_2, \ldots$ are linearly independent over $\mathbf{C}(x)$ and, by the above discussion, A is not D-finite.

In the remaining case $\deg_y Q \geq 1$. Differentiation of $A' = R(x, A) = P(x, A)/Q(x, A)$ by x gives $A^{(k)} = R_k(x, A)$ where $R_k(x, y) \in \mathbf{C}(x, y)$. For example,

$$\begin{aligned} R_2 &= \frac{(P_x + P_y R_1)Q - P(Q_x + Q_y R_1)}{Q^2} \\ &= \frac{P_x Q - P Q_x}{Q^2} + \frac{P(P_y Q - P Q_y)}{Q^3}. \end{aligned}$$

Let α, $Q(x,\alpha)=0$, be a pole of $R_1(x,y)$ of order $\mathrm{ord}_\alpha(R_1)=\mathrm{ord}_\alpha(P/Q)=-\mathrm{ord}_\alpha(Q)=l\geq 1$. We have $\mathrm{ord}_\alpha((P_xQ-PQ_x)Q^{-2})\leq 2l$ and $\mathrm{ord}_\alpha(P(P_yQ-PQ_y)Q^{-3})=3l+\mathrm{ord}_\alpha(P_yQ-PQ_y)=2l+1$ since $\mathrm{ord}_\alpha(P)=0$, $\mathrm{ord}_\alpha(P_yQ)\leq -l$, and $\mathrm{ord}_\alpha(PQ_y)=-l+1$. So $\mathrm{ord}_\alpha(R_2)=2l+1$. In general, the same argument shows that $\mathrm{ord}_\alpha(R_{k+1})=2\cdot\mathrm{ord}_\alpha(R_k)+1$. Hence $\mathrm{ord}_\alpha(R_k)=2^{k-1}l+2^{k-1}-1$, $k=1,2,\ldots$. This is a strictly increasing sequence and we conclude again, since $R_0,R_1,R_2,\ldots$ are linearly independent over $\mathbf{C}(x)$, that A is not D-finite. ■

Proposition 2 and Theorem 3 show that $I(x)$ is not D-finite and we can summarize the results of this section in the following corollary.

Corollary 4 *The sequences* (i_n), (Com_n), *and* (s_n) *are not P-recursive.*

3 Asymptotics

We turn now to the computation of an asymptotic expansion for the numbers s_n. We will prove that:

Theorem 5

$$s_n=\frac{n!}{\mathrm{e}^2}\left(1-\frac{4}{n}+\frac{2}{n(n-1)}+O(n^{-3})\right).$$

Our methods are such that, in principle, higher order terms could be obtained as a matter of brute force computation. In order to carry out this expansion we will first consider permutations which may not be simple, but whose non-trivial blocks all have length greater than some fixed value m. We will apply inclusion-exclusion arguments (dressed in the form of generating functions [5, 6]), an argument which allows us to reduce the number of terms considered, and a bootstrapping approach.

The case $m=2$, was already considered by Kaplansky [7]. Permutations of this type are those in which no two elements consecutive in position are also consecutive in value (in either order). These were called irreducible permutations by Atkinson and Stitt [2], but there is no standard terminology in the field. Indeed the permutations that we have referred to as plus and minus indecomposable have also been called irreducible in other contexts.

An amusing equivalent form for the case $m = 2$ is that the number of such permutations is also the number of ways of placing n mutually non-attacking *krooks* on an $n \times n$ chessboard. A krook is a piece which can move either like a king, or a rook in chess. Kaplansky's expansion is:

$$\frac{n!}{\mathrm{e}^2}\left(1 - \frac{2}{n(n-1)} + O(n^{-3})\right).$$

In fact he derives asymptotic forms for the number of permutations containing exactly r blocks of length 2 for any r. Our methods parallel his, and could also be used to derive such detailed information.

The decomposition provided by Theorem 1 of a permutation into its maximal proper blocks represents a top down view of how non-simple permutations are constructed from simple ones. There is a corresponding bottom-up view that focuses on minimal blocks, put together in an arbitrary order. By a *minimal block* in π we mean a non-singleton block in π minimal with respect to inclusion. Note that the pattern of each minimal block is that of a simple permutation. Any permutation can be decomposed into minimal blocks and singletons, e.g., $3524716 = (3524)(7)(1)(6)$. However, this decomposition is not unique, for two essentially different reasons. The first one is that decompositions $\pi = \sigma[\alpha_1, \alpha_2, \ldots, \alpha_k]$, where σ is arbitrary and α_i are simple, are not unique because it may be possible to coalesce singletons into simple blocks, or vice versa. Thus besides $3524716 = 2413[2413, 1, 1, 1]$ we also have $3524716 = 3524716[1, 1, 1, 1, 1, 1, 1]$. The second problem is that we require any two minimal blocks to be disjoint. While this is necessarily true whenever either of them has length more than 2, two minimal blocks of length 2 may intersect, as in 123. Thus we consider decompositions $\pi = \sigma[\alpha_1, \alpha_2, \ldots, \alpha_k]$ where σ is arbitrary and each α_i is either 1, a simple permutation of length at least 4, or the identity permutation of length at least 2 or its reverse. We refer to blocks of the latter type as *clusters* in π.

By using clusters we have solved the second problem but the non-uniqueness remains and, moreover, we have introduced another source of it: consecutive (reversed) identical permutations may coalesce into longer (reversed) identical permutations, as in $345612 = 21[1234, 12] = 231[12, 12, 12]$. To remedy the non-uniqueness we introduce the notion of *marking* a permutation. A *marked permutation* (π, M) consists of a permutation π and a collection M of minimal blocks of π. A *marked cluster* in (π, M) is a maximal chain of marked overlapping minimal blocks of length 2 (a marked cluster may be a proper subset of a maximal cluster). Let $\mathcal{B}_1$ denote the set of all simple permutations of length at least 4 and $\mathcal{B}_2$ denote the set of all identical permutations of length at least 2 and their reversals. Marking makes our decomposition unique:

Theorem 6 *Let X be the set of all marked permutations (π, M) and Y be the set of all sequences $(\sigma; \alpha_1, \alpha_2, \ldots, \alpha_k)$ where σ is any permutation of length $k \geq 1$ and $\alpha_i \in \{1\} \cup \mathcal{B}_1 \cup \mathcal{B}_2$. There is a bijection between the sets X and Y such that if $(\pi, M) \mapsto (\sigma; \alpha_1, \alpha_2, \ldots, \alpha_k)$, where r of the α_i belong to $\mathcal{B}_1$ and s of them to $\mathcal{B}_2$, then*

$$\pi = \sigma[\alpha_1, \alpha_2, \ldots, \alpha_k]$$

and $|M| = r + l - s$ where l is the total length of the α_i belonging to $\mathcal{B}_2$.

Proof: Given a marked permutation, collapse its marked minimal blocks of length at least 4 and its marked clusters into singletons. This gives the permutation σ. If the i-th term of σ was not obtained by collapse then $\alpha_i = 1$, otherwise α_i equals to the corresponding element of $\mathcal{B}_1 \cup \mathcal{B}_2$. Since each $\alpha_i \in \mathcal{B}_1$ contributes 1 to $|M|$ and each $\alpha_i \in \mathcal{B}_2$ of length m contributes $m - 1$, we have $|M| = r + l - s$. It is clear that $\pi = \sigma[\alpha_1, \alpha_2, \ldots, \alpha_k]$ and that (π, M) can be uniquely recovered from $(\sigma; \alpha_1, \alpha_2, \ldots, \alpha_k)$. ■

Now suppose m to be some fixed value (we will later make choices of m suitable for our purposes, but will always assume that $m \geq 2$ since smaller values of m are trivial). Each permutation π has an associated collection $B_m(\pi)$ consisting of the minimal blocks of π whose length is less than or equal to m. So, if π is simple and of length greater than m, $B_m(\pi)$ is empty, while for $\pi = 5672413$, $B_2(\pi) = \{56, 67\}$, and $B_4(\pi) = \{56, 67, 2413\}$. An *$m$-marking* of π is simply a subset of $B_m(\pi)$. We consider the generating function:

$$F_m(x, v) = \sum_{\pi} x^{|\pi|} \sum_{M \subseteq B_m(\pi)} v^{|M|} = \sum_{\pi} x^{|\pi|} (1 + v)^{|B_m(\pi)|}.$$

Then of course $F_m(x, -1)$ is the ordinary generating function for permutations all of whose non-singleton blocks have length greater than m.

We remark that $F_m(x, t - 1)$ is the generating function where the coefficient of $x^n t^k$ is precisely the number of permutations of length n with k minimal blocks of length less than or equal to m.

Let

$$S_m(x) = \sum_{j=4}^{m} s_j x^j.$$

We apply the bijection of Theorem 6 to marked permutations which contain no marked minimal blocks of length more than m. It follows that the generating function of the corresponding permutations $\alpha \in \{1\} \cup \mathcal{B}_1 \cup \mathcal{B}_2$, in which x counts the length and v the contribution to $|M|$, is

$$x + vS_m(x) + \frac{2vx^2}{1 - vx}.$$

So:

$$F_m(x, v) = \sum_{k \geq 1} k! \left(x + \frac{2vx^2}{1 - vx} + vS_m(x) \right)^k$$

from which it follows that:

$$f_m(x) := F_m(x, -1) = \sum_{k \geq 1} k! \left(x - \frac{2x^2}{1 + x} - S_m(x) \right)^k . \tag{4}$$

Before using this equation to derive asymptotic information about s_n we digress briefly to show how it can be used to obtain an alternative derivation of (2). Instead of using $S_m(x)$ in (4), use $S(x)$. This gives us $f_\infty(x)$, an ordinary generating function for permutations having no minimal block. The only such permutation is 1 so $f_\infty(x) = x$. That is:

$$x = F(x - \frac{2x^2}{1 + x} - S(x))$$

which yields (2) after applying $F^{\langle -1 \rangle}$ to both sides.

Now recall that $f_m(x)$ is the generating function for permutations all of whose blocks have length greater than m. In order to make use of these generating functions in the asymptotic computation of s_n we must determine a suitable value of m so that f_m provides useful information about s_n. To that end the following lemma is useful.

Lemma 7 *If $p_{n,k}$ denotes the number of permutations of length n which contain a minimal block of length k then for any fixed positive integer c:*

$$\sum_{k=c+2}^{n-c} \frac{p_{n,k}}{n!} = O(n^{-c}).$$

Proof: First observe that

$$p_{n,k} \leq s_k(n-k+1)(n-k+1)!$$

since the right hand side counts the number of ways to choose the structure of a block of length k, to choose its minimal element, and to arrange it with other elements, so it overcounts permutations with more than one such block.

The estimate given then follows directly by using the fact that $s_k \leq k!$. Only the two extreme terms in the sum can have magnitude as large as $O(n^{-c})$, and the remaining terms have magnitude $O(n^{-c-1})$. Since there are fewer than n terms, the result follows. ∎

So when seeking an asymptotic expansion of $s_n/n!$ with an error term of $O(n^{-c-1})$ we may count instead the permutations which contain no blocks of length less than or equal to $c+2$, or greater than or equal to $n-c$. In particular, as a direct consequence of the result quoted above due to Kaplansky [7] we obtain:

Observation 8

$$\frac{s_n}{n!} = \frac{1}{\mathrm{e}^2} + O(n^{-1}).$$

An alternative proof of this result follows from a more general theorem of Bender and Richmond [3] which provides the first order asymptotics of a class of series which include the inverse series of $F(x)$.

We will set as our goal to obtain the asymptotics of $s_n/n!$ with error term $O(n^{-3})$. However, the technique we use is completely general, and could be applied, at the expense of a great deal of tedious computation, to any fixed error bound of this type. By the remarks above, we may ignore minimal block sizes between 5 and $n-3$ inclusive. We first consider $f_4(x)$ which enumerates permutations having no minimal blocks of size less than or equal to 4. Recall that:

$$f_4(x) = \sum_{k\geq 1} k! \left(x - \frac{2x^2}{1+x} - 2x^4 \right)^k.$$

So:

$$\frac{1}{n!}[t^n]f_4(t) \quad = \quad \frac{1}{n!}\sum_{k=0}^{\infty} k!\,[t^n]\left(t - \frac{2t^2}{1+t} - 2t^4 \right)^k$$

$$\begin{aligned}
&= \frac{1}{n!}\sum_{k=0}^{\infty} k!\,[t^{n-k}]\left(1-\frac{2t}{1+t}-2t^3\right)^k \\
&= \frac{1}{n!}\sum_{l=0}^{n}(n-l)!\,[t^l]\left(1-\frac{2t}{1+t}-2t^3\right)^{n-l} \\
&= \frac{1}{n!}\sum_{l=0}^{n}(n-l)!\sum_{i=0}^{l}(-2)^i\binom{n-l}{i}[t^l]\left(\frac{t}{1+t}+t^3\right)^i \\
&= \frac{1}{n!}\sum_{l=0}^{n}(n-l)!\sum_{i=0}^{l}(-2)^i\binom{n-l}{i}[t^{l-i}]\left(\frac{1}{1+t}+t^2\right)^i. \qquad (5)
\end{aligned}$$

Consider now any fixed value of l in equation (5). In order to obtain terms whose order in n is n^{-2} or more, we need only consider the values $l-2 \le i \le l$. Despite the fact that we sum over values of l running from 0 through n, we may safely ignore the other terms. As we shall see in computing the three significant terms the summation over l does not affect the order of the terms.

So, the three terms that we need to consider are:

$$\begin{aligned}
&\tfrac{(n-l)!}{n!}(-2)^l\tbinom{n-l}{l}+ \\
&\tfrac{(n-l)!}{n!}\left((-2)^{l-1}\tbinom{n-l}{l-1}(-l+1)\right)+ \\
&\tfrac{(n-l)!}{n!}\left((-2)^{l-2}\tbinom{n-l}{l-2}\left((-l+2)(-l+1)/2+l-2\right)\right).
\end{aligned} \qquad (6)$$

Each of these terms will be converted to the form:

$$\frac{(-2)^l}{l!}\,(\text{an asymptotic expansion in } n)\,.$$

Since the first two and the first part of the third, are the same as those arising in the $m=2$ case, we can make use of their known form, that is, use the asymptotics from Kaplansky's result, leaving only the term

$$\begin{aligned}
\frac{(n-l)!(-2)^{l-2}(l-2)}{n!}\binom{n-l}{l-2} &= \frac{(-2)^l}{l!}\left(\frac{l(l-1)(l-2)}{4}\,\frac{(n-l)!(n-l)!}{n!(n-2l+2)!}\right) \\
&= \frac{(-2)^l}{l!}\left(\frac{l(l-1)(l-2)}{4n(n-1)}+O(n^{-3})\right)
\end{aligned}$$

Summing this expression over l gives $-2\mathrm{e}^{-2}/n(n-1)+O(n^{-3})$.

Now we combine this additional term with Kaplansky's results to give the asymptotic expansion of $[t^n]f_4(t)$ through three terms as:

$$[t^n]f_4(t) = \frac{n!}{\mathrm{e}^2}\left(1-\frac{4}{n(n-1)}+O(n^{-3})\right).$$

Finally we use this in establishing the second order asymptotics of s_n. From Observation 8 applied to s_{n-1} we obtain:

$$s_{n-1} = \frac{n!}{\mathrm{e}^2}\left(\frac{1}{n} + O(n^{-2})\right).$$

Furthermore, the number of permutations of length n containing a simple block of length $n-1$ is precisely $4s_{n-1}$. Since, in computing the $1/n$ term in the expansion of s_n we can ignore contributions arising from blocks of length $n-2$, and since the events of having a simple block of length from 2 to 4, and having a simple block of length $(n-1)$ are disjoint:

$$\begin{aligned} s_n &= [t^n]f_4(t) - 4s_{n-1} + O(n^{-2}n!); \\ &= \frac{n!}{\mathrm{e}^2}\left(1 - \frac{4}{n} + O(n^{-2})\right). \end{aligned}$$

We apply this bootstrap approach once more to get the second order behaviour. We now know that:

$$\begin{aligned} s_{n-1} &= \frac{n!}{\mathrm{e}^2}\left(\frac{1}{n} - \frac{4}{n(n-1)} + O(n^{-3})\right) \\ s_{n-2} &= \frac{n!}{\mathrm{e}^2}\left(\frac{1}{n(n-1)} + O(n^{-3})\right). \end{aligned}$$

Furthermore there are $18s_{n-2}$ permutations of length n containing a simple block of length $n-2$. However, of these $8s_{n-2}$ also contain a simple block of length 2. So:

$$\begin{aligned} s_n &= [t^n]f_4(t) - 4s_{n-1} - 10s_{n-2} + O(n^{-3}n!) \\ &= \frac{n!}{\mathrm{e}^2}\left(1 - \frac{4}{n} + \frac{2}{n(n-1)} + O(n^{-3})\right), \end{aligned}$$

as we claimed at the beginning of this section.

Finally, in this section we note that the asymptotic estimate of s_n is, as might be expected, a poor approximation. For example, $s_{20} = 264111424634864638$ and our asymptotic estimate has a relative error of about 3.89×10^{-3}.

4 Congruences

In this section we derive congruence properties of the numbers Com_n for the moduli 2^a and 3 (from which follow similar congruences for s_n). Our main tool is the following result that follows immediately from the Lagrange inversion formula.

Lemma 9

$$n \cdot \mathrm{Com}_n = [x^{n-1}] \left(\sum_{k \geq 0} (-1)^k (2!x + 3!x^2 + \cdots)^k \right)^n .$$

For a prime p, let $\mathrm{ord}_p(n)$ denote the largest integer m such that p^m divides n. As the following table shows, $\mathrm{ord}_2(\mathrm{Com}_n)$ is unexpectedly large:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$\mathrm{ord}_2(\mathrm{Com}_n)$	0	1	1	2	2	4	4	4	4	5	5	15	13	12	12	8	8	9	9	10	10	12	12	14	14	15	15	17	17	22

In Theorem 11 we give a lower bound on $\mathrm{ord}_2(\mathrm{Com}_n)$ which is tight for infinitely many n and we completely characterize the values of n for which the equality is attained.

For convenience we note the following result that follows directly from the well-known formula

$$\mathrm{ord}_p(m!) = \left\lfloor \frac{m}{p} \right\rfloor + \left\lfloor \frac{m}{p^2} \right\rfloor + \cdots$$

Lemma 10 *For all m, $\mathrm{ord}_2((m+1)!) \geq \left\lceil \frac{m}{2} \right\rceil$ where equality holds if and only if $m = 1$ or 2. Also, $\mathrm{ord}_3(m!) \leq m - 1$ for all m.*

Theorem 11 *Let $m = \lfloor n/2 \rfloor$. Then*

$$\mathrm{ord}_2(\mathrm{Com}_n) \geq \left\lceil \frac{n-1}{2} \right\rceil .$$

Equality holds if and only if $\binom{3m}{m}$ is odd and this happens if and only if the binary expansion of m has no two consecutive unit digits.

Proof: Let the numbers b_k, $k \geq 0$, be defined by

$$\sum_{k\geq 0} b_k x^k = \sum_{k\geq 0} (-1)^k (2!x + 3!x^2 + \cdots)^k.$$

Thus $b_0 = 1$ and for $k \geq 1$,

$$b_k = \sum_{\substack{c_1,c_2,\ldots,c_s \geq 1 \\ c_1+c_2+\cdots+c_s=k}} (-1)^s \cdot (c_1+1)! \cdot (c_2+1)! \cdot \ldots \cdot (c_s+1)!.$$

By Lemma 9,

$$n \cdot \mathrm{Com}_n = \sum_{\substack{k_1,k_2,\ldots,k_n \geq 0 \\ k_1+k_2+\cdots+k_n=n-1}} b_{k_1} b_{k_2} \ldots b_{k_n}.$$

By Lemma 10, $\mathrm{ord}_2((c+1)!) \geq c/2$ for all c. Hence, for all k and n,

$$\mathrm{ord}_2(b_k) \geq \frac{k}{2} \quad \text{and} \quad \mathrm{ord}_2(n \cdot \mathrm{Com}_n) \geq \frac{n-1}{2}.$$

In particular, for odd n we have $\mathrm{ord}_2(\mathrm{Com}_n) = \mathrm{ord}_2(n \cdot \mathrm{Com}_n) \geq (n-1)/2$.

To obtain the more exact result of the theorem we need the following better estimates for $\mathrm{ord}_2(b_k)$:

$$\mathrm{ord}_2(b_k) \begin{cases} = k/2 & \text{for even } k; \\ = (k+1)/2 & \text{for } k \equiv 1 \bmod 4; \\ > (k+1)/2 & \text{for } k \equiv 3 \bmod 4. \end{cases}$$

To prove them we look more closely at the sum for b_k. Suppose first that k is even. Then the sum has exactly one summand with ord_2 equal to $k/2$, namely that with $c_1 = c_2 = \ldots = c_{k/2} = 2$ (by Lemma 10, $\mathrm{ord}_2((c+1)!) = c/2$ only if $c = 2$), and the other summands have ord_2 bigger than $k/2$. Hence $\mathrm{ord}_2(b_k) = k/2$. Now suppose that k is odd. Then each summand has an odd number of odd c_i's. The summands t with three and more odd c_i's satisfy $\mathrm{ord}_2(t) \geq (k+3)/2$ (each odd c_i contributes $1/2$ to $k/2$). The same is true if t has only one odd c_i but that c_i is not 1 (by Lemma 10, $\mathrm{ord}_2((c+1)!) \geq (c+3)/2$ for odd $c > 1$), or if some even c_i is not 2 (Lemma 10). The remaining summands t, in which $c_i = 2$ with multiplicity $(k-1)/2$ and once $c_i = 1$, satisfy $\mathrm{ord}_2(t) = (k+1)/2$. We see that, for odd k, $\mathrm{ord}_2(b_k) = (k+1)/2$ if and only if the number of the remaining summands is odd. This number equals $(k-1)/2 + 1 = (k+1)/2$. So $\mathrm{ord}_2(b_k) = (k+1)/2$ if and only if $k \equiv 1$ mod 4.

Let $n = 2m + 1$ be odd. If s is a summand of the above sum for $n \cdot \mathrm{Com}_n$, then $\mathrm{ord}_2(s) = (n-1)/2$ if and only if all k_i in s are even; other summands t have $\mathrm{ord}_2(t) > (n-1)/2$. It follows that $\mathrm{ord}_2(\mathrm{Com}_n) = (n-1)/2$ if and only if the number of the former summands s is odd. This number equals

$$[x^{n-1}]\left(\sum_{r\ge 0} x^{2r}\right)^n = [x^{n-1}]\frac{1}{(1-x^2)^n} = [x^{n-1}]\sum_{r\ge 0}\binom{n+r-1}{r}x^{2r} = \binom{3m}{m}.$$

Let $n = 2m$ be even. We know that $\mathrm{ord}_2(b_k) = k/2$ for even k and $\mathrm{ord}_2(b_k) \ge (k+1)/2$ for odd k. In the sum for $n \cdot \mathrm{Com}_n$, every composition $k_1 + k_2 + \cdots + k_n = n - 1$ of $n - 1$ has an odd number of odd parts. For any t-tuple $l_1, l_2, \ldots, l_t$, where t and all l_i are odd and $l_1 + \cdots + l_t \le n - 1$, we let $S(l_1, l_2, \ldots, l_t)$ denote the sum of those $b_{k_1} b_{k_2} \ldots b_{k_n}$ with $k_1 + k_2 + \cdots + k_n = n - 1$ in which $k_i = l_i$, $1 \le i \le t$, and k_i is even for $i > t$. It follows that

$$n \cdot \mathrm{Com}_n = \sum \binom{n}{t} S(l_1, l_2, \ldots, l_t)$$

where we sum over all mentioned t-tuples $l_1, l_2, \ldots, l_t$. By the properties of ord_2 and of the numbers b_k, $\mathrm{ord}_2(S(l_1, l_2, \ldots, l_t)) \ge (n + t - 1)/2$. Also, for odd t we have $\mathrm{ord}_2(\binom{n}{t}) = \mathrm{ord}_2(\frac{n}{t}\binom{n-1}{t-1}) = \mathrm{ord}_2(n) - \mathrm{ord}_2(t) + \mathrm{ord}_2(\binom{n-1}{t-1}) \ge \mathrm{ord}_2(n)$, and $\mathrm{ord}_2(\binom{n}{1}) = \mathrm{ord}_2(n)$. It follows that $\mathrm{ord}_2(\mathrm{Com}_n) \ge n/2$ and, moreover, $\mathrm{ord}_2(\mathrm{Com}_n) = n/2$ if and only if

$$\mathrm{ord}_2\left(\sum_{l \le n,\, l \text{ odd}} S(l)\right) = n/2.$$

In the last sum still many summands have ord_2 bigger than $n/2$: if $l \equiv 3$ mod 4 then $\mathrm{ord}(S(l)) > n/2$. On the other hand, if $l \equiv 1$ mod 4 then each summand $b_l b_{k_2} \ldots b_{k_n}$ in $S(l)$ has $\mathrm{ord}_2(b_l b_{k_2} \ldots b_{k_n}) = n/2$. We conclude that $\mathrm{ord}_2(\mathrm{Com}_n) = n/2$ if and only if the number $c(n)$ of compositions of $n - 1$ into n parts, where the first part is $\equiv 1$ mod 4 and the remaining $n - 1$ parts are even (zero parts are allowed), is odd. We have

$$\begin{aligned} c(n) &= [x^{n-1}]\frac{x}{1-x^4}\cdot\frac{1}{(1-x^2)^{n-1}} = [x^{n-1}]\frac{x}{1+x^2}\cdot\frac{1}{(1-x^2)^n} \\ &\equiv [x^{n-1}]\frac{x}{1-x^2}\cdot\frac{1}{(1-x^2)^n} = [x^{n-1}]\frac{x}{(1-x^2)^{n+1}} \bmod 2 \end{aligned}$$

$$\begin{aligned} &= \binom{3m-1}{m-1} \equiv \frac{3m}{m}\binom{3m-1}{m-1} \bmod 2 \\ &= \binom{3m}{m}. \end{aligned}$$

It was noted by Kummer [9], see also Singmaster [11], that $\mathrm{ord}_p(\binom{a+b}{b})$ is equal to the number of carries required when adding a and b in the p-ary notation. Applying this for $p = 2$, $a = m$, and $b = 2m$, we get the stated criterion. ■

Corollary 12 *For all $n \geq 3$,*

$$s_n \equiv \begin{cases} \;\;\,2 \mod 2^{(n-1)/2} & \text{for odd } n; \\ -2 \mod 2^{n/2} & \text{for even } n. \end{cases}$$

Let

$$C_n = \frac{1}{n+1}\binom{2n}{n}$$

be the nth Catalan number.

Proposition 13 *For all n,* $\mathrm{Com}_n \equiv C_{n-1} \bmod 3$.

Proof: We have, for every non-negative integer k,

$$(2!x + 3!x^2 + \cdots)^k = (2x)^k + 3a_k(x)$$

with $a_k(x) \in \mathbf{Z}[[x]]$. Thus

$$\begin{aligned} \sum_{k\geq 0}(-1)^k(2!x + 3!x^2 + \cdots)^k &= \frac{1}{1+2x} + 3\sum_{k\geq 0}(-1)^k a_k(x) \\ &= \frac{1}{1+2x} + 3b(x) \end{aligned}$$

with $b(x) \in \mathbf{Z}[[x]]$. Let $m = \mathrm{ord}_3(n)$. Since $\mathrm{ord}_3(k!) \leq k-1$ for every k (Lemma 10), we have

$$\mathrm{ord}_3\Big(3^k\tbinom{n}{k}\Big) \geq m+1 \text{ for } k = 1, 2, \ldots, n.$$

By Lemma 9,

$$\begin{aligned} n \cdot \mathrm{Com}_n = [x^{n-1}]\left(\frac{1}{1+2x} + 3b(x)\right)^n &\equiv [x^{n-1}]\frac{1}{(1+2x)^n} \bmod 3^{m+1} \\ &= (-2)^{n-1}\binom{2n-2}{n-1}. \end{aligned}$$

Canceling in the last congruence the common factor 3^m, we get

$$\frac{n}{3^m} \cdot \mathrm{Com}_n \equiv \frac{(-2)^{n-1}}{3^m}\binom{2n-2}{n-1} \equiv \frac{1}{3^m}\binom{2n-2}{n-1} \bmod 3.$$

Since $n/3^m \not\equiv 0 \bmod 3$, we can divide by it and get

$$\mathrm{Com}_n \equiv \frac{1}{n}\binom{2n-2}{n-1} \bmod 3.$$

■

Corollary 14 *For all $n > 2$,*

$$s_n \equiv -C_{n-1} + (-1)^n \bmod 3.$$

5 Concluding remarks

The simplicity property for permutations does not seem to have been studied until very recently [10, 1]. We have begun the study of the numbers s_n by showing that they are not P-recursive, giving the first few terms of their asymptotic expansion, and showing that they satisfy some unexpected congruence properties.

These results suggest a number of natural continuations. Although, in principle, we could obtain more terms of the asymptotic expansion the entire expansion remains elusive, and computing it seems to be rather a difficult problem. On the other hand we have some computational evidence to suggest that the sequence Com_n has additional congruence properties, particularly with respect to odd primes.

We suggest also some algorithmic problems that are natural counterparts to the enumerative results:

- How can one efficiently generate simple permutations in lexicographic order?

- Is it possible to generate simple permutations uniformly at random in worst-case linear time per permutation?

- How efficiently can one recognise a simple permutation?

With regards to the final question, there is a natural dynamic programming algorithm that achieves the task in $O(n^2)$ time; so the issue is whether one can do better.

References

[1] M.H. Albert and M.D. Atkinson, Simple permutations, partial well-order, and enumeration. In M.H. Albert ed., *Proceedings, Permutation Patterns 2003*, `www.cs.otago.ac.nz/trseries/oucs-2003-02.pdf`, 2003, pp. 5–9.

[2] M.D. Atkinson and T. Stitt, Restricted permutations and the wreath product. *Discrete Math.*, **259** (2002), 19–36.

[3] Edward A. Bender and L. Bruce Richmond, An asymptotic expansion for the coefficients of some power series. II. Lagrange inversion. *Discrete Math.*, **50** (1984), 135–141.

[4] Louis Comtet, *Advanced combinatorics.* D. Reidel, 1974.

[5] P. Flajolet and R. Sedgewick, *Analytic Combinatorics—Symbolic Combinatorics*, Preprint published electronically at, `http://algo.inria.fr/flajolet/Publications/books.html`, 2002.

[6] I. P. Goulden and D. M. Jackson, *Combinatorial enumeration.* John Wiley & Sons, 1983.

[7] Irving Kaplansky, The asymptotic distribution of runs of consecutive elements, *Ann. Math. Statistics*, **16** (1945), 200–203.

[8] Martin Klazar, Non-P-recursiveness of numbers of matchings or linear chord diagrams with many crossings, *Adv. Appl. Math.*, **30** (2003), 126–136.

[9] E. E. Kummer, Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgezetzen, *J. Reine Angew. Math.*, **44** (1852), 93–146.

[10] M. M. Murphy, *Restricted permutations, antichains, atomic classes and stack sorting*, PhD thesis, University of St. Andrews, 2002.

[11] David Singmaster, Notes on binomial coefficients. I. A generalization of Lucas' congruence, *J. London Math. Soc. (2)*, **8** (1974), 545–548.

[12] N.J.A. Sloane, The on-line encyclopedia of integer sequences, `http://www.research.att.com/~njas/sequences/`, 2003.

[13] Richard P. Stanley, *Enumerative combinatorics. Vol. 2*, volume 62 of *Cambridge Studies in Advanced Mathematics*, Cambridge University Press, 1999.