Stories about groups and sequences

Peter J. Cameron

School of Mathematical Sciences
Queen Mary and Westfield College
Mile End Road
London E1 4NS
U.K.

Beyond Ghor there was a city. All its inhabitants were blind. A king with his entourage arrived near by. He brought his army and camped in the desert. He had a mighty elephant, which he used in attack and to increase the people's awe.

The populace became anxious to see the elephant, and some sightless ones from among this blind community ran to find it. As they did not even know the form or shape of the elephant they groped sightlessly, gathering information by touching some part of it. Each thought he knew something, because he could feel a part.

When they returned to their fellow-citizens, eager groups clustered around them. Each of these was anxious to learn the truth from those who were themselves astray. They asked about the form, the shape of the elephant, and they listened to all they were told.

The man whose hand had reached an ear was asked about the elephant's nature. He said: "It is a large, rough thing, wide and broad, like a rug."

And the one who had felt the trunk said: "I have the real facts about it. It is like a straight and hollow pipe, awful and destructive."

The man who had felt its feet and legs said: "It is mighty and firm, like a pillar."

Mualana Jalaluddin Rumi (13th century) (from [34])

Abstract

The main theme of this article is that counting orbits of an infinite permutation group on finite subsets or tuples is very closely related to combinatorial enumeration; this point of view ties together various disparate "stories".

1 Two-graphs and even graphs

The first story originated with Neil Sloane, when he was compiling the first edition of his dictionary of integer sequences [35]. He observed that certain counting sequences appeared to agree.

The first sequence enumerates *even graphs*, those in which any vertex has even valency (so that the graph is a disjoint union of Eulerian graphs). These graphs were enumerated by Robinson [29] and Liskovec [18].

The second sequence counts switching classes of graphs. If Γ is a graph on the vertex set X, and Y is a subset of X, the result of *switching* Γ with respect to Y is obtained by deleting all edges between Y and its complement, putting in all edges between Y and its complement which didn't exist before, and leaving the rest unaltered. Switching is an equivalence relation on the graphs with vertex set X; the equivalence classes are called *switching classes*. This concept was introduced by Seidel [30] for studying strongly regular graphs.

The final sequence counts two-graphs. A *two-graph* on a set X consists of a set $\mathcal{T}$ of *triples* or 3-element subsets of X with the property that any 4-element subset of $\mathcal{T}$ contains an even number of elements of $\mathcal{T}$. Two-graphs were introduced by G. Higman in a construction of Conway's third sporadic group. The theory has been developed in many directions: Seidel has written several surveys [31], [33], [32]. They also link several themes in combinatorics, including equiangular lines in Euclidean space, and double covers of complete graphs.

It was already known that switching classes and two-graphs are equinumerous. There is a map from graphs on the set X to two-graphs on X, as follows: the triples of the two-graph are all 3-sets which contain an odd number of edges of the graph. Every two-graph is obtained in this way, and graphs Γ_1 and Γ_2 give the same two-graph if and only if they lie in the same switching class. So there is a natural bijection from switching classes to two-graphs.

It was also known that switching classes and even graphs on an odd number of vertices are equinumerous. (Any switching class on an odd number of vertices contains a unique even graph, obtained by taking any graph in the class and switching with respect to the set of vertices of odd degree.) But no such correspondence exists if the number of vertices is even. Mallows and Sloane [21] proved that the numbers were equal by deriving a formula for the number of switching classes and observing that it coincides with the Robinson–Liskovec formula for the number of even graphs.

The "right" explanation [6] actually shows that the classes are dual. Let X be a set of n points, and V the set of all graphs on the vertex set X. Each graph can be represented by a binary vector of length $n(n-1)/2$ whose ones give the positions of the edges. So V is a vector space over GF(2) of dimension $n(n-1)/2$. The addition in V corresponds to taking the symmetric difference of the edge sets of the two graphs. We consider two subsets of V:

- U, the set of complete bipartite graphs;
- W, the set of even graphs.

It is easy to see that U is a subspace of V, spanned by the stars. Now a graph is even if and only if it is orthogonal to all stars; so $W = U^\perp$, and W is also a subspace.

The cosets of U in V are precisely the switching classes of graphs. So V/U is the set of switching classes. Since $W = U^\perp$, this quotient V/U is isomorphic to the dual space W^* of W, not just as vector space, but as module for the symmetric group on X. Now a group acting on a finite vector space has equally many orbits on the space and on its dual, by Brauer's lemma [4]; and the orbits of the symmetric group are the isomorphism classes. So the numbers of switching classes and even graphs are equal.

Recently, I noticed another feature, which may be related in some way to this duality. As noted above, an even graph is the disjoint union of Eulerian graphs. A similar-looking decomposition holds for two-graphs. We define a relation $\sim$ on the point set of a two-graph by the rule that $x \sim y$ if and only if either $x = y$ or no triple contains x and y. From the definition of a two-graph, it is easy to see that this is an equivalence relation, and is even a congruence, that is, membership of a triple in $\mathcal{T}$ is unaffected if we replace some of its points by equivalent ones. Thus, a two-graph is described by a partition of X, with no structure on the parts of the partition, and the structure of a *reduced* two-graph (one in which all $\sim$-classes are singletons) on the set of parts. (By contrast, for even graphs, we have an Eulerian graph on each part of the partition, and no structure on the set of parts; this is, in some vague sense, "dual" to the preceding.)

The numbers of Eulerian graphs and of reduced two-graphs on n points agree for $n \leq 4$ but differ for $n = 5$.

2 Groups and counting

Let G be a permutation group on a set Ω. Usually Ω will be infinite. The group G is said to be *oligomorphic* if the number of orbits of G on the set of n-subsets of Ω is finite for every positive integer n. (More about the derivation of this term below.) So every finite permutation group is oligomorphic. If G is oligomorphic, we let $f_n(G)$ (or just f_n, if the group is clear) denote the number of orbits of G on n-sets.

Design theorists will recognise this set-up. Suppose that we want to construct a t-design on Ω with block size k admitting the group G. Let $T_1, \ldots, T_a$ be the orbits on t-sets, and $K_1, \ldots, K_b$ the orbits on k-sets, where $a = f_t$, $b = f_k$. Now we build a collapsed incidence matrix $M = (m_{ij})$ of size $a \times b$, where m_{ij} is the number of k-sets in the jth orbit which contain a fixed t-set from the ith orbit. Now the game is to select a subset of the columns of M such that the submatrix has constant row sums; then the union of the corresponding orbits is the block set of the design.

This doesn't work if Ω is infinite, since the numbers m_{ij} may be infinite. However, collapsing the matrix the other way does make sense: let $P = (p_{ij})$, where p_{ij} is the number of t-sets in the ith orbit which are contained in a fixed k-set from the jth orbit. We will return to this later; but, unfortunately, I have nothing more to say about constructing designs!

The concept which links this kind of orbit counting to combinatorial enumeration is that of a homogeneous relational structure. A *relational structure* X on Ω consists of a number of relations on X of various arities. Thus, many of our favourite structures (graphs, digraphs, tournaments, total or partial orders, two-graphs) are relational. An *induced substructure* of a relational structure on a subset of Ω is obtained by simply taking the restrictions of all the relations to this subset. Now X is *homogeneous* if every isomorphism between finite substructures of X can be extended to an automorphism of X.

The classical example of a homogeneous structure is the rational numbers $\mathbb{Q}$ as ordered set. Given any two n-sets of rationals, arranged in increasing order as $a_1 < a_2 < \cdots < a_n$ and $b_1 < b_2 < \cdots < b_n$, there is a unique isomorphism between the substructures, taking a_i to b_i for $i = 1, \ldots, n$. This can be extended to an order-preserving map on all the rationals by "filling in" the intervals (a_i, a_{i+1}) with linear maps, and translating the two ends suitably.

Based on this example, Fraïssé [13] gave a necessary and sufficient condition for a class $\mathcal{C}$ of finite structures to be all the finite substructures of a countable homogeneous structure. I will give only a brief description of Fraïssé's condition here (it is discussed in detail in [7]). It is required that $\mathcal{C}$ is closed under isomorphism; closed under taking induced substructures; contains only countably many structures up to isomorphism; and has the *amalgamation property* (which asserts that, given two structures $B_1, B_2 \in \mathcal{C}$ with a common substructure A, there is a structure $C \in \mathcal{C}$ in which B_1 and B_2 can both be embedded, so that their intersection is at least A). The first three conditions are usually obvious, but the amalgamation property may require more effort to verify. Many familiar classes of finite structures (graphs, tournaments, posets, triangle-free graphs, two-graphs, ...) satisfy the condition, and many others (bipartite graphs, trees, ...) can be made to satisfy it after small modification. For example, graphs with a fixed bipartition satisfy Fraïssé's conditions.

Now let X be a homogeneous structure, and $\mathcal{C}$ the class of its finite substructures. If G is the automorphism group of X, then G-orbits on n-sets correspond to isomorphism classes of n-element structures in $\mathcal{C}$ (unlabelled substructures of X). Moreover, given any permutation group on a countable set, it is possible to construct a structure on which the group acts "homogeneously". So the problem of calculating the numbers $f_n(G)$ for oligomorphic groups G is identical to that of enumerating unlabelled structures in a class satisfying Fraïssé's condition (a *Fraïssé class*, I will say for short).

The term "oligomorphic" is derived from "few shapes", and is chosen to express this relationship between the group orbits and the isomorphism classes of structures ("shapes") in a class with only finitely many of any given finite size ("few").

3 An inequality and a Ramsey problem

Because of the connection described in the last section, any general result on orbit numbers for oligomorphic groups is a metatheorem about enumerating structures in Fraïssé classes. The most basic result of this kind is that the numbers f_n are non-decreasing: $f_n \leq f_{n+1}$.

This was proved for finite permutation groups by Livingstone and Wagner [19], using character theory of the symmetric group. This result can be translated into a proof using Block's lemma together with the fact that the reduced incidence matrices defined in the last section have full rank provided that $|\Omega| \geq t + k$. As mentioned there, the matrix P is meaningful even when Ω is infinite, and can be shown to have full rank, from which the inequality can be deduced (taking $t = n$, $k = n + 1$).

A second, completely different proof was found by Pouzet [25], based on Ramsey's Theorem. The essential ingredient can be stated as a Ramsey theorem as follows:

Theorem 3.1 *Suppose that $t \leq k$, and let the t-subsets of the infinite set Ω be partitioned into finitely many classes T_i ($1 \leq i \leq a$), all non-empty. For any k-set U, let $p_i(U)$ denote the number of t-subsets of U in the class T_i. Let $P = (p_{ij})$ be the matrix whose columns are the distinct vectors $(p_1(U), \ldots, p_a(U))^\top$ which occur. Then, after re-ordering rows and columns if necessary, the matrix P is upper triangular with non-zero diagonal (that is, $p_{ij} = 0$ for $i > j$, while $p_{ii} \neq 0$).*

Like all good Ramsey theorems, this one has a finite version as well: it holds if Ω is sufficiently large in terms of t, k, a. Here the proof gives "sufficiently large" as a vast, iterated Ramsey number; yet there is some evidence that the result holds for sets of quite modest size. Nobody knows the true value of this Ramsey function.

Note that the fact that the rows of P are linearly independent is a simple consequence of the Ramsey theorem, and the inequality follows directly. (We take the classes of t-sets to be the orbits of G. Now two k-sets giving rise to different columns lie in different orbits, so f_k is at least equal to the number of distinct columns, which is at least the number f_t of rows.)

Macpherson, in [20] and other papers, has proved some powerful results about the rate of growth of the sequence $(f_n(G))$. For example, if G is primitive (that is, preserves no non-trivial equivalence relation), then either $f_n(G) = 1$ for all n, or the sequence grows at least exponentially.

4 Direct and wreath products

Next we turn to two methods of constructing new groups from old. If our groups are automorphism groups of homogeneous structures, then these two constructions translate into operations on the finite substructures, and hence on the sequences enumerating them. These operations are quite general, and do not depend on having a group around. (This point is the heart of the philosophy of these notes. In fact, a combinatorial setting more general than group orbits has been developed by A. Joyal [16] and his school, under the name *species*. This is very close in spirit to what I am doing here.)

The operations on sequences can often be expressed concisely in terms of their generating functions. Accordingly, if G is oligomorphic, we let

$$f_G(t) = \sum_{n=0}^{\infty} f_n(G)t^n.$$

(Note that $f_0(G) = 1$, since there is a unique empty set.)

First, let's have a couple of groups to feed into the constructions. Let S denote the symmetric group on an infinite set, and A the group of order-preserving permutations of the rational numbers. Then $f_n(S) = f_n(A) = 1$ for all n. (This is clear for S, and follows for A from our proof of the homogeneity of $\mathbb{Q}$.) Hence $f_S(t) = f_A(t) = 1/(1-t)$. The Fraïssé class corresponding to S consists of finite sets without any additional structure; that for A consists of finite totally ordered sets. In each case, there is just one object of each size n.

Let H be a permutation group on a set Γ, and K a permutation group on Δ. The *direct product* $H \times K$ (the set of all ordered pairs (h, k) with $h \in H$ and $k \in K$, with pointwise operations) acts on the disjoint union of the sets Γ and Δ, where the first component of a pair acts on Γ and the second component acts on Δ. Now a finite subset of $\Gamma \cup \Delta$ has the form $\Gamma_0 \cup \Delta_0$, where Γ_0 and Δ_0 are finite subsets of Γ and Δ respectively; two such sets lie in the same orbit of $H \times K$ if and only if their intersections with Γ lie in the same H-orbit, and similarly for Δ and K. So the sequence $(f_n(H \times K))$ is the *convolution* of the sequences $(f_n(H))$ and $(f_n(K))$:

$$f_n(H \times K) = \sum_{i=0}^{n} f_i(H)f_{n-i}(K),$$

and the generating functions simply multiply: $f_{H\times K} = f_H f_K$. Note that the terms of the sequence $(f_n(H \times S))$ are the partial sums of the sequence $(f_n(H))$.

More importantly, we see that a structure in the Fraïssé class for $H \times K$ is just the disjoint union of structures for H and K. So the direct product of permutation groups corresponds to the disjoint union of combinatorial structures. For example, the objects in the Fraïssé class for $S \times S$ can be taken to be finite sets whose elements are coloured red and blue; and $f_n(S \times S) = n + 1$, since an n-set can contain $0, 1, 2, \ldots, n$ blue elements.

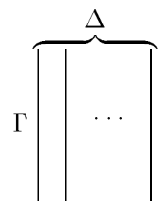

Figure 1: $\Gamma \times \Delta$ as a covering of Δ

There is another well-known permutation action of the direct product, on the Cartesian product of the sets Γ and Δ: the pair (h,k) maps (γ,δ) to $(\gamma h, \delta k)$. (This is the *product action* of $H \times K$.) If H and K are oligomorphic, then so is $H \times K$ in this action. However, the number of orbits on n-sets is not uniquely determined by the corresponding numbers for H and K. (*Exercise:* check that, in the product action, $f_2(S \times S) = 3$, while $f_2(A \times A) = 4$.) There are some very interesting questions here, but I won't say any more about this.

The other construction is the *wreath product* of permutation groups. It is convenient to build up the action first. The group $G = H \operatorname{Wr} K$ acts on the set $\Gamma \times \Delta$; but the factors should not be regarded as having the same status. Rather, think of $\Gamma \times \Delta$ as the disjoint union of $|\Delta|$ copies of Γ, each copy indexed by a point of Δ, as in Figure 1. (Formally, the copy Γ_δ of Γ indexed by δ is $\{(\gamma,\delta) : \gamma \in \Gamma\}$.) In topological terms, we regard $\Gamma \times \Delta$ as a covering of Δ whose *fibres* are the sets Γ_δ, each isomorphic to Γ.

The *base group* B of the wreath product consists of all permutations built from $|\Delta|$ independently chosen elements of H, each acting on the corresponding fibre. It is a cartesian product of $|\Delta|$ copies of H. The *top group* T is the group K, permuting the fibres by acting on their indices according to its given action on Δ. The wreath product is now the product BT. (In group-theoretic terms, B is normalised by T and $B \cap T = 1$, so the wreath product is the semi-direct product of B by T.)

What do the orbits of $H \operatorname{Wr} K$ on n-sets look like? Each n-set is partitioned by its intersections with the fibres; these intersections can be independently permuted to any other sets in the same fibre by the base group. However, the way in which the set of parts of the partition is permuted by the top group is less easy to describe.

Suppose that H and K are automorphism groups of homogeneous structures. Then an n-element structure in the Fraïssé class for $H \operatorname{Wr} K$ consists of a partition of the point set, together with independently chosen structures from the Fraïssé class for H on each part of the partition, and a structure from the Fraïssé class for K on the set of parts.

This combinatorial "composition", as with the disjoint union for the direct product, is meaningful even if there are no groups around. Consider the example in the first section. The class of even graphs is the composition of the class of

Eulerian graphs with the Fraïssé class for S; while the class of two-graphs is the composition of the Fraïssé class for S with the class of reduced two-graphs. (If there were homogeneous structures for the relevant classes, with automorphism groups $Even$, $Eulerian$, $TwoGr$ and $RedTwoGr$, then we would have

$$Even \sim Eulerian \,\mathrm{Wr}\, S, \qquad TwoGr \sim S \,\mathrm{Wr}\, RedTwoGr,$$

where $\sim$ means that the orbit counting sequences (f_n) are the same. (Unfortunately, the homogeneous structure exists only in the case of two-graphs.) These relations express formally the puzzle at the end of the first section.

It turns out that the sequence $(f_n(H \,\mathrm{Wr}\, K))$ is not determined by the corresponding sequences for H and K. We need the sequence $(f_n(H))$ and more detailed information about K. Later, I will describe what information we actually need. Here, I will describe the situation in two particularly important examples. We have

$$f_{H \,\mathrm{Wr}\, S}(t) = \prod_{i=1}^{\infty}(1-t^i)^{-f_i(H)} = \exp\left(\sum_{j=1}^{\infty}\frac{f_H(t^j)-1}{j}\right),$$

while

$$f_{H \,\mathrm{Wr}\, A}(t) = \frac{1}{2-f_H(t)}.$$

These relations also describe the counting functions for the compositions of classes of structures with S or A.

I will take the viewpoint that, with any oligomorphic group K, there is associated an operator (which I also denote by K) on integer sequences, so that

$$(f_n(H \,\mathrm{Wr}\, K)) = K(f_n(H)).$$

If convenient, the operator can be taken to act on generating functions. So, for example, if the sequence f counts connected graphs of some type (e.g. Eulerian graphs), then Sf counts disjoint unions of such graphs (e.g. even graphs), while Af also describes disjoint unions but where there is a total order on the set of components. Bernstein and Sloane [3] refer to the operators S and A as EULER and INVERT respectively.

There is also a *product action* of the wreath product, on the set of functions from Δ to Γ. It is not oligomorphic unless H is oligomorphic and K is a finite permutation group (that is, Δ is finite). As in the case of the direct product, I will not consider this action.

5 N-free graphs and posets

In an experiment involving a number of nuisance factors with discrete levels, the statistician needs to allow for the fact that each nuisance factor may contribute

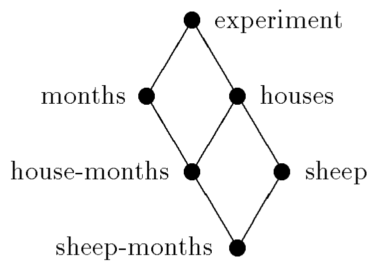

Figure 2: An experiment

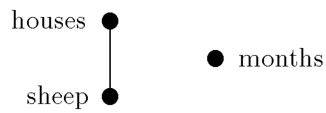

Figure 3: A poset

to the variance of responses. The relationship among these factors therefore needs to be clarified before the experiment can be designed (that is, before the assignment of treatments to experimental units can be decided). Here is an example. Suppose that we are testing various treatments on sheep. The sheep are kept in a number of houses for a number of months (a month being the period of one treatment). A single experimental unit is a sheep for a month, or a sheep-month. The relevant nuisance factors (apart from trivial ones) are houses, sheep, house-months, and months, which are partially ordered as shown in Figure 2.

This poset is a distributive lattice, and hence is representable as the lattice of ancestral sets (up-sets) in a simpler poset, formed by sheep, houses, and months, as in Figure 3.

In statistical terminology, sheep are *nested* (!) in houses, since there is no relation between the fifth sheep (say) in different houses. On the other hand, houses and months are *crossed*, since both "same house" and "same month" are potentially significant. In general, *crossing* two posets consists of taking their disjoint union, and *nesting* them to taking their ordered sum (where one is above the other). Statisticians had worked out rules for dealing with nesting and crossing and their iterates [23], but it turns out that a similar analysis can

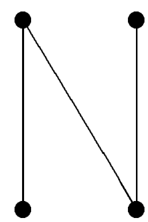

Figure 4: N

be developed for nuisance factors based on any poset (a *poset block structure*, see Speed and Bailey [36]).

Poset block structures give a large class of imprimitive association schemes whose P and Q matrices can be calculated exactly. Moreover, they are homogeneous (assuming the poset is finite; the association scheme may be finite or infinite). But my concern here is the question, posed by Bailey [1]: How typical are structures obtained by nesting and crossing? In particular, how many posets are obtained in this way, and how does this number compare to the total number of posets?

The symbol N will denote the graph or the poset which is shown in Figure 4. A graph or poset is called *N-free* if it doesn't contain N as an induced substructure. The class of N-free graphs has been studied in many contexts, under many different names. I summarise the main facts.

- The complement of an N-free graph is N-free.
- An N-free graph with more than one vertex is connected if and only if its complement is disconnected.
- The class of N-free graphs is the smallest class containing the one-vertex graph and closed under complementation and disjoint union.
- The edges of an N-free graph can be oriented to form an N-free poset.
- A poset is N-free if and only if it can be built from the one-element poset by nesting and crossing.

We see that, for $n > 1$, the numbers of connected and disconnected N-free graphs on n vertices are equal. Let a be the sequence enumerating connected N-free graphs. Then we have

$$a_1 = 1, \qquad (Sa)_n = 2a_n \quad \text{for } n > 1.$$

This gives a recurrence relation for a_n, since $(Sa)_n$ is equal to a_n plus terms involving a_i for $i < n$; so the numbers are easily calculated. It is not an easy recurrence to solve, but it can be shown that the sequence grows exponentially. The number a_n is a lower bound for the number of N-free posets.

We "bracket" the number of N-free posets as follows. An *N-free biposet* is a set supporting two posets, which are complementary (in the sense that any two distinct points are comparable in exactly one of the posets) and both N-free. Any N-free graph and its complement can be oriented to form an N-free biposet. (*Exercise:* show that, if we set $x < y$ when this relation holds in either poset of an N-free biposet, the result is a total order.) Given the order $1 < \cdots < m$ and biposets $B_1, \ldots, B_m$, we can combine them to get a new biposet B whose diconnected poset is the disjoint union of the connected posets of the B_i and whose connected poset is the ordered sum of the disconnected posets of the B_i. Hence, if b is the sequence enumerating N-free biposets for which the first poset is connected, then the total number of N-free biposets is $2b_n$ for $n > 1$, and we have

$$b_1 = 1, \qquad (Ab)_n = 2b_n \quad \text{for } n > 1.$$

This also gives a recurrence which implies that b_n grows exponentially. This recurrence can be solved explicitly: if $b(t)$ is the generating function, and $u(t) = b(t) - 1$ (so that $u(0) = 0$), we have

$$1/(1-u) = 1 + 2u - t,$$

giving $u = \frac{1}{4}(1 + t - \sqrt{1 - 6t + t^2})$. The Binomial Theorem now gives a formula for the coefficients. The function u has a singularity at $t = 3 - 2\sqrt{2}$, so this is its radius of convergence, and the exponential constant is $3 + 2\sqrt{2}$.

Now let c and d be the sequences enumerating connected and disconnected N-free posets, where we use the strange convention that $c_1 = d_1 = 1$. This case is a curious mixture of the two preceding. Since any disconnected N-free poset is a disjoint union of connected ones, and any connected N-free poset (on more than one element) an ordered sum of disconnected ones, we get the mutual recurrence

$$c_1 = d_1 = 1, \qquad (Sc)_n = (Ad)_n = c_n + d_n \quad \text{for } n > 1.$$

This enables the sequences to be calculated. They grow exponentially, with exponential constant approximately 4.62 (see Cameron [10] for more precise asymptotics). If $c(t)$ and $d(t)$ are the generating functions of the sequences, then

$$c(t) + d(t) - t - 1 = \frac{1}{2 - d(t)} = \prod_{i=1}^{\infty} (1 - t^i)^{-c_i}.$$

In any case, we have more than enough information to answer the motivating question. Since there are roughly $2^{n^2/4}$ posets altogether (indeed, this many two-level posets), only a vanishingly small proportion of them are obtained by nesting and crossing.

6 Algebraic interlude

There is a graded algebra which can be constructed from a permutation group, such that the dimensions of its homogeneous components are the numbers of orbits of the group on n-sets. Its algebraic structure can give a bit more insight into the combinatorics of the orbits.

For any infinite set Ω, let V_n denote the set of all functions from $\binom{\Omega}{n}$ (the set of n-element subsets of Ω) to your favourite field of characteristic zero (which I will take to be the rational numbers here). Each V_n is a rational vector space, and V_0 has dimension 1 (there is only one empty set). Now let

$$\mathcal{A} = \bigoplus_{n=0}^{\infty} V_n$$

be the direct sum of these spaces. We define a multiplication on $\mathcal{A}$ by the rule that, for any $f \in V_k$, $g \in V_l$, the product fg is the function in V_{k+l} defined by

$$fg(M) = \sum_{K \in \binom{M}{k}} f(K)g(M \setminus K)$$

for any $(k+l)$-set M. This makes $\mathcal{A}$ a commutative, associative, graded algebra over $\mathbb{Q}$. (It is in fact the reduced incidence algebra of the poset of finite subsets of Ω, but this fact plays no role here. I also remark that Glynn [14] has made use of a similar algebra, where the supports of the k-set and l-set to which f and g are applied in defining the product are not required to be disjoint. This algebra has very different properties. Glynn uses it to study reconstruction problems.)

An element of V_n is called a *homogeneous element of degree n* in the algebra $\mathcal{A}$. (This has no connection with our earlier usage of the word "homogeneous".) A particular homogeneous element of degree 1 is the constant function e with value 1. Multiplication by e induces a linear map from V_n to V_{n+1} for each n; this map is represented by the matrix P of Section 2, and Theorem 3.1 implies that it is a non-zero-divisor.

Now let G be a permutation group on Ω. Then G acts on each space V_n, by permuting the arguments of the functions. Let V_n^G be the space of functions in V_n fixed by G. Since a function is fixed by G if and only if it is constant on the orbits of G, we have

$$\dim(V_n^G) = f_n(G)$$

if G is oligomorphic. Furthermore, we define

$$\mathcal{A}^G = \sum_{n=0}^{\infty} V_n^G$$

to be the set of fixed points of G in $\mathcal{A}$. If G fixes two functions, it fixes their product; so $\mathcal{A}^G$ is a subalgebra of $\mathcal{A}$. For oligomorphic groups G, we see that the generating function $f_G(t)$ is the Poincaré series of $\mathcal{A}^G$. In particular, if S is the symmetric group on Ω, then $\mathcal{A}^S$ is the polynomial algebra in one variable over $\mathbb{Q}$, the generator being the element e defined above.

If G is oligomorphic, then V_n^G is spanned by the characteristic functions of the G-orbits on n-sets; each orbit corresponds to an isomorphism type of n-element structures in the Fraïssé class of G. According to our philosophy, it is possible to define an analogous algebra for more general classes of finite structures. I leave it as an exercise to write out the precise definition of this algebra.

We now consider the structure of $\mathcal{A}^G$ when G is a direct or wreath product. The direct product is straightforward: we have

$$\mathcal{A}^{H\times K} = \mathcal{A}^H \otimes_{\mathbb{Q}} \mathcal{A}^K.$$

Wreath products are more difficult, but there are results in some special cases. First, let $G = S \operatorname{Wr} K$. If K is a finite permutation group on a set of size n, then it can be represented as a group of $n \times n$ matrices (using permutation matrices corresponding to the elements of K). Such a linear group K has a ring $I(K)$ of invariants, the polynomial functions on $\mathbb{Q}^n$ fixed by K. It turns out that $\mathcal{A}^{S \operatorname{Wr} K}$ is isomorphic to $I(K)$. In particular, the generating function $f_{S \operatorname{Wr} K}(t)$ is the *Molien series* [22] of the linear group K. If K is the symmetric group S_n then, by Newton's Theorem, $I(K)$ is a polynomial ring generated by the elementary symmetric functions, which have degrees $1, 2, \ldots, n$; and we have

$$f_{S \operatorname{Wr} S_n}(t) = \prod_{i=1}^{n} (1 - t^i)^{-1}.$$

There is a completely different situation in which we can guarantee that $\mathcal{A}^G$ is a polynomial ring generated by homogeneous elements. Suppose that G is the automorphism group of a homogeneous structure, whose Fraïssé class has a "good notion of connectedness". (I will not define this precisely. It holds for graphs, etc. In general, what is required is that every structure can be uniquely expressed as the disjoint union of connected structures, and that given an arbitrary structure and a partition of its points, the structure "contains" (as a substructure) the disjoint union of the induced substructures on its parts.) Then it can be shown that $\mathcal{A}^G$ is a polynomial algebra. Its generators are in one-to-one correspondence with the connected structures.

Now another interpretation of the S-transform is that, if a sequence f enumerates the number of polynomial generators of given degree in a polynomial algebra, then the nth term of Sf is the degree of the nth homogeneous component of the algebra. So the relation between connected and arbitrary structures is exactly mirrored in the algebra.

A special case occurs for the group $H \operatorname{Wr} S$. Recall that a structure in the Fraïssé class of this group consists of a set with a partition, having a structure in the Fraïssé class of H on each part of the partition. Taking the connected structures as those with just one part, we have a "good notion of connectedness"; so $\mathcal{A}^{H \operatorname{Wr} S}$ is a polynomial algebra with $f_n(H)$ generators of degree n for each n. Note that the structure of $\mathcal{A}^{H \operatorname{Wr} S}$ does not depend on the detailed structure of $\mathcal{A}^H$, only on its Poincaré series.

I end this section with a puzzle. There is a countable homogeneous two-graph, since finite two-graphs form a Fraïssé class. Let G be its automorphism group, and consider $\mathcal{A}^G$. Is it a polynomial algebra? The answer is not known. If it is, then the number of polynomial generators of degree n is equal to the number of Eulerian graphs on n vertices. Also, how do reduced two-graphs fit into the picture?

The general pattern of this puzzle is a group G for which the sequence $(a_n) = S^{-1}(f_n(G))$ has a natural combinatorial interpretation; we want to know whether $\mathcal{A}^G$ is a polynomial algebra with generators enumerated by (a_n).

Here is an example where this approach succeeded, and connected the theory here with a very different part of mathematics. Let q be a positive integer. It is known that there is a partition of the set of rational numbers into q disjoint dense subsets $S_1, \ldots, S_q$, and that any two such partitions are related by an order-preserving permutation. Let $G(q)$ be the group of permutations of $\mathbb{Q}$ which preserve the order and the subsets $S_1, \ldots, S_q$. An orbit of $G(q)$ on n-sets is specified by the word $x_1 \ldots x_n$ in the alphabet $A = \{1, \ldots, q\}$, where x_i is the index of the set containing the i^{th} point of the n-set (in the order induced by $\mathbb{Q}$). Every word of length n is realised; so $f_n(G(q)) = q^n$.

Now $\mathcal{A}^{G(q)}$ is the algebra spanned by the set A^* of all words in the alphabet A; multiplication of two words is given by the sum of all words obtained by "shuffling" them together. For example, using $\{a, b\}$ instead of $\{1, 2\}$ for the alphabet, we have

$$(ab) \cdot (aab) = abaab + 3aabab + 6aaabb.$$

This is the *shuffle algebra*, which arises in the theory of free Lie algebras (see Reutenauer [28]). It was proved by Radford [26] that the shuffle algebra on a given alphabet is a polynomial algebra generated by the *Lyndon words*. In order to explain these, we assume that the alphabet A is totally ordered, and take the lexicographic order on the words. Now a *Lyndon word* is a word which is smaller (in this order) than any proper cyclic shift of itself; that is, w is a Lyndon word if, whenever $w = xy$ is a proper factorisation, we have $w < yx$. Now the combinatorial assertions required for Radford's theorem are the following:

(a) any word has a unique expression as a concatenation $w_1 w_2 \ldots w_n$, where $w_1, \ldots, w_n$ are Lyndon words and $w_1 \geq w_2 \geq \ldots \geq w_n$;

(b) of all the words which can be obtained by shuffling Lyndon words $w_1, \ldots, w_n$ together, the lexicographically greatest is the concatenation in non-increasing order.

Now we take the "connected" words to be the Lyndon words, and the relation of "involvement" to be lexicographic order reversed; and this result fits into the previous formalism.

Note that the number of Lyndon words of length n is $\frac{1}{n}\sum_{d|n}\mu(d)q^{n/d}$, where μ is the Möbius function. This is a well-known expression, which also counts (among other things) the number of monic irreducible polynomials of degree n over the finite field of order q, if q is a prime power. But that is another story (see Bailey *et al.* [2]).

7 Reconstruction

The algebraic considerations of the last section are also related to the vertex reconstruction conjecture for graphs. Viewed in this way, we have a reconstruction problem for the age of any oligomorphic group. The details differ greatly from one class to another.

Let G be the automorphism group of the random graph, so that the Fraïssé class of G is the class of all finite graphs. We can regard the vector space V_n as having a basis which consists of the isomorphism types of n-vertex graphs. Let $T_{n,n-1}$ be the linear map from V_n to V_{n-1} which takes each n-vertex graph to the sum of its $(n-1)$-vertex induced subgraphs. Then $T_{n,n-1}$ is the map represented by the matrix M of Section 2; its dual is the map $T_{n-1,n}$ from V_{n-1} to V_n induced by multiplication by the element e of the preceding section, with matrix P as in Section 2.

Now two n-vertex graphs are *hypomorphic* if they have the same deck of vertex-deleted subgraphs; that is, if their images under $T_{n,n-1}$ are equal. So if X and Y are hypomorphic, then $X - Y \in \ker(T_{n,n-1})$. Moreover, for any X and Y, if $aX + bY \in \ker(T_{n,n-1})$, with $ab \neq 0$, then $b = -a$, and X and Y are hypomorphic.

So the *vertex reconstruction conjecture* for graphs can be stated in the form: *For $n > 2$, the kernel of $T_{n,n-1}$ has minimum weight greater than* 2. (The *minimum weight* of a subspace, as in coding theory, is the smallest number of non-zero coordinates of a non-zero vector in that subspace.)

We could thus ask the question: *What is the minimum weight of* $\ker(T_{n,n-1})$*?* For example, a trivial upper bound for the minimum weight is $1 + n/2$ if n is even. For, if $X_{n,k}$ is the graph with n vertices and k disjoint edges, then

$$\langle X_{n,0}, X_{n,1}, \ldots, X_{n,n/2}\rangle T_{n,n-1} \subseteq \langle X_{n-1,0}, X_{n-1,1}, \ldots, X_{n-1,n/2-1}\rangle.$$

So some non-zero element in $\langle X_{n,0}, \ldots, X_{n,n/2}\rangle$ belongs to the kernel of $T_{n,n-1}$. This can surely be improved; but is the minimum weight bounded by an absolute constant?

We can generalise further, and ask: *What is the minimum weight of* $\ker(T_{n,m})$ *for $m < n$?* (We define $T_{n,m}$ to be the linear map taking an n-vertex graph to the sum of its m-vertex subgraphs.) Since

$$T_{n,l}T_{l,m} = \binom{n-m}{l-m} T_{n,m}$$

for $m < l < n$, the minimum weight of $\ker(T_{n,m})$ decreases as m decreases. *Is there an absolute constant k such that $\ker(T_{n,n-k})$ has minimum weight 2 for all n?*

Two further generalisations suggest themselves. First, what happens if we work instead over a field of non-zero characteristic p (such as the integers mod p)? If p divides n, then $\ker(T_{n,n-1})$ has minimum weight 1: any graph with all its vertex-deleted subgraphs isomorphic belongs to the kernel (for example, any vertex-transitive graph).

Second, these questions can be posed for other Fraïssé (or more general) classes of structures. As an example, consider strings of length n over a binary alphabet $\{a, b\}$. As earlier, we consider these as sets with a total order whose elements are partitioned into two distinguished subsets. So a substructure is a (not necessarily consecutive) substring. The class of such strings is the Fraïssé class of the group $G(2)$ of order-preserving permutations of $\mathbb{Q}$ which fix two complementary dense subsets.

Now $T_{n,m}$ maps a string to the sum of its m-element substrings, counted with multiplicities. Call two strings u and v *m-equivalent* if they have the same image; that is, if each string of length m has the same multiplicity in u and v. (This can be extended to strings of length less than m by defining such a string to be m-equivalent only to itself.) For example, the strings $X = abbbaab$ and $Y = baabbba$ of length 7 are 3-equivalent, since $T_{7,3}$ maps both X and Y to

$$aaa + 3aab + 6aba + 6abb + 3baa + 6bab + 6bba + 4bbb.$$

Now the obvious question is: *What is the smallest n, as a function of m, for which there are two m-equivalent binary strings of length n?* The answer is not known, and the known upper and lower bounds are very far apart. John Dixon [11] proved a result characterising m-equivalence in purely algebraic terms. He showed that two strings are m-equivalent if and only if, when regarded as words in the generators of the free nilpotent group of class m, they are equal.

The *edge reconstruction conjecture* for graphs can be fitted into this formalism to some extent as well. Let G be the symmetric group on an infinite set (say $\mathbb{N}$), in its induced action on the set $\Omega = \binom{\mathbb{N}}{2}$ of 2-element subsets of $\mathbb{N}$. Now an n-element member of the Fraïssé class of G consists of a graph with n edges (in other words, an n-vertex graph which is a line graph, in a specified way: so the triangle counts twice, according as it is the line graph of a triangle or of a star). The edge-reconstruction conjecture asserts that $\ker(T_{n,n-1})$ has minimum weight greater than 2 in this class, provided that $n > 3$. Questions like those posed earlier for vertex-reconstruction can now be asked.

There are further links between edge-reconstruction and finite permutation groups; but that is another story.

8 Cycle index

Now we come to the rule for calculating the sequence operator corresponding to any oligomorphic group. We will also see how to count orbits on ordered n-tuples of distinct elements (which amounts to the same thing as enumerating labelled structures in the Fraïssé class of the group).

We begin with a little Pólya theory. Let Ω be a finite set of size n. For any permutation g of Ω, we define the *cycle index* $z(g)$ of g to be $s_1^{c_1(g)} s_2^{c_2(g)} \cdots s_n^{c_n(g)}$, where $s_1, s_2, \ldots, s_n$ are independent indeterminates, and $c_i(g)$ is the number of cycles of length i in the cycle decomposition of g. If G is a permutation group on Ω, the *cycle index* of G is the average of the cycle indices of its elements:

$$Z(G) = \frac{1}{|G|} \sum_{g \in G} z(g).$$

The role of the cycle index in enumeration problems is well-known.

Clearly it is impossible to define the cycle index of an infinite group by anything like this formula; so we adopt a different approach. Let G be oligomorphic. Choose representatives for the orbits of G on finite subsets of Ω. For each such representative Δ, let $H(\Delta)$ be the group induced on Δ by its setwise stabiliser in G. Now define the *modified cycle index* $\tilde{Z}(G)$ of G to be

$$\tilde{Z}(G) = \sum_{\Delta} Z(H(\Delta)),$$

where the sum is over the orbit representatives. This is meaningful, since by assumption there are only finitely many orbits of size n, and hence a monomial of weight n occurs only finitely many times in the sum (where the weight of $s_1^{c_1} s_2^{c_2} \cdots s_n^{c_n}$ is defined to be $c_1 + 2c_2 + \cdots + nc_n$).

This procedure is meaningful for finite groups G, but it gives nothing new: in fact, for a finite group G, $\tilde{Z}(G)$ is obtained from $Z(G)$ by the substitution replacing s_i by $s_i + 1$ for all i. (For experts in Pólya theory, this is an exercise.)

I now list three pairs of facts about the modified cycle index: first, its values for the groups S and A; second, its behaviour under taking direct and wreath products; and third, a couple of interesting specialisations of it. First, another definition. If G is oligomorphic on Ω, we let $F_n(G)$ be the number of G-orbits on n-tuples of distinct elements of Ω. The finiteness of this number for all n is equivalent to the oligomorphy of G; indeed, we have

$$f_n \leq F_n \leq n! f_n$$

for all n. If G is the automorphism group of a homogeneous relational structure X, then $F_n(G)$ is the number of labelled n-element structures in the Fraïssé class (that is, the number of structures on the set $\{1, 2, \ldots, n\}$ which are embeddable in X). As standard in enumeration theory, we describe the sequence (F_n) by an *exponential generating function* given by

$$F_G(t) = \sum_{n=0}^{\infty} \frac{F_n(G)t^n}{n!}.$$

- $\tilde{Z}(S) = \exp\left(\sum_{j=1}^{\infty} \frac{s_j}{j}\right)$.
- $\tilde{Z}(A) = \dfrac{1}{1 - s_1}$.
- $\tilde{Z}(H \times K) = \tilde{Z}(H)\tilde{Z}(K)$.
- $\tilde{Z}(H \operatorname{Wr} K)$ is obtained from $\tilde{Z}(K)$ by substituting $\tilde{Z}(H)(s_i, s_{2i}, \ldots) - 1$ for s_i, for $i = 1, 2, \ldots$.
- $f_G(t)$ is obtained from $\tilde{Z}(G)$ by substituting t^i for s_i for $i = 1, 2, \ldots$.
- $F_G(t)$ is obtained from $\tilde{Z}(G)$ by substituting t for s_1 and 0 for s_i for $i = 2, 3, \ldots$.

It follows from the direct product rule and the two specialisations that, as well as $f_{H\times K}(t) = f_H(t)f_K(t)$, we also have $F_{H\times K}(t) = F_H(t)F_K(t)$. But, because these are exponential generating functions, the convolution rule for sequences is a little different, namely

$$F_n(H \times K) = \sum_{k=0}^{n} \binom{n}{k} F_k(H)F_{n-k}(K).$$

This is the so-called *exponential convolution.*

The fifth of the six points gives us the rule for calculating the sequence $(f_n(H \operatorname{Wr} K))$ from $(f_n(H))$: $f_{H \operatorname{Wr} K}(t)$ is obtained from $\tilde{Z}(K)$ by substituting $f_H(t^i) - 1$ for s_i, for $i = 1, 2, \ldots$. We see that the information about K we require is its modified cycle index. Accordingly, for any oligomorphic group K, we can define an operator K on sequences by using this rule, so that

$$K(f_n(H)) = (f_n(H \operatorname{Wr} K)).$$

In a similar way, wreath products define operators on the sequences $(F_n(H))$. These operators are much easier to work with, since they are just given by substitution in the exponential generating functions, after first removing the constant term:

$$F_{H\,\mathrm{Wr}\,K}(t) = F_K(F_H(t) - 1).$$

The most famous case of this occurs when H is the symmetric group S. We have $F_S(t) = \exp(t)$, and $F_{S\,\mathrm{Wr}\,K}(t) = F_K(\exp(t) - 1)$. In particular, $F_{S\,\mathrm{Wr}\,S}(t) = \exp(\exp(t) - 1)$, the exponential generating function for the sequence of *Bell numbers*. (The nth Bell number counts partitions of an n-set, that is, Fraïssé structures for the group $S\,\mathrm{Wr}\,S$.) This operation has another interpretation. If $F_n^*(G)$ denotes the number of orbits of G on all n-tuples (of not necessarily distinct elements), then we have

$$F_n^*(G) = F_n(S\,\mathrm{Wr}\,G),$$

as can be seen by replacing identical points of Δ in an n-tuple (where G acts on Δ) by distinct points of the fibre over that point. Furthermore, this relation is equivalent to

$$F_n^*(G) = \sum_{k=1}^{n} S(n,k) F_k(G),$$

where $S(n,k)$ is the *Stirling number of the second kind*, the number of partitions of an n-set into k parts. The operator on sequences given by the above formula is called STIRLING by Bernstein and Sloane [3].

"Dual" to this operator, in some sense, is the operator which maps $(F_n(G))$ to $(F_n(G\,\mathrm{Wr}\,S))$, given by $F_{G\,\mathrm{Wr}\,S}(t) = \exp(F_G(t) - 1)$. This operator, referred to as EXP in [3], maps the sequence enumerating labelled connected structures in some class to arbitrary labelled structures in the class; the same job that S (or EULER) does for the unlabelled structures. Explicitly, it is given by the recurrence

$$A_n = \sum_{k=1}^{n} \binom{n-1}{k-1} C_k A_{n-k},$$

where $(C_n) = (F_n(G))$ counts connected objects and $(A_n) = (F_n(G\,\mathrm{Wr}\,S))$ counts arbitrary ones.

9 A product identity

This section contains a proof of the identity

$$\mathrm{e}^{t/(1-t)} = \prod_{n=1}^{\infty} (1 - t^n)^{-\phi(n)/n},$$

where ϕ is Euler's totient function. We need another example of an oligomorphic group.

Let C be the group of all permutations preserving the cyclic order on the complex roots of unity. (The cyclic order is a ternary relation R which holds for (x, y, z) when the points are visited in this order starting at x and proceeding in an anticlockwise sense around the circle; so, if $R(x, y, z)$ holds, then $R(y, z, x)$ holds but $R(x, z, y)$ doesn't.) The group C is transitive, and the stabiliser of a point preserves a linear order on the remaining points; so the stabiliser is isomorphic to A. Using this fact, or by showing that the relational structure is homogeneous (much as we did for A earlier), we see that C has just one orbit on n-sets for every $n > 0$, and the stabiliser of an n-set induces on it the cyclic group C_n of order n.

Now C_n contains $\phi(d)$ elements of order d for each divisor d of n; and each of these elements has n/d cycles of length d. So we have

$$\begin{aligned}\tilde{Z}(C) &= 1 + \sum_{n=1}^{\infty} \frac{1}{n} \sum_{d|n} \phi(d) s_d^{n/d} \\ &= 1 + \sum_{d=1}^{\infty} \frac{\phi(d)}{d} \sum_{m=1}^{\infty} \frac{s_d^m}{m} \\ &= 1 - \sum_{d=1}^{\infty} \frac{\phi(d)}{d} \log(1 - s_d).\end{aligned}$$

Since $f_n(C) = 1$ for all n, we have $f_C(t) = 1/(1-t) = 1 + t/(1-t)$. Hence

$$1 + \frac{t}{1-t} = 1 - \sum_{d=1}^{\infty} (\phi(d)/d) \log(1 - t^d).$$

Now subtracting 1 from each side, taking the exponential, and replacing the dummy variable d by n gives the result.

Note that, having worked out $\tilde{Z}(C)$, we can write down the sequence operator corresponding to C, in terms of its action on generating functions:

$$(Cf)(t) = 1 - \sum_{n=1}^{\infty} \frac{\phi(n)}{n} \log(2 - f(t^n)).$$

Having added C to our repertoire, it is interesting to consider the group $C \operatorname{Wr} S$. A member of the Fraïssé class for it consists of a set carrying a partition with a circular order on each part. This is precisely the specification of a permutation, decomposed into disjoint cycles. So the group $C \operatorname{Wr} S$ "represents" permutations.

The numbers of permutations and of total orders on an n-set are both equal to $n!$. So there should be some relation between $C \operatorname{Wr} S$ and A. However, the bijection between linear orders and permutations is not a "natural" one:

we must first choose a distinguished order λ, and then any other order is a permutation of λ.

We know already that $\tilde{Z}(A) = 1/(1-s_1)$. A straightforward calculation, using the value of $\tilde{Z}(C)$ found above, shows that $\tilde{Z}(C \operatorname{Wr} S) = \prod_{n\geq 1}(1-s_n)^{-1}$. These two expressions are different; but, to compute the e.g.f. for the number of labelled structures, we substitute t for s_1 and 0 for s_n $(n > 1)$; the results are the same, as they should be:

$$F_A(t) = F_{C \operatorname{Wr} S}(t) = (1-t)^{-1}.$$

10 Stirling numbers

We already saw that Stirling numbers are involved with the formalism of wreath products. It is possible to define and generalise them using this philosophy.

I begin with a brief course on Stirling numbers. The *Stirling number of the first kind*, $S(n,k)$, is the number of partitions of an n-set into k parts. We see immediately that the sum $\sum_{k=1}^{n} S(n,k) = B(n)$ (the *Bell number*) is the total number of partitions of an n-set, which we recognise as $F_n(S \operatorname{Wr} S)$.

The *unsigned Stirling number of the second kind*, $s(n,k)$, is the number of permutations of an n-set with k disjoint cycles. Thus we have $\sum_{k=1}^{n} s(n,k) = n! = F_n(A)$. It is more useful to re-interpret this in the light of the remarks in the last section. A permutation with k cycles is given by a partition into k parts with a cyclic order on each part; and we have $\sum_{k=1}^{n} s(n,k) = F_n(C \operatorname{Wr} S)$.

This immediately suggests a generalisation. Let G be any oligomorphic permutation group. We define the *generalised Stirling number* $S[G](n,k)$ to be the number of partitions of an n-set into k parts, with a member of the Fraïssé class for G on each part. Thus we have $\sum_{k=1}^{n} S[G](n,k) = F_n(G \operatorname{Wr} S)$. In this notation, the "classical" Stirling numbers are $S(n,k) = S[S](n,k)$ and $s(n,k) = S[C](n,k)$.

It is clear that the generalised Stirling numbers $S[G](n,k)$ are determined by the numbers $F_n(G)$. This can be expressed most concisely in terms of the exponential generating functions:

$$\sum_{n=k}^{\infty} S[G](n,k)t^n/n! = (F_G(t)-1)^k/k!.$$

From this, the equation $F_{G \operatorname{Wr} S}(t) = \exp(F_G(t)-1)$ is obtained by summing over k.

The generalised Stirling numbers have a composition property:

$$\sum_{l=k}^{n} S[G](n,l)S[H](l,k) = S[G \operatorname{Wr} H](n,k).$$

For consider $S[G](n,l)S[H](l,k)$. This counts pairs consisting of a partition of $\{1,\ldots,n\}$ into l parts with a G-structure on each part, and a partition of the set of parts into k parts with an H-structure on each part. (Here "G-structure" is short for "member of the Fraïssé class of G".) Viewed otherwise, we have a partition of $\{1,\ldots,n\}$ into k parts, each part carrying a partition into "subparts" with a G-structure on each subpart and an H-structure on the set of subparts (in other words, a $G\,\mathrm{Wr}\,H$-structure), subject to the condition that there are l subparts altogether. Summing over l removes the final condition and yields $S[G\,\mathrm{Wr}\,H](n,k)$.

This result can be expressed more compactly in matrix form. Let $T[G]$ be the triangular array of generalised Stirling numbers associated with G, the infinite lower triangular mtrix with (n,k) entry $S[G](n,k)$. Then we have

$$T[G]T[H] = T[G\,\mathrm{Wr}\,H].$$

For example, $T[S]$ and $T[C]$ are the arrays of classical Stirling numbers; and we have

$$T[C]T[S] = T[C\,\mathrm{Wr}\,S] = T[A].$$

The numbers $S[A](n,k)$ are the *Lah numbers* $L(n,k)$, sometimes called "Stirling numbers of the third kind": see Lah [17], Bridgeman [5]. Unlike the classical Stirling numbers, there is a closed formula for the Lah numbers:

$$L(n,k) = \frac{(n-1)!}{(k-1)!}\binom{n}{k} = \frac{n!}{k!}\binom{n-1}{k-1}.$$

This can be shown by using the formula

$$\sum_{n\geq k} L(n,k)t^n/n! = \left(\frac{t}{1-t}\right)^k/k!$$

and computing the coefficient of t^n on the right-hand side.

In a similar manner, it can be shown that

$$\sum_{k=1}^{n} S[G](n,k)F_k(H) = F_n(G\,\mathrm{Wr}\,H).$$

This property generalises the STIRLING transform we met earlier.

There is another remarkable property of classical Stirling and Lah numbers. Let $S^*[G](n,k) = (-1)^{n-k}S[G](n,k)$ be the *signed* generalised Stirling numbers, and let $T^*[G]$ be the corresponding triangular array. Then

$$\sum_{l=k}^{n} S(n,l)(-1)^{l-k}s(l,k) = \delta_{nk},$$

or in other words

$$T[S]T^*[C] = I.$$

It follows that also $T[C]T^*[S] = I$ and $T[A]T^*[A] = I$. I do not know whether this inversion relation has analogues for other groups.

11 Stabilisers and derivatives

We've seen that the group-theoretic operations of direct and wreath product "correspond" to multiplication and composition of formal power series. It is possible to interpret differentiation in similar terms. In this section, I assume that the permutation group G is transitive on Ω, though it is possible to formulate the results more generally.

The *stabiliser* G_α of the point $\alpha \in \Omega$ is the subgroup of G consisting of the permutations which fix α. We consider it as a permutation group on $\Omega \setminus \{\alpha\}$. Now we have

$$\tilde{Z}(G_\alpha) = \frac{\partial}{\partial s_1}\tilde{Z}(G).$$

It follows that

$$F_{G_\alpha}(t) = \frac{\mathrm{d}}{\mathrm{d}t}F_G(t).$$

(In fact, it is easy to see this directly. Differentiating an exponential generating function corresponds to shifting the terms of the sequence one place to the left, so the preceding equation says

$$F_n(G_\alpha) = F_{n+1}(G).$$

The correspondence between orbits of G_α on n-tuples and of G on $(n+1)$-tuples can be described thus: take an orbit of G on $(n+1)$-tuples, select all the tuples which begin with α, and delete α from them.)

On the other hand, the sequence $(f_n(G_\alpha))$ is not determined by $(f_n(G))$.

The Fraïssé class for G_α is obtained from that for G by distinguishing a point x in each finite substructure and deleting x. (This is not the same as just deleting a point, since it leaves a shadow, the extra structure obtained when x was distinguished. For example, if the objects in the Fraïssé class are graphs, then by distinguishing and deleting x we specify a subset of the remaining vertices, those which were joined to x.) In view of the effect on the generating function, I will denote this operation on Fraïssé classes by ∂.

Two-graphs provide an example (see Seidel [31]). If x is a point of the two-graph (X, T), there is a unique graph in the corresponding switching class with the property that x is an isolated vertex. Thus, if Gr and $TwoGr$ denote the classes of graphs and two-graphs, we have

$$Gr = \partial TwoGr.$$

In combinatorial terms, it is more natural to leave the point x in, obtaining a "rooted" structure. This is easily handled: adding the fixed point back in corresponds to taking the direct product of G_α with the trivial group acting on a single point, whose modified cycle index is $1 + s_1$.

Having defined derivatives, we can consider differential equations. For example, is there a group G for which $G_\alpha \cong G \times G$? For such a group, the function $F = F_G$ satisfies $F' = F^2$, $F(0) = 1$, with solution $F(t) = (1-t)^{-1}$. Thus $F_n(G) = n!$. This sequence is the same as the one realised by the group A. Indeed, the stabiliser of 0 in A has two orbits, the positive and the negative rationals; each orbit, as ordered set, is isomorphic to $\mathbb{Q}$, and A_0 induces all order-preserving permutations on each. So indeed $G = A$ satisfies the original equation. (The fact that $\partial A = A \times A$, where A is the class of finite total orders, can be regarded as the basis for the recursive QUICKSORT algorithm [15] for sorting a list: select an element 0, partition the list into elements before and after 0, and sort these two sublists.)

The group $G = C \operatorname{Wr} S$ also satisfies $F_n(G) = n!$, corresponding combinatorially to the fact that any permutation can be decomposed into a disjoint union of cycles. This group, like A itself, satisfies the related equation $G_\alpha \cong A \times G$.

What about the differential equation $G_\alpha = G \operatorname{Wr} G$? It can be shown that no such group exists. Nevertheless, we obtain an interesting integer sequence $(F_n(G))$ for such a non-existent group. With $f(t) = F_G(t) - 1$, we have

$$f'(t) = 1 + f(f(t)), \qquad f(0) = 0,$$

somewhat reminiscent of the Feigenbaum–Cvitanović equation

$$g(t) = -\alpha g(g(t/\alpha))$$

(Feigenbaum [12]). The unique power series solution does not converge in any neighbourhood of 0. Is the a combinatorial interpretation of the coefficients (a class of structures enumerated by them)? The first few terms of the sequence are 1, 2, 7, 37, 269, 2535, 29738, 421790, 7076459, … .

12 The probability of connectedness

According to Cayley's Theorem, the number of labelled trees on n points is n^{n-2}. It is a surprising fact, proved by Rényi [27] in 1959, that the number of labelled forests on n points is asymptotic to cn^{n-2}, where $c = \sqrt{\mathrm{e}}$; that is, the probability that a random forest on $\{1, 2, \ldots, n\}$ is connected tends to $1/\sqrt{\mathrm{e}}$ as $n \to \infty$. (I am grateful to Dominic Welsh for this reference.) Moreover, for labelled forests of rooted trees, the limiting probability of connectedness is $1/\mathrm{e}$.

In terms of our earlier notation, if $C_n = n^{n-2}$ and (A_n) is the sequence obtained by applying the operator EXP to (C_n), then $\lim_{n\to\infty} A_n/C_n = \sqrt{\mathrm{e}}$. And, if we put $C_n = n^{n-1}$ instead, the limit is e.

One could ask more generally: for which classes of structures (with a notion of connectedness) is it true that the probability of connectedness for a labelled or unlabelled structure tends to a limit strictly between zero and one? A class of examples is provided by the N-free graphs. As we saw, exactly half of the N-free graphs on n points are connected if $n > 1$, and this is true for labelled or unlabelled structures, since complementation gives a bijection between connected and disconnected structures. Furthermore, it can be shown that the probability that a (labelled or unlabelled) N-free poset is connected tends to the golden ratio as the number of points tends to infinity (see [10]).

In the unlabelled case, it is easy to handle rooted trees, since the number of forests of rooted trees on n vertices is equal to the number of rooted trees on $n+1$ vertices. (Take a new root, and join it to all the old roots.) Since these numbers grow exponentially with constant $2.95576\ldots$ [24], the limiting probability of connectedness is the reciprocal of this number, namely $0.33832\ldots$. It appears that exponential growth for the number of n-element unlabelled structures is necessary for the probability of connectedness to be strictly between 0 and 1, though I cannot prove such a precise result.

In terms of groups, the question becomes: for which oligomorphic groups G is it true that either $\lim_{n\to\infty} F_n(G \operatorname{Wr} S)/F_n(G)$, or $\lim_{n\to\infty} f_n(G \operatorname{Wr} S)/f_n(G)$, exists and is finite and greater than 1? Having formulated the question in this way, it immediately generalises. We can replace the group S by any oligomorphic group, take the wreath product in either order, or use direct product instead of wreath product. For more on this, see [10].

13 Two-graphs revisited

The last story, like the first, is about two-graphs, and is taken from Cameron [9], which contains all references for this section (and is available electronically).

There is a simple construction for two-graphs from trees, as follows. Let T be a tree with edge set Ω. Now let $\mathcal{T}$ consist of all triples of edges which do not lie on a path in the tree (those for which the paths connecting them in the tree form a subtree containing a trivalent vertex). It is easily verified that $(\Omega, \mathcal{T})$ is a two-graph (by considering the four possible configurations of four edges). These two-graphs arose in the work of Tsaranov [37] on a class of groups related to Coxeter groups. Which two-graphs are produced by the construction?

The *pentagon* and *hexagon* two-graphs refer to the two-graphs associated, as in the first section, with the switching classes of the pentagon and hexagon graphs respectively. In [8], I proved that a two-graph arises from a tree by the construction described if and only if it doesn't contain either the pentagon or the hexagon two-graph as an induced substructure. Moreover, non-isomorphic trees give rise to non-isomorphic two-graphs. This solves the counting problem for unlabelled pentagon- and hexagon-free two-graphs: the number on n points is equal to the number of trees with n edges, calculated by Otter [24].

However, there is a further difficulty associated with counting the labelled pentagon- and hexagon-free two-graphs. For example, a path with n edges can have its edges labelled in $n!/2$ different ways, but all of these give rise to the null two-graph (the two-graph with no triples).

The solution to the problem comes by showing that the two-graph obtained from a tree T is reduced (in the sense of the first section) if and only if the tree is *series-reduced*, that is, has no vertices of valency 2. So we should first count the series-reduced edge-labelled trees. The number of these with n edges turns out to be

$$x_n = \frac{1}{n}\sum_{j=0}^{n-1}(-1)^j \binom{n+1}{j}\binom{n-1}{j} j!(n+1-j)^{n-1-j}$$

for $n \geq 2$, with $x_1 = 1$. Then the number of labelled pentagon- and hexagon-free two-graphs is given by the STIRLING transform

$$\sum_{k=1}^{n} S(n,k)x_k.$$

We have a language to describe this behaviour. We can associate a sequence operator with a class of objects even if it is not the Fraïssé class associated with some group: define the "modified cycle index" to be the sum of the cycle indices of the automorphism groups of the unlabelled structures in the class, and then use the same formalism as described earlier. Now series-reduced trees (counted by edges) and reduced pentagon- and hexagon-free two-graphs have the same modified cycle index, because of the correspondence, and hence define the same sequence operator. If we denote this class by SRT, then the class of all pentagon- and hexagon-free two-graphs corresponds to $S \,\mathrm{Wr}\, SRT$, and the class of all trees to $A \,\mathrm{Wr}\, SRT$ apart from a slight mismatch for paths. (The edges on a path have two possible orders which cannot be distinguished, but which are counted twice by $A \,\mathrm{Wr}\, SRT$.)

The class of pentagon-free two-graphs (those containing no induced pentagon) is also interesting. It is closely connected with the class of N-free graphs; in fact, the operator ∂, applied to the class of pentagon-free two-graphs, gives the class of N-free graphs (like the relation between two-graphs and graphs). Its members can also be represented by trees (in a different way); and it can be enumerated by techniques similar to those described. This is also found in [8], [9].

End note

Jalaluddin Rumi was one of the leading Sufi poets. The story of the blind people and the elephant is common to several other religious traditions, including Quakers and Buddhists.

References

[1] R. A. Bailey, Designs: mappings between structured sets, pp. 22–51 in *Surveys in Combinatorics, 1989* (ed. J. Siemons), Cambridge Univ. Press, Cambridge, 1989.

[2] R. A. Bailey, P. J. Cameron and D. G. Fon-Der-Flaass, in preparation.

[3] M. Bernstein and N. J. A. Sloane, Some canonical sequences of integers, *Linear Algebra Appl.*, to appear.

[4] R. Brauer, On the connection between the ordinary and the modular characters of groups of finite order, *Ann. Math.* **42** (1941), 926–935.

[5] T. Bridgeman, Lah's triangle — Stirling numbers of the third kind, preprint, July 1995.

[6] P. J. Cameron, Cohomological aspects of two-graphs, *Math. Z.* **157** (1977), 101–119.

[7] P. J. Cameron, *Oligomorphic Permutation Groups*, London Math. Soc. Lecture Notes **152**, Cambridge University Press, Cambridge, 1990.

[8] P. J. Cameron, Two-graphs and trees, *Discrete Math.* **127** (1994), 63–74.

[9] P. J. Cameron, Counting two-graphs related to trees, *Electronic J. Combinatorics* **2** (1995), #R4.

[10] P. J. Cameron, On the probability of connectedness, in preparation.

[11] J. D. Dixon, personal communication (1985).

[12] M. J. Feigenbaum, Quantitative universality for a class of nonlinear transformations, *J. Statist. Phys.* **19**, 25–52.

[13] R. Fraïssé, Sur certains relations qui généralisent l'ordre des nombres rationnels, *C. R. Acad. Sci. Paris* **237** (1953), 540–542.

[14] D. Glynn, Rings of geometries, I, *J. Combinatorial Theory* (A) **44** (1987), 34–48; II, *ibid.* (A) **49** (1988), 26–66.

[15] C. A. R. Hoare, Quicksort, *Computer Journal* **5** (1962), 10–15.

[16] A. Joyal, Une théorie combinatoire des séries formelles, *Advances Math.* **42** (1981), 1–82.

[17] I. Lah, Eine neue Art von Zahlen, ihre Eigenschaften und Anweldung in der mathematischen Statistik, *Mitt. Math. Statistik* **7** (1955), 203–212.

[18] V. A. Liskovec, Enumeration of Euler graphs, *Vescī Akad. Navuk BSSR Ser. Fīz–Mat. Navuk* (1970), 38–46.

[19] D. Livingstone and A. Wagner, Transitivity of finite permutation groups on unordered sets, *Math. Z.* **90** (1965), 393–403.

[20] H. D. Macpherson, The action of an infinite permutation group on the unordered subsets of a set, *Proc. London Math. Soc.* (3) **51** (1983), 471–486.

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

[22] T. Molien, Über die Invarianten der lineare Substitutionsgruppe, *Sitzungsber. König. Preuss. Akad. Wiss.* (1897), 1152–1156.

[23] J. A. Nelder, The analysis of randomized experiments with orthogonal block structure, *Proceedings of the Royal Society, Series A*, **283** (1965), 147–178.

[24] R. Otter, The number of trees, *Ann. Math.* (2) **49** (1948), 583–599.

[25] M. Pouzet, Application d'une propriété combinatoire des parties d'un ensemble aux groupes et aux relations, *Math. Z.* **150** (1976), 117–134.

[26] D. E. Radford, A natural ring basis for the shuffle algebra and an application to group schemes, *J. Algebra* **58** (1979), 432–454.

[27] A. Rényi, Some remarks on the theory of trees, *Publ. Math. Inst. Hungar. Acad. Sci.* **4** (1959), 73–85.

[28] C. Reutenauer, *Free Lie Algebras*, London Math. Soc. Monographs (New Series) **7**, Oxford University Press, 1993.

[29] R. W. Robinson, Enumeration of Euler graphs, *Proof Techniques in Graph Theory* (Proc. Second Ann Arbor Graph Theory Conf., Ann Arbor 1968), 147–153, Academic Press, New York 1969.

[30] J. J. Seidel, Strongly regular graphs of L_2-type and of triangular type, *Proc. Kon, Nederl. Akad. Wetensch.* (A) **70** (1967), 188–196.

[31] J. J. Seidel, A survey of two-graphs, pp. 481–511 in *Proc. Int. Colloq. Teorie Combinatorie*, Accad. Naz. Lincei, Roma, 1977.

[32] J. J. Seidel, More about two-graphs, in *Combinatorics, Graphs and Complexity* (Proc. 4th Czech Symp., Prachatice 1990), 297–308, *Ann. Discrete Math.* **51** (1992).

[33] J. J. Seidel and D. E. Taylor, Two-graphs: A second survey, in *Algebraic Methods in Graph Theory*, Szeged, 1978.

[34] Idries Shah (ed.), *World Tales*, Harcourt Brace Jovanovich, New York, 1979.

[35] N. J. A. Sloane, *A Handbook of Integer Sequences*, Academic Press, New York, 1973.

[36] T. P. Speed and R. A. Bailey, Factorial dispersion models, *Internat. Statist. Review* **55** (1987), 261–277.

[37] S. Tsaranov, On a generalization of Coxeter groups, *Algebra Groups Geom.* **6** (1989), 281–318.