# Some counting problems related to permutation groups

Peter J. Cameron

*School of Mathematical Sciences, Queen Mary and Westfield College, London E1 4NS, U.K.*

**Abstract**

This paper discusses investigations of sequences of natural numbers which count the orbits of an infinite permutation group on $n$-sets or $n$-tuples. It surveys known results on the growth rates, cycle index techniques, and an interpretation as the Hilbert series of a graded algebra, with a possible application to the question of smoothness of growth. I suggest that these orbit-counting sequences are sufficiently special to be interesting but sufficiently common to support a general theory.

> 'I count a lot of things that there's no need to count,' Cameron said. 'Just because that's the way I am. But I count all the things that need to be counted.'
>
> Richard Brautigan, *The Hawkline Monster*

## 1 Three counting problems

This paper is a survey of the problem of counting the orbits of an infinite permutation group on $n$-sets or $n$-tuples, especially the aspects closest to algebraic combinatorics. Much of the material surveyed here can be found elsewhere, for example in [4].

We begin by discussing three counting problems in different areas of mathematics and their relations.

### *1.1 Enumeration of finite structures*

A *relational structure* $M$ consists of a set $X$ and a family of relations on $X$. These relations can have arbitrary arities, and there may be a finite or infinite number of relations. Many familiar structures have only a single relation:

graphs, directed graphs, total or partial orders, and so on. However, for a general (non-uniform) hypergraph we would need a $k$-ary relation for each cardinality $k$ of hyperedges.

The *age* of $M$, written $\mathrm{Age}(M)$, is the class of all finite relational structures (in the same language) which are embeddable in $M$. (This terminology was invented by Fraïssé [7], who says that the structure $M$ is *younger than* $N$ if the age of $M$ is contained in that of $N$.)

**Problem.** How many (a) *labelled*, (b) *unlabelled* structures in $\mathrm{Age}(M)$?

As standard in combinatorial enumeration, labelled structures are based on the set $\{1, 2, \ldots, n\}$; unlabelled structures are isomorphism types.

### *1.2 Counting orbits*

A permutation group $G$ on a set $X$ is *oligomorphic* if $G$ has only finitely many orbits on $X^n$, for all $n$: equivalently, on the set of $n$-subsets of $X$, or on the set of $n$-tuples of distinct elements of $X$. (The term 'oligomorphic' suggests 'few shapes'. We will see later that orbits are often associated with 'shapes' of finite substructures of some structure whose automorphism group is $G$, and 'few' is interpreted as 'only finitely many'. The word 'oligomorphic' is also used in computer science to describe viruses which exist in only a few distinct forms and so can be recognised.)

**Problem.** How many orbits on (a) $n$-sets, (b) $n$-tuples of distinct elements, (c) all $n$-tuples, does a given oligomorphic group have?

### *1.3 Types of a first-order theory*

Let $T$ be a complete consistent theory in the first-order language $L$. An *$n$-type* over $T$ is a set $S$ of formulae in $L$ with free variables $x_1, \ldots, x_n$, maximal subject to being consistent with $T$. Thus a type encodes everything that can be said (in the first-order language) about $n$ elements in some model of $T$.

We say that $T$ is *$\aleph_0$-categorical* if it has a unique countable model (up to isomorphism). This is equivalent to there being only finitely many $n$-types for each $n$. This is part of the celebrated theorem of Engeler, Ryll-Nardzewski and Svenonius, about which we shall say more later.

**Problem.** How many $n$-types?

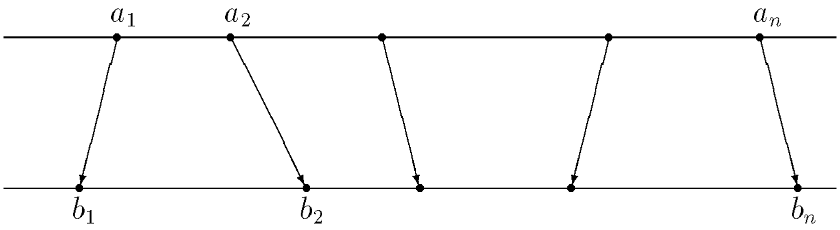


Fig. 1. Order-automorphism of $\mathbb{Q}$

### *1.4 An example*

Let $M$ be the totally ordered set $\mathbb{Q}$. Recall *Cantor's Theorem*, which asserts that any countable dense totally ordered set with no least or greatest element is isomorphic to $\mathbb{Q}$. Since all these properties apart from countability are first-order, the theory of $M$ is $\aleph_0$-categorical.

The age of $M$ consists of all finite ordered sets: there is one unlabelled structure, and $n!$ labelled structures, on $n$ elements.

Its automorphism group is transitive on $n$-sets for every $n$. This is because, given any two $n$-tuples of rational numbers, each in increasing order, we can find a piecewise-linear order-preserving map taking the first $n$-tuple to the second (see Figure 1). We also see that there are $n!$ orbits on ordered $n$-tuples of distinct elements.

An $n$-type specifies, of each pair of variables, whether they are equal, and, if not, which is greater. So the number of $n$-types is equal to the number of *preorders* (reflexive and transitive relations $P$ such that, for all $x$ and $y$, either $P(x, y)$ or $P(y, x)$ holds) on the set $\{1, 2, \ldots, n\}$. This number is

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

where $S(n,k)$is the Stirling number of the second kind, since a preorder is specified by an equivalence relation and a total order on its equivalence classes.

### *1.5 Connections*

As the example suggests, there are close connections between the three problems.

A structure $M$ is *homogeneous* if any isomorphism between finite induced substructures of $M$ can be extended to an automorphism of $M$. Thus, the

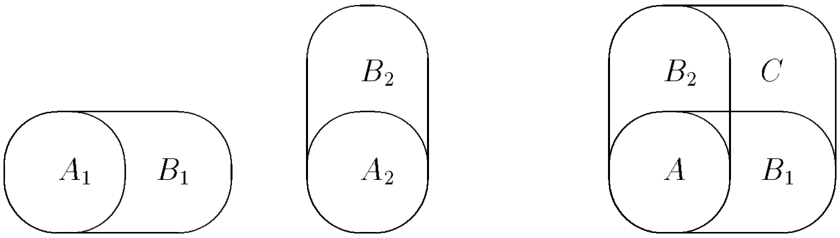


Fig. 2. The Amalgamation Property

ordered set $\mathbb{Q}$ is homogeneous.

**Theorem 1 (Fraïssé's Theorem)** *A class $\mathcal{C}$ of finite structures is the age of a countable homogeneous structure $M$ if and only if it is closed under isomorphism, closed under taking induced substructures, contains only countably many members up to isomorphism, and has the* amalgamation property*.*

*If these conditions hold, then $M$ is unique up to isomorphism.*

The amalgamation property asserts that, if two structures $B_1$ and $B_1$ in $\mathcal{C}$ have isomorphic substructures, then they may be embedded in a larger substructure $C \in \mathcal{C}$ so that the isomorphic substructures coincide (see Figure 2).

We call a class $\mathcal{C}$ which satisfies the hypotheses of this theorem a *Fraïssé class*, and the homogeneous structure $M$ its *Fraïssé limit.*

Now if $M$ is homogeneous, then the number of orbits of its automorphism group on $n$-tuples of distinct elements (resp. on $n$-sets) is equal to the number of labelled (resp. unlabelled) structures in its age.

There is a natural topology on the symmetric group of countable degree (pointwise convergence) with the properties that

(a) a subgroup is closed if and only if it is the automorphism group of a homogeneous relational structure;
(b) the closure of a subgroup is the largest overgroup with the same orbits on $X^n$ for all $n$.

Hence counting labelled/unlabelled structures in a Fraïssé class is equivalent to counting orbits of a permutation group on $n$-sets/$n$-tuples of distinct elements.

We turn now to the connection with counting types.

The theorem of Engeler, Ryll-Nardzewski and Svenonius says more than we have seen so far:

(a) for a countable structure $M$, the theory of $M$ is $\aleph_0$-categorical if and only if $\mathrm{Aut}(M)$ is oligomorphic;
(b) if these condition holds, then all $n$-types are realised in $M$, and two $n$-tuples realise the same type if and only if they are in the same orbit of $\mathrm{Aut}(M)$.

Thus, if $T$ is $\aleph_0$-categorical, counting $n$-types of $T$ is equivalent to counting orbits of $\mathrm{Aut}(T)$ on $n$-tuples of elements in the unique countable model of $T$.

Moreover, as we have seen, for any oligomorphic group $G$, the closure of $G$ is the automorphism group of a homogeneous relational structure, whose theory is $\aleph_0$-categorical.

So the enumeration problem for a Fraïssé class (for which the answer is finite for all $n$), the orbit-counting problem for an oligomorphic permutation group, and the type-counting problem for an $\aleph_0$-categorical theory, are all 'equivalent'. We will focus on the orbit-counting version from now on.

## 2 Three counting sequences

We consider the classes of sequences which can arise in this situation.

### *2.1 The sequences*

Let $G$ be an oligomorphic permutation group on $X$. Let

- $f_n(G) =$ number of $G$-orbits on $n$-subsets;
- $F_n(G) =$ number of $G$-orbits on $n$-tuples of distinct elements;
- $F_n^*(G) =$ number of $G$-orbits on all $n$-tuples.

Then $f_n$ and $F_n$ count unlabelled and labelled $n$-element structures in a Fraïssé class, while $F_n^*$ counts $n$-types in an $\aleph_0$-categorical theory. We take as a convention that the zeroth term in each sequence is 1: there is a single empty set or tuple.

These sequences are, of course, related. We have:

**Theorem 2** *(a)* $F_n^* = \sum_{k=1}^{n} S(n,k)F_k$, *where* $S(n,k)$ *is the Stirling number of the second kind;*

*(b)* $f_n \le F_n \le n!\, f_n$.

Thus $F$ determines $F^*$ and *vice versa.* The series $(f_n)$ is more difficult to work with than $(F_n)$, but for this reason more interesting. The examples $G = S$ (the symmetric group) and $G = A$ (the group of order-preserving permutations of $\mathbb{Q}$) show that equality is possible in each inequality in (b).

The fundamental problem is, *Which sequences occur?*

Let $\mathfrak{f}$ and $\mathfrak{F}$ be the sets of $f$- and $F$-sequences arising from oligomorphic groups. A compactness argument shows that both are closed in the space $\mathbb{N}^{\mathbb{N}}$ of all integer sequences (in the topology of pointwise convergence). In particular, each of these sets has cardinality $2^{\aleph_0}$, the same as the whole of $\mathbb{N}^{\mathbb{N}}$. So the conditions we are looking for should be local ones!

The first such result is the following.

**Theorem 3** *For all $N \ge 0$, we have $F_{n+1} \ge F_n$ and $f_{n+1} \ge f_n$.*

The first inequality is trivial: each orbit on $(n+1)$-tuples is obtained by 'extending' a unique orbit on $n$-tuples. Moreover, equality holds if and only if $F_n = F_{n+1} = 1$ (that is, $G$ is $(n+1)$-transitive. The second inequality, however, is much less trivial. Two completely different proofs are known, one using linear algebra and finite combinatorics (we will discuss this later), the other a strengthened version of Ramsey's Theorem.

For example, if $G$ is the group of order-preserving permutations of $\mathbb{Q}$, then we have $f_n = 1$, $F_n = n!$, and

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

### *2.2 Growth rates*

Apart from Theorem 3, very few local conditions are known. One of these asserts that, if $f_n = f_{n+2}$, then $G$ has a fixed set of cardinality at most $n$ and acts on the complement as a $(n+2)$-set-transitive group (one with $f_{n+2} = 1$). So, if the sequence $(f_n)$ is not ultimately constant, then it grows at least linearly with slope $\frac{1}{2}$.

We now look at some examples of possible growth rates. First, we define two group-theoretic constructions. Let $G_1$ and $G_2$ be permutation groups on $X_1$ and $X_2$. Then the *direct product* $G_1 \times G_2$ acts on the disjoint union $X_1 \cup X_2$: an ordered pair $(g_1, g_2)$ acts on $X_1$ as $g_1$ and on $X_2$ as $g_2$.

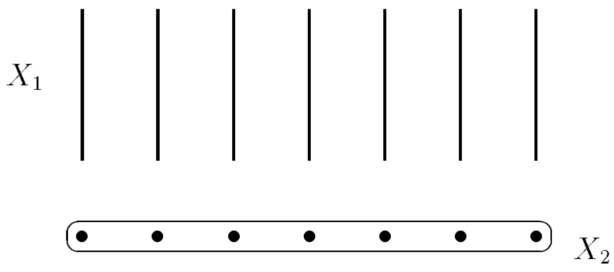


Fig. 3. Wreath product

The *wreath product* is a little more complicated. It acts on $X_1 \times X_2$, which we regard as a covering of $X_2$ with all the fibres bijective with $X_1$. The wreath product $G_1 \operatorname{Wr} G_2$ is generated by two types of permutation:

- the *base group*, which fixes each fibre setwise and acts on it as an element of $G_1$ (these elements chosen independently);
- the *top group*, which permutes the fibres as an element of $G_2$ acting on $X_2$.

(See Figure 3.) We let $S$ denote the infinite symmetric group, $S_k$ the finite symmetric group of degree $k$, and $A$ the group of order-automorphisms of $\mathbb{Q}$.

The following list illustrates some known growth rates.

*Polynomial growth.* For example, if $S^k$ is the direct product of $k$ copies of $S$, then an orbit of $S^k$ on $n$-sets is specified by giving the number $x_i$ of points in the intersection of the $n$-set with the $i$th orbit, for $i = 1, \ldots, k$. So $f_n(S^k)$ is the number of choices of $k$ non-negative integers with sum $n$, which is $\binom{n+k-1}{k-1}$. This is a polynomial of degree $k-1$ in $n$, with leading coefficient $1/(k-1)!$.

Similarly, $f_n(S \operatorname{Wr} S_k)$ is the number of partitions of $n$ with at most $k$ parts, which is a polynomial of degree $k-1$ with leading coefficient $1/(k!(k-1)!)$.

Note, in particular, that $f_n(S \operatorname{Wr} S_2) = 1 + \lfloor n/2 \rfloor$. This shows that the result asserting that $(f_n)$ is either ultimately constant or at least linear with slope $\frac{1}{2}$ is best possible.

*Fractional exponential growth.* For example, $f_n(S \operatorname{Wr} S) = p(n)$, the *partition function*, which is roughly $\exp(n^{1/2}))$. More generally, $f_n(S \operatorname{Wr} S \operatorname{Wr} S_k)$ is very roughly $\exp(n^{(k+1)/(k+2)}$.

It is worth noting that the iterated wreath product of at least three copies of $S$ has the property that $(f_n)$ grows faster than any fractional exponential but slower than straight exponential.

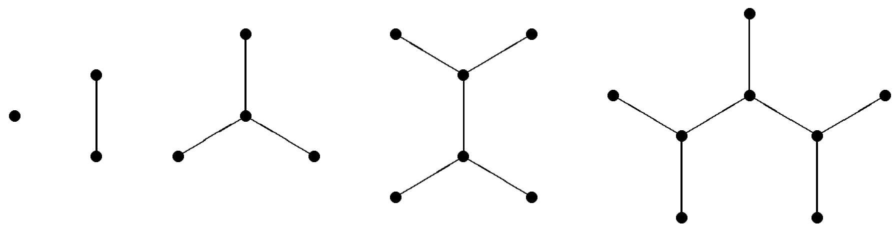

Fig. 4. Boron trees

*Exponential growth.* Here there is a wide variety of examples, of which I note three.

- $f_n(S_2 \mathrm{Wr}\, A) = F_n$, the $n$th Fibonacci number. (This is a simple exercise.)
- Boron trees. A boron tree is a tree in which all vertices have valency 1 or 3. The leaves are hydrogen atoms, and the non-leaves boron atoms, in an imaginary version of hydrocarbon chemistry in which trivalent boron replaces tetravalent carbon. Figure 4 shows the boron trees with at most five leaves. The leaves of a boron tree carry a quaternary relation $R(a, b; c, d)$, which holds whenever the paths $ab$ and $cd$ in the tree are disjoint. The class of such relational structures is a Fraïssé class. The automorphism group of its Fraïssé limit has $f_n \sim an^{-5/2}c^n$, where $c = 2.483\cdots$.
- This example will be important later. Let $q$ be a positive integer. Then it is possible to partition $\mathbb{Q}$ into $q$ pairwise disjoint dense subsets in a unique way up to order-preserving permutations. Any orbit on $n$-sets is parametrised by a word of length $n$ in an alphabet $A$ with $q$ symbols. (Associate a symbol with each of the $q$ sets; then the word records the sets containing the $n$ points in order.) Thus, if $G(q)$ denotes the group of permutations preserving the order and fixing the $q$ sets, then $f_n(G(q)) = q^n$.

*Factorial growth.* Consider the class of finite sets carrying two independent total orders. Such a set is described by the permutation which takes the first order to the second. Since the structures form a Fraïssé class, we obtain a group with $f_n = n!$ . Similarly, by taking $k$ independent orders, we obtain $f_n = (n!)^k$.

Another example is the group induced by $S$ on the set of unordered pairs from the original set. For this group, $f_n$ is the number of graphs with $n$ edges and no isolated vertices (up to isomorphism). The asymptotics of this sequence appear to be unknown.

*Exponential of a polynomial.* The most famous example arises as follows. The class of all finite graphs is a Fraïssé class. Its Fraïssé limit is the celebrated *countable random graph* $R$ discovered by Erdős and Rényi [6]. Thus, $f_n(\mathrm{Aut}(R))$ is the number of $n$-vertex graphs up to isomorphism, which is asymptotically $2^{n(n-1)/2}/n!$ (since almost all finite graphs have trivial automorphism group).

It is worth observing here that there is no upper bound to the growth rates which can be achieved: it is possible to construct a Fraïssé class of relational structures with any given finite number of $k$-ary relations for all $k$, and in which these relations hold only for $k$-tuples with all elements distinct. If there are $a_k$ relations of arity $k$, and they are independent, then clearly $f_n \geq 2^{a_n}$.

The question is much more interesting over languages with only finitely many relations. It is clear that, for a homogeneous structure over such a language, $f_n$ is bounded above by the exponential of a polynomial (precisely, by

$$2^{n^{k_1}+\cdots+n^{k_r}},$$

where $k_1, \ldots, k_r$ are the arities of the relations. It is not clear what happens for arbitrary structures.

However, the most interesting groups and structures (those with the greatest amount of symmetry) are those with the *slowest* growth rates.

Some restrictions on growth rate are known:

**Theorem 4** *(a) For homogeneous binary relational structures, either*

- $c_1 n^d \leq f_n \leq c_2 n^d$ *(for some* $d \in \mathbb{N}$*,* $c_1, c_2 > 0$*), or*
- $f_n$ *grows faster than polynomially.*

*(b) In the latter case,* $f_n > \exp(n^{1/2-\epsilon})$ *for* $n > n_0(\epsilon)$*.*

The first part is due to Pouzet [14], the second to Macpherson [12]. A much more dramatic result was proved by Macpherson [11] in the case of primitive groups (those which preserve no non-trivial equivalence relation):

**Theorem 5** *If* $G$ *is primitive, then either* $f_n = 1$ *for all* $n$*, or* $f_n > c^n$ *for all sufficiently large* $n$*, where* $c > 1$*.*

Macpherson's proof gives $c = \sqrt[5]{2} - \epsilon$. Of the earlier examples, only those associated with boron trees are primitive. The slowest growth known for a primitive group is roughly $2^{n-2}/n$. We discuss this example later.

### *2.3 Smoothness*

Sequences arising from groups should grow smoothly. In particular, for polynomial growth, $\log f_n / \log n$ should tend to a limit (and, for growth of degree $d$

in Pouzet's Theorem, $f_n/n^d$ should tend to a limit); for fractional exponential growth, $\log\log f_n/\log n$; for exponential, $\log f_n/n$; and so on. *How do you state a general conjecture?*

(Actually we might expect such smoothness to fail for very rapid growth. As we noted, examples can be constructed of Fraïssé classes with large numbers of $k$-ary relations. If these numbers grow very irregularly, then probably the numbers of orbits will do so too. We return to this below.)

Another type of question has been considered. We look at the motivation for this question later.

Define an operator $S$ on sequences of natural numbers by the rule that $Sa = b$ if

$$\sum_{n=0}^{\infty} b_n x^n = \prod_{k=1}^{\infty} (1-x^k)^{-a_k}.$$

Is it true that, if $f = Sa$ counts orbits of a group, then $a_n/f_n$ tends to a limit (possibly 0 or 1)?

(This question has something to do with smoothness of growth, since, if $Sa = b$, then $b_n = a_n + F(a_1, \ldots, a_{n-1})$ for some function $F$.

## 3 An algebra

The most immediate connection of the subject of this paper with algebraic combinatorics is that we can define a graded algebra over $\mathbb{C}$ with the property that the degree of the $n$th homogeneous component is $f_n$. This algebra is the topic of the present section.

### *3.1 Construction*

Let $X$ be an infinite set. For any non-negative integer $n$, let $V_n$ be the set of all functions from the set of $n$-subsets of $X$ to $\mathbb{C}$. This is a vector space over $\mathbb{C}$.

Define

$$\mathcal{A} = \bigoplus_{n\geq 0} V_n,$$

with multiplication defined as follows: for $f \in V_m$, $g \in V_n$, let $fg$ be the function in $V_{m+n}$ whose value on the $(m+n)$-set $A$ is given by

$$fg(A) = \sum_{\substack{B \subseteq A \\ |B|=m}} f(B)g(A \setminus B).$$

This is the *reduced incidence algebra* of the poset of finite subsets of $X$.

If $G$ is a permutation group on $X$, let $\mathcal{A}^G$ be the subalgebra of $A$ of the form $\bigoplus_{n\geq 0} V_n^G$, where $V_n^G$ is the set of functions fixed by $G$.

If $G$ is oligomorphic, then $\dim(V_n^G)$ is equal to the number $F_n(G)$ of orbits of $G$ on $n$-sets, since a function is fixed if and only if it is constant on each orbit.

### *3.2 Integral domain?*

The algebra $\mathcal{A}$ has any divisors of zero. The characteristic function $f$ of a single $n$-set satisfies $f^2 = 0$. If the group $G$ has this $n$-set as one of its orbits, then $f \in \mathcal{A}^G$.

I *conjecture* that *if $G$ has no finite orbits, then $\mathcal{A}^G$ is an integral domain.*

This would have as a consequence a smoothness result for the sequence $(f_n)$, in view of the following result:

**Theorem 6** *Let $\mathcal{A} = \bigoplus V_n$ be a graded algebra which is an integral domain, with* $\dim(V_n) = a_n$. *Then $a_{m+n} \geq a_m + a_n - 1$ for all $m, n$.*

In fact, a stronger conjecture can be made. Let $e$ denote the constant function in $V_1$ with value 1. Then $e \in V_1^G$ for any permutation group $G$. It can be shown by finite combinatorial arguments that *$e$ is not a zero-divisor.* (The inequality $f_{n+1}(G) \geq f_n(G)$ follows: for multiplication by $e$ is a linear map from $V_n^G$ to $V_{n+1}^G$, and the fact that $e$ is not a zero-divisor shows that its kernel is zero.) I conjecture that *if $G$ has no finite orbits, then $e$ is prime in $\mathcal{A}^G$* (in the sense that $\mathcal{A}^G/e\mathcal{A}^G$ is an integral domain). This conjecture also has a consequence for smoothness, namely

$$(f_{m+n} - f_{m+n-1}) \geq (f_m - f_{m-1}) + (f_n - f_{n-1}) - 1,$$

since the dimension of the $n$th homogeneous component of $\mathcal{A}^G/e\mathcal{A}^G$ is $f_n - f_{n-1}$.

These conjectures are still open after more than twenty years. Recently [5] I proved the following. Call a permutation group $G$ *entire* if $\mathcal{A}^G$ is an integral domain, and *strongly entire* if $\mathcal{A}^G/e\mathcal{A}^G$ is an integral domain. (It is easy to see that the second condition implies the first.) We call $H$ a *transitive extension* of $G$ if $H$ is transitive and the stabiliser of the point $x$, acting on the points different from $x$, is isomorphic to $G$ as permutation group.

**Theorem 7** *Let $G$ be (strongly) entire, and $H$ a transitive extension of $G$. Then $H$ is (strongly) entire.*

### *3.3 Polynomial algebra?*

There are a few cases in which the structure of the algebra $\mathcal{A}^G$ can be determined. For a simple example, if $G = S$, the symmetric group, then $\mathcal{A}^G$ is a polynomial ring in one variable (generated by $e$). Also, we have

$$\mathcal{A}^{G_1 \times G_2} \cong \mathcal{A}^{G_1} \otimes_{\mathbb{C}} \mathcal{A}^{G_2},$$

so that $\mathcal{A}^{S^k}$ is isomorphic to the polynomial ring in $k$ variables, in agreement with our formula

$$f_n(S^k) = \binom{n+k-1}{k-1}.$$

Moreover, if $H$ is a finite permutation group of degree $k$, then $S \,\mathrm{Wr}\, H$ is the extension of $S^k$ by $H$, and we see that $\mathcal{A}^{S \mathrm{Wr} H}$ is the ring of invariants of $H$ (thought of as acting as a linear group by permutation matrices). In particular, $\mathcal{A}^{S \mathrm{Wr} S_k}$ is isomorphic to the ring of symmetric polynomials in $k$ variables.

The other cases where the structure is known are instances of a general procedure.

Let $M$ be the Fraïssé limit of $\mathcal{C}$, and $G = \mathrm{Aut}(M)$. Suppose that the following properties hold:

- there is a notion of *disjoint union* in $\mathcal{C}$;
- there is a partial order of *involvement* on the $n$-element structures in $\mathcal{C}$, so that if a structure is partitioned in any manner, then it involves the disjoint union of the induced substructures on its parts;
- there is a notion of *connected structure* in $\mathcal{C}$, so that every structure is uniquely expressible as the disjoint union of connected structures.

**Theorem 8** *Under the above assumptions, $\mathcal{A}^G$ is a polynomial algebra generated by homogeneous elements. The generators are the characteristic functions of the isomorphism types of connected structures in $\mathcal{C}$.*

Now the operator $S$ that we defined earlier on integer sequences plays two roles in this context:

- Let $\mathcal{C}$ be a class of structures, each of which is uniquely expressible as a disjoint union of 'connected' substructures. Suppose that the sequence $a = (a_n)$ enumerates (unlabelled) connected structures in $3matthcalC$. Then $b = Sa$ enumerates all unlabelled structures in $\mathcal{C}$.
- Let $A$ be a graded algebra which is a polynomial algebra in homogeneous generators; let the sequence $a = (a_n)$ enumerate the generators by degree. Then the sequence $b = Sa$ is the Hilbert sequence of $A$.

The first fact motivates the question in the earlier section concerning whether $a_n/f_n$ tends to a limit, where $f = Sa$ and $f_n = f_n(G)$ for some permutation group $G$. In the case where the Fraïssé class $\mathcal{C}$ satisfies the hypotheses of the above theorem, the question is equivalent to the following: *Let $p_n$ be the probability that a random $n$-element structure in $\mathcal{C}$ is connected. Does $p_n$ tend to a limit as $n \to \infty$?* See [1] for more information on the probability of connectedness.

### *3.4 Examples*

**Example 9** Let $\mathcal{C}$ be any Fraïssé class, $M$ its Fraïssé limit, and $G = \mathrm{Aut}\, M$. Then, regardless of the structure of $\mathcal{A}^G$, it is true that $\mathcal{A}^{G \mathrm{Wr} S}$ is a polynomial algebra, where $S$ is the symmetric group. For an orbit of $G \,\mathrm{Wr}\, S$ on $n$-sets is described by a partition of an $n$-set with a structure from $\mathcal{C}$ on each part, and no relation between the parts; the class of such partitioned structures is the Fraïssé class corresponding to $G \,\mathrm{Wr}\, S$. Now we interpret 'connected structure' to be one in which the partition has just one part; 'disjoint union' of structures to mean that points of different constituent structures lie in distinct parts; and 'involvement' to be inclusion of all the relations (other than the equivalence relation defining the partition). The axioms for Theorem 8 are satisfied.

The polynomial generators of $\mathcal{A}^{G \mathrm{Wr} S}$ correspond to the orbits of $G$ on $n$-sets, so are enumerated by $(f_n(G))$. We see, incidentally, that the sequence $(f_n(G \,\mathrm{Wr}\, S))$ is obtained from the sequence $(f_n(G))$ by applying the operator $S$. This was the reason for the choice of name. In the next section we will generalise this sequence operator.

**Example 10** We met the *random graph* $R$ of Erdős and Rényi. This is the Fraïssé limit of the class of finite graphs. It is the unique countable homogeneous graph $R$ containing all finite graphs. Let $G = \mathrm{Aut}(R)$.

If we take the usual graph-theoretic notions of connectedness and disjoint union, and let involvement mean 'spanning subgraph', then the axioms before Theorem 8 are satisfied. the algebra $\mathcal{A}^G$ is a polynomial algebra, whose generators correspond to connected graphs.

The group $G$ has a transitive extension $H$, which can be described as follows. A *two-graph* is a collection $\mathcal{T}$ of 3-subsets of a set $X$ having the property that any 4-subset of $H$ contains an even number of members of $\mathcal{T}$. The class of finite two-graphs is a Fraïssé class, and the automorphism group of its Fraïssé limit is a transitive extension of $G$.

This leads to a curious problem. It follows from Theorem 7 that $\mathcal{A}^H$ is an integral domain (and that $e$ is prime in $\mathcal{A}^H$. *Is it a polynomial algebra?* The best chance of proving this would be to identify a class of 'connected' two-graphs.

Now Mallows and Sloane [13] showed that two-graphs and even graphs (graphs with all valencies even) on $n$ points are equinumerous (but there is no natural bijection). Hence, if $\mathcal{A}^H$ is a polynomial algebra, then the number of polynomial generators of degree $n$ is equal to the number of Eulerian (connected even) graphs on $n$ vertices.

**Example 11** Recall the group $G(q)$ preserving the order on $\mathbb{Q}$ and $q$ dense subsets which partition $\mathbb{Q}$. We have $f_n(G(q)) = q^n$, and the orbits of $G(q)$ on $n$-sets are described by words in an alphabet of length $q$. Now the $n$th homogeneous component of $\mathcal{A}^{G(q)}$ is spanned by the words of length $n$. The multiplication is defined on words as follows: the product of two words is the sum (with appropriate multiplicities) of all words which can be obtained by 'shuffling' together the two words in all possible ways. For example,

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

This is the *shuffle algebra*, which arises in the theory of free Lie algebras (see Reutenauer [16], which is a reference for what follows).

A *Lyndon word* is one (like $aabab$) which is strictly smaller (in the lexicographic order) than any proper cyclic permutation of itself. Now, if we interpret 'connected' to mean 'Lyndon word', 'disjoint union' to mean 'concatenation in decreasing lexicographic order', and 'involvement' to be the reverse of lexicographic order, then the axioms are satisfied. This says, in essence, that any word can be expressed uniquely as a concatenation of Lyndon words in decreasing lexicographic order (as $ab.aab$ in the example), and that, of all the words obtained by shuffling Lyndon words together, the greatest is the concatenation in decreasing lexicographic order. We conclude that the shuffle algebra is a polynomial algebra generated by the Lyndon words. This is a result of Radford [15].

Now we get a puzzle similar to that in the last case: it turns out that the groups $G(q)$ have transitive extensions $H(q)$ (so that $H(q)$ is strongly entire, by Theorem 7), but it is unknown whether $\mathcal{A}^(H(q))$ is a polynomial algebra. Here are some further details on the case $q = 2$.

The Fraïssé class corresponding to $H(2)$ consists of what have been called *local orders*, *locally transitive tournaments*, or *vortex-free tournaments* by authors in very different areas: permutation groups [3], model theory [10], and computational geometry [9]. These are tournaments which contain neither a 3-cycle dominating a vertex, nor a 3-cycle dominated by a vertex, as induced sub-tournaments. The Fraïssé limit can be described as follows. Choose a countable dense set on the unit circle with the property that it contains no two antipodal points. (If we choose one of each antipodal pair of complex roots of unity at random, then with probability 1, the resulting set is dense.) Now an arc joins $x$ to $y$ if the angular distance from $x$ to $y$ (in the anticlockwise direction) is smaller than that from $y$ to $x$.

The number $f_n(H(2)$ of $n$-vertex tournaments with this property, up to isomorphism, is given by

$$\frac{1}{2n} \sum_{\substack{d|n \\ d \text{ odd}}} \phi(d) 2^{n/d}.$$

From this, by applying the inverse of the operator $S$, it is possible to calculate the hypothetical sequence enumerating the polynomial generators (assuming that the algebra is polynomial). The sequence, which begins 1, 0, 1, 0, 2, 1, 4, 4, 12, 15 . . ., appears to be unknown.

Note that $f_n(H(2)) \sim 2^{n-1}/n$. If we use instead the group $H^*(2)$ of automorphisms and anti-automorphisms of the tournament (where an anti-automorphism reverses all arcs), we see that $f_n(H^*(2)) \sim 2^{n-2}/n$. This is the example, promised earlier, of a primitive group with slowest known growth rate.

## 4 Cycle index

The class of oligomorphic groups appears to be the largest class of infinite permutation groups to which the theory of cycle index for finite permutation groups can be naturally extended. This has been adequately discussed elsewhere, so only a sketch will be given here. The challenge is to connect this material with the algebra of the last section.

We begin with a brief recall of the cycle index of a finite permutation group. Let $c_i(g)$ denote the number of cycles of length $i$ in the cycle decomposition of $g$, where $g$ is a permutation of a finite set of cardinality $n$. Then the cycle index of $g$ is

$$z(g) = s_1^{c_1(g)} s_2^{c_2(g)} \cdots s_n^{c_n(g)},$$

a monomial in the indeterminates $s_1, \ldots, s_n$. If $G$ is a group of permutations of a set of $n$ elements, its cycle index is the average cycle index of its elements:

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

Clearly there is no hope of extending this definition to an infinite permutation group. However, if $G$ is oligomorphic, we can proceed as follows. Choose representatives for the orbits of $G$ on finite sets. Let $G(\Delta)$ denote the group of permutations of $\Delta$ induced by its setwise stabiliser in $G$. Then we define the *modified cycle index* of $G$ by

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

where the sum is over the orbit representatives. This is well-defined: for a monomial $s_1^{a_1} \cdots s_n^{a_n}$ occurs only in the summands $G(\Delta)$ for which

$$\sum i a_i = |\Delta|,$$

and there are only finitely many of these, since $G$ is oligomorphic. The result is a formal power series in infinitely many indeterminates. (By convention, we take the cycle index of a 'permutation group on the empty set' to be 1.)

If it happens that $G$ is the automorphism group of a homogeneous structure $M$, then $\tilde{Z}(G)$ is the sum of the cycle indices of the automorphism groups of the unlabelled structures in the age of $M$. This agrees with Joyal's definition of the cycle index of a species [8].

This definition works equally well if $G$ is a finite group. But in this case, we get nothing new: it can be shown that

$$\tilde{Z}(G) = Z(G; s_i \leftarrow s_i + 1).$$

(We use the notation $F(s_i \leftarrow t_i)$ for the result of substituting $t_i$ for $s_i$ in the polynomial or formal power series $F$.) In this sense, then, our modified cycle index is a genuine extension of the cycle index of a finite group.

The next three results summarise the behaviour of the modified cycle index under group-theoretic constructions, how we obtain the counting sequences $(f_n(G))$ and $(F_n(G))$ as specialisations, and the modified cycle index of some special groups. As is usual in combinatorial enumeration, we represent the sequence $(f_n(G))$ (which counts unlabelled structures) by the ordinary generating function $f_G(x) = \sum_{n\geq 0} f_n(G)x^n$, and the sequence $(F_n(G))$ (which counts labelled structures) by the exponential generating function $F_G(x)) = \sum_{n\geq 0} F_n(G)x^n/n!$. As earlier, $S$ is the infinite symmetric group and $A$ the group of order-preserving permutations of $\mathbb{Q}$.

**Proposition 12** *(a)* $\tilde{Z}(G \times H) = \tilde{Z}(G)\tilde{Z}(H)$.
*(b)* $\tilde{Z}(G \,\mathrm{Wr}\, H) = \tilde{Z}(H; s_n \leftarrow \tilde{Z}(G; s_m \leftarrow s_{mn}) - 1)$.
*(c) If $H$ is a transitive extension of $G$, then* $\tilde{Z}(G) = \partial\tilde{Z}(H)/\partial s_1$.

**Proposition 13** *(a)* $f_G(x) = \tilde{Z}(G;_n \leftarrow x^n)$.
*(b)* $F_G(x) = \tilde{Z}(G; s_1 \leftarrow x, s_n \leftarrow 0$ *for* $n > 0)$.

**Proposition 14** *(a)* $\tilde{Z}(S) = \exp\left(\sum_{n\geq 1} \frac{s_n}{n}\right)$.
*(b)* $\tilde{Z}(A) = 1/(1 - s_1)$.

*4.2 Sequence operators*

From Propositions 12 and 13, we see that $(f_n(G \,\mathrm{Wr}\, H))$ is determined by $(f_n(G))$ and the modified cycle index of $H$. We can define an operator associated with any oligomorphic group $H$ (which will also be denoted by $H$) formally, as follows: if $a = (a_n)$, then $Ha = (b_n)$, where, setting $a(x) = \sum a_n x^n$ and $b(x) = \sum b_n x^n$, we have

$$b(x) = \tilde{Z}(H; s_n \leftarrow a(x^n) - 1).$$

Thus, $S$ is the operator we met earlier, while we see from Proposition 14 that $Aa = b$ means

$$b(x) = \frac{1}{2 - a(x)}.$$

Now the earlier question about the probability of connectedness can be generalised: *Is it true that, for any oligomorphic group $H$, if $Ha = b$ and the* *sequence $b$ is realised by some oligomorphic permutation group, then $a_n/b_n$ tends to a limit as $n \to \infty$?*

Bernstein and Sloane [2] discuss a number of operators on sequences. Among their list are $S$ and $A$ (which they refer to as EULER and INVERT respectively). They do not consider any other operators of the above form.

Other sequence operators could be defined from groups. Here are two examples:

- For a fixed oligomorphic group $H$, we could consider the operator which takes $(f_n(G))$ to $(f_n(G \times H)$. By Propositions 12 and 13, this is just the convolution with the sequence $(f_n(H))$. In particular, if $H = S$, this replaces a sequence by the sequence of its partial sums.
- We could use the sequences $F_n$ instead of $f_n$. Since

$$F_{G\times H}(x) = F_G(x)F_H(x)$$

and

$$F_{G\mathrm{Wr}H}(x) = F_H(F_G(x) - 1),$$

these operators will be exponential convolution (for the direct product) and substitution in the exponential generating function (for the wreath product).

## References


[1] E. A. Bender, P. J. Cameron, A. M. Oddlyzko and L. B. Richmond, Connectedness, classes, and cycle index, *Discrete Math.*, to appear.

[2] M. Bernstein and N. J. A. Sloane, Some canonical sequences of integers, *Linear Algebra Appl.* **228** (1995), 57–72.

[3] P. J. Cameron, Orbits of permutation groups on unordered sets, II, *J. London Math. Soc.* (2) **23** (1981), 249–265.

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

[5] P. J. Cameron, On an algebra related to orbit-counting, *J. Group Theory* **1** (1998), 173–179.

[6] P. Erdős and A. Rényi, Asymmetric graphs, *Acta Math. Acad. Sci. Hungar.* **14** (1963), 295–315.

[7] R. Fraïssé, *Theory of Relations*, North-Holland, Amsterdam, 1986.

[8] A. Joyal, Une theorie combinatoire des séries formelles, *Adv. Math.* **42** (1981), 1–82.

[9] D. E. Knuth, *Axioms and Hulls*, Lecture Notes in Computer Science **606**, Springer, Berlin, 1992.

[10] A. H. Lachlan, Countable homogeneous tournaments, *Trans. Amer. Math. Soc.* **284** (1984), 431–461.

[11] H. D. Macpherson, The action of an infinite permutation group on the unordered subsets of a set, *Proc. London Math. Soc.* (3) **46** (1983), 471–486.

[12] H. D. Macpherson, Growth rates in infinite graphs and permutation groups, *Proc. London Math. Soc.* (3) **51** (1985), 285–294.

[13] 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.

[14] M. Pouzet, Application de la notion de relation presque-enchaînable au dénombrement des restrictions finies d'une relation, *Z. Math. Logik Grundl. Math.* **27** (1981), 289–332.

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

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