# Counting problems from infinite permutation groups

CSG notes
Peter J. Cameron
November 2005

A permutation group $G$ on an infinite set $\Omega$ is said to be *oligomorphic* if the number of orbits of $G$ on $\Omega^n$ is finite for all natural numbers $n$. (By convention, there is one orbit on $\Omega^0$.

Let

- $F_n^*(G) =$ number of $G$-orbits on $\Omega^n$, the set of all $n$-tuples of elements of $\Omega$;
- $F_n(G) =$ number of $G$-orbits on $(\Omega)_n$, the set of $n$-tuples of distinct elements of $\Omega$;
- $f_n(G) =$ number of $G$-orbits on $\binom{\Omega}{n}$, the set of $n$-element subsets of $\Omega$.

It is easy to see (and we do so in a moment) that the finiteness of one of the three numbers $F_n^*(G)$, $F_n(G)$ and $f_n(G)$ implies the finiteness of the others.

The purpose of these notes is to point out two things:

- the problem of determining the sequences $(F_n^*)$, $(F_n)$ or $(f_n)$ include many familiar combinatorial enumeration problems;
- these sequences behave much better than arbitrary sequences of natural numbers, and it would be nice to know why.

Throughout the notes, $G$ is a permutation group on an infinite set $\Omega$.

## 1 Basic results

First we see why the finiteness conditions on the three sequences are all equivalent.

**Proposition 1.1** *Let $G$ be a permutation group on $\Omega$. If any one of $F_n^*(G)$, $F_n(G)$ and $f_n(G)$ is finite, then so are the others; and moreover, $F_m^*(G)$, $F_m(G)$ and $f_m(G)$ are finite for all $m \leq n$.*

**Proof** The initial segment of length $m$ of an $n$-tuple is an $m$-tuple; and if two $n$-tuples lie in the same orbit, so do their initial segments. So $F_m(G) \leq F_n(G)$.

Each $G$-orbit on $n$-sets gives rise to between 1 and $n!$ orbits on $n$-tuples of distinct elements. So $f_n(G) \leq F_n(G) \leq n!\, f_n(G)$.

Finally we have

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

where $S(n,m)$ is the *Stirling number of the second kind*, the number of partitions of an $n$-set with $m$ parts. For given any $n$-tuple $(\alpha_1, \ldots, \alpha_n)$, we obtain an equivalence relation on $\{1, \ldots, n\}$ by putting $i \equiv j$ if and only if $\alpha_i = \alpha_j$; then, if there are $m$ equivalence classes, we get a $m$-tuple of distinct elements by taking the entries $\alpha_i$ indexed by the smallest elements in the equivalence classes in order. This process respects the action of $G$ and so yields the desired equation. Thus, if $F_n^*(G)$ is finite, so is $F_n(G)$; and if $F_m(G)$ is finite for all $m \leq n$, then $F_n^*(G)$ is finite. ∎

The proof gives us the first part of the next result. A permutation group $G$ is *$n$-transitive* if $F_n(G) = 1$, that is, any $n$-tuple of distinct points can be mapped to any other by some element of $G$.

**Proposition 1.2** *(a) $F_n(G) \geq F_{n-1}(G)$ for $n > 0$, with equality if and only if $G$ is $n$-transitive.*

*(b) $f_n(G) \geq f_{n-1}(G)$ for $n > 0$.*

**Proof** (a) As in the preceding proposition, mapping each $n$-tuple of distinct points to its initial segment of size $n-1$ gives a surjective function from orbits on $(\Omega)_n$ to orbits on $(\Omega)_{n-1}$. If equality holds, then for every $(n-1)$-tuple, all possible extensions to an $n$-tuple lie in the same orbit. So the stabiliser of $n-1$ points acts transitively on the remaining points. It is easy to see that this implies $n$-transitivity.

(b) This is much less trivial, and I remark that a characterisation of the case of equality is not known, despite a lot of effort. Two different proofs are known. I will deduce the result from a Ramsey-type theorem which will be stated without proof. There is also a proof using linear algebra. ∎

Suppose that the $(n-1)$-element subsets of a set $\Omega$ are coloured with $r$ colours $c_1, \ldots, c_r$. Then the *colour scheme* of an $n$-set $X$ is $(a_1, \ldots, a_r)$, where $a_i$ is the number of subsets of $X$ which have colour $c_i$.

**Proposition 1.3** *Suppose that the $(n-1)$-subsets of an infinite (or sufficiently large finite) set $\Omega$ are coloured with $r$ colours, all of which are used. Then at least $r$ colour schemes of $n$-sets occur.* ∎

**Proof of Proposition 1.2** Associate a colour with each $G$-orbit on $\binom{\Omega}{n-1}$. If there are $f_{n-1}(G) = r$ orbits, then we have $r$ colours, so at least $r$ colour schemes of $n$-sets occur. But $n$-sets with different colour schemes lie in different orbits; so $f_n(G) \geq r$. ■

Now let $\mathfrak{F}^*$, $\mathfrak{F}$ and $\mathfrak{f}$ denote the sets of all sequences $(F_n^*(G))$, $(F_n(G))$, $(f_n(G))$ respectively arising from oligomorphic permutation groups. Our main problem can now be stated:

**Problem 1** Characterise the sets $\mathfrak{F}^*$, $\mathfrak{F}$ and $\mathfrak{f}$.

We will see shortly that each set has cardinality $2^{\aleph_0}$, and that $\mathfrak{F}^* \subset \mathfrak{F}$.

I will also speak of the $\mathfrak{F}$-sequence of a permutation group $G$ to mean the sequence $(F_n(G))$, and similarly for the other two types.

Here are two further properties depending on results from first-order logic.

**Proposition 1.4** *A sequence of positive integers is realised as $F_n^*(G)$ for some oligomorphic group $G$ if and only if every initial subsequence of it is so realised. Similarly for $F_n(G)$ or $f_n(G)$.*

**Proof** We can write first-order sentences saying that we have a group acting on a set with $a_n$ orbits on $n$-tuples for all $n$. The sequence is realisable if and only if this set is satisfiable. The *compactness theorem* of first-order logic asserts that a set of sentences is satisfiable if and only if every finite subset is satisfiable. ■

**Proposition 1.5** *A sequence of positive integers is realised as $F_n^*(G)$ for some oligomorphic group $G$ if and only if it is realised by such a group of countable degree.*

**Proof** This uses the other pillar of first-order model theory, the downward Löwenheim–Skolem theorem, asserting that if a set of sentences in a countable language is satisfiable, it is satisfiable in a countable structure. ■

## 2 A few examples

The obvious first example is the symmetric group on $\Omega$ (consisting of all permutations), which we denote by $S$ in these notes. Clearly we have $F_n(S) = f_n(S) = 1$ for all $n$. Thus we have

$$F^*(n)(S) = \sum_{m=1}^{n} S(n,m) = B(n),$$

where the *Bell number* $B(n)$ is the number of partitions of an $n$-set.

According to our earlier terminology, $F_n(G) = 1$ for all $n$ means that $G$ is $n$-transitive for all $n$; we say that the group $G$ is *highly transitive* if this holds. Analogously, we say that $G$ is *n-set-transitive* if $f_n(G) = 1$, and is *highly set-transitive* if this holds for all $n$. Clearly the symmetric group has both these properties. The next few groups are highly set-transitive but not highly transitive.

The group $A$ is the group of order-preserving permutations of the ordered set $\mathbb{Q}$ of rational numbers. A picture shows that $G$ is $n$-set transitive: given any two $n$-tuples of distinct rationals, arrange them in increasing order, map the first $n$-tuple to the second so as to preserve the order, and extend this to a piecewise-linear order-preserving map on the whole of $\mathbb{Q}$. Thus $f_n(A) = 1$. The proof shows that $F_n(A) = n!$, since each ordering of an $n$-tuple corresponds to a single orbit. From this we see that $F_n^*(A) = \sum_{m=1}^{n} S(n,m)\,m!$, the number of labelled *preorders* (or *preferential arrangements* of $n$ points; these are orderings where we are allowed to be indifferent about two elements.

The group $B$ is the group of permutations which preserve or reverse the ordered set $\mathbb{Q}$. Again we have $f_n(B) = 1$ for all $n$. Moreover, $F_n(B) = n!/2$ for $n \geq 2$. In particular, $B$ is 2-transitive but not 3-transitive.

The group $C$ is the group of permutations which preserve the circular order on the set of complex roots of unity. (We could take the whole circle; using the roots of unity gives us a countable set. A circular order is a ternary relation which holds for three points $a,b,c$ if they occur in anticlockwise order on the circle.) We have $f_n(C) = 1$ and $F_n(C) = (n-1)!$ for $n \geq 2$. In particular, $C$ is 2-transitive but not 3-transitive.

Combining these two ideas, the group $D$ is the group of permutations which preserve or reverse the circular order on the set of roots of unity. Then $f_n(D) = 1$ and $F_n(D) = (n-1)!/2$ for $n \geq 3$. So $D$ is 3-transitive but not 4-transitive.

The next theorem characterises these groups.

**Theorem 2.1** *A permutation group which is highly homogeneous but not highly transitive preserves or reverses a linear or circular order. In particular, if its degree is countable, then it is a subgroup of one of the groups $A,B,C,D$ described above.* ■

# 3 Characterisations and closure properties

In this section we give two reinterpretations of the condition of oligomorphy.

The first is taken from model theory in first-order logic. A first-order theory is said to be $\aleph_0$-*categorical* if it has a unique countable model up to isomorphism. An *n-type* over a first-order theory $T$ is a set of $n$-variable formulae maximal with respect to being consistent in $T$; it is *realised* in a model $M$ of $T$ if there exist $a_1,\ldots,a_n \in M$ such that the formulae in the type hold when these points are satisfied for their variables (we say that $(a_1,\ldots,a_n)$ is a *realising n-tuple*. Now the following theorem is due to Engeler, Ryll-Nardzewaki and Svenonius.

**Theorem 3.1** *The theory of a countable first-order structure M is $\aleph_0$-categorical if and only if the automorphism group of M is oligomorphic. Moreover, if this holds, then every n-type of the theory is realised in M, and the realising tuples for the types are precisely the orbits of* $\mathrm{Aut}(M)$ *on* $M^n$. ■

Hence the sequences $(F_n^*(G))$ for oligomorphic groups $G$ are precisely the sequences counting types over an $\aleph_0$-categorical theory.

**Proposition 3.2** *A sequence of positive integers is realised as $F_n^*(G)$ for some oligomorphic group G if and only if every initial subsequence of it is so realised. Similarly for $F_n(G)$ or $f_n(G)$.*

**Proof** We can write first-order sentences saying that we have a group acting on a set with $a_n$ orbits on $n$-tuples for all $n$. The sequence is realisable if and only if this set is satisfiable. The *compactness theorem* of first-order logic asserts that a set of sentences is satisfiable if and only if every finite subset is satisfiable. ■

The second connection is with the theory developed by Fraïssé. For convenience, we consider *relational structures* only; such a structure is a set carrying specified relations of given arities. (For example, a graph, or a partial order, is a structure over a language with a single binary relation.)

A relational structure $M$ is called *homogeneous* if every isomorphism between finite substructures of $M$ can be extended to an automorphism of $M$. (Here, as throughout this section, a substructure is always an *induced* substructure, that is, we take a subset of $M$ and all instances of relations whose arguments lie in the subset.)

A class $\mathscr{C}$ of finite relational structures has the *amalgamation property* if, whenever $A, B_1, B_2 \in \mathscr{C}$ and $f_i : A \to B_i$ are embeddings for $i = 1,2$, there exists $C \in \mathscr{C}$ and embeddings $g_i : B_i \to C$ for $i = 1,2$ such that $f_1 g_1 = f_2 g_2$. Informally, this just says that $B_1$ and $B_2$ can be “glued together” along a common substructure $A$ (but note that the glueing might identify some points outside $A$).

The *age* of a relational structure $M$ is the class of all finite relational structures (over the same language) which can be embedded in $M$ as induced substructures. Fraïssé characterised the ages of countable homogeneous structures as follows:

**Theorem 3.3** *A class $\mathscr{C}$ of finite relational structures is the age of a countable relational structure $M$ if and only if the following conditions hold:*

*(a) $\mathscr{C}$ is closed under isomorphism;*

*(b) $\mathscr{C}$ is closed under taking induced substructures;*

*(c) $\mathscr{C}$ contains only countably many members up to isomorphism;*

*(d) $\mathscr{C}$ has the amalgamation property.*

*Moreover, if these conditions hold, then $M$ is unique up to isomorphism.* ■

A class satisfying (a)–(d) is called a *Fraïssé class*, and the unique countable structure $M$ of which it is the age is its *Fraïssé limit*.

The connection with oligomorphic groups is as follows.

**Proposition 3.4** *Suppose that $M$ is the Fraïssé limit of a Fraïssé class $\mathscr{C}$. Then $G = \mathrm{Aut}(M)$ is oligomorphic if and only if $M$ contains only finitely many $n$-element structures up to isomorphism for each natural number $n$. If this holds, then $f_n(G)$ is equal to the number of unlabelled $n$-element structures in $\mathscr{C}$ (that is, structures up to isomorphism), while $F_n(G)$ is equal to the number of labelled $n$-element structures in $\mathscr{C}$ (that is, structures on the point set $\{1,\ldots,n\}$).* ■

A permutation group $G$ is a *dense subgroup* of a permutation group $H$ (on the same set $\Omega$) if $G$ and $H$ have the same orbits on $\Omega^n$ for all $n$. (This arises from a natural topology on the symmetric group which we do not require here.)

**Proposition 3.5** *Any permutation group on a countable set $\Omega$ is a dense subgroup of the automorphism group of a homogeneous relational structure $M$ on $\Omega$.* ■

Thus the problems of characterising the sequences $(f_n(G))$ and $(F_n(G)$ for oligomorphic groups $G$ are precisely those of counting unlabelled and labelled structures in Fraïssé classes, assuming that the numbers are finite.

Here is a simple example. It is very easy to see that the class of finite graphs is a Fraïssé class. So there is a countable homogeneous graph containing all finite graphs: this is the famous *random graph*, or *Rado graph*. Its automorphism group $G$ has the property that $f_n(G)$ and $F_n(G)$ are the numbers of unlabelled and labelled $n$-vertex graphs.

We also need to look at a stronger condition. A class $\mathscr{C}$ of finite relational structures is said to satisfy the *strong amalgamation property* if, in the definition of the amalgamation property, no extra identifications are made in the glueing; that is, the images of $B_1$ and $B_2$ inside $C$ intersect precisely in the image of $A$. We say that a Fraïssé class is *strong* if it has the strong amalgamation property, and transfer this term also to its Fraïssé limit $M$, the automorphism group $\mathrm{Aut}(M)$ of $M$, and any dense subgroup $G$ of $\mathrm{Aut}(M)$.

**Proposition 3.6** *The permutation group $G$ on $\Omega$ is strong if and only if the subgroup of $G$ fixing pointwise any finite set of points does not fix any additional points.* ■

Let $\mathfrak{F}^*_{\mathrm{s}}$, $\mathfrak{F}_{\mathrm{s}}$ and $\mathfrak{f}_{\mathrm{s}}$ denote the sets of all sequences in $\mathfrak{F}^*$, $\mathfrak{F}$ or $\mathfrak{f}$ respectively which are realised by strong oligomorphic groups. Here are some simple facts these classes.

**Proposition 3.7** *(a) We have $\mathfrak{F}^* \subset \mathfrak{F}$.*

*(b) The set $\mathfrak{F}^*$ is closed under pointwise multiplication.*

*(c) The set $\mathfrak{F}_{\mathrm{s}}$ is closed under pointwise multiplication.*

*(d) We have $\mathfrak{F}_{\mathrm{s}} \subset \mathfrak{f}_{\mathrm{s}}$.*

**Proof** We'll see the proofs of (a) and (b) shortly; here are the others. For (c), let $\mathscr{C}_1$ and $\mathscr{C}_2$ be strong Fraïssé classes realising two sequences in $\mathfrak{F}$. Let $\mathscr{C} = \mathscr{C}_1 \wedge \mathscr{C}_2$ be the class whose members consist of a $\mathscr{C}_1$ structure and a $\mathscr{C}_2$-structure imposed on the same set. The $\mathfrak{F}$-sequence for $\mathscr{C}$ is the product of those for $\mathscr{C}_1$ and $\mathscr{C}_2$; and it is easily seen that $\mathscr{C}$ satisfies strong amalgamation. (This fails without the strong condition, since amalgamation of the $\mathscr{C}_1$ and $\mathscr{C}_2$ structures might require incompatible identifications.)

For (d), let $\mathscr{L}$ be the class of finite totally ordered sets. Then unlabelled $\mathscr{C} \wedge \mathscr{L}$-structures correspond in a natural way to labelled $\mathscr{C}$-structures. Moreover, $\mathscr{L}$ satisfies strong amalgamation. ■

Parts (b) and (c) raise an obvious question:

**Problem 2** Is $\mathfrak{F}$ closed under pointwise multiplication?

Here's a possible counterexample. The sequence $1,1,2,4,10,26,76,\ldots$ (whose $n$th term is the number of solutions of $g^2 = 1$ in $S_n$) belongs to $\mathfrak{F}$: the group preserving a partition of $\Omega$ into parts of size 2 realises this sequence. This group is not strong: the stabiliser of a point fixes the other point in the same part. Is its pointwise square in $\mathfrak{F}$?

We conclude by showing that the above classes are uncountable, and that there is no upper bound on their growth rates.

Let $a_1, a_2, \ldots$ be any sequence of positive integers. Consider the Fraïssé class consisting of a set carrying $a_1$ unary relations, $a_2$ binary relations, and so on, where the relations are unrestricted except for the fact that they only hold for tuples with all members distinct. Then if $|X| = m$, all the relations of arity greater than $m$ are trivial on $X$, so there are only finitely many structures on $X$ up to isomorphism; but clearly this number is (much) greater than $a_m$. Moreover, the structures we have constructed form a Fraïssé class. Taking $a_n \in \{0,1\}$ for all $n$, it is easy to see that the sequences are distinct; so there are $2^{\aleph_0}$ of them.

# 4 Generating functions and cycle index

We can represent sequences by generating functions. As suggested by the relationship with labelled and unlabelled counting problems, we use the *exponential generating function*

$$F_G(z) = \sum_{n\geq 0} \frac{F_n(G)}{n!} z^n, \qquad F_G^*(z) = \sum_{n\geq 0} \frac{F_n^*(G)}{n!} z^n$$

for sequences in $\mathfrak{F}$ and $\mathfrak{F}^*$, and the *ordinary generating function*

$$f_G(z) = \sum_{n\geq 0} f_n(G) z^n$$

for sequences in $\mathfrak{f}$.

Note that, for example, $f_G(z)$ is an analytic function in some neighbourhood of the origin if and only if the growth of $(f_n(G))$ is no faster than exponential. We will see that this is not usually the case!

Familiar properties of Stirling numbers show that

$$F_G^*(z) = F_G(\mathrm{e}^z - 1).$$

For some of our earlier examples, we have

| $G$ | $F_G(z)$ | $f_G(z)$ |
|---|---|---|
| $S$ | $\mathrm{e}^z$ | $1/(1-z)$ |
| $A$ | $1/(1-z)$ | $1/(1-z)$ |
| $C$ | $1-\log(1-z)$ | $1/(1-z)$ |

In fact there is a more general generating function from which all these can be obtained; this is defined as follows.

- If $g$ is a permutation on a finite set, we put
$$z(g) = \prod_{i\geq 1} s_i^{c_i(g)},$$
where $s_i$ are indeterminates and $c_i(g)$ is the number of cycles of length $i$ in the cycle decomposition of $g$.

- If $G$ is a finite permutation group, we put
$$Z(G) = \frac{1}{|G|}\sum_{g\in G} z(g).$$
This is the usual cycle index of $G$.

- If $G$ is a finite or oligomorphic permutation group, the *modified cycle index* of $G$ is defined by
$$\tilde{Z}(G) = \sum_A Z(G[A]),$$
where $A$ runs over a set of representatives of $G$-orbits on finite sets, and $G[A]$ denotes the finite permutation group induced on $A$ by its setwise stabiliser.

The name “modified cycle index” is used because, if $G$ is a finite permutation group, then
$$\tilde{Z}(G) = Z(G; s_i \leftarrow s_i + 1),$$
the right-hand side meaning that each variable $s_i$ is replaced by $s_i + 1$. But for infinite permutation groups, we get something new.

**Exercise** Calculate the modified cycle index for each of the groups $S$, $A$, $C$.

The univariate generating functions are specialisations of $\tilde{Z}(G)$ as follows:

- $f_G(z) = \tilde{Z}(G; s_i \leftarrow z^i)$;
- $F_G(z) = \tilde{Z}(G; s_1 \leftarrow z, s_i \leftarrow 0 \text{ for } i > 1)$.

# 5 Direct products

Let $G_1$ and $G_2$ be permutation groups on sets $\Omega_1$ and $\Omega_2$ respectively.

The direct product of $G_1 \times G_2$ of $G_1$ and $G_2$ has two natural actions as a permutation group. Each is oligomorphic if $G_1$ and $G_2$ are.

The first is the so-called *intransitive action*, on the disjoint union of the sets $\Omega_1$ and $\Omega_2$. An ordered pair $(g_1, g_2)$ acts as $g_1$ on $\Omega_1$ and as $G_2$ on $\Omega_2$. It is easy to see that we have

$$F_n(G_1 \times G_2) = \sum_{k=0}^{n} \binom{n}{k} F_k(G_1) F_{n-k}(G_2), \qquad f_n(G_1 \times G_2) = \sum_{k=0}^{n} f_k(G_1) f_{n-k}(G_2).$$

This can be stated more concisely in terms of generating functions as

$$F_{G_1 \times G_2}(z) = F_{G_1}(z) F_{G_2}(z), \qquad f_{G_1 \times G_2}(z) = f_{G_1}(z) f_{G_2}(z).$$

Indeed, we have that

$$\tilde{Z}(G_1 \times G_2) = \tilde{Z}(G_1) \tilde{Z}(G_2),$$

from which the other results follow.

So the class $\mathfrak{f}$ is closed under *convolution*, and the class $\mathfrak{F}$ under *exponential convolution*.

The second natural action of the direct product is the *product action* on $\Omega_1 \times \Omega_2$, in which the factors act coordinatewise: that is,

$$(\alpha_1, \alpha_2)^{(g_1, g_2)} = (\alpha_1^{g_1}, \alpha_2^{g_2}).$$

It is possible to describe the modified cycle index of $G_1 \times G_2$ in this action, but the description is not straightforward. See [2].

We mention just one example here. $f_n(A \times A)$ (with the product action) is equal to the number of “incidence matrices”, or zero-one matrices with exactly $n$ ones and no row or column consisting entirely of zeros. See [3].

Using the product action of the direct product, we can prove part (b) of Proposition 3.7. Let $G_1$ and $G_2$ be permutation groups whose $\mathfrak{F}^*$-sequences are $s_1$ and $s_2$ respectively. Then $G_1 \times G_2$, in the product action, realises the pointwise product of $s_1$ and $s_2$. ■

# 6 Wreath products

Let $G_1$ and $G_2$ be permutation groups on sets $\Omega_1$ and $\Omega_2$ respectively.

The *wreath product* $G_1 \operatorname{Wr} G_2$ of $G_1$ and $G_2$ is defined as abstract group as follows. The *base group* $B$ is a Cartesian product of $|\Omega_2|$ copies of $G_1$ (this can be regarded as the set of functions from $\Omega_2$ to $G_1$ with pointwise multiplication. The *top group* $T$ is a copy of $G_2$, acting on $B$ by permuting the factors of the Cartesian product as it permutes the elements of $\Omega_2$ (that is, acting on the arguments of the functions). The semidirect product of $B$ by $T$ (with this action) is the wreath product. Note that the action of $G_1$ on $\Omega_1$ plays no role in this definition.

Like the direct product, the wreath product has two natural actions as a permutation group. The first is the *imprimitive action*, which is oligomorphic if $G_1$ and $G_2$ are. We take $\Omega$ to be $\Omega_1 \times \Omega_2$, regarded as a set of copies of $\Omega_1$ indexed by $\Omega_2$. Now the base group acts on $\Omega$: a given factor of the Cartesian product acts on the corresponding copy of $\Omega_1$. The top group acts by permuting the copies of $\Omega_1$ (by acting on the index set $\Omega_2$).

For the cycle index in this action, we have the substitution rule

$$\tilde{Z}(G_1 \operatorname{Wr} G_2) = \tilde{Z}(G_2; s_i \leftarrow \tilde{Z}(G_1, s_j \leftarrow s_{ij}) - 1).$$

This gives the formulae for the $\mathfrak{F}$- and $\mathfrak{f}$-sequences:

- $F_{G_1 \operatorname{Wr} G_2}(z) = F_{G_2}(F_{G_1}(z) - 1)$,
- $f_{G_1 \operatorname{Wr} G_2}(z) = \tilde{Z}(G_2; s_i \leftarrow f_{G_1}(z^i) - 1)$.

We see that $\mathfrak{F}$ is closed under substitution of generating functions (after making the constant term of the substituted function zero).

The wreath product allows us to prove part (a) of Proposition 3.7. Let $G$ be a permutation group whose $\mathfrak{F}^*$-sequence is $s$; that is, the number of orbits of $G$ on $n$-tuples is $s_n$. Now consider the group $S \operatorname{Wr} G$ in its imprimitive action. Each $n$-tuple of points in the domain of $G$ (that is, of blocks of imprimitivity for the wreath product) can be lifted to an $n$-tuple of distinct points in the domain of

$S\,\mathrm{Wr}\,G$; moreover, two $n$-tuples are in the same $G$-orbit if and only if their lifts are in the same $S\,\mathrm{Wr}\,G$-orbit.

This can also be seen from looking at the substitution rule. We see that

$$F_{S\mathrm{Wr}G}(z) = F_G(\mathrm{e}^z - 1),$$

and the right-hand side is $F^*_G(z)$, by our observation on Stirling numbers. ■

We see, however, that the $\mathfrak{f}$-sequence of a wreath product is not obtainable from the $\mathfrak{f}$-sequences of its factors alone; we need the modified cycle index of the top group.

The other action of the wreath product is the *power action* on the set of functions from $\Omega_2$ to $\Omega_1$, where the base group acts coordinatewise, and the top group permutes the argument of the functions. This group is oligomorphic if $G_1$ is oligomorphic and $\Omega_2$ is finite. This case is more complicated and little is known other than the formula

$$F^*_n(G) = Z(G_2; s_i \leftarrow F_n(G_1)^i)$$

(see [2]).

# 7 Primitive groups

One of the remarkable discoveries of Macpherson is that an $\mathfrak{f}$-sequence of a primitive group either is constant or grows at least exponentially. His result, as refined by Merola, is as follows:

**Theorem 7.1** *There is an absolute constant $c$ with the property that, if $G$ is a primitive oligomorphic group which is not highly set-transitive, then*

*(a) (Macpherson [4]) $f_n(G) \geq c^n/p(n)$ for some polynomial $p$;*

*(b) (Merola [6]) $F_n(G) \geq c^n n!/p(n)$ for some polynomial $p$.* ■

Macpherson proved part (a) with $c = \sqrt[5]{2} = 1.149\ldots$; Merola, in addition to proving (b), improved the constant to $1.324\ldots$. The proofs are rather long! Merola's Theorem throws some light on a problem mentioned earlier. The sequence whose $n$th term is the square of the number of involutions in $S_n$ grows as $n!$ times a subexponential function; so if there is a group $G$ realising this as the $\mathfrak{F}$-sequence, then $G$ must be imprimitive.

This theorem shows that, at least for primitive groups, exponential growth is the slowest we can have, and it is important to understand the structures for which the growth of the $\mathfrak{f}$-sequence is no faster than exponential. Empirically, these structures seem to arise from two sources: ordered sets and trees; and their asymptotic behaviour is very well-behaved. Indeed, in all cases which have been examined, the "exponential constant" $\lim_{n\to\infty}(f_n(G))^{1/n}$ exists. (This limit is infinite if the growth is faster than exponential.)

**Problem 3** Is it true that $\lim_{n\to\infty}(f_n(G))^{1/n}$ exists for any primitive oligomorphic group $G$? If so, what are the possible values of the exponential constant? In particular, what is the smallest value greater than 1, and what is the smallest limit point (if any)?

We continue this section with some examples.

**Example** A *tournament* is a directed graph in which each pair of distinct vertices is joined by a directed edge in just one direction. A tournament is said to be a *local order* if it does not contain a 4-point subtournament consisting of a vertex dominating or dominated by a 3-cycle. The finite local orders form a Fraïssé class, whose Fraïssé limit $T$ is more easily described as follows. Take a countable dense set of points on the unit circle containing no antipodal pair of points. (If we consider the set of all complex roots of unity, and randomly choose one out of each pair $\{\omega,-\omega\}$, then the resulting set is dense with probability 1.) Now put a directed edge from $x$ to $y$ if the shorter arc from $x$ to $y$ is in the anticlockwise direction. The result is the universal homogeneous local order $T$. We see that $\mathrm{Aut}(T)$ is 2-set transitive, hence primitive; and $f_n(\mathrm{Aut}(T))$ is equal to the number of isomorphism types of $n$-vertex local order, which is asymptotically $2^{n-1}/n$. (In fact, by taking the larger group $G$ of permutations which preserve or reverse the edge directions, we obtain $f_n(G)\sim 2^{n-2}/n$, the slowest known growth rate for a primitive but not highly set-transitive group.

This can be generalised as follows. Take any positive integer $r\geq 2$, and take a countable dense set of points on the unit circle with the property that out of any collection of $r$ equally-spaced points we take at most one. Now define $r$ binary relations $R_0,R_1,\ldots,R_{r-1}$ by the rule that $(x,y)\in R_i$ if and only if the angle (in the positive sense) from $x$ to $y$ lies in the range $(2i\pi/r,2(i+1)\pi/r)$. If $r$ is odd, then $R_{(r-1)/2}$ is a symmetric relation, and defines an undirected graph; the others define $\lfloor(r-1)/2\rfloor$ converse pairs of directed graphs. This structure is homogeneous, and the number of orbits on $n$-sets of its automorphism group satisfies $f_n(G)\sim r^{n-1}/n$.

This shows that every positive integer occurs as the exponential constant in the growth rate of $(f_n(G))$ for some primitive group $G$.

**Example** The next example is not primitive but it is closely related to the preceding one and we will refer to it again later. This group is the stabiliser of a point in the preceding one.

Take the rational numbers and colour them with $r$ colours so that every colour class is dense. The structure consists of the total order and the $r$ colour classes. It is unique up to isomorphism and is homogeneous; the automorphism group $G$ satisfies $f_n(G) = r^n$. Indeed, each orbit of $G$ on $n$-sets is parametrised by a word of length $n$ in an alphabet of $r$ symbols, where the word $a_1 \cdots a_n$ indexes the orbit on $n$-tuples whose $i$th element (in increasing order) has colour $a_i$ for $i = 1, \ldots, n$.

**Example** A *boron tree* is a finite tree in which every vertex has valency 1 or 3. (Boron trees describe the analogue of hydrocarbons in a boron-based chemistry.) On the set of leaves of a boron tree, we can define a 4-place relation as follows. Given four points $a, b, c, d$, there is a unique partition into two sets of size 2 such that the paths joining vertices in the same set do not intersect. Write $R(a, b; c, d)$ if this partition is $ab \mid cd$. (See Figure 1). The relational structures obtained in this way form a Fraïssé class; the boron tree is uniquely recoverable from the quaternary relation on the set of leaves. Thus, if $G$ is the automorphism group of the Fraïssé limit, then $f_n(G)$ is equal to the number of boron trees with $2n-2$ vertices, which is asymptotically $An^{-5/2}c^n$, where $c = 2.483\ldots$. Note in passing that this group is 3-transitive but not 4-transitive, is 5-set transitive, and has $f_6 = f_7 = 2$. (All these assertions can be proved by drawing diagrams like Figure 1.)

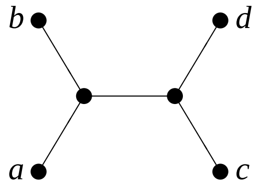

Figure 1: A boron tree

There are many variations on this example, quite a few of which have exponential growth of $(f_n(G))$.

# 8 A graded algebra

Further light on the $\mathfrak{f}$-sequences comes from the fact that there is a graded algebra whose Hilbert series is the $\mathfrak{f}$-series of any given oligomorphic group.

Let $\mathbb{F}$ be any field, and $\Omega$ an infinite set. Let $V_n$ denote the vector space of all functions from $\binom{\Omega}{n}$ to $\mathbb{F}$ (with pointwise addition and scalar multiplication), and

$$A = \bigoplus_{n\geq 0} V_n.$$

We define a multiplication on $A$ as follows. For $f \in V_m$, $g \in V_n$, and $X$ an $(m+n)$-element subset of $\Omega$, we set

$$(fg)(X) = \sum_{Y\subseteq X, |Y|=m} f(Y)g(X\setminus Y).$$

Extend by linearity to the whole of $A$. This makes $A$ into a commutative and associative graded algebra. (This is sometimes referred to as the *reduced incidence algebra* of the poset of finite subsets of $\Omega$.)

Now let $G$ be a permutation group on $\Omega$, and let $V_n^G$ be the subspace of $G$-fixed functions in $V_n$, and

$$A^G = \bigoplus_{n\geq 0} V_n^G.$$

A function is fixed by $G$ if and only if it is constant on the orbits of $G$. So, if $G$ is oligomorphic, then

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

That is, the generating function $f_G(z) = \sum_{n\geq 0} f_n(G)z^n$ is the *Hilbert series* of $A^G$.

The algebra $A^G$ may contain divisors of zero. For example,

- if the characteristic of $\mathbb{F}$ is $p > 0$, then $f^p = 0$ for any $f \in V_n^G$.
- if $G$ has a finite orbit $X$ on $\Omega$ with, say, $|X| = n$, and $f \in V_n$ is the characteristic function of $\{X\}$, then $f \in V_n^G$ and $f^2 = 0$.

From now on we will make two blanket assumptions to exclude these cases:

- we assume that the characteristic of $\mathbb{F}$ is zero, and where necessary, that $\mathbb{F} = \mathbb{C}$;
- we assume that $G$ has no finite orbits on $\Omega$.

**Conjecture 1** Under the above assumptions, $A^G$ is an integral domain.

Let $e$ denote the constant element of $V_1$ with value 1. Then of course $e \in V_1^G$ for any group $G$. It is known that $e$ is not a zero-divisor. (This is essentially the content of the linear algebra proof of the inequality $\mathfrak{f}_{n+1}(G) \geq \mathfrak{f}_n(G)$ referred to earlier: conversely, if we know that $e$ is not a zero-divisor, then multiplication by $e$ is a monomorphism from $V_n^G$ to $V_{n+1}^G$, so the inequality follows.)

**Conjecture 2** Under the above assumptions, $e$ is prime in $A^G$ (so that $A^G/\langle e\rangle$ is an integral domain.

Conjecture 2 implies Conjecture 1. For if $fg = 0$ with $f, g$ non-zero, we can assume that $f$ and $g$ are homogeneous of smallest possible degree. Then $e$ divides $fg$, so (w.l.o.g.) $e$ divides $f$, say $f = ef'$. Then $ef'g = 0$, so $f'g = 0$, contradicting the assumed minimality.

We say that $G$ is *entire* if $A^G$ is an integral domain and *strongly entire* if $e$ is prime in $A^G$. These concepts would have the following implications for the growth of the $\mathfrak{f}$-sequence:

- If $G$ is entire, then
$$\mathfrak{f}_{m+n}(G) \geq \mathfrak{f}_m(G) + \mathfrak{f}_n(G) - 1$$
for all $m, n \geq 0$;
- If $G$ is strongly entire, then
$$\mathfrak{f}_{m+n+1}(G) - \mathfrak{f}_{m+n}(G) \geq (\mathfrak{f}_{m+1}(G) - \mathfrak{f}_m(G)) + (\mathfrak{f}_{n+1}(G) - \mathfrak{f}_n(G)) - 1$$
for all $m, n \geq 0$.

In other words, if $G$ is entire, then the $\mathfrak{f}$-sequence is almost concave, and if $G$ is strongly entire, then its first difference sequence is almost concave. The proof uses a little elementary dimension theory from algebraic geometry: here we do need the field to be algebraically closed. See [1].

It is also possible to show that a supergroup or a transitive extension of a (strongly) entire group is (strongly) entire.

Now we turn to some examples.

**Highly set-transitive groups** If $G = S$, or indeed if $G$ is highly set-transitive, then $A^G \cong \mathbb{C}[x]$, the polynomial ring in one variable (generated by the element $e$).

**Direct products** Let $G_i$ be oligomorphic on $\Omega_i$ for $i = 1,2$, and let the direct product $G_1 \times G_2$ have its intransitive action on $\Omega_1 \times \Omega_2$. Then

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

In particular, if $G = S^n$, the direct product of $n$ copies of $S$ (acting with $n$ orbits), then $A^G \cong \mathbb{C}[x_1, \ldots, x_n]$, the polynomial ring in $n$ homogeneous generators of degree 1.

**Wreath products** With $G_1$ and $G_2$ as above, we take the wreath product $G = G_1 \operatorname{Wr} G_2$ in its imprimitive action. In general we cannot determine the structure of $A^G$. However, if $G_1 = S$ and $G_2$ is a *finite* permutation group of degree $n$, then $A^G$ is isomorphic to the ring of invariants of the finite permutation group $G_2$ in the polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$. In particular, if $G = S \operatorname{Wr} S_n$, then $A^G$ is a polynomial ring in $n$ homogeneous generators of degrees $1, 2, \ldots, n$.

**Fraïssé classes** Suppose that the Fraïssé class $\mathscr{C}$ has a notion of "connectedness" satisfying a few simple properties. (The first of these properties is that every object in $\mathscr{C}$ should be uniquely expressible as a "sum" of connected ones.) Suppose that there are $a_n$ connected structures on $n$ vertices in $\mathscr{C}$ (up to isomorphism). Then it is possible to show that, if $G$ is the automorphism group of the Fraïssé limit of $\mathscr{C}$, then $A^G$ is a polynomial ring in $a_n$ homogeneous generators of degree $n$ for all $n$: the generators are indexed by the connected structures in $\mathscr{C}$.

In this situation, the sequence $(f_n(G))$ and the sequence $a_n$ determine each other. One compact way of describing the relationship is the identity

$$f_G(z) = \prod_{n \geq 1} (1 - z^i)^{-a_i}.$$

This result has a number of special cases.

- Let $G = H \operatorname{Wr} S$ for some oligomorphic group $H$. The Fraïssé class $\mathscr{C}(G)$ for $G$ consists of all disjoint unions of structures in the Fraïssé class $\mathscr{C}(H)$ for $H$; if we call a $\mathscr{C}(G)$-structure "connected" if it is a single $\mathscr{C}(H)$-structure, the axioms are satisfied. So $A^G$ is a polynomial algebra with $f_n(H)$ homogeneous generators of degree $n$ for all $n$, and is independent of the structure of $A^H$. The equation

$$f_{H \mathrm{Wr} S}(z) = \prod_{n \geq 0} (1 - z^n)^{-f_n(H)}$$

is a translation of the equation

$$f_{H \operatorname{Wr} S}(z) = \tilde{Z}(S; s_i \leftarrow f_H(z^i) - 1).$$

- The class of all finite graphs is a Fraïssé class; the Fraïssé limit is the *Rado graph*, or *countable random graph $R$*. Thus, if $G = \mathrm{Aut}(R)$, then $A^G$ is a polynomial algebra; the number of generators of degree $n$ is equal to the number of connected graphs on $n$ vertices.

- Consider the second example of the previous section, where $G$ is the automorphism group of $\mathbb{Q}$ partitioned into $r$ dense subsets, and the orbits on $n$-sets are indexed by words of length $n$ in an alphabet of $r$ symbols. In this case, $A^G$ is the *shuffle algebra*: the product of two words is equal to the sum of all words obtained by "shuffling" the factors together. So, for example,

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

  It can be shown that the *Lyndon words*, those which are lexicographically smaller than all their cyclic shifts, play the role of connected structures, so the shuffle algebra is polynomial (a result of Radford [7]).

I conclude with one puzzle. Let $G$ be the automorphism group of the random graph $R$. Then, as we saw, $A^G$ is a polynomial algebra, and hence an integral domain. Now there is a transitive extension of $G$, defined as follows.

A *two-graph $\mathscr{T}$* on a set $\Omega$ is a collection of 3-element subsets of $\Omega$ with the property that any 4-subset of $\Omega$ contains an even number of members of $\mathscr{T}$. Let $\Omega'$ be the vertex set of $R$, and $\Omega = \Omega' \cup \{\infty\}$, where $\infty$ is a new symbol. Let $\mathscr{T}$ be the set of 3-subsets of $\Omega$ which contain an odd number of edges of the graph consisting of $R$ with isolated vertex $\infty$. Then $G^* = \mathrm{Aut}(\mathscr{T})$ is a transitive extension of $G$. Since $A^G$ is an integral domain, so is $A^{G^*}$. *Is it a polynomial algebra?*

The two-graph $\mathscr{T}$ is homogeneous, so $f_n(G^*)$ is equal to the number of $n$-vertex two-graphs. Thus, if the algebra is polynomial, then the number $a_n$ of generators of degree $n$ satisfies

$$\sum_{n \geq 0} f_n(G^*) z^n = \prod_{n \geq 1} (1 - z^n)^{-a_n}.$$

Said otherwise, if there were a notion of connectedness for two-graphs with the required properties, then the required number of generators of degree $n$ would be equal to the number of connected objects on $n$ vertices, and we might hope to construct the generators from these objects. Unfortunately, there is no such notion.

However, Mallows and Sloane [5] showed that the number of two-graphs on $n$ points is equal to the number of *even graphs* (graphs with all vertices of even valency) on $n$ vertices. There is an obvious notion of connectedness for these, the connected objects being the *Eulerian graphs*. Is there a way of constructing generators from Eulerian graphs?

There is no natural bijection between two-graphs and even graphs: the relationship between these two classes is one of "duality" rather than "isomorphism". So the structure of $A^{G^*}$ is unknown, despite these tantalising hints!

# References

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

[2] P. Cameron, D. Gewurz and F. Merola, Product action, to appear.

[3] P. Cameron, T. Prellberg and D. Stark, Asymptotic enumeration of incidence matrices, to appear.

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

[5] 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.

[6] F. Merola, Orbits on $n$-tuples for infinite permutation groups, *Europ. J. Combinatorics* **22** (2001), 225–241.

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