Orbits on n-tuples

Peter J. Cameron

Queen Mary, University of London

`p.j.cameron@qmw.ac.uk`

Computation, Models and Groups
Cambridge, 11-12 January 2001

Introduction

Let G be a permutation group on a set Ω (usually infinite). Then G is *oligomorphic* if, for each natural number n, the number F_n of G-orbits on n-tuples of distinct elements of Ω is finite.

The main question is: what can be said about the growth of the sequence F_n?

This question may be easier than the corresponding question about the number of orbits of G on n-element subsets, but has been less studied. In terms of combinatorial enumeration, it corresponds to counting labelled, rather than unlabelled, structures.

Connection with model theory

A countable first-order structure is *countably categorical* if it is the unique countable model of its first-order theory.

Theorem M is countably categorical if and only if $\mathrm{Aut}(M)$ is oligomorphic.

If so, then the number of n-types of the theory of M is

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

where the coefficients $S(n,k)$ are the *Stirling numbers* of the second kind.

Moreover, every oligomorphic group of countable degree which is closed (in the topology of pointwise convergence) is the automorphism group of a countably categorical structure.

Generating function

Let $F(x)$ be the exponential generating function of (F_n), the formal power series

$$F(x) = \sum_{n=0}^{\infty} \frac{F_n x^n}{n!}.$$

In general this is only a formal power series, but of course we can ask: when does it converge in some neighbourhood of the origin?

Note that $F^*(x) = F(\mathrm{e}^x - 1)$, where $F^*(x)$ is the exponential generating function for the sequence (F_n^*), so one series converges if and only if the other does.

Finite groups

Suppose that Ω is finite. Boston *et al.* proved:

Theorem The probability generating function for the number of fixed points of a random element of G is $F(x-1)$.

(The p.g.f. is the polynomial $\sum p_i x^i$, where p_i is the proportion of elements in G having exactly i fixed points.)

In particular, the proportion of fixed-point-free elements in G is $F(-1)$.

For some oligomorphic groups, $F(-1)$ is defined (e.g. by analytic continuation), but it is not clear whether any meaning can be assigned to it.

Digression: linear groups

The result of Boston *et al.* can be written as

$$\frac{F_i}{i!} = \sum_{j=i}^{n} \binom{j}{i} p_j,$$

which can be inverted to give

$$p_i = \sum_{j=i}^{n} (-1)^{j-i} \binom{j}{i} \frac{F_j}{j!}.$$

There is an analogue for linear groups over $\mathrm{GF}(q)$. We replace $i!$ (the order of the symmetric group) by $|\mathrm{GL}(i,q)|$, and $\binom{j}{i}$ by the Gaussian coefficient $\begin{bmatrix} j \\ i \end{bmatrix}_q$; also, let L_i be the number of orbits of a linear group $G \leq \mathrm{GL}(n,q)$ on *linearly independent* i-tuples, and P_i the proportion of elements of G whose fixed point set is precisely an i-dimensional subspace. Then

$$\frac{L_i}{|\mathrm{GL}(i,q)|} = \sum_{j=i}^{n} \begin{bmatrix} j \\ i \end{bmatrix}_q P_j,$$

which can be inverted to give

$$P_i = \sum_{j=i}^{n} (-1)^{j-i} q^{(j-i)(j-i-1)/2} \begin{bmatrix} j \\ i \end{bmatrix}_q \frac{L_j}{|\mathrm{GL}(j,q)|}.$$

Digression: cycle index

The result of Boston *et al.* is in fact a special case of an older result, which considers cycles of arbitrary length instead of just fixed points.

The probability generating function for the numbers of cycles of all possible lengths is the classical *cycle index* of the permutation group, as developed by Redfield, Pólya, de Bruijn and others. It is a polynomial in indeterminates $s_1, s_2, \ldots$, where s_i records cycles of length i. If we set $s_i = 1$ for all $i > 1$, we obtain the p.g.f. for fixed points.

Now we have three (actual or potential) generalisations of the result: to oligomorphic groups; to linear groups; and to cycles of arbitrary length. The possibility of combining two (or all three) of these generalisations exists, but has not been fully realised.

Macpherson's Theorem

A permutation group is *primitive* if it preserves no non-trivial equivalence relation. (Note that in the countably categorical case, an invariant equivalence relation would be definable without parameters.) A permutation group is *highly transitive* if $F_n = 1$ for all n, so that $F(x) = \mathrm{e}^x$ converges everywhere.

Dugald Macpherson proved:

Theorem If G is oligomorphic and primitive but not highly transitive, then

$$F_n \geq \frac{n!}{p(n)}$$

for some polynomial p. In particular, $F(x)$ has radius of convergence at most 1.

For example, the group of order-preserving permutations of the rational numbers has $F_n = n!$ for all n, so that $F(x) = 1/(1-x)$, with radius of convergence 1.

Highly homogeneous groups

A permutation group is *highly homogeneous* if it permutes transitively the set of all n-element subsets of Ω, for all natural numbers n. I proved the following:

Theorem If G is highly homogeneous but not highly transitive, then there is a linear or circular order preserved or reversed by G.

We have $F_n = n!$, $n!/2$, $(n-1)!$, and $(n-1)!/2$ in the four cases (for large enough n).

Merola's Theorem

Francesca Merola recently strengthened Macpherson's Theorem as follows.

Theorem There is a constant $c > 1$ such that, if G is primitive but not highly homogeneous, then

$$F_n \geq \frac{c^n n!}{p(n)}$$

for some polynomial p. In particular, the radius of convergence of $F(x)$ is at most $1/c$.

Her proof gives $c = 1.174\ldots$, but it is conjectured that the result holds with $c = 2$ (this would be best possible).

Groups with slow growth

Thus for primitive groups other than the highly homogeneous ones, the slowest possible growth rate is an exponential times a polynomial.

Problem: What can be said about those groups for which $F(x)$ nas non-zero radius of convergence (that is, F_n grows no faster than $c^n n!$ for some c?

Empirically, the known examples come from either "circular" or "treelike" objects, or combinations of these.There appears to be a big overlap with the primitive *Jordan groups* classified by Adeleke, Macpherson and Neumann.

Examples

Example 1 Take a dense subset of the set of complex roots of unity containing one of x and $-x$ for all x. An arc joins x to y if $0 < \arg(y/x) < \pi$. We have $F_n = (2n-2)!!$.

Example 2 Take the amalgamation class of endvertex structures of boron trees (trees in which each vertex has valency 1 or 3). We have $F_n = (2n-5)!!$.

Example 3 Embed the trees of Example 2 in the plane. The leaves are then circularly ordered, and we may impose the structure of Example 1 on them.

Smoothness

The numbers F_n should grow not only rapidly but also smoothly in general. It is hard to formulate a general problem which is informative for all oligomorphic groups. For groups of small growth, we can ask the following question.

Problem: Is it true that $(F_n/n!)^{1/n}$ tends to a limit? Is it even true that F_n/nF_{n-1} tends to a limit? If so, what are the possible values of the limit?

Outline of the proof, I

Merola's proof follows the main steps of Macpherson's.

Let $\mathcal{E}(c)$ be the class of oligomorphic groups which satisfy

$$F_n \leq \frac{c^n n!}{p(n)}$$

for some polynomial p. Note that a transitive group belongs to $\mathcal{E}(c)$ if and only if the point stabiliser does.

We prove, by induction on k, that (for a suitable constant $c > 1$) a primitive but not highly homogeneous group in $\mathcal{E}(c)$ is k-transitive.

The induction step from k to $k+1$ is trivial if $k \geq 3$. If G is a primitive group in$\mathcal{E}(c)$, then G is k-transitive, so G_α is $(k-1)$-transitive (and hence primitive), hence G_α is k-transitive, hence G is $(k+1)$-transitive.

Outline of the proof, II

The other important ingredient is the following. If we can find $f(n)$ sets of size n in different G-orbits, such that the group of permutations induced on each set by its setwise stabiliser has order at most $g(n)$, then we have

$$F_n \geq \frac{f(n)n!}{g(n)}.$$

So the trick is to choose $f(n)$ and $g(n)$ so that $f(n)/g(n)$ grows exponentially. This requires some fine tuning!

The proof involves doing this for a variety of different combinatorial structures.

Beginning the induction

Case $k = 2$**:** If G is not 2-homogeneous, then it is a group of automorphisms of a graph. If G is 2-homogeneous but not 2-transitive, then it is a group of automorphisms of a tournament.

Case $k = 3$**:** If G is not 3-homogeneous, it is a group of automorphisms of one of a variety of combinatorial structures including Steiner systems, 2-trees, etc. If G is 3-homogeneous but not 2-primitive, it preserves a treelike structure. If G is 2-primitive then we can apply the arguments of the preceding case to G_α.

For each class of structures we have to choose c sufficiently small for the proof to work. The smallest value $c = 1.174\ldots$ occurs in the case of tournaments.