Oligomorphic permutation groups: growth rates and algebras

Peter J. Cameron

p.j.cameron@qmul.ac.uk

Gregynog Mathematics Colloquium 22 May 2007

The definition

Let $G$ be a permutation group on an infinite set $\Omega$. Then $G$ has a natural induced action on the set of all $n$-tuples of elements of $\Omega$, or on the set of $n$-tuples of distinct elements of $\Omega$, or on the set of $n$-element subsets of $\Omega$. It is easy to see that if there are only finitely many orbits on one of these sets, then the same is true for the others.

We say that $G$ is oligomorphic if it has only finitely many orbits on $\Omega^n$ for all natural numbers $n$.

We denote the number of orbits on all $n$-tuples, resp. $n$-tuples of distinct elements, $n$-sets, by $F_n^*(G)$, $F_n(G)$, $f_n(G)$ respectively.

Examples, 1

Let $S$ be the symmetric group on an infinite set $X$. Then $S$ is oligomorphic and

- $F_n(S) = f_n(S) = 1$,
- $F_n^*(S) = B(n)$, the $n$th Bell number (the number of partitions of a set of size $n$).

Let $A = \text{Aut}(Q, <)$, the group of order-preserving permutations of $Q$. Then $A$ is oligomorphic and

- $f_n(A) = 1$;
- $F_n(A) = n!$;
- $F_n^*(A)$ is the number of preorders of an $n$-set.

Examples, 2

Consider the group $S^r$ acting on the disjoint union of $r$ copies of $X$.

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

Consider $S^r$ acting on $\Omega^r$. Then $F_n^*(S^r) = B(n)^r$. From this we can find $F_n(S^r)$ by inversion:

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

for any oligomorphic group $G$, where $s(n,k)$ is the signed Stirling number of the second kind.

For $A^2$ acting on $Q^2$, $f_n(A^2)$ is the number of zero-one matrices (of unspecified size) with $n$ ones and no rows or columns of zeros.

Examples, 3

Let $G = S \text{ Wr } S$, the wreath product of two copies of $S$. Then $F_n(G) = B(n)$ and $f_n(G) = p(n)$, the number of partitions of $n$.

Let $G = S_2 \text{ Wr } A$, where $S_2$ is the symmetric group of degree 2. Then $f_n(G)$ is the $n$th Fibonacci number.
Examples, 4
There is a unique countable random graph $R$: that is, if we choose a countable graph at random (edges independent with probability $\frac{1}{2}$, then with probability 1 it is isomorphic to $R$.

- $R$ is universal, that is, it contains every finite or countable graph as an induced subgraph;
- $R$ is homogeneous, that is, any isomorphism between finite induced subgraphs of $R$ can be extended to an automorphism of $R$.

If $G = \text{Aut}(R)$, then $F_n(G)$ and $f_n(G)$ are the numbers of labelled and unlabelled graphs on $n$ vertices.

Connection with model theory, 1
If a set of sentences in a first-order language has an infinite model, then it has arbitrarily large infinite models. In other words, we cannot specify the cardinality of an infinite structure by first-order axioms.

Cantor proved that a countable dense total order without endpoints is isomorphic to $\mathbb{Q}$. Apart from countability, the conditions in this theorem are all first-order sentences.

What other structures can be specified by countability and first-order axioms? Such structures are called countably categorical.

Connection with model theory, 2
In 1959, the following result was proved independently by Engeler, Ryll-Nardzewski and Svenonius:

**Theorem 1.** A countable structure $M$ over a first-order language is countably categorical if and only if $\text{Aut}(M)$ is oligomorphic.

In fact, more is true: the types over the theory of $M$ are all realised in $M$, and the sets of $n$-tuples which realise the $n$-types are precisely the orbits of $\text{Aut}(M)$ on $M^n$.

Growth of $(f_n(G))$, 1
Several things are known about the behaviour of the sequence $(f_n(G))$:

- it is non-decreasing;
- either it grows like a polynomial (that is, $an^k \leq f_n(G) \leq bn^k$ for some $a, b > 0$ and $k \in \mathbb{N}$), or it grows faster than any polynomial;
- if $G$ is primitive (that is, it preserves no non-trivial equivalence relation on $\Omega$), then either $f_n(G) = 1$ for all $n$, or $f_n(G)$ grows at least exponentially;
- if $G$ is highly homogeneous (that is, if $f_n(G) = 1$ for all $n$), then either there is a linear or circular order on $\Omega$ preserved or reversed by $G$, or $G$ is highly transitive (that is, $F_n(G) = 1$ for all $n$).
- There is no upper bound on the growth rate of $(f_n(G))$.

Growth of $(f_n(G))$, 2
Examples suggest that much more is true. For any reasonable growth rate, appropriate limits should exist:

- for polynomial growth of degree $k$, $\lim (f_n(G)/n^k)$ should exist;
- for fractional exponential growth (like $\exp(n^{c})$), $\lim (\log \log f_n(G)/\log n)$ should exist;
- for exponential growth, $\lim (\log f_n(G)/n)$ should exist;

and so on.

I do not know how to prove any of these things; and I do not know how to formulate a general conjecture.

A Ramsey-type theorem

**Theorem 2.** Let $X$ be an infinite set, and suppose that the $n$-element subsets of $\Omega$ are coloured with $r$ different colours (all of which are used). Then there is an ordering $(c_1, \ldots, c_r)$ of the colours, and infinite subsets $Y_1, \ldots, Y_r$ of $X$, such that, for $i = 1, \ldots, r$, the set $Y_i$ contains an $n$-set of colour $c_i$ but none of colour $c_j$ for $j > i$. 

The existence of $Y_1$ is the classical theorem of Ramsey. There is a finite version of the theorem, and so there are corresponding ‘Ramsey numbers’. But very little is known about them!

**Monotonicity**

**Corollary 3.** The sequence $(f_n(G))$ is non-decreasing.

**Proof.** Let $r = f_n(G)$, and colour the $n$-subsets with $r$ colours according to the orbits. Then by the Theorem, there exists an $(n + 1)$-set containing a set of colour $c_i$ but none of colour $c_j$ for $j > i$. These $(n + 1)$-sets all lie in different orbits; so $f_{n+1}(G) \geq r$.

There is also an algebraic proof of this corollary. We’ll discuss this later.

**A graded algebra, 1**

Let $\binom{\Omega}{n}$ denote the set of $n$-subsets of $\Omega$, and $V_n$ the vector space of functions from $\binom{\Omega}{n}$ to $C$.

We make $\mathcal{A} = \bigoplus_{n \geq 0} V_n$ into an algebra by defining, for $f \in V_n$, $g \in V_m$, the product $fg \in V_{n+m}$ by

$$(fg)(K) = \sum_{M \in \binom{\Omega}{n+m}} f(M)g(K \setminus M)$$

for $K \in \binom{\Omega}{n+m}$, and extending linearly.

$\mathcal{A}$ is a commutative and associative graded algebra over $C$, sometimes referred to as the *reduced incidence algebra* of finite subsets of $\Omega$.

**A graded algebra, 2**

Now let $G$ be a permutation group on $\Omega$, and let $V_n^G$ denote the set of fixed points of $G$ in $V_n$. Put

$$\mathcal{A}[G] = \bigoplus_{n \geq 0} V_n^G,$$

a graded subalgebra of $\mathcal{A}$.

If $G$ is oligomorphic, then the dimension of $V_n^G$ is $f_n(G)$, and so the Hilbert series of the algebra $\mathcal{A}[G]$ is the ordinary generating function of the sequence $(f_n(G))$.

What properties does this algebra have?

Note that it is not usually finitely generated since the growth of $(f_n(G))$ is polynomial only in special cases.

**A non-zero-divisor**

Let $e$ be the constant function in $V_1$ with value 1. Of course, $e$ lies in $\mathcal{A}[G]$ for any permutation group $G$.

**Theorem 4.** The element $e$ is not a zero-divisor in $\mathcal{A}$.

This theorem gives another proof of the monotonicity of $(f_n(G))$. For multiplication by $e$ is a monomorphism from $V_n^G$ to $V_{n+1}^G$, and so $f_{n+1}(G) = \dim V_{n+1}^G \geq \dim V_n^G = f_n(G)$.

**An integral domain**

If $G$ has a finite orbit $\Delta$, then any function whose support is contained in $\Delta$ is nilpotent.

The converse, a long-standing conjecture, has recently been proved by Maurice Pouzet:

**Theorem 5.** If $G$ has no finite orbits on $\Omega$, then $\mathcal{A}[G]$ is an integral domain.

**Consequences**

Pouzet’s Theorem has a consequence for the growth rate:

**Theorem 6.** If $G$ is oligomorphic, then

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

**Proof.** Multiplication maps $V_m^G \otimes V_n^G$ into $V_{m+n}^G$; by Pouzet’s result, it is injective on the projective Segre variety, and a little dimension theory gets the result.
Brief sketch of the proof

Let \( F \) be a family of subsets of \( \Omega \). A subset \( T \) is \textit{transversal} to \( F \) if it intersects each member of \( F \). The \textit{transversality} of \( F \) is the minimum cardinality of a transversal.

A lemma due to Peter Neumann shows that, if \( G \) has no finite orbits on \( \Omega \), then any orbit of \( G \) on finite sets has infinite transversality.

Pouzet shows that, if \( f \in V_m \) and \( g \in V_n \) satisfy \( fg = 0 \), then the transversality of \( \text{supp}(f) \cup \text{supp}(g) \) is finite, and is bounded by a function of \( m \) and \( n \). (Here \( \text{supp}(f) \) denotes the support of \( f \).)

These two results clearly conflict with each other.

Comments

Here is Pouzet’s theorem again:

\textbf{Theorem 7.} If \( f \in V_m \) and \( g \in V_n \) satisfy \( fg = 0 \), then the transversality of \( \text{supp}(f) \cup \text{supp}(g) \) is finite, and is bounded by a function of \( m \) and \( n \).

The proof of this makes it clear that it is another kind of ‘Ramsey theorem’. If \( \tau(m,n) \) denotes the smallest \( t \) such that the transversality is at most \( t \), then we have the interesting problem of finding \( \tau(m,n) \). Pouzet shows that \( \tau(m,n) \geq (m+1)(n+1) - 1 \). On the other hand, the upper bounds coming from his proof are really astronomical!