Lists of exceptions

Peter J. Cameron

University of St Andrews

Computational Algbra
CAUL, Lisboa, July 2014

Lists

In his inaugural lecture as Professor of Poetry at Oxford, W. H. Auden gave 'four questions which, could I examine a critic, I would ask him'. He said, 'If a critic could truthfully answer "yes" to all four, then I should trust his judgment implicitly on all literary matters.' The first … was 'Do you like, and by like I really mean like, not approve of on principle, long lists of proper names such as the Old Testament genealogies or the Catalogue of Ships in the Iliad?'

Tiresias, *Notes from Overground*, 1984.

Lists of primitive groups

My talk is about lists, specifically lists of proper names of primitive permutation groups of small degree.
Several theorems say, "Except for the symmetric and alternating groups and a finite list, primitive groups have such-and-such a property". I will give a number of examples.
Computer algebra is often required to work out the lists explicitly.

Some definitions

Let G be a permutation group acting on a finite set Ω, with $|\Omega| = n > 1$, and t an integer with $0 < t < n$. We say that G is

- transitive if any point of Ω can be moved to any other by some element of G;
- t-transitive if G acts transitively on the set of t-tuples of distinct elements of Ω;
- t-homogeneous, or t-set transitive, if G acts transitively on the set of t-element subsets of Ω;
- primitive if G is transitive and the only equivalence relations on Ω preserved by G are the relation of equality and the relation with a single equivalence class.

In the definition of primitivity, we require G to be transitive simply to rule out the trivial group acting on a set of $n = 2$ points.

Two examples

Here are two examples of theorems of the type I am concerned with. For each exception I give the degree, the number of the group in the GAP list of primitive groups of that degree, and a proper name for the group.

Theorem

Let G be a 4-transitive group of degree n which is not the symmetric or alternating group of that degree. Then G is one of the following: $(11, 6, M_{11})$, $(12, 4, M_{12})$, $(23, 5, M_{23})$, $(24, 1, M_{24})$.

Theorem

For $4 \le t \le n/2$, *let G be a t-homogeneous but not t-transitive group of degree n. Then G is one of the following:* $(9, 8, \mathrm{PSL}(2, 8))$, $(9, 9, \mathrm{P\Gamma L}(2, 8))$, $(33, 2, \mathrm{P\Gamma L}(2, 32))$.

Commentary

Re Theorem 1: The Classification of Finite Simple Groups (CFSG), together with earlier work of a number of authors, gives us a complete list of the 2-transitive groups; this list can be found in various places. From the list we can read off that the only 4-transitive groups, apart from symmetric and alternating groups, are the four Mathieu groups listed. We have no proof, and no prospect of one, without using CFSG.

Re Theorem 2: Livingstone and Wagner proved in 1964 that, for $5 \leq t \leq n/2$, a t-homogeneous group is t-transitive. The analogous result for $t = 4$ is a theorem of Kantor from the early 1970s, proved before CFSG was announced. At about the same time Kantor also found all the t-homogeneous but not t-transitive groups for $t = 2$ and $t = 3$.

What does CFSG do for us?

From the Classification of Finite Simple Groups, we do not learn everything about finite permutation groups, but we do learn a great deal. For example,

- All the 2-transitive groups are known. A theorem of Burnside shows that such a group has a unique minimal normal subgroup, which is either elementary abelian or simple. In the second case, we apply CFSG (with a lot of extra work!); in the first, the group is the semidirect product of the additive group of a vector space by a subgroup of the multiplicative group which is transitive on non-zero vectors, and all such groups can be determined (they have at most one non-abelian composition factor).
- All the rank 3 permutation groups (those having just three orbits on pairs of distinct points) are known, by similar but harder arguments.

- Primitive groups are small (order at most $n^{1+\log_2 n}$), with some exceptions (including the Mathieu groups).
- Primitive groups are rare. The set of natural numbers for which there is a primitive group of degree n other than the symmetric and alternating groups has density zero; the number of numbers $n \leq x$ in this set is asymptotically $2x/\log x$.
- Primitive groups of small degree (up to 4095) are known; there are lists in GAP up to degree 2499 (the rest may appear sometime).

Outline

I will now discuss two areas in which theorems of this type have been proved:

- subsets with small or trivial stabilisers;
- theory of transformation semigroups.

Subsets with small stabilisers

The first topic goes back to a theorem I proved with Peter Neumann and Jan Saxl in 1984:

Theorem

With the exception of the symmetric and alternating groups and a finite list, if G is a primitive permutation group on Ω, then there is a subset of Ω whose setwise stabiliser in G is trivial; that is, G has a regular orbit on the power set of Ω.

The list of exceptions was computed by Ákos Seress in 1997, and is on the next slide. Note that the GAP numbering has changed since then!

There is an asymptotic form of this theorem: If G is primitive but not symmetric or alternating, then the proportion of G-orbits on the power set which are regular tends to 1 as $n \to \infty$.

Seress' list

Theorem

A primitive permutation group of degree n, not S_n or A_n, has a regular orbit on the power set unless it is one of the following:
$(5, 2, D_{10})$, $(5, 3, \mathrm{AGL}(1, 5))$, $(6, 1, \mathrm{PSL}(2, 5))$, $(6, 2, \mathrm{PGL}(2, 5))$, $(7, 4, \mathrm{AGL}(1, 7))$, $(7, 5, \mathrm{PSL}(3, 2))$, $(8, 2, \mathrm{A\Gamma L}(1, 8))$, $(8, 4, \mathrm{PSL}(2, 7))$, $(8, 5, \mathrm{PGL}(2, 7))$, $(8, 3, \mathrm{AGL}(3, 2))$, $(9, 2, 3^2 : D_8)$, $(9, 5, \mathrm{A\Gamma L}(1, 9))$, $(9, 6, \mathrm{ASL}(2, 3))$, $(9, 7, \mathrm{AGL}(2, 3))$, $(9, 8, \mathrm{PSL}(2, 8))$, $(9, 9, \mathrm{P\Gamma L}(2, 8))$, $(10, 2, S_5)$, $(10, 3, \mathrm{PSL}(2, 9))$, $(10, 5, \mathrm{P\Sigma L}(2, 9))$, $(10, 4, \mathrm{PGL}(2, 9))$, $(10, 6, M_{10})$, $(10, 7, \mathrm{P\Gamma L}(2, 9))$, $(11, 1, \mathrm{PSL}(2, 11))$, $(11, 2, M_{11})$, $(12, 4, \mathrm{PGL}(2, 11))$, $(12, 1, M_{11})$, $(12, 2, M_{12})$, $(13, 7, \mathrm{PSL}(3, 3))$, $(14, 2, \mathrm{PGL}(2, 13))$, $(15, 4, \mathrm{PSL}(4, 2))$, $(16, 12, \mathrm{A\Gamma L}(2, 4))$, $(16, 17, 2^4 : A_6)$, $(16, 16, 2^4 : S_6)$, $(16, 20, 2^4 : A_7)$, $(16, 11, \mathrm{AGL}(4, 2))$, $(17, 7, \mathrm{PSL}(2, 16) : 2)$, $(17, 8, \mathrm{P\Gamma L}(2, 16))$, $(21, 7, \mathrm{P\Gamma L}(3, 4))$, $(22, 1, M_{22})$, $(22, 2, M_{22} : 2)$, $(23, 5, M_{23})$, $(24, 1, M_{24})$, $(32, 3, \mathrm{AGL}(5, 2))$.

Ákos Seress, 1958–2013

One of the heroes of computational permutation group theory

First variation: automorphism groups of hypergraphs

A (uniform) hypergraph is a "graph" in which edges contain k vertices, for some $k \geq 2$.

Frucht showed that every group is the automorphism group of a graph. But not every permutation group is the automorphism group of a graph acting on the vertices (for example, 2-transitive groups cannot be). László Babai and I gave a replacement for this missing result.

Automorphism groups of hypergraphs

Theorem

Apart from the alternating groups and finitely many others, every primitive group is the full automorphism group (acting on vertices) of a hypergraph.

Babai and I showed further that

- we can assume that the hypergraph is edge-transitive;
- asymptotically we can take the cardinality of edges in the hypergraph to be $n^{1/2+o(1)}$ – this is essentially best possible.

Spiga's list

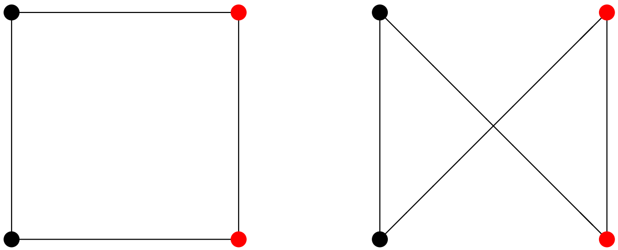
The finite list of exceptions in the preceding theorem was computed by Pablo Spiga (not yet published)

Theorem

If G is a primitive group which is not an alternating group and is not the automorphism group of a hypegraph, then G is one of the following: $(5, 1, C_5)$, $(5, 3, \mathrm{AGL}(1, 5))$, $(6, 2, \mathrm{PGL}(2, 5))$, $(7, 1, C_7)$, $(7, 3, C_7 : C_3)$, $(8, 1, \mathrm{AGL}(1, 8))$, $(8, 2, \mathrm{A\Gamma L}(1, 8))$, $(8, 4, \mathrm{PSL}(2, 7))$, $(9, 1, C_3^2 : C_4)$, $(9, 4, \mathrm{AGL}(1, 9))$, $(9, 3, M_9)$, $(9, 6, \mathrm{ASL}(2, 3))$, $(9, 8, \mathrm{PSL}(2, 8)$, $(9, 9, \mathrm{P\Gamma L}(2, 8))$, $(10, 3, \mathrm{PSL}(2, 9))$, $(10, 4, \mathrm{PGL}(2, 9))$.

Second variation: switching classes

The operation of switching with respect to a set of vertices interchanges edges and non-edges between the set and its complement, while leaving edges within the set or within its complement unchanged. This gives an equivalence relation on the class of all graphs on a given vertex set, whose equivalence classes are called switching classes.



History and connections

The operation of switching was introduced by Jaap Seidel in the 1960s, in connection with metric problems in elliptic geometry (specifically, the congruence order of the elliptic plane).
It has connections with systems of equiangular lines in Euclidean geometry, doubly transitive groups (similar ideas were used by Graham Higman to give a combinatorial construction of Conway's group Co_3), combinatorial geometry, and cohomology of groups.
Seidel wrote several surveys on this topic which are highly recommended.

The Seidel tree in Eindhoven

A representation theorem

The automorphism group of a switching class of graphs contains the automorphism group of every graph in the class as a subgroup.
Here is a Frucht-type theorem which is a converse to the preceding remark.

Theorem

Given any finite group G, there is a switching class $\mathcal{S}$ of graphs with the properties

- $\mathrm{Aut}(\mathcal{S}) = G$;
- *for each subgroup $H \leq G$, there is a graph $\Gamma \in \mathcal{S}$ with* $\mathrm{Aut}(\Gamma) = H$.

Primitivity and rigidity

Here is the theorem relevant to the subject of this talk. Pablo Spiga and I completed the proof a week or so ago. The paper should appear on the arXiv this week.

Theorem

Let $\mathcal{S}$ be a switching class of graphs on n vertices, whose automorphism group G is primitive. Then, if G is not the symmetric group or one of a finite number of exceptions, there is a graph $\Gamma \in \mathcal{S}$ such that $\mathrm{Aut}(\Gamma)$ is the trivial group. The list of exceptions is: $(5, 2, D_{10})$, $(6, 1, \mathrm{PSL}(2, 5))$, $(9, 2, 3^2 : D_8)$, $(10, 5, \mathrm{P\Sigma L}(2, 9))$, $(14, 1, \mathrm{PSL}(2, 13))$, *and* $(16, 16, 2^4 : S_6)$.

João Araújo

João was the person who seduced me into working on the connections between permutation groups and transformation semigroups. He had a hand in most of the results to follow.

Second theme: transformation semigroups

Recently, results about finite permutation groups (often depending on CFSG) have been used to study transformation semigroups.

A transformation semigroup S on Ω may or may not contain any permutations of Ω: if it does, then they form a permutation group, which is the group of units of the semigroup.

However, even if there are no permutations in S, we have a group to hand, namely the normaliser of S in the symmetric group, the group

$$N(S) = \{g \in \mathrm{Sym}(\Omega) : g^{-1}Sg = S\}.$$

We will see that this group has a big influence on S.

Levi–McFadden and McAlister

The following is the prototype for results of this kind. Let S_n and T_n denote the symmetric group and full transformation semigroup on $\{1, 2, \ldots, n\}$.

Theorem

Let $f \in T_n \setminus S_n$, and let S be the semigroup generated by the conjugates $g^{-1}fg$ for $g \in S_n$. Then

- *S is idempotent-generated;*
- *S is regular;*
- *$S = \langle S_n, f \rangle \setminus S_n$.*

In other words, semigroups of this form, with normaliser S_n, have *very nice* properties!

The general problem

Problem

- *Given a semigroup property P, for which pairs* (G, f)*, with* $f \in T_n \setminus S_n$ *and* $G \leq S_n$*, does the semigroup* $\langle g^{-1}fg : g \in G \rangle$ *have property P?*
- *Given a semigroup property P, for which pairs* (G, f) *as above does the semigroup* $\langle G, f \rangle \setminus G$ *have property P?*
- *For which pairs* (G, f) *are the semigroups of the preceding parts equal?*

Further results

The following portmanteau theorem lists some previously known results.

Theorem

- *(Levi) For any* $f \in T_n \setminus S_n$*, the semigroups* $\langle g^{-1}fg : g \in S_n \rangle$ *and* $\langle g^{-1}fg : g \in A_n \rangle$ *are equal.*
- *(Araújo, Mitchell, Schneider)* $\langle g^{-1}fg : g \in G \rangle$ *is idempotent-generated for all* $f \in T_n \setminus S_n$ *if and only if* $G = S_n$ *or* $G = A_n$ *or* G *is one of three specific groups.*
- *(Araújo, Mitchell, Schneider)* $\langle g^{-1}fg : g \in G \rangle$ *is regular for all* $f \in T_n \setminus S_n$ *if and only if* $G = S_n$ *or* $G = A_n$ *or* G *is one of nine specific groups.*

The lists

Here are the lists of Araújo, Mitchell and Schneider.

Theorem

- *The three groups other than* S_n *and* A_n *for which* $\langle G, f\rangle$ *is idempotent-generated for all non-permutations* f *are* $(5, 3, \mathrm{AGL}(1, 5))$, $(6, 1, \mathrm{PSL}(2, 5))$ *and* $(6, 2, \mathrm{PGL}(2, 5))$.
- *The nine groups other than* S_n *and* A_n *for which* $\langle G, f\rangle$ *is regular for all non-permutations* f *are* $(5, 1, C_5)$, $(5, 2, D_{10})$, $(5, 3, \mathrm{AGL}(1, 5))$, $(6, 1, \mathrm{PSL}(2, 5))$, $(6, 2, \mathrm{PGL}(2, 5))$, $(7, 4, \mathrm{AGL}(1, 7))$, $(8, 5, \mathrm{PGL}(2, 7))$, $(9, 8, \mathrm{PSL}(2, 8))$ *and* $(9, 9, \mathrm{P\Gamma L}(2, 8))$.

Some equivalent properties

Theorem (Araújo, Cameron)

Given k with $1 \leq k \leq n/2$, the following are equivalent for a subgroup G of S_n:

- *for all rank k transformations f, f is regular in $\langle G, f \rangle$;*
- *for all rank k transformations f, $\langle f, G \rangle$ is regular;*
- *for all rank k transformations f, f is regular in $\langle g^{-1}ag : g \in G \rangle$;*
- *for all rank k transformations f, $\langle g^{-1}fg : g \in G \rangle$ is regular.*

Moreover, we have a complete list of the possible groups G with these properties for $k \geq 5$, and partial results for smaller values.

The four equivalent properties above translate into a property of G which we call the k-universal transversal property, which is a variant of k-homogeneity.

Our second theorem

Theorem (André, Araújo, Cameron)

We have a complete list (in terms of the rank and kernel type of f) for pairs (G,f) for which $\langle G,f\rangle \setminus G = \langle S_n,f\rangle \setminus S_n$.

As we saw, these semigroups have very nice properties.

Partition homogeneity and transitivity

For a partition λ, we say a permutation group G is λ-homogeneous if it is transitive on partitions of shape λ, and λ-transitive if it is transitive on ordered partitions of shape λ.

We have a complete classification of the groups which are λ-homogeneous but not λ-transitive, except when $\lambda = (1, 1, \ldots, 1)$ (in this case, every permutation group is λ-homogeneous but only the symmetric group is λ-transitive).

Moreover, we have a description of λ-transitive groups: the largest part λ_1 of λ must be greater than $n/2$, and G must be t-homogeneous, where $t = n - \lambda_1$. All such groups can be listed.

Using these results, we classify all pairs (G, f) such that $\langle G, f\rangle \setminus G = \langle S_n, f\rangle \setminus S_n$.

Our third theorem

Theorem (Araújo, Cameron, Mitchell, Neunhöffer)

The semigroups $\langle G, f\rangle \setminus G$ and $\langle g^{-1}fg : g \in G\rangle$ are equal for all $f \in T_n \setminus S_n$ if and only if $G = S_n$, or $G = A_n$, or G is the trivial group, or G is one of five specific groups, namely $(5, 3, \mathrm{AGL}(2, 5))$, $(6, 1, \mathrm{PSL}(2, 5))$, $(5, 2, \mathrm{PGL}(2, 5))$, $(9, 8, \mathrm{PSL}(2, 8))$ and $(9, 9, \mathrm{P\Gamma L}(2, 8))$.

Problem

It would be good to have a more refined version of this where the hypothesis refers only to all maps of rank k, or just a single map f.

A taste of the proofs

Here is a sample theorem, stated a little imprecisely.

Theorem

Let G be a transitive permutation group of degree n, satisfying $\log|G| = o(n^{1/2})$. Then the number of orbits of G on the power set is close to $2^n/|G|$, and almost all these orbits are regular.

Now, using CFSG, it is known that primitive groups satisfy the hypothesis, with the exception of S_n and A_n, S_m and A_m acting on 2-sets (with $n = m(m-1)/2$) and subgroups of $S_m \wr S_2$ containing A_m^2 (with $n = m^2$.) Clearly S_n and A_n are genuine exceptions, and the other groups here can be handled directly. For example, for S_n on 2-sets, the orbits are isomorphism classes of graphs, and almost all graphs have trivial automorphism group.

Suppose that o is the number of G-orbits on $\mathcal{P}(\{1,\ldots,n\})$, and o^* the number of these which are not regular. Let $o(G) = 2^n/|G|(1+\epsilon_1)$ and $o^* = \epsilon_2 o$. Since a non-regular orbit has size at most $|G|/2$, a short calculation gives $(1+\epsilon_1)(1-\epsilon_2/2) \geq 1$, so it suffices to show that ϵ_1 is small.
Let the minimal degree of G (the smallest number of points moved by a non-trivial element) be μ and the base size (the smallest number of points whose stabiliser is trivial) be b. Then $b\mu \geq n$, and $|G| \geq 2^b$; so $o \leq 2^n/|G| + 2^{n-\mu/2}$.
From this it follws that, if $\log_2 |G| = \delta n^{1/2}$, then

$$\epsilon_1 \leq 2^{n^{1/2}(\delta - 1/(2\delta))},$$

so if $\delta \leq c$ for some $c < 1/\sqrt{2}$, then $\epsilon_1 = o(1)$ as $n \to \infty$.

Computer systems such as GAP include lists of all primitive permutation groups with degrees into the thousands. So as long as we have a bound on n which is not too large, it is possible in principle to check all primitive groups with degree up to this bound. This is in essence what Seress and Spiga did. Sometimes the checks might be rather slow. For example, how do we test whether a primitive group G preserves a switching class with the property that no graph in that class has trivial automorphism group?

Fortunately the asymptotic results suggest that most graphs in such a switching class will have trivial group, so we just sample until we find one that does.