Numerical and graphical invariants of permutation groups

Peter J. Cameron
University of St Andrews

Asymptotic Group Theory
Budapest, August 2015

Happy birthday!

We are here to celebrate an important equation:

$$\mathrm{Age}(\mathrm{P}^3) = |A_5|$$

It is a great pleasure to celebrate the birthday of my friend Péter Pál Pálfy in Budapest, in a meeting on asymptotic group theory.

- On my first visit to Budapest, I lectured about infinite permutation groups.
- In a restaurant just round the corner, Laci Babai and I planned a conference on “Group Theory: Finite to Infinite”.
- My paper with Laci and P^3 was about finite groups, but has been of some importance in the study of locally finite groups.

However, today I will stick to finite groups.
The most recent material is joint work with Colva Roney-Dougal; I am grateful to her for comments on the whole thing [but remaining mistakes are mine!].

Overview

I will begin with a brief survey of three graphs associated with finite groups: the commuting graph, the power graph, and the generating graph.

The third of these has the drawback that it is non-trivial only for 2-generated groups (though of course this class includes the finite simple groups). One of the big open questions suggests a more general approach.

I will introduce a chain of equivalence relations on a finite group. The point at which this chain stabilises is related to various other group parameters such as the maximal generator number of a maximal subgroup and the maximum size of a minimal generating set of G.

I will then discuss several further parameters related to these, defined in terms of the subgroup lattice or permutation bases.

The commuting graph

The vertices of the commuting graph of a group G are the elements of G, two vertices joined if they commute.

Since any two vertices are joined by a path of length 2 through a central element, it is customary to remove the centre of G.

The commuting graph was defined by Gruenberg and Kegel in an unpublished manuscript in 1975, along with the related prime graph (whose vertices are the prime divisors of $|G|$, two primes p and q joined if G contains an element of order pq.) It is relevant to the study of the module structure of the augmentation ideal of kG.

Morgan and Parker showed that, if the centre of G is trivial, then any connected component of the commuting graph of G has diameter at most 10.

However, Giudici and Parker found examples of groups (of 2-power order) whose commuting graph has arbitrarily large diameter.

The power graph

The power graph $P(G)$ of a group G has as vertices the elements of G, with an edge from x to y if one is a power of the other. There is a natural directed version $\vec{P}(G)$, where we put a directed arc from x to y if x is a power of y.

Neither graph determines G. For example, if G has exponent 3, then $P(G)$ is the friendship graph consisting of a number of triangles with a common vertex.

However, one surprising fact is that, if G and H are groups such that $P(G)$ and $P(H)$ are isomorphic, then $\vec{P}(G)$ and $\vec{P}(H)$ are isomorphic (though not every isomorphism between undirected power graphs is an isomorphism between directed power graphs).

If y is a power of x, then x and y commute; so (apart from the question of whether the centre is included) the power graph is a spanning subgraph of the commuting graph.

Generation

I now turn to graphs and parameters related to generating sets for G.

Bear in mind the following example. Let G be a finite p-group. By the Burnside basis theorem, a set of elements generates G if and only if the images generate $G/\Phi(G)$ (where $\Phi(G)$ is the Frattini subgroup of G).

Now $G/\Phi(G)$ is elementary abelian, and so a vector space over a prime field. So generating sets correspond to bases in the vector space: any two have the same cardinality, and any independent set is contained in a generating set.

Of course, things are not so simple in arbitrary groups!

The generating graph

The generating graph $\Gamma(G)$ of G is the graph whose vertices are the elements of G, with two vertices x and y adjacent if $\langle x, y \rangle = G$.

Note that this graph is a null graph if G is not 2-generated.

Also, the Frattini subgroup $\Phi(G)$ consists of the elements of G which can be dropped from any generating set. So, if G is not cyclic, then the vertices in the Frattini subgroup are isolated, and we may delete them.

If G is 2-generated and not abelian, then pairs of elements which generate G do not commute, so the generating graph is a spanning subgraph of the complement of the commuting graph.

The spread conjecture

Breuer, Guralnick and Kantor showed that, in a finite simple group, every non-identity element belongs to a 2-element generating set; in other words, after removing the identity, the generating graph has no isolated vertices. They conjectured that a group has this property if and only if all its nontrivial quotients are cyclic.

This was proved for S_n (for $n > 4$) by Sophie Piccard in 1939.

More generally, the spread of a graph is the largest number s such that any s vertices have a common neighbour. The spread of a group is the spread of its generating graph. Thus G has spread $\neq 0$ if and only if 1 is the only isolated vertex in $\Gamma(G)$.

There has been a lot of research by Burness, Crestani, Guest and others on the following conjecture:

Conjecture

There is no finite almost simple group which has spread precisely 1*; that is, such a group with non-zero spread has spread at least* 2.

Reduction, 1

My work with Colva Roney-Dougal reported here began with the observation that the generating graph of a finite simple group has huge automorphism group. For example, the generating graph of A_5 has automorphism group of order $2^{31}.3^7.5 = 23482733690880$.
There is a simple reason for this. If two elements of order 3 or 5 generate the same cyclic subgroup, then they have the same neighbours in $\Gamma(G)$, and can be permuted arbitrarily. So, if we define a relation $\equiv_g$ on G by the rule that $x \equiv_g y$ if x and y have the same neighbours, then $\Gamma(A_5)$ has 6 equivalence classes of size 4, 10 of size 2, and 16 singletons. The normal subgroup fixing all equivalence classes has order $(4!)^6.(2!)^{10}$, and the quotient is isomorphic to S_5.

Reduction, 2

There is a natural way to define an induced subgraph on the set of equivalence classes of $\equiv_g$: two classes are joined if some (equivalently, any) pair of vertices one in each class are joined. The letter g stands for "graph" or "generating".
This quotient operation preserves many graph-theoretic properties, for example,

- clique number;
- chromatic number;
- total domination number;
- spread.

Also, the automorphism of the quotient graph $\Gamma(G)/\equiv_g$ is much more closely related to the group G. For example, for $G = A_5$, this group is $\mathrm{Aut}(A_5) = S_5$.

Automorphism groups

Let $\overline{\Gamma}(G)$ denote the reduced graph $\Gamma(G)/\equiv_g$. We regard this as a vertex-weighted graph, where the weight of a vertex is the size of the corresponding equivalence class. Let $\mathrm{Aut}_w(\overline{\Gamma}(G))$ denote the group of automorphisms of this graph preserving the weights.

The automorphism group of G acts on $\overline{\Gamma}(G)$; let $\mathrm{Aut}^*(G)$ be the induced group on this graph.

Theorem

$$\mathrm{Aut}^*(G) \leq \mathrm{Aut}_w(\overline{\Gamma}(G)) \leq \mathrm{Aut}(\overline{\Gamma}(G)).$$

The right-hand inequality can be strict. If $G = \mathrm{PSL}(2,16)$ then there is an automorphism of $\overline{\Gamma}(G)$ which interchanges classes corresponding to elements of orders 3 and 5: the full automorphism group is $C_2 \times \mathrm{PSL}(2,16)$. However, these vertices have different weights.

Reduction, 3

Here is another equivalence relation defined on a group G which does not depend on G being 2-generated. We write $x \equiv_m y$ if, for any finite set Z of elements of G,

$$\langle x, Z \rangle = G \Leftrightarrow \langle y, Z \rangle = G.$$

It is not hard to show that $x \equiv_m y$ if x and y lie in the same maximal subgroups of G. (So m in the notation could stand for "maximal subgroups".)
Clearly $x \equiv_m y$ implies $x \equiv_g y$, since $x \equiv_g y$ means that the condition holds for all singleton sets Z.

Groups of non-zero spread

Lucchini and Maróti have shown that groups of non-zero spread fall into one of the following types:

- cyclic groups;
- $C_p \times C_p$, for p prime;
- G is the semi-direct product of an elementary abelian group with an irreducible subgroup of its Singer cycle;
- G has a normal subgroup T^r, where T is non-abelian simple; the quotient has order rm, where m divides $|\mathrm{Out}(T)|$, and permutes the factors cyclically.

Theorem

Let G be a soluble group of non-zero spread. Then

- $\equiv_m$ *and* $\equiv_g$ *coincide on G;*
- *all cases in which* $\mathrm{Aut}^*(G) = \mathrm{Aut}_w(\overline{\Gamma}(G))$ *are known.*

A chain of equivalence relations

The equivalence $\equiv_g$ can be generalised as follows.
Let r be a positive integer. We define an equivalence relation $\equiv_m^{(r)}$ on G by the rule that $x \equiv_m^{(r)} y$ if

$$(\forall z_1, \ldots, z_{r-1} \in G)((\langle x, z_1, \ldots, z_{r-1} \rangle = G) \Leftrightarrow (\langle y, z_1, \ldots, z_{r-1} \rangle = G)).$$

Here m stands for "maximal subgroups", as we will see later.
Note that $\equiv_m^{(2)}$ coincides with $\equiv_g$ defined earlier.
The relations get finer as r increases: so we define $\equiv_m$ to be the limiting value for large r, and $\psi(G)$ to be the smallest value of r for which $\equiv_m^{(r)}$ coincides with $\equiv_m$.

An example

Example

Let G be the symmetric group S_4. Then

- $\equiv_m^{(1)}$ is the universal relation with a single class, as G is not 1-generated.
- G is 2-generated, but double transpositions lie in no 2-element generating set, so they are all equivalent to the identity in $\equiv_2$, which has 14 classes.
- For $r \geq 3$, the double transpositions are all equivalent; two other non-identity elements are $\equiv_m^{(r)}$-equivalent if and only if each is a power of the other; there are 15 classes. So $\psi(S_4) = 3$.

A conjecture and a problem

Conjecture

There are numbers a and b such that $\equiv_m^{(r)}$ *is*

- *constant (with a single class) for* $r \leq a$*;*
- *strictly decreasing in the refinement order for* $a \leq r \leq b$*;*
- *constant for* $r \geq b$*.*

If true, then we would have $a = d(G)$ and $b = \psi(G)$.
We further conjecture that, if G is simple (or almost simple and 2-generated) then $a = b = 2$. This has been checked up to order around 10^4.
An enumeration problem: how many $\equiv_m$ classes in the symmetric group S_n? The series begins

$$1, 2, 5, 15, 67, 362, 1479, \ldots$$

An asymptotic result

Theorem

Let G be S_n or A_n. Then for almost all elements $x, y \in G$ (all but a proportion tending to 0 as $n \to \infty$), the following are equivalent:

- $x \equiv_m y$;
- $x \equiv_g y$;
- *the cycles of x and y induce the same partition of $\{1, \ldots, n\}$.*

The proof depends on the theorem of Łuczak and Pyber, which states that for almost all $x \in S_n$, the only transitive subgroups of S_n containing x are S_n and (possibly) A_n. The equivalence holds for all such elements.

Some group parameters

Recall that $d(G)$ denotes the minimum number of elements which generate G.
Let $m(G)$ be the maximum of $d(M)$ over all maximal subgroups M of G. This parameter has been studied by Burness, Liebeck and Shalev, who showed, among other things, that $m(G) \leq 4$ for any finite simple group G.
Also, let $\mu(G)$ be the maximum size of an independent generating set for G (a generating set of which no proper subset is generating). This parameter arose in work of Diaconis and Saloff-Coste on the rate of convergence of the product-replacement algorithm, and was studied by Whiston (who showed that $\mu(S_n) = n - 1$) and others.

Bounds for $\psi(G)$

The equivalence relation $\equiv_m^{(r)}$ on G is the universal relation (any two elements are related) if $r < d(G)$, since no r-tuples generate G. This is false for $r = d(G)$; indeed, for this value, there are at least $d(G) + 1$ equivalence classes (since, if $G = \langle x_1, \ldots, x_r \rangle$, then the identity, $x_1, \ldots, x_r$ are pairwise inequivalent. Thus $\psi(G) \geq d(G)$. The next result gives some upper bounds.

Theorem

$$d(G) \leq \psi(G) \leq \min\{\mu(G), m(G) + 1\}.$$

Theorem

Let G be a group of prime power order. Then

$$d(G) = \psi(G) = \mu(G),$$

and the $\equiv_m$-classes are the cosets of the Frattini subgroup $\Phi(G)$.

Proof that $\psi(G) \le \mu(G)$

We have to show that, if $\mu = \mu(G)$, and $x \equiv_m^{(\mu)} y$, then $x \equiv_m y$.
So suppose that we have $x \equiv_m^{(\mu)} y$, and let $G = \langle x, z_1, \ldots, z_{r-1} \rangle$.
Suppose that $r \le \mu$. Since the relations $\equiv_m^{(r)}$ get finer as r increases, we have $G = \langle y, z_1, \ldots, z_{r-1} \rangle$.
So suppose that $r > \mu$. In this case, our generating set is larger than μ, and so some element is redundant.
If x is redundant, then $G = \langle z_1, \ldots, z_{r-1} \rangle = \langle y, z_1, \ldots, z_{r-1} \rangle$, as required.
Suppose that x is not redundant. Then G is generated by a subset of the given generators of size μ including x, without loss of generality $\{x, z_1, \ldots, z_{\mu-1}\}$. Since, by assumption, $x \equiv_m^{(\mu)} y$, we have $G = \langle y, z_1, \ldots, z_{\mu-1} \rangle = \langle y, z_1, \ldots, z_{r-1} \rangle$.

Combinatorics of generating sets

If you know about matroids, you will recognise that, in a p-group, the minimal generating sets are the bases of a matroid, which is just a projective space over $\mathrm{GF}(p)$ “blown up” with loops and parallel elements.

Is there any analogue for arbitrary groups?

One possible setting is provided by the recent work of Rhodes and Silva on Boolean representations of simplicial complexes.

The Boolean representable complexes are more general than matroids but not as general as arbitrary simplicial complexes.

Details have not yet been worked out.

A note on group parameters

A (finite) group parameter is simply a real-valued function on the class of finite groups, which is isomorphism-invariant.
If p denotes any group parameter, then we define the parameter p' as follows:

$$p'(G) = \max_{H \leq G} p(H).$$

So, for example, if $d(G)$ is the minimum number of generators of G, then $d'(G)$ is the smallest number for which every subgroup of G can be generated by d' elements.
Note that p' is monotonic ($H \leq G$ implies $p'(H) \leq p'(G)$). In particular, if p is monotonic, then $p = p'$.

Some further parameters

In the remainder of the talk I will consider the parameters $d(G)$ (minimum number of generators) and μ (maximum size of an independent generating set), together with their "derived" parameters d' and μ', and also the parameter $l(G)$, the length of the longest chain of subgroups of G. (The last parameter is monotonic, so $l'(G) = l(G)$.)
All these parameters are known for symmetric groups:

Theorem

- $l(S_n) = \left\lceil \frac{3n}{2} \right\rceil - b(n) - 1$, *where* $b(n)$ *is the number of ones in the base* 2 *representation of* n.
- $\mu(S_n) = \mu'(S_n) = n - 1$.
- $d(S_n) = 2$, $d'(S_n) = \left\lfloor \frac{n}{2} \right\rfloor$ *for* $n > 3$.

The non-trivial parts are due to Cameron, Solomon and Turull; Whiston; and McIver and Neumann.

Base measures

A base for a permutation group G on a set Ω is a sequence of points of Ω whose pointwise stabiliser in G is trivial. It is irredundant if no point is fixed by the stabiliser of its predecessors; and minimal if no point is fixed by the stabiliser of all the other points.

Now let $b_1(G), b_2(G), b_3(G)$ be the maximum, over all permutation actions of G (not necessarily transitive or faithful!), of

- the maximum size of an irredundant base (for $b_1(G)$);
- the maximum size of a minimal base (for $b_2(G)$);
- the minimum base size (for $b_3(G)$).

Some results

Theorem

- $b_3(G) \leq b_2(G) \leq b_1(G)$.
- $b_1(G) = l(G)$.
- *If G is a non-abelian simple group, then to calculate $b_3(G)$ it is only necessary to consider primitive actions of G.*

An example of a group in which the inequalities in the first part are all strict is $G = \mathrm{PSL}(2,7)$; we have $b_1(G) = 5$, $b_2(G) = 4$, $b_3(G) = 3$.

Boolean semilattices

An join-semilattice of a lattice Λ is a subset of Λ which is closed under join and contains the bottom element (the join of the empty set), while a meet-semilattice is a subset closed under meet and containing the top element (the meet of the empty set).
Let $B(n)$ denote the Boolean lattice of all subgroups of an n-set. For any group G, let $\Lambda(G)$ denote the lattice of subsets of G.

Theorem

The following are equivalent for the group G:

- *$B(n)$ is embeddable as a join-semilattice in $\Lambda(G)$;*
- *$B(n)$ is embeddable as a meet-semilattice in $\Lambda(G)$.*

The quaternion group Q_8 shows that these conditions are not equivalent to embeddability of $B(n)$ as a lattice in $\Lambda(G)$.

A connection

Theorem

- *The largest n such that $B(n)$ is embeddable as a join-semilattice of $\Lambda(G)$ is $\mu'(G)$.*
- *The largest n such that $B(n)$ is embeddable as a meet-semilattice of $\Lambda(G)$ with the minimal element a normal subgroup of G is $b_2(G)$.*

As a corollary, we see that $b_2(G) \leq \mu'(G)$ for any group G.

Conjecture

The condition on the minimal element can be deleted in the above theorem.

If so, then we would have $b_2(G) = \mu'(G)$.

References

- Sophie Piccard, Sur les bases du group symétrique et du groupe alternant, *Math. Ann.* **116** (1939), 752–767.
- G. L. Morgan and C. W. Parker, The diameter of the commuting graph of a finite group with trivial centre, *J. Algebra* **393** (2013), 41–59; arXiv 1301.2341.
- M. R. Giudici and C. W. Parker, There is no upper bound for the diameter of the commuting graph of a finite group, *J. Combinatorial Theory* (A) **120** (2013), 1600–1603; arXiv 1210.0348.
- T. Breuer, R. M. Guralnick and W. M. Kantor, Probabilistic generation of finite simple groups, II, *J. Algebra* **320** (2008), 443–494.
- T. C. Burness and S. Guest, On the uniform spread of almost simple linear groups *Nagoya Math. J.* **209** (2013), 35–109.
- T. C. Burness and E. Crestani, On the generating graph of direct powers of a simple group, *J. Algebraic Combinatorics* **38** (2013), 329–350.
- A. Lucchini and A. Maróti, Some results and questions related to the generating graph of a finite group, Proceedings of Ischia Group Theory Conference 2008.
- P. J. Cameron, Some measures of finite groups related to permutation bases, arXiv 1408.0968.
- John Rhodes and Pedro Silva, *Boolean Representations of Simplicial Complexes and Matroids*, Springer Monographs in Mathematics, 2015.