How big is the symmetric group?

Peter J Cameron

School of Mathematical Sciences
Queen Mary, University of London
London E1 4NS, U.K.
p.j.cameron@qmul.ac.uk

PGGT, Birmingham, 17 April 2002

Order, composition factors, generators

The order of S_n is $n!$ (trivial).

The number of composition factors of S_n is 2 for $n \neq 2,4$ (known to Galois?).

$d(G)$ is the minimum number of generators of the group G. We have $d(S_n) = 2$ (elementary: for example, $(1,2,\ldots,n)$ and $(1,2)$ generate S_n).

So the symmetric group is both very big and very small!

Generators of subgroups

$d'(G)$ is the maximum of $d(H)$ over all subgroups $H \leq G$.

McIver and Neumann showed that $d'(S_n) = \lfloor n/2 \rfloor$ for $n > 3$. This is a lower bound, as is shown by

$$\langle (1,2),(3,4),\ldots,(2m-1,2m) \rangle$$

where $m = \lfloor n/2 \rfloor$. Showing it is an upper bound is harder!

Jerrum gave a more elementary proof that $d'(S_n) \leq n-1$. In fact he showed that any subgroup of S_n has a "nice" generating set with the properties

- a "nice" generating set contains at most $n-1$ elements;
- if S is "nice" and $g \in S_n$, then we can compute a "nice" generating set for $\langle S, g \rangle$ efficiently.

This can be used to compute a base and strong generating set of an arbitrary subgroup in polynomial time.

Length of subgroup chain

$l(G)$ is the length of the longest chain of subgroups in G.

Note that $d'(G) \leq l(G)$ for any group G; this was the original motivation for studying $l(G)$ (Babai).

If N is a normal subgroup of G, then $l(G) = l(N) + l(G/N)$. Thus we only have to compute $l(S)$ for all simple groups S.

This has been done for many families of simple groups (Solomon, Turull).

Length of subgroup chain

Cameron, Solomon and Turull showed (using CFSG) that

$$l(S_n) = \lceil 3n/2 \rceil - b(n) - 1,$$

where $b(n)$ is the number of ones in the base 2 representation of n. So $d'(S_n) < l(S_n)$ for $n \geq 4$.

It is easy to find a subgroup chain whose length is the right-hand side of the above formula. To show that no longer chain is possible, we take a chain

$$S_n > G > \cdots$$

and analyse the possibilities for G, ultimately using the O'Nan–Scott Theorem and CFSG.

Probably the use of CFSG here can be avoided!

Independent generating sets

A set $S \subseteq G$ is independent if $s \notin \langle S \setminus \{s\} \rangle$ for all $s \in S$; that is, no element of s can be written as a word in the remaining elements.

$\mu^*(G)$ is the size of the largest independent subset of G; and $\mu(G)$ is the size of the largest independent generating set of G. Clearly $\mu(G) \leq \mu^*(G)$. Equality holds in abelian groups, p-groups, dihedral groups, and (as we will see) symmetric groups, but not in general. (Whiston gives counterexamples in $\mathrm{PSL}(2,p)$ for suitable primes p.) It would be interesting to know more about this! Also, $\mu(G)$ is the size of the largest minimal (w.r.t. inclusion) generating set of G.

The parameter $\mu(G)$ occurs in the paper of Diaconis and Saloff-Coste on the rate of convergence of the product replacement algorithm on a finite group. The time required until the distribution is near-random depends very sensitively on $\mu(G)$.

Another application is given later.

Independent generating sets

Whiston proved that $\mu(S_n) = \mu^*(S_n) = n-1$. Again, the lower bound is straightforward (the set

$$\{(1,2),(2,3),\ldots,(n-1,n)\}$$

is an independent generating set). For the upper bound, CFSG is required; if G is the subgroup generated by all but one element of an independent generating set of largest size, then $\mu(S_n) \leq \mu(G)+1$, and we have to analyse G.

Cameron and Cara used Whiston's result to determine all independent generating sets of S_n of size $n-1$. There are two types; one consists of transpositions corresponding to the edges of a tree; the other contains one transposition, the other elements being 3-cycles or double transpositions.

Coset geometries

Let G be a group, and $(G_i : i \in I)$ a family of subgroups of G. for $J \subseteq I$, let $G_J = \bigcap_{j \in J} G_j$. Suppose that the following three conditions hold:

(G1) The subgroups G_J, for $J \subseteq I$, are all distinct.

(G2) If $J \subseteq I$ and $|J| < |I| - 1$, then $G_J = \langle G_{J \cup \{k\}} : k \in I \setminus J \rangle$.

(G3) If a family $(G_j x_j : j \in J)$ of right cosets have pairwise non-empty intersection, for $j \in J$, then there is an element of G lying in all these cosets.

The coset geometry $C(G,(G_i : i \in I))$ has type set I; the varieties of type i are the right cosets of G_i, and two varieties are incident if their intersection is non-empty. The group G acts as a flag-transitive automorphism group of the geometry.

Coset geometries

The coset geometry is called residually weakly primitive, or RWPri, if the following condition holds:

(G4) For any $J \subset I$, there exists $k \in I \setminus J$ such that $G_{J\cup\{k\}}$ is a maximal subgroup of G_J.

This means that the group G_J acts primitively on the varieties of at least one type in the residue of the standard flag of type J.

The rank of a coset geometry for G is at most $\mu^*(G)$, while the rank of an RWPri coset geometry is at most $\mu(G)$. In general, it is not true that equality holds, and so we have two new measures of the size of a group:

- the maximum rank of a coset geometry;
- the maximum rank of an RWPri coset geometry.

Coset geometries

Cameron and Cara showed that all the minimal generating sets for S_n of size $n-1$ give rise to RWPri coset geometries. Hence we conclude:

The maximum rank of a coset geometry for S_n is $n-1$. Any geometry which meets this bound is RWPri, and all such geometries are known.

The diagram of the geometry corresponding to an independent generating set of the first type (transpositions corresponding to the edges of a tree T) is the line graph of T. For the second type, the unique transposition in the set corresponds to an isolated node of the diagram.

Other measures?

Both $l(G)$ and $\mu^*(G)$ are determined by the subgroup lattice $\mathcal{L}(G)$ of G; they are, essentially, the longest chain and the largest Boolean lattice, respectively, which can be embedded in $\mathcal{L}(G)$. These measures can easily be generalised: we can ask about embedding other posets in the subgroup lattice of G. One natural measure which springs to mind is the size of the largest antichain in $\mathcal{L}(G)$.

Needless to say, there are many other measures which have been used in different circumstances: the number of conjugacy classes (the Monster is a remarkably small group in this sense); the degree of the smallest faithful permutation representation, or matrix representation (important if we have to do computation in the group); and so on.

Other measures?

One can also look at the relation between different measures, or between the measure of a group and a subgroup or quotient. We have seen examples of both of these: e.g. $d'(G) \leq l(G)$ and $\mu^*(G) \leq l(G)$; and $l(G) = l(N) + l(G/N)$ for any normal subgroup N of G.

A similar relation used by Whiston is

$$\mu(G) \leq \mu(G/N) + \mu^*(N)$$

for any normal subgroup N of G. It would be interesting to know when the bound is met.

Also, given a measure m, we can define $m'(G)$ to be the maximum of $m(H)$ over all subgroups H of G (as we did to get from d to d'). If the measure m is not monotonic, this will give us something new; but m' will then of course be monotonic.

References

L. Babai, On the length of subgroup chains in the symmetric group, *Commun. Algebra* **14** (1986), 1729–1736.

P. J. Cameron and Ph. Cara, Independent generating sets and geometries for symmetric groups, in preparation.

P. J. Cameron, R. Solomon and A. Turull, Chains of subgroups in symmetric groups, *J. Algebra* **127** (1989), 340–352.

P. Diaconis and L. Saloff-Coste, Walks on generating sets of groups, *Invent. Math.* **134** (1998), 251–299.

M. R. Jerrum, A compact representation for permutation groups, *J. Algorithms* **7** (1986), 60–78.

A. McIver and P. M. Neumann, Enumerating finite groups, *Quart. J. Math.* (2) **38** (1987), 473–488.

R. Solomon and A. Turull, Chains of subgroups in groups of Lie type, I–III, *J. Algebra* **132** (1990), 174–184; *J. London Math. Soc.* (2) **42** (1990), 93–100; *ibid.* (2) **44** (1991), 437–444.

J. Whiston, Maximal independent generating sets of the symmetric group, *J. Algebra* **232** (2000), 255–268.