Mathematics with and without CFSG

Peter J. Cameron
University of St Andrews

YRM
2016

University of St Andrews
August 2016

Classification of Finite Simple Groups

The Classification of Finite Simple Groups (CFSG for short) is the greatest single collective achievement of mathematics. It is

- easy to state;
- hard to prove (the first proof ran to about 15000 pages, with contributions from hundreds of mathematicians);
- easy to apply (group theorists have developed powerful tools for this); and
- of very wide applicability in mathematics; but
- the proof has a somewhat tangled history.

I aim to tell you about some of this (not the proof!).

The theorem

A group is simple if it has no normal subgroups except itself and the trivial group. According to the Jordan–Hölder theorem, every finite group can be built from finite simple groups (though we do not completely understand the building process!)

Theorem

A finite simple group is one of the following:

- *a cyclic group of prime order;*
- *an alternating group A_n, for $n \geq 5$;*
- *a group of Lie type; or*
- *one of* 26 *sporadic groups, with orders ranging from* 7920 *to* 808017424794512875886459904961710757005754368000000000.

The groups

The groups are now fairly well understood. There is no mystery in the cyclic groups of prime order, apart from the mystery of the primes! The alternating group A_n consists of all even permutations of $\{1, \ldots, n\}$ (those where the number of cycles has the same parity as n). Groups of Lie type are closely related to certain matrix groups over finite fields; they fall into a number of families, parametrised by a field order and (for some families) a dimension. The sporadic groups are best understood as individuals.

For applications, the most important things we need to know about simple groups (and groups closely related to them) are

- the maximal subgroups;
- the matrix representations.

Much of this information is available in computer packages such as Magma and GAP, or on-line at the Atlas of Finite Group Representations.

First consequences of CFSG

These are things which were conjectured long before the theorem was proved, but were (and still are) out of reach without CFSG. (Here and later, I annotate theorems proved using CFSG.)

Theorem (CFSG)

- *A finite simple group can be generated by two elements (and there is a great deal of freedom in choosing the generators).*
- *The outer automorphism group of a finite simple group is soluble (and has a particularly easy structure to understand).*
- *There is no finite 6-transitive permutation group apart from symmetric and alternating groups.*

Here, a permutation group is k-transitive if any k distinct points can be mapped to any other k distinct points by some group element.

How many groups?

Since simple groups are the building blocks for all groups, their classification should give us information on how many groups there are. Peter Neumann proved:

Theorem

If there exists a constant c_1 such that the number of simple groups of order n is bounded by $n^{c_1 \log^2 n}$, then there exists a constant c_2 so that the number of groups of order n is bounded by $n^{c_2 \log^2 n}$.

It is a consequence of CFSG that there are at most two simple groups of order n for any n. So an unconditional form of Neumann's bound follows from CFSG.
It is known that, for prime powers n, there is a lower bound for the number of groups, also of the form $n^{c \log^2 n}$.

Some history

The cyclic, alternating and classical groups and five of the sporadic groups (the Mathieu groups) were known by the early 20th century. The remaining groups of Lie type (the exceptional groups) were discovered by Chevalley, Steinberg, Ree and Tits in the 1950s. In the 1960s, Feit and Thompson proved the Odd Order Theorem (no simple group apart from cyclic groups can have odd order), introducing many new techniques; and Brauer introduced methods for studying involutions (elements of order 2).

At this point it looked as if the classification might be feasible. But then in 1965, Janko discovered a sporadic simple group of order 175560 …

Over the next fifteen years or so, the remaining sporadic simple groups popped up, seemingly randomly. But Daniel Gorenstein masterminded an approach to the classification; work on this ran concurrently with the new discoveries, and the hope was that the two threads would converge.

In 1980, this seemed to have happened, and Gorenstein announced the completion of the classification project (apart from a few details, such as the construction of J_4 and the identification of the "groups of Ree type"), which were solved soon afterwards.

But there was a much larger problem which was not realised. One of the important cases in the proof, the "quasithin case", was rumoured to have been completed; but the rumour was wrong. It took 25 years to fill this lacuna (during which time the precise definition of a quasithin group changed!)

The gap was eventually filled by Michael Aschbacher and Steve Smith, and the last part of the proof published in 2011.

Work continues on finding a “better” proof.

Is CFSG true? 35 years on from Gorenstein’s announcement, nobody has found any evidence to the contrary, either by finding another simple group, or by discovering that using it leads to a contradiction. So, very likely, yes.

Is the proof correct? Certainly not, but hopefully the mistakes can be fixed before the expertise is lost. The proof of the Odd Order Theorem (about 400 pages long) has been formalised by Georges Gonthier and colleagues in 2012, and checked using the Coq computer proof assistant. Maybe the same will be done for CFSG one day.

Should we happily use the theorem? I will comment on this later …

Following Gorenstein's announcement in 1980, people began using the theorem, though the more prudent clearly labelled their results as depending on the (yet unproved) CFSG.

I was one of those people; I spent a term on sabbatical at the University of Sydney, where I gave a course of lectures on the consequences of CFSG for permutation group theory (which became my most-cited paper).

Applications were found in computer science (the graph isomorphism problem), and number theory (relative Brauer groups), as well as other parts of group theory (such as profinite groups) and combinatorics (e.g. distance-transitive graphs). I will discuss some of these in the remainder of this lecture.

To use or not to use CFSG?

Right from 1980, many people took the pragmatic view that a theorem is made to be used. Since the proof was not complete, we should acknowledge that. But now that the proof is complete, there is no problem, right?

The counter-argument is that this is a theorem whose proof is so long that it is not possible, even in principle, for a mathematician who wishes to use it to check the entire proof. So the principle “take nothing on trust” is violated.

But CFSG is such an important and useful theorem that we would sacrifice a lot of mathematics by not using it.

You have to make up your mind about this. Perhaps it is not too dissimilar from using the Axiom of Choice. (With AC, we can assume it or its negation; with CFSG, we can’t assume the negation, just use it or not.)

A paper of J.-P. Serre

Jean-Pierre Serre, On a theorem of Jordan, *Bull. Amer. Math. Soc.* **40** (2003), 429–440.

Theorem

Let f be a polynomial of degree n over $\mathbb{Z}$, with $n \geq 2$, which is irreducible in $\mathbb{Q}[x]$. Then the set of primes p for which f has no roots mod p has a density, which is at least $1/n$.

Theorem

Let $f : T \to S$ be a finite covering of a topological space S. Assume that every fibre has cardinality n, where $n \geq 2$, and that T is arcwise connected and non-empty. Then there is a continuous map $\phi : \mathbb{S}^1 \to S$ which cannot be lifted to T.

A theorem of Jordan

C. Jordan, Recherches sur les substitutions, *J. Liouville* **17** (1872), 351–367.

Theorem

Let G be a finite group acting transitively on a set Ω, with $|\Omega| = n > 1$. Then G contains a fixed-point-free element.

For a simple counting argument (which some people call *Burnside's Lemma*) shows that the average number of fixed points of elements of G is 1. But the identity fixes more than one point; so some element fixes less than 1.

The two theorems I quoted from Serre's paper follow from this, with a tailpiece: P. J. Cameron and A. M. Cohen, On the number of fixed point free elements in a permutation group, *Discrete Math.* **106/107** (1992), 135–138.

Theorem

With the same hypotheses, at least $|G|/n$ elements of G are fixed-point-free.

A theorem of Fein, Kantor and Schacher

B. Fein, W. M. Kantor and M. Schacher, Relative Brauer groups, II, *Crelle* **328** (1981), 39–57.

Theorem (CFSG)

Let G be a finite group acting transitively on a set Ω, with $|\Omega| = n > 1$. Then G contains a fixed-point-free element of prime-power order.

They used this to prove the following result:

Theorem (CFSG)

Let K be a global field (a finite extension of $\mathbb{Q}$ or of $\mathbb{F}(x)$ for a finite field $\mathbb{F}$), L a finite extension of K. Then the relative Brauer group of L over K is infinite.

In other words, there are infinitely many “inequivalent” finite-dimensional central simple algebras over K which become matrix algebras when tensored with L.

Sketch proof

Let G act transitively on Ω, with $|\Omega| = n > 1$.
Standard reductions from permutation group theory allow us to assume that

- G acts primitively, that is, a point stabiliser is a maximal subgroup;
- G is simple.

So we need to know that, if G is simple and H a maximal subgroup, there is a conjugacy class of elements *of prime power order* disjoint from H. This is done case-by-case using detailed knowledge of the finite simple groups.

Two features

- The two theorems in the FKS paper are equivalent. Thus, a direct proof that relative Brauer groups are infinite would allow the result about f.p.f. elements of prime power order to be proved without CFSG. (Nobody has done this yet.)
- The proof is algorithmic: it gives a polynomial-time algorithm for finding a f.p.f. element of prime power order. But the algorithm is of course quite complicated, and we need CFSG to prove its correctness.

That led me to wonder whether one could make Jordan's theorem algorithmic. The second remark above shows that there is a polynomial-time algorithm to find a f.p.f. element. But can we do it more simply?

There is a simple randomized algorithm. Since at least $|G|/n$ elements are f.p.f., if we choose elements at random, then after n choices the probability of failure is about $1/e$, and after n^2 choices it is exponentially small.

The question was answered by Vikraman Arvind, who “derandomized” the simple algorithm above. Here is a brief outline of his method (see arXiv 1301.0379).

Jordan tells us that the average number of fixed points in a transitive permutation group G on Ω is 1. A simple extension (with the same proof) shows that the average number of fixed points in any coset of G in the symmetric group on Ω is also 1. The same is not true for groups G which are not transitive; but there is a simple way to compute the average in any coset.

So start with the transitive group G; successively compute the stabilisers of points, and in each stabiliser find a coset where the average number of fixed points is no greater than in the step before (and is strictly smaller at the first step.)

At the end, the stabiliser is the identity, so a coset is a single element, which has fewer than one fixed point, that is, is f.p.f., as required.

Which prime? Isbell's conjecture

J. R. Isbell, Homogeneous games, II, *Proc. Amer. Math. Soc.* **11** (1960), 159–161.

In 1960, John Isbell was studying game theory (in the sense of von Neumann and Morgenstern). The theory of n-player games is quite complicated, and Isbell wanted a condition which would ensure that the game was fair, that is, no player should have an advantage.

He did so by requiring that the automorphism group of the game acts transitively on the set of players. He called such a game homogeneous.

He showed that a homogeneous simple game on n players exists if and only if there is a transitive subgroup G of the symmetric group S_n containing no fixed-point-free element of 2-power order.

For which n does such a group exist?

Isbell made the following conjecture:

Conjecture

Let n be a positive integer for which the 2-part of n is "sufficiently large" compared to the odd part (that is, there is a function f such that $n = 2^a \cdot b$ where $a \geq f(b)$). Then any transitive group of degree n contains a fixed-point-free element of 2-power order; hence there is no homogeneous game for n players.

Remarkably, this conjecture is still open, even using CFSG! There is an obvious extension from the prime 2 to arbitrary primes; slightly more progress has been made for primes at least 5, but the conjecture has not been solved for any prime.

Chains of subgroups

The length $l(G)$ of a group G is the length of the longest chain of subgroups in G. It is a nice measure of the complexity of G: it depends on the composition factors of G (the simple “building blocks”), but not on how they are put together.

I am proud of the following formula which I found in the early 1980s: see P. J. Cameron, R. Solomon and A. Turull, Chains of subgroups in symmetric groups, *J. Algebra* **127** (1989), 340–352.

Theorem (CFSG)

$$l(S_n) = \left\lceil \frac{3n}{2} \right\rceil - b(n) - 1,$$

where $b(n)$ is the number of ones in the base 2 representation of n.

The theorem depends only weakly on CFSG, and will no doubt be proved without it one day. It is not hard to build a chain of the stated length; the problem is to show that no chain can be longer. So take a chain

$$S_n = G_0 > G_1 > \ldots > G_l = \{1\}.$$

If G_1 is intransitive, or transitive but imprimitive (i.e. preserves a partition of $\{1, \ldots, n\}$), then we can use induction. If G_1 is primitive, it follows from CFSG that its order is quite small, and the length of the chain is at most $1 + \log_2 |G_1|$.

Indeed, there are elementary bounds for the orders of primitive groups which are nearly good enough …

László Babai

L. Babai, On the order of uniprimitive permutation groups, *Annals of Mathematics* **113** (1981), 553–568.

Theorem

If G is a primitive subgroup of S_n which is not 2-transitive, then $|G| \leq n^{4n^{1/2}\log n}$.

The best bound previously had been exponential, due to Wielandt. Babai's bound is almost best possible, but using CFSG it is possible to refine it considerably, to get order $n^{\log n}$ with "known" exceptions.

Babai's proof used elementary combinatorics but very little group theory. He later gave a bound for 2-transitive groups which was subsequently improved by Pyber. (Using CFSG, we know all the 2-transitive finite permutation groups.)

Graph isomorphism

Very recently, Babai has shown that the isomorphism of n-vertex graphs can be tested in quasi-polynomial time, that is time $O(\exp(\log^c n))$ for some constant c.
This is a substantial and beautiful piece of work, and probably one of the best results in complexity theory in the last year.
His proof uses CFSG, in the way we have just seen (that is, the fact that primitive groups are small with known exceptions).
Again, it seems that it might be possible to avoid the use of CFSG here, and Pyber is working on this …