Using the finite simple groups

Cheryl E. Praeger[1]

The finite simple group classification, announced by Daniel Gorenstein in February 1981, was one of the greatest triumphs of late twentieth century mathematics, and to this day its ramifications continue to drive cutting-edge developments across many areas of mathematics. The list of finite simple groups is surprisingly short: for each prime p, the cyclic group C_p of order p is simple; for each integer n at least 5, the group of all even permutations of a set of size n forms the simple alternating group A_n; there are finitely many additional infinite families of simple groups called *finite simple groups of Lie type*; and there are precisely 26 further examples, called the *sporadic simple groups*, of which the largest is the Monster*.

Already in 1981, some consequences of the classification were 'waiting expectantly in the wings'. For example, we immediately could list all the finite groups of permutations under which all point-pairs were equivalent (the 2-transitive permutation groups) [3].

1. Simple groups and algebraic graph theory

For other problems it was unclear for a number of years whether the simple group classification could be applied successfully in their solution. One of the most famous of these was a 1965 conjecture of Charles Sims at the interface between permutation group theory and graph theory. It was a question about finite primitive permutation groups. The primitive groups form the building blocks for permutation groups in a somewhat similar way to the role of the finite simple groups as building blocks (composition factors) for finite groups. Sims conjectured that there is a function f on the positive integers such that, for a finite primitive permutation group in which a point stabiliser H has an orbit of size d, the cardinality of H is at most $f(d)$. In graph theoretic language: for a vertex-primitive graph or directed graph of valency d (each vertex is joined to d other vertices), there are at most $f(d)$ automorphisms (edge-preserving permutations) fixing any given vertex. Proof of the Sims conjecture [5] in 1983 required detailed information about the

Invited technical paper, communicated by Jon Borwein.

[1]Centre for Mathematics of Symmetry and Computation, School of Mathematics and Statistics, University of Western Australia, Crawley, WA 6009. Email: cheryl.praeger@uwa.edu.au

The author acknowledges support of Australian Research Council Federation Fellowship FF0776186.

*containing 808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000 elements!

subgroup structure of the Lie-type simple groups, and was one of the first non-trivial applications of the finite simple group classification in Algebraic Graph Theory, see [6, Section 4.8C]. The new approach in [5] was later developed into a standard framework for applying the simple group classification to many problems about primitive permutation groups and vertex-primitive graphs.

Stunning new applications of the simple group classification in Algebraic Graph Theory continue to appear, and many new applications are accompanied by deep new results on the structure and properties of the simple groups. The most recent exciting developments relate to expander graphs. These are graphs or networks which are simultaneously sparse and highly connected. They have important applications for design and analysis of robust communication networks, for the theory of error-correcting codes, the theory of pseudo-randomness, and many other uses, beautifully surveyed in [11]. A family of finite graphs, all of the same valency but containing graphs of arbitrarily large size, is an *expander family* if there is a constant c such that the ratio $|\partial A|/|A|$ is at least c for every subset A of vertices of any of the graphs Γ in the family, where A contains at most half of the vertices of Γ and ∂A is the set of vertices of Γ at distance 1 from A. The new results confirm that many families of Cayley graphs for simple Lie-type groups of bounded rank are expander families. This flurry of activity began with a spectacular breakthrough by Helfgott [9] in 2008 for the two-dimensional projective groups $\mathrm{PSL}(2,p)$ over fields of prime order p. The strongest current results for bounded rank Lie type groups are consequences of new results for 'growth in groups' by Pyber and Szabo [19], and independently by Breuillard, Green and Tao [2] for the finite Chevalley groups.

2. Simple groups, primes and permutations

Several results about permutation groups have 'simple' statements making no mention of simple groups, but their only known proofs rely on the simple group classification, often on simple group theory developed long after the classification was announced. In fact many recent results in this area demand a deep and subtle understanding of the finite simple groups, especially their subgroup structure, element statistics, and their representations.

A surprising link between the number of primes and the finite simple groups was discovered soon after the announcement of the simple group classification. It is a result due to Cameron, Neumann and Teague [4] in 1982. Each positive integer $n \geq 5$ occurs as the index of a maximal subgroup of a simple group, namely the simple alternating group A_n has a maximal subgroup A_{n-1} of index $|A_n|/|A_{n-1}| = n$. Let's call n a *maximal index* if $n = |G|/|H|$ for some non-abelian simple group G and maximal subgroup H with $(G,H) \neq (A_n, A_{n-1})$. It was proved in [4] that

$$\max(x)/\pi(x) \to 1 \quad \text{as} \quad x \to \infty,$$

where $\max(x)$ is the number of maximal indices at most x and $\pi(x)$ is the number of primes at most x. The limiting density of the set of maximal indices is 'explained' by the fact that, for each prime p, the projective group $\mathrm{PSL}(2,p)$ acts primitively on the projective line $\mathrm{PG}(1,p)$ of size $p+1$, and so has a maximal subgroup of

index $p+1$. The major motivation that led to this result was its consequence for primitive permutation groups, also proved in [4]: the number $D_{\mathrm{prim}}(x)$ of integers $n \leq x$ for which there exists a primitive permutation group on n points (that is, of *degree* n), other than S_n and A_n, satisfies $D_{\mathrm{prim}}(x)/\pi(x) \to 2$ as $x \to \infty$. Beside the primitive actions of $\mathrm{PSL}(2,p)$ of degree $p+1$, the cyclic group C_p acts primitively of degree p, thus accounting for the limiting density ratio 2.

Two decades later I extended this result with Heath-Brown and Shalev in [8] as part of our investigation of quasiprimitive permutation groups, a strictly larger family of permutation groups than the primitive groups and important in combinatorial applications**. The crucial quantity we needed, in order to determine the behaviour of the degrees of quasiprimitive permutation groups, turned out to be the number $\mathrm{sim}(x)$ of *simple indices* at most x, where by a simple index we mean an index $|G|/|H|$ of an arbitrary subgroup H of a non-abelian simple group G such that $(G,H) \neq (A_n, A_{n-1})$. We proved that $\mathrm{sim}(x)/\pi(x)$ also approaches a limit as $x \to \infty$, and we proved that this limit is the number

$$h = \sum_{n=1}^{\infty} \frac{1}{n\phi(2n)} = 1.763085\ldots,$$

where $\phi(m)$ is the Euler phi-function, the number of positive integers at most m and coprime to m. The analogous consequence (which had been our principal motivation for studying $\mathrm{sim}(x)$) was that the ratio $D_{\mathrm{qprim}}(x)/\pi(x)$ of the number $D_{\mathrm{qprim}}(x)$ of degrees $n \leq x$ of quasiprimitive permutation groups, apart from S_n and A_n, to $\pi(x)$ approaches $h+1$ as $x \to \infty$. In this case also, these ratios are accounted for by various subgroups of the simple groups $\mathrm{PSL}(2,p)$.

My 'all-time favourite' example of a deep result with a deceptively uncomplicated statement is due to Isaacs, Kantor and Spaltenstein [12] in 1995: let G be *any group of permutations* of a set of size n and let p be any prime dividing the order $|G|$ of G (that is, the cardinality of G). Then there is at least one chance in n that a uniformly distributed random element of G has a cycle of a length that is a multiple of p. The hypotheses of this result are completely general, giving no hint that the assertion has anything at all to do with simple groups. However the only known proof of this result relies on the finite simple group classification, and in particular uses subtle information about maximal tori and Weyl groups of simple Lie-type groups. These techniques were the same as those introduced in 1992 by Lehrer [13] to study the representations of finite Lie-type groups. I recently worked with Alice Niemeyer and others to understand the precise conditions needed for this approach to be effective. We developed an estimation method in [16] and used it to underpin several Monte Carlo algorithms for computing with Lie-type simple groups (in [14], [15]). It produces sharper estimates for the proportions of various kinds of elements of Lie-type simple groups than alternative geometric approaches.

**A permutation group is quasiprimitive if each of its nontrivial normal subgroups is transitive. Each primitive permutation group has this property, and so do many other permutation groups.

3. Simple groups and involutions

One of the first hints that understanding the finite simple groups might be a tractable problem was the seminal 'Odd order paper' of Feit and Thompson [7] in 1963 in which they proved that every finite group of odd order is soluble, or equivalently, that every non-abelian finite simple group contains a non-identity element x such that $x^2 = 1$. Such an element is called an *involution*, and the Feit–Thompson result, that each non-abelian finite simple group contains involutions, had been conjectured more than 50 years earlier by Burnside in 1911. The centraliser of an involution x consists of all the group elements g that centralise x in the sense that $xg = gx$. The involution centralisers in finite simple groups are subgroups that often involve smaller simple groups. Several crucial steps in the simple group classification involved systematic analyses of the possible involution centralisers in simple groups, resulting in a series of long, deep and difficult papers characterising the simple groups containing various kinds of involution centralisers.

Some important information about the simple groups can be found computationally, and key for this are efficient methods for constructing their involution centralisers. To construct an involution, one typically finds by random selection an element of even order that powers up to an involution, then uses Bray's ingenious algorithm [1] to construct its centraliser. This worked extremely well in practice for computing with the sporadic simple groups. A more general development of Bray's method into proven Monte Carlo algorithms for Lie-type simple groups over fields of odd order required delicate estimates of various element proportions in simple groups — first given in a seminal paper of Parker and Wilson [17] (available as a preprint for several years before its publication), and then in full detail in [10]. The estimates and complexity analysis give a lower bound on the algorithm performance, but do not match the actual (excellent) practical performance. A major program is in train to find a realistic analysis and the first parts have been completed [14], [18].

The classification of the finite simple groups was a watershed for research in algebra, combinatorics, and many other areas of mathematics. It changed almost completely the problems studied and the methods used. To realise further the power of the classification for future applications, new detailed information is needed about the simple groups — and this will be gained both as new theory and through new computational advances.

References

[1] Bray, J.N. (2000). An improved method for generating the centralizer of an involution. *Arch. Math. (Basel)* **74,** 241–245.

[2] Breuillard, E., Green, B. and Tao, T. (2010). Approximate subgroups of linear groups. *Geom. Funct. Anal.* (To appear.) arXiv:1005.1881v1.

[3] Cameron, P.J. (1981). Finite permutation groups and finite simple groups. *Bull. London Math. Soc.* **13,** 1–22.

[4] Cameron, P.J., Neumann, P.M. and Teague, D.N. (1982). On the degrees of primitive permutation groups. *Math. Zeit.* **180,** 141–149.

[5] Cameron, P.J., Praeger, C.E., Seitz, G.M. and Saxl, J. (1983). On the Sims' conjecture and distance transitive graphs. *Bull. Lond. Math. Soc.* **15,** 499–506.

[6] Dixon, J.D. and Mortimer, B. (1996). *Permutation Groups*. Springer, New York.
[7] Feit, W. and Thompson, J.G. (1963). Solvability of groups of odd order. *Pacific J. Math.* **13,** 775–1029.
[8] Heath-Brown, D.R., Praeger, C.E. and Shalev, A. (2005). Permutation groups, simple groups and sieve methods. *Israel J. Math.* **148,** 347–375.
[9] Helfgott, H.A. (2008). Growth and generation in $\mathrm{SL}_2(Z/pZ)$. *Annals of Math.* **167,** 601–623.
[10] Holmes, P.E., Linton, S.A., O'Brien, E.A., Ryba, A.J.E. and Wilson, R.A. (2008). Constructive membership in black-box groups. *J. Group Theory* **11,** 747–763.
[11] Hoory, S., Linial, N. and Widgerson, A. (2006). Expander graphs and their applications. *Bull. Amer. Math. Soc.* **43,** 439–561.
[12] Isaacs, I.M., Kantor, W.M. and Spaltenstein, N. (1995). On the probability that a group element is p-singular. *J. Algebra* **176,** 139–181.
[13] Lehrer, G.I. (1992). Rational tori, semisimple orbits and the topology of hyperplane complements. *Comment. Math. Helv.* **67,** 226–251.
[14] Lübeck, F., Niemeyer, A.C. and Praeger, C.E. (2009). Finding involutions in finite Lie type groups of odd characteristic. *J. Algebra* **321,** 3397–3417.
[15] Niemeyer, A.C., Popiel, T. and Praeger, C.E. (2010). Finding involutions with eigenspaces of given dimensions in finite classical groups. *J. Algebra* **324,** 1016–1043.
[16] Niemeyer, A.C. and Praeger, C.E. (2010). Estimating proportions of elements in finite simple groups of Lie type. *J. Algebra* **324,** 122–145.
[17] Parker, C.W. and Wilson, R.A. (2010). Recognising simplicity of black-box groups by constructing involutions and their centralisers. *J. Algebra* **324,** 885–915.
[18] Praeger, C.E. and Seress, Á. Probabilistic generation of finite classical groups in odd characteristic by involutions. *J. Group Theory*. In press. doi: 10.1515/JGT.2010.061
[19] Pyber, L. and Szabó, E. Growth in finite simple groups of Lie type of bounded rank. (Submitted.) arXiv:1005.1858.

Cheryl Praeger is Winthrop Professor of Mathematics at the University of Western Australia, and in 2007 she became the first pure mathematician to be awarded an Australian Research Council Federation Fellowship. For her achievements and service to mathematics, she was elected a Fellow of the Australian Academy of Science, and appointed a Member of the Order of Australia (AM). She was President of the Australian Mathematical Society from 1992 to 1994, and is currently on the Executive Committee of the International Mathematical Union.