Simple Groups, Permutation Groups, and Probability

Aner Shalev

Abstract. We survey recent progress, made using probabilistic methods, on several conjectures concerning finite groups.

1991 Mathematics Subject Classification: Primary 20D06; Secondary 20P05, 20B15.

1 Random generation

In recent years probabilistic methods have proved useful in the solution of several difficult problems concerning finite groups; these involve conjectures on finite simple groups and on finite permutation groups. In some cases the probabilistic nature of the problem is apparent from its very formulation; but in other cases the use of probability, or counting, seems surprising, and cannot be anticipated by the nature of the problem.

In some branches of mathematics it is quite common to use probabilistic methods, or related non-constructive methods, in order to prove existence theorems (Cantor's proof of the existence of transcendental numbers is a classical example). However, this is less common in group theory. Indeed, it is our hope that the probabilistic approach will have sufficiently many group-theoretic applications so as to become a standard tool in group theory.

The roots of the subject lie in a series of 7 papers by Erdős and Turán (starting with [ET1]) in which they study the properties of random permutations. For example they show that most permutations in the symmetric group S_n have order about $n^{\frac{1}{2}\log n}$, and have about $\log n$ cycles.

Dixon [D] used the Erdős-Turán theory to settle an old conjecture of Netto, proving that two randomly chosen elements of the alternating group A_n generate A_n with probability $\to 1$ as $n \to \infty$. He proposed the following generalization:

Conjecture 1 (Dixon, 1969): Two randomly chosen elements of a finite simple group G generate G with probability $\to 1$ as $|G| \to \infty$.

Here G and its Cartesian powers are regarded as probability spaces with respect to the uniform distribution.

At the time this was a rather daring conjecture, since the Classification of Finite Simple Groups was not yet available. Invoking the Classification Theorem (which we do throughout) it remained to prove the conjecture for the simple groups of Lie type.

A breakthrough was made in 1990 by Kantor and Lubotzky, who proved Dixon's conjecture for classical groups and for some small rank exceptional groups of Lie type [KL]. The remaining exceptional groups were handled by Liebeck and myself in 1995 [LiSh1], so we have:

Theorem 1 (Dixon, Kantor, Lubotzky, Liebeck, Shalev): *Dixon's conjecture holds.*

This result has quantitative versions. Let $m(G)$ denote the minimal index of a proper subgroup of G. Then it turns out that the probability that two randomly chosen elements of a finite simple group G do not generate G is approximately $m(G)^{-1}$ (up to a multiplicative constant); see [Ba], [K], [LiSh3] for this and for more refined estimates.

We also obtain results on random generation by special pairs of elements. In their paper [KL] Kantor and Lubotzky pose the following:

Conjecture 2 (Kantor-Lubotzky, 1990): A randomly chosen involution and a randomly chosen additional element of a finite simple group G generate G with probability $\to 1$ as $|G| \to \infty$.

This was settled in [LiSh3], so we have:

Theorem 2 (Liebeck-Shalev, 1996): *Kantor-Lubotzky's conjecture holds.*

We also show in [LiSh3] that a finite simple group which is not a Suzuki group is almost surely generated by a random element of order 3 and a random additional element.

A related question raised in [KL] is as follows. Let G be a finite simple group, and let $x \in G$ be a non-identity element. Let $P_x(G)$ denote the probability that x and a randomly chosen element of G generate G. What can be said about $P_x(G)$? Guralnick, Kantor and Saxl constructed examples where $P_x(G) \to 0$. It is shown in [GKS], [Sh1], [LiSh5], [GLSSh] that, unless G is alternating or a classical group over a field of bounded size (in which case $P_x(G)$ may be bounded away from 1), we have $P_x(G) \to 1$ as $|G| \to \infty$ (regardless of the choices of x). Another interesting result which was just established in [GK] is that $P_x(G)$ is always positive, namely, every non-identity element of a finite simple group sits in some generating pair.

Recently G. Robinson asked if a finite simple group is randomly generated by two conjugate elements. By [Sh2], [LiSh5], [GLSSh] we have:

Theorem 3 (Guralnick-Liebeck-Saxl-Shalev, 1998) *Let G be a finite simple group and let $x, y \in G$ be randomly chosen elements. Then the elements x and $y^{-1}xy$ generate G with probability tending to 1 as $|G| \to \infty$.*

We conclude this section with a remark on profinite groups. A profinite group G has a canonical normalized Haar measure which turns it into a probability space. If, for some positive integer k, G is generated with positive probability by k randomly chosen elements, we say that G is positively finitely generated. The first examples of such groups occurred in the context of field arithmetic, and their research was continued in [KL], [Bh], [M], [MSh], [BPSh]. Positively finitely generated groups have been characterized as profinite groups in which the number of index n maximal subgroups grows polynomially with n [MSh]. However, we are still unable to find a structural characterization of such groups, or even to formulate a reasonable conjecture.

2 The modular group

We now turn to some recent applications of the probabilistic approach. The first concerns the longstanding problem of finding the finite simple quotients of the modular group $\mathrm{PSL}_2(\mathbb{Z})$, namely the finite simple groups that can be generated by two elements of orders 2 and 3 respectively. Groups with this property are termed $(2,3)$-generated. The interest in this problem arose in geometric contexts, namely actions of finite groups on Riemann surfaces. Partial answers were provided throughout this century. For example, Miller showed in 1901 that the alternating groups of degree at least 9 are $(2,3)$-generated. The $(2,3)$-generation problem for $\mathrm{PSL}_2(q)$ was studied by Brahana and Sinkov in the 20s and 30s and was solved by Macbeath in the 60s. Some classical groups with large Lie rank were handled by Tamburini and others. In 1996 Di Martino and Vavilov showed that the simple groups $\mathrm{PSL}_n(q)$ are $(2,3)$-generated provided q is odd and $(n,q) \neq (2,9)$.

The proofs of these and many other results in the field are based on explicit constructions of generators of orders 2 and 3. This approach seems to fail for various families of classical groups, for example those with "intermediate" Lie rank. While some simple groups are not $(2,3)$-generated, the following conjecture was recently posed (see [W]).

Conjecture 3 (Di Martino-Vavilov, Wilson): All finite simple groups of Lie type except some of low rank in characteristic 2 or 3 are quotients of $\mathrm{PSL}_2(\mathbb{Z})$.

In [LiSh2] we address this problem for classical groups, using a probabilistic approach. Let $P_{2,3}(G)$ denote the probability that a random involution and a random element of order 3 generate G.

Theorem 4 (Liebeck-Shalev, 1996): *Let $G \neq \mathrm{PSp}_4(q)$ be a finite simple classical group. Then $P_{2,3}(G) \to 1$ as $|G| \to \infty$. If $G = \mathrm{PSp}_4(p^k)$ $(p \geq 5)$ then $P_{2,3}(G) \to 1/2$ as $|G| \to \infty$.*

This gives rise to the following.

Theorem 5 (Liebeck-Shalev, 1996): *Except for $\mathrm{PSp}_4(2^k)$, $\mathrm{PSp}_4(3^k)$ and finitely many other groups, all finite simple classical groups can be obtained as quotients of $\mathrm{PSL}_2(\mathbb{Z})$.*

The groups $\mathrm{PSp}_4(2^k)$ and $\mathrm{PSp}_4(3^k)$ turn out to be genuine exceptions.

The $(2,3)$-generation problem for exceptional groups of Lie type has just been solved by Lübeck and Malle [LM]. Using character theory (and computer calculations) they show that, except for the Suzuki groups and the group $G_2(2)'$, all simple exceptional groups of Lie type are obtained as quotients of the modular group. Combining this with Theorem 5 we see that Conjecture 3 is now confirmed up to finitely many exceptions.

3 Free groups

It is interesting that results on random generation, and Theorem 1 in particular, can be applied in the study of residual properties of free groups.

Let F_d be the free group on d generators ($d \geq 2$). It is well known that F_d is residually finite, and even residually p for any prime p. The following problem concerning residual properties of free groups was raised by Magnus, and then by Gorchakov and Levchuk.

Magnus problem: is F_d residually X for any infinite collection X of finite simple groups?

In other words, suppose X is an infinite collection of finite simple groups; does it follow that

$$\cap\{N \lhd F_d : F_d/N \in X\} = 1?$$

Since F_d is residually F_2, the question is reduced to the case $d = 2$. Several partial answers were given in the past three decades, and a complete positive solution to the problem was given by T. Weigel in 1993 [We1-We3].

In order to outline our approach to the problem, first note that it suffices to show that for every $1 \neq w = w(u, v) \in F_2$, almost all finite simple groups G have a generating pair x, y such that $w(x, y) \neq 1$. To prove this we establish a stronger result of a probabilistic nature [DPSSh].

Theorem 6 (Dixon-Pyber-Seress-Shalev): *Fix $1 \neq w = w(u, v) \in F_2$. Let G be a finite simple group, and let $x, y \in G$ be randomly chosen elements. Then, as $|G| \to \infty$ we have* $\text{Prob}(\langle x, y\rangle = G \ \wedge \ w(x, y) \neq 1) \to 1$.

The proof of Theorem 6 starts with the following reduction. Applying Theorem 1, we know that $\text{Prob}(\langle x, y\rangle = G) \to 1$. Hence it suffices to prove that the probability that $w(x, y) \neq 1$ tends to 1 as $|G| \to \infty$. The last statement has the advantage that it no longer deals with generating pairs. We just have to show that (as $|G| \to \infty$) most pairs in G^2 do not satisfy a given relation. This can be proved using some algebraic geometry and suitable combinatorial tricks. Recently Pyber developed these ideas further in his study of dense free subgroups of profinite groups.

4 Permutation groups

Several of the recent applications of the probabilistic approach involve permutation groups. Let me start with a counting problem. How many maximal subgroups does the symmetric group S_n have up to conjugacy? In 1989 Babai showed, using the Classification Theorem, that S_n has at most $n^{(1+o(1)) \log^3 n}$ conjugacy classes of maximal subgroups [Ba].

In [LiSh4] this is improved as follows.

Theorem 7 (Liebeck-Shalev, 1996): *S_n has $n/2 + o(n)$ conjugacy classes of maximal subgroups.*

Note that the intransitive subgroups, which have the form $S_k \times S_{n-k}$, already yield $n/2$ classes of maximal subgroups. Therefore Theorem 7 asserts that, in some sense, almost all maximal subgroups of S_n are the obvious intransitive ones.

The methods of [LiSh4] are also relevant in counting all maximal subgroups of S_n. In this context let me mention the following general conjecture.

Conjecture 4 (Wall, 1961): The number of maximal subgroups of a finite group G is less than $|G|$.

This conjecture was confirmed by Wall for soluble groups [Wa]. We show in [LiSh4] that it also holds for symmetric groups of sufficiently large degree.

We now turn to other applications involving permutation groups. Recall that a base for a permutation group is a subset of the permutation domain whose pointwise stabilizer is trivial. Bases play an important role in computational group theory and in estimating orders of primitive permutation groups. The base size $b(G)$ of G is defined as the minimal size of a base for G, and is the subject of several conjectures. We start with

Conjecture 5 (Babai, 1982): There is a function f such that, if $G \leq S_n$ is a primitive group not involving A_d as a section, then $b(G) \leq f(d)$.

See Pyber's excellent survey [P1]. First positive evidence was provided in 1996 by Seress, who showed that $b(G) \leq 4$ for G soluble. Then, in the joint work [GSSh] with Gluck and Seress, we show the following.

Theorem 8 (Gluck-Seress-Shalev, 1998): *Babai's conjecture holds.*

This provides a structural explanation for the celebrated Babai-Cameron-Pálfy theorem, stating that the order of the groups above is polynomial in n [BCP]. The original proof in [GSSh] yields $f(d) = O(d^2)$. A modified proof from [LiSh5] yields $f(d) = O(d)$; this implies the best bounds in the Babai-Cameron-Pálfy theorem, recently obtained by Pyber [P2].

We also settle another base conjecture, posed by Cameron in [Ca].

Conjecture 6 (Cameron, 1990): Let G be an almost simple primitive permutation group. Then $b(G) \leq c$ with known exceptions.

Here c denotes an absolute constant (not depending on G). The exceptions are A_m, S_m acting on subsets or partitions, and subspace actions of classical groups. Conjecture 6 has just been settled in [LiSh5].

Theorem 9 (Liebeck-Shalev, 1998): *Cameron's conjecture holds. Moreover, there is an absolute constant c such that, excluding the prescribed exceptions, almost all c-tuples from the permutation domain form a base for G.*

This establishes a probabilistic version of the conjecture, posed in the paper [CK] by Cameron and Kantor, where the cases $G = A_m, S_m$ are settled.

The following challenging base conjecture is still open [P1].

Conjecture 7 (Pyber, 1993): The base size of a primitive subgroup G of S_n is at most $c \log |G| / \log n$.

5 Hints of proofs

Since a subset X of a group G generates G if and only if it is not contained in any maximal subgroup M of G, the proofs of the results on random generation are intimately related with information concerning the subgroup structure of finite simple groups. More specifically, for a real number s and a finite simple group G, define

$$\zeta_G(s) = \sum_{M \max G} |G : M|^{-s}.$$

Then it is easy to see that the probability that two randomly chosen elements x, y of G do not generate G is bounded above by $\zeta_G(2)$. Hence, to prove Theorem 1 it suffices to show that $\zeta_G(2) \to 0$ as $|G| \to \infty$, which is what we do. Aschbacher's theorem for classical groups (see [A], [KLi]), and its analogs for exceptional groups (see [LiSe1], [LST]), are the main tools in this proof.

The asymptotic behavior of $\zeta_G(s)$ for other values of s is crucial in proving additional results on random generation. For example, the proof of Theorem 4, which involves counting elements of orders 2 and 3 in classical groups and in their maximal subgroups, eventually boils down to estimating $\zeta_G(66/65)$. Once Theorem 4 is proved, it serves as an essential tool in the proofs of other results, such as Theorems 2 and 3

Our results on base size rely on information concerning fixed point ratios for permutation groups. This is a classical field of research which has been very active in the past 120 years or so, since the days of Jordan [J]. Denote the number of fixed points of a permutation x by $\mathrm{fix}(x)$. The basic question is how large $\mathrm{fix}(x)$ can be, assuming x is a non-identity element of a primitive permutation group (satisfying some mild conditions). The main tool in the proof of Cameron's conjecture is the following result from [LiSh5].

Theorem 10 (Liebeck-Shalev, 1998): *There is a constant $\epsilon > 0$ such that if G is an almost simple classical group over a field with q elements with an n-dimensional natural module, and G acts primitively on a set Ω in a non subspace action, then*

(i) $\mathrm{fix}(x)/|\Omega| < |x^G|^{-\epsilon}$ *for all elements $x \in G$ of prime order, and*

(ii) $\mathrm{fix}(x)/|\Omega| < q^{-\epsilon n}$ *for all non-trivial elements $x \in G$.*

Here $|x^G|$ denotes the size of the conjugacy class of x in G. For large n the bound in part (ii) improves the $4/3q$ upper bound of [LS] (which holds with fewer exceptions).

To demonstrate the relevance of Theorem 10 in the context of Cameron's conjecture let G be as above, and let $B(G, k)$ denote the probability that a randomly chosen k-tuple $(\omega_1, \ldots, \omega_k)$ of elements of Ω forms a base for G. Given a permutation $x \in G$, the probability the x fixes a randomly chosen letter $\omega \in \Omega$ is $\mathrm{fix}(x)/|\Omega|$. Hence the probability that x fixes $\omega_1, \ldots, \omega_k$ is $(\mathrm{fix}(x)/|\Omega|)^k$. Now, if $(\omega_1, \ldots, \omega_k)$ is not a base for G, then some element $x \in G$ of prime order fixes $\omega_1, \ldots, \omega_k$. Letting P denote the set of elements of prime order in G, and applying part (i) of Theorem 10, we obtain

$$1 - B(G, k) \leq \sum_{x \in P} (\mathrm{fix}(x)/|\Omega|)^k < \sum_{x \in P} |x^G|^{-k\epsilon}.$$

Invoking information on conjugacy classes in classical groups, one can then show that, with a suitable choice of k, the right hand side of the above inequality tends to 0 as $|G| \to \infty$; therefore $B(G,k) \to 1$.

Theorem 10 has several other applications. For example, it is used in proving Theorem 3 for classical groups. It also reduces the genus conjecture of Thompson and Guralnick (see [GT]) to the case of subspace actions of classical groups.

The interested reader is referred to the more detailed survey [Sh3] and the references therein.

References

[A] M. Aschbacher, On the maximal subgroups of the finite classical groups, *Invent. Math.* 76 (1984), 469-514.

[Ba] L. Babai, The probability of generating the symmetric group, *J. Comb. Th. Ser. A* 52 (1989), 148-153.

[BCP] L. Babai, P.J. Cameron and P.P. Pálfy, On the orders of primitive groups with restricted nonabelian composition factors, *J. Algebra* 79 (1982), 161-168.

[Bh] M. Bhattacharjee, The probability of generating certain profinite groups by two elements, *Israel J. Math.* 86 (1994), 311-320.

[BPSh] A. Borovik, L. Pyber and A. Shalev, Maximal subgroups in finite and profinite groups, *Trans. Amer. Math. Soc.* 348 (1996), 3745-3761.

[Ca] P.J. Cameron, Some open problems on permutation groups, in *Groups, Combinatorics and Geometry* (eds: M.W. Liebeck and J. Saxl), London Math. Soc. Lecture Note Series 165, Cambridge University Press, Cambridge, 1992, 340-350.

[CK] P.J. Cameron and W.M. Kantor, Random permutations: some group-theoretic aspects, *Combinatorics, Probability and Computing* 2 (1993), 257-262.

[D] J.D. Dixon, The probability of generating the symmetric group, *Math. Z.* 110 (1969), 199-205.

[DPSSh] J.D. Dixon, L. Pyber, Á. Seress and A. Shalev, Residual properties of free groups: a probabilistic approach, in preparation.

[ET1] P. Erdős and P. Turán, On some problems of a statistical group theory. I, *Z. Wahrscheinlichkeitstheorie Verw. Gabiete* 4 (1965), 175-186.

[GSSh] D. Gluck, Á. Seress and A. Shalev, Bases for primitive permutation groups and a conjecture of Babai, *J. Algebra* 199 (1998), 367-378.

[GK] R.M. Guralnick and W.M. Kantor, Probabilistic generation of finite simple groups, to appear.

[GKS] R.M. Guralnick, W.M. Kantor and J. Saxl, The probability of generating a classical group, *Comm. in Alg.* 22 (1994), 1395-1402.

[GLSSh] R.M. Guralnick, M.W. Liebeck, J. Saxl and A. Shalev, Random generation of finite simple groups, Preprint, 1998.

[GT] R.M. Guralnick and J.G. Thompson, Finite groups of genus zero, *J. Algebra* 131 (1990), 303-341.

[J] C. Jordan, Théorèmes sur les groupes primitifs, *J. Math. Pures Appl.* 16 (1871), 383-408.

[K] W.M. Kantor, Some topics in asymptotic group theory, in *Groups, Combinatorics and Geometry* (eds: M.W. Liebeck and J. Saxl), London Math. Soc. Lecture Note Series 165, Cambridge University Press, Cambridge, 1992, 403-421.

[KL] W.M. Kantor and A. Lubotzky, The probability of generating a finite classical group, *Geom. Ded.* 36 (1990), 67-87.

[KLi] P.B. Kleidman and M.W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Series 129, Cambridge University Press, 1990.

[LS] M.W. Liebeck and J. Saxl, Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces, *Proc. London Math. Soc.* (3) 63 (1991), 266-314.

[LST] M.W. Liebeck, J. Saxl and D. Testerman, Simple subgroups of large rank in groups of Lie type, *Proc. London Math. Soc.* 72 (1996), 425-457.

[LiSe1] M.W. Liebeck and G.M. Seitz, Maximal subgroups of exceptional groups of Lie type, finite and algebraic, *Geom. Ded.* 35 (1990), 353-387.

[LiSe2] M.W. Liebeck and G.M. Seitz, On the subgroup structure of exceptional groups of Lie type, to appear in *Trans. Amer. Math. Soc.*

[LiSh1] M.W. Liebeck and A. Shalev, The probability of generating a finite simple group, *Geom. Ded.* 56 (1995), 103-113.

[LiSh2] M.W. Liebeck and A. Shalev, Classical groups, probabilistic methods, and the (2,3)-generation problem, *Annals of Math.* 144 (1996), 77-125.

[LiSh3] M.W. Liebeck and A. Shalev, Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky, *J. Algebra* 184 (1996), 31-57.

[LiSh4] M.W. Liebeck and A. Shalev, Maximal subgroups of symmetric groups, *J. Comb. Th. Ser. A* 75 (1996), 341-352.

[LiSh5] M.W. Liebeck and A. Shalev, Permutation groups, simple groups, and probability, submitted.

[LM] F. Lübeck and G. Malle, $(2,3)$-generation of exceptional groups, to appear in *J. London Math. Soc.*

[ŁP] T. Łuczak and L. Pyber, On random generation of the symmetric group, *Combinatorics, Probability and Computing* 2 (1993), 505-512.

[M] A. Mann, Positively finitely generated groups, *Forum Math.* 8 (1996), 429-459.

[MSh] A. Mann and A. Shalev, Simple groups, maximal subgroups, and probabilistic aspects of profinite groups, *Israel. J. Math.* 96 (1997), 449-468 (Amitsur memorial issue).

[P1] L. Pyber, Asymptotic results for permutation groups, in *Groups and Computation* (eds: L. Finkelstein and W.M. Kantor), DIMACS Series on Discrete Math. and Theor. Computer Science 11, AMS 1993, 197-219.

[P2] L. Pyber, Palfy-Wolf type theorems for completely reducible subgroups of $\mathrm{GL}(n, p^a)$, in preparation.

[Sh1] A. Shalev, A theorem on random matrices and some applications, *J. Algebra* 199 (1998), 124-141.

[Sh2] A. Shalev, Random generation of simple groups by two conjugate elements, *Bull. London Math. Soc.* 29 (1997), 571-576.

[Sh3] A. Shalev, Probabilistic group theory, to appear in *Groups '97 - Bath/St Andrews*, London Math. Soc. Lecture Note Series, Cambridge University Press.

[Wa] G.E. Wall, Some applications of the Eulerian function of a finite group, *J. Austral. Math. Soc.* 2 (1961), 35-59.

[We1] T. Weigel, Residual properties of free groups, *J. Algebra* 160 (1993), 16-41.

[We2] T. Weigel, Residual properties of free groups, II, *Comm. Alg.* 20 (1992), 1395-1425.

[We3] T. Weigel, Residual properties of free groups, III, *Israel J. Math.* 77 (1992), 65-81.

[W] J.S. Wilson, Economical generating sets for finite simple groups, in *Groups of Lie type and Their Geometries* (eds: W.M. Kantor and L. Di Martino), London Math. Soc. Lecture Note Series 207, Cambridge University Press, Cambridge, 1995, 289-302.

Aner Shalev
Institute of Mathematics
Hebrew University
Jerusalem 91904, Israel