ICM 1998, Berlin, Aug. 18–27

Abstracts of Plenary and Invited Lectures

Section:

2. Algebra

1991 MS Classification: 20P05, 20D06, 20B15
Shalev, Aner, Hebrew University, Jerusalem, Israel
Simple groups, permutation groups, and probability

In recent years probabilistic methods have proved useful in the solution of several difficult problems concerning finite 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 in order to prove existence theorems; 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 papers by Erdős and Turán in which they study the properties of random permutations. In 1969 Dixon 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 proceeded to conjecture that a similar result holds for arbitrary (nonabelian) finite simple groups. Our first result settles Dixon's conjecture in the affirmative.

Theorem 1 (Liebeck-Shalev, 1995): *Two random elements of a finite simple group G generate G with probability $\to 1$ as $|G| \to \infty$.*

Our work follows important results of Kantor and Lubotzky. Like other results presented below, it applies the Classification of Finite Simple Groups. It is interesting that Theorem 1 can be applied in the study of residual properties of free groups.
We also obtain results on random generation by special pairs of elements.

Theorem 2: (i) (Liebeck-Shalev, 1996) *A finite simple group is almost surely generated by a random involution and a random additional element.*
(ii) (Guralnick-Liebeck-Saxl-Shalev, 1998[1]) *A finite simple group is almost surely generated by a random element and a random conjugate of it.*

Part (i) above settles a conjecture of Kantor and Lubotzky (1990), and part (ii) solves a question of G. Robinson.

[1] work still in preprint form

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. Partial answers were provided throughout this century using explicit constructions. Focusing on classical groups we show that (with some exceptions) almost all pairs of elements of orders 2 and 3 are generating pairs. As a result we deduce the following.

Theorem 3 (Liebeck-Shalev, 1996): *Except* $\mathrm{PSp}_4(2^k)$, $\mathrm{PSp}_4(3^k)$ *and finitely many other groups, all finite simple classical groups can be obtained as a quotient of the modular group.*

The groups $\mathrm{PSp}_4(2^k)$ and $\mathrm{PSp}_4(3^k)$ are genuine exceptions.
Let us now turn to applications which involve 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. In 1981 Babai conjectured that primitive permutation groups with no large alternating sections have small bases. We settle this as follows.

Theorem 4 (Gluck-Seress-Shalev, 1998): *A primitive permutation group not involving A_d has a base of size bounded in terms of d.*

This provides a structural explanation for the celebrated Babai-Cameron-Pálfy theorem, stating that the order of the groups above is polynomial in n. The core of the proof of Theorem 4 is probabilistic.
We also settle another base conjecture, posed by Cameron in 1990.

Theorem 5 (Liebeck-Shalev, 1998[1]) *There is an absolute constant c such that if G is an almost simple primitive permutation group, then G has a base of size at most c, with known exceptions.*

The exceptions are alternating or symmetric groups acting on subsets or partitions, and classical groups in subspace actions. We actually find c such that almost all c-tuples from the permutation domain form a base. The proof involves improvements of previous bounds on minimal degrees of permutation groups, which in turn have some other applications.