Groups, probability and representations

Aner Shalev

My main area of expertise is Group Theory, which is regarded by many as the science of Symmetry. Indeed groups arise naturally in many branches of mathematics as collections of symmetries of various objects (in Geometry, Topology, Number Theory, Combinatorics, and so on).

While Group Theory contributes immensely to many areas of mathematics and natural sciences, it also benefits from other mathematical disciplines, such as Probability, Representation Theory, Lie theory, Algebraic geometry, etc. This interplay between group theory and other mathematical branches is often in the focus of my work.

Probabilistic methods played a major role in settling various open problems and conjectures in finite simple groups, finite groups in general, as well as various infinite groups; these include Dixon's conjecture on generation of finite simple groups by two random elements, the study of finite simple quotients of the modular group, important conjectures regarding the base size of permutation groups stated by Cameron, Babai and Pyber, covering of Riemann surfaces and the genus conjecture of Guralnick and Thompson, problems suggested by Magnus and others on residual properties of some infinite groups, and other fields of research.

In recent years representation theory joined the probabilistic approach as another essential tool in solving longstanding problems such as the Ore conjecture of 1951, stating that every element of a (non-abelian) finite simple group is a commutator, the study of Fuchsian groups, as well as of word maps and Waring type problems, and a related problem of Serre on profinite groups.

Let me describe the latter topic in a bit more detail.

By a *word* we mean a non-trivial element $w = w(x_1, \dots, x_d)$ of the free group F_d on $x_1, \dots, x_d$. Given a word w and a group G we consider the *word map* $w : G^d \to G$ sending $(g_1, \dots, g_d)$ to $w(g_1, \dots, g_d)$. The *image* of the word map, denoted by $w(G)$, has been the focus of extensive study. Other objects of study are the *kernel* of the word map w, i.e., the inverse image of 1, and more generally fibers $w^{-1}(g)$ of the word map (where $g \in G$).

A fundamental result of Borel asserts that word maps on simple algebraic groups are dominant. Since then the theory of word maps was studied by many researchers including Larsen, Liebeck, Nikolov, Segal, Tiep, Guralnick, O'Brien, Bors, myself and others.

Recall that Hilbert's celebrated solution to the classical Waring problem shows that every positive integer is a sum of $g(n)$ nth powers. This is a deep extension of Lagrange's celebrated 4 squares theorem. Analogous problems in group theory have recently garnered much attention. Waring type problems in group theory are attempts to present all group elements as a short product of some special elements (e.g. elements of $w(G)$, of a conjugacy class C of G, etc). It has been shown that if w is any non-trivial word and G is a large enough finite simple group, then every element of G is a product of two values of w.

The distribution of word maps on finite and infinite groups also attracted a lot of attention, leading to recent solutions of various probabilistic Waring type problems. Probabilistic methods and character methods in group theory have proved extremely useful in this and related contexts. In particular, new strong character bounds for finite simple groups were discovered recently, and led to a variety of applications, e.g. to random walks and their mixing times, subgroup growth and representation varieties.

The interdisciplinary approach briefly described here, focusing on the interplay between group theory and other disciplines, has already proved useful and fruitful in tackling major classical problems, and is likely to produce additional progress in the future.