Black Box Groups

A 'black box' is a device or an algorithm which produces (almost) uniformly distributed independent random elements from a finite group X. These elements are usually presented, say, as matrices or permutations, so that we can compare them and decide whether two elements are equal or not, can invert and multiply the elements, etc. In some cases we can determine the orders of elements (this is a computationally easy task for permutations, but might happen to be unfeasible in the case of matrices).

On the basis of this randomised information, how one can guess, within the given bounds for error, the isomorphism type of X? How one can prove that X is isomorphic to a given group?

The black box recognition of finite groups is a practical problem which arises in computational algebra. Assume that we are given two matrices x and y of size, say, 100 by 100 over a finite field. We want to determine the isomorphism type of the group X generated by x and y. The potentially astronomical size of X makes it unthinkable to construct its multiplication table. The only known practical approach to the problem is to study properties (orders, or some reasonable approximations of orders, or eigenvalues) of random products of x and y and guess X from the assembled statistics of properties of individual random elements. It can be shown, for example, that most finite simple groups have very distinctive statistics of orders of elements which allow to tell one group from another.

My lectures will cover the main ideas of the rapidly developing theory of black box groups. I have the intention to avoid very messy technical detail involved in identification of particular groups and concentrate on the conceptual issues of the theory and its surprisingly rich connections with other mathematical disciplines. A few examples will be concerned mostly with the identification of alternating and symmetric groups, where technical complications are minimal and a basic knowledge of algebra will suffice for the understanding of the entire proof.

I will also discuss the current trends in the new emerging area on non-deterministic algorithms for infinite groups.

I plan to cover most (or at least some, depending on the particular interests of the audience) of the following topics.

1. Black box recognition of rational polynomials with generic (that is, alternating or symmetric) Galois groups (an algorithm due to Davenport and Smith; essentially it is a randomised version of van der Waerden's residue algorithm for computation of Galois groups).

2. Constructive recognition of symmetric groups via Goldbach's conjecture (Bratus' and Pak).

3. Construction of black boxes: the Product Replacement Algorithm of Leedham-Green et al. and its (conjectural) conceptual explanation via Kazhdan's Property (T) for the group of automorphisms of the free group (Lubotzky and Pak).

4. Black boxes for centralisers of involutions and the Diakonis-Shashahani non-commutative harmonic analysis on finite groups.

5. Commutative versions of black box groups: the Miller-Rabin primality test in the computational number theory and Simmon's attack on the repeated use of the modulus in the RSA cryptographic protocol.

6. Construction of black boxes for normal subgroups in black box groups and the Andrews-Curtis Conjecture in algebraic topology.

7. Model-theoretic connections: pseudofinite groups.

8. Non-deterministic algorithms on infinite groups:

* Multiplicative measures on the free groups and Flajolet's "Bolzano samplers".

* Measuring rational and algebraic languages.

* The worst case complexity versus "generic complexity".

* A case study: "generic" complexity of the conjugacy problem on amalgamated products of free groups.

* Genetic algorithms in group-theoretic problems.