

Model Theory of Black Box Groups: Guesswork, Computation, Proof

Alexandre V. Borovik
University of Manchester

Leeds Logic Seminar, 25 April 2007

A *black-box group* \mathbf{X} is a device or a procedure which produces random (almost) uniformly distributed and (reasonably) independent elements from an unknown finite group X . These elements are encoded as 0–1 strings of uniform length N ; the black box can also perform in fixed time some operations on group elements: given strings representing $g, h \in G$, it can compute the strings representing $g \cdot h, g^{-1}$ and decide whether $g = h$. Sometimes additional information could be given, for example, the order of a much larger finite group G which contains X as a subgroup. To *recognize* a black box group \mathbf{X} means to determine, in time polynomial in N and within given probability of error, the names of non-abelian composition factors of X and get at least some information about the abelian factors (notice that the abelian case is harder—to recognise $\mathbb{Z}/n\mathbb{Z}$ means to factorise n into primes).

My talk will start by describing the very peculiar place of black box recognition of finite groups (BBR) among currently known probabilistic and deterministic methods in computational algebra. BBR is widely used in practical computations: for example, the classical Miller-Rabin primality test in computational number theory is its special case. Very frequently, BBR solves problems where no alternative method is known. BBR is routinely used for calculation in groups of astronomic size, infinite in every practical sense. Practical implementations of BBR are robust and error-safe.

However, from the theoretical viewpoint, BBR is remarkable for its unprecedented level of structural sophistication; indeed, it provides (practically usable!) *recursive* algorithms for recognition of simple groups which imitate *inductive* proof of the classification of finite simple groups. This is possible only because of a distinctive model-theoretic flavour of BBR: at its core lies probabilistic checking of certain first order formulae, and the computations are done, in effect, in a (infinite) pseudofinite group. BBR works because it does so at the level of elementary equivalence, not isomorphism of groups. This last observation points to an even more surprising aspect of BBR: some its methods happened to work in the classification of simple groups of finite Morley rank.

I will conclude my talk by listing a number of open problems.