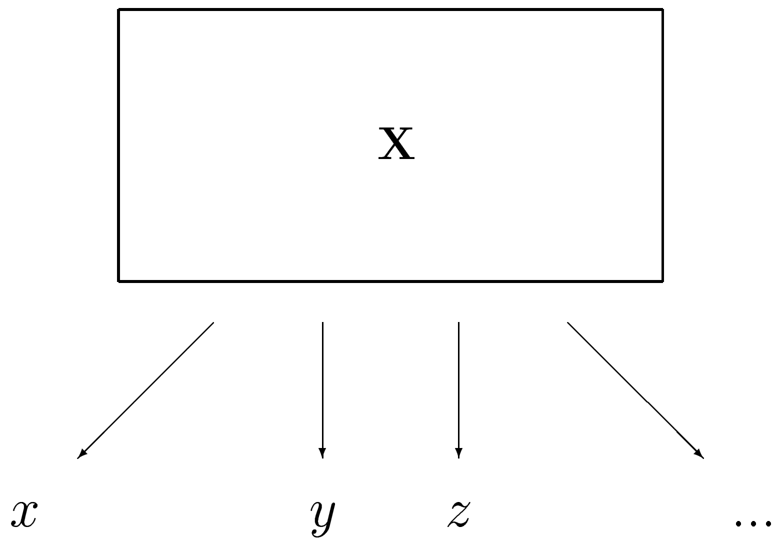
Black Box Groups and other Non-Deterministic Problems of Group Theory

Alexandre Borovik

Lyon, 7 April 2003

Black Box Group

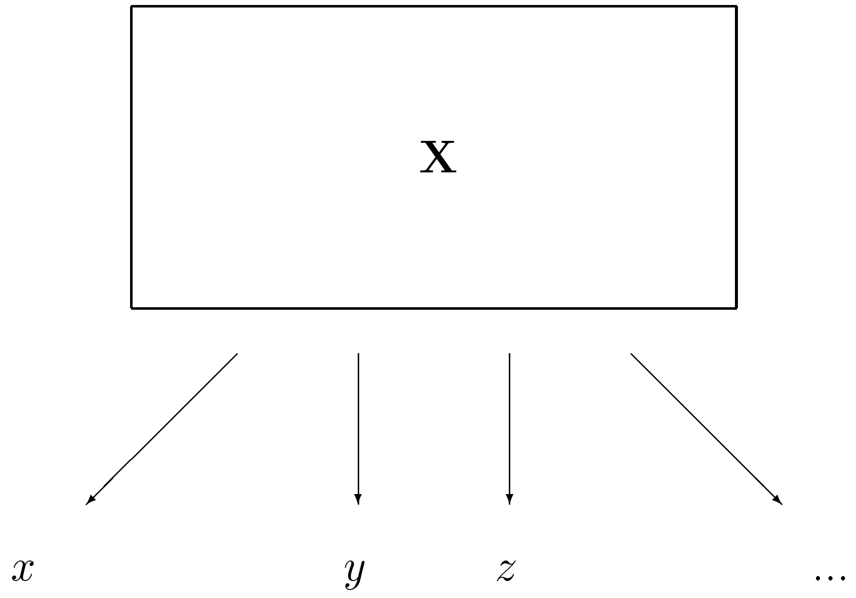


random, independent, uniformly distributed elements random, independent, uniformly distributed elements

given as

- permutations, or
- matrices in $GL_n(q)$,
- $\ldots$

“Format”: $n^2 \log q$



- (sometimes) find orders: $|x|$

Aim: determine $\mathbf{X}$

Recognition of black box is highly technical and uses CFSG.

Two simple examples in my lectures later:

- Recognition of Sym_n and Alt_n as Galois groups (Davenport-Smith)
- Constructive recognition of Sym_n (Bratus'-Pak).

In this talk, I concentrate on a general set-up and realtions to combinatorial group theory

Generation of random elements,

Leedham-Green et al.:

$\Gamma_k(G)$ set of generating k-tuples

graph with edges:

$$(g_1, \ldots, g_i, \ldots, g_k) \longrightarrow (g_1, \ldots, g_j^{\pm 1} g_i, \ldots, g_k)$$

$$(g_1, \ldots, g_i, \ldots, g_k) \longrightarrow (g_1, \ldots, g_i g_j^{\pm 1}, \ldots, g_k)$$

Walk randomly over this graph and choose random g_i.

Random walk on $\Gamma_k(G)$

Pak: For k large, the mixing time is polynomial in $\log |G|$.

Mixing time: number t of steps s.t. after t steps

$$\frac{1}{2} \sum_{v \in \Gamma} \left| P(\text{get at } v) - \frac{1}{\#\Gamma} \right| < \frac{1}{e}$$

Lubotzky–Pak:

If $Aut\, F_k$ satisfies Kazhdan property (T), then mixing time of a random walk on a component of $\Gamma_k(G)$

$$\text{mix} \leqslant C(k) \cdot \log_2 |G|.$$

Kazhdan property (T)

G a topological group, $Q \subset G$ a compact set

$$K = \inf_{\rho} \inf_{v \neq 0} \max_{q \in Q} \frac{\|\rho(q)(v) - v\|}{\|v\|} > 0$$

ρ: all unitary representations without fixed non-zero vectors

Centralisers of involutions in black box groups

Global exponent

Assume that we know a computationally feasible E such that $x^E = 1$ for all $x \in \mathbf{X}$.

Factorise

$$E = 2^l \cdot m \quad , m \text{ odd.}$$

Construction of involutions:

$$\begin{aligned} E &= 2^l \cdot m \quad , m \text{ odd} \\ x &\mapsto x^m, (x^m)^2, \ldots, (x^m)^{2^r} \neq 1, 1 \\ \mathrm{i}(x) &:= (x^m)^{2^r} \quad \text{is an involution} \end{aligned}$$

Involutions in black box groups, commutative case:

Simmons' attack on repeated use of moduli in RSA.

- The key server distributes keysets (n, d, e) with
$$de \equiv 1 \bmod (\phi(n)),$$
reusing n but keeping the factorisation $n = pq$ secret.

- However, the user knows n and $de \equiv 1 \bmod (\phi(n))$

- $E = de$ is a global exponent of $(\mathbb{Z}/n\mathbb{Z})^*$

However, the user can factorise n:

- $(\mathbb{Z}/n\mathbb{Z})^*$ is a black box group of global exponent $E = de$.
- Find an involution $x \neq -1$ in $(\mathbb{Z}/n\mathbb{Z})^*$.
- Since
$$x^2 - 1 \equiv 0 \bmod n,$$
we have
$$n \mid (x-1)(x+1).$$
- Calculation of $\gcd(n, x-1)$ and $\gcd(n, x+1)$ yields a non-trivial factor of n.

Centralisers of involutions:

If t is an involution, we have a map

$$\zeta : \mathbf{X} \longrightarrow C_{\mathbf{X}}(t)$$

$$\begin{aligned}
\zeta_1 : \mathbf{X} &\longrightarrow C_{\mathbf{X}}(t) \\
x &\mapsto (t \cdot t^x)^{(m+1)/2} \cdot x^{-1}, \quad |t \cdot t^x| \text{ odd} \\
\zeta_2 : \mathbf{X} &\longrightarrow C_{\mathbf{X}}(t) \\
x &\mapsto \mathrm{i}(t \cdot t^x), \quad |t \cdot t^x| \text{ even} \\
\zeta &= \zeta_1 \cup \zeta_2
\end{aligned}$$

Cumulative product:

$$\begin{aligned} z &:= 1 \\ z &:= z \cdot \zeta(x) \quad \text{for running} \quad x \in \mathbf{X} \end{aligned}$$

shows a good performance as a black box for $C_{\mathbf{X}}(t)$.

Application [B and Parker-Wilson]:

Computation of $O_p(\mathbf{X})$ for matrix black box groups $\mathbf{X}$ in characteristic $p > 2$.

- For large p, unipotent and non-semisimple elements occur with probability $\sim 1/p$ and are "invisible": a random element is semisimple.
- Computations are essentially done in **pseudofinite** groups.

$\boxed{\text{more on this in my lectures}}$

Why does ζ work?

If $c \in C_{\mathbf{X}}(t)$,

$$\begin{aligned} \zeta_1(cx) &= (tt^{cx})^{(m+1)/2} \cdot x^{-1} \cdot c^{-1} \\ &= (tt^{x})^{(m+1)/2} \cdot x^{-1} \cdot c^{-1} \\ &= \zeta_1(x) \cdot c^{-1} \end{aligned}$$

If $x \in \mathbf{X}$ are uniformly distributed and independent,

then $\zeta_1(x)$ are uniformly distributed and independent in $C_{\mathbf{X}}(t)$

Black box in X generates a black box in $C_{\mathrm{X}}(t)$.

What about involutions $\zeta_2(x)$?

- They generate a normal subgroup in $C_{\mathbf{X}}(t)$.
- What can be said about normal subgroups of black box groups?

Structural theory of black box groups

- If $\mathbf{X}$ is non-simple, how one can find a normal subgroup?

$$\mathbf{X} = \mathbf{X}' \implies \text{there are involutions } t$$

$$\mathbf{Y} \lhd \mathbf{X} \implies \mathbf{Y} \cap C_{\mathbf{X}}(t) \lhd C_{\mathbf{X}}(t)$$

- How one can construct a good black box for the normal closure

$$\left\langle y_1^{\mathbf{X}}, \ldots, y_k^{\mathbf{X}} \right\rangle?$$

Andrews–Curtis graph for $N \lhd G$

$$\Delta_k(G,N) = \left\{(h_1,\ldots,h_k) \mid \langle h_1^G,\ldots,h_k^G\rangle = N\right\}$$

Edges:

$$(x_1,\ldots,x_k) \longrightarrow (x_1,\ldots,x_ix_j,\ldots,x_k),\ i \neq j$$

$$(x_1,\ldots,x_k) \longrightarrow (x_1,\ldots,x_i^{-1},\ldots,x_k)$$

$$(x_1,\ldots,x_k) \longrightarrow (x_1,\ldots,x_i^w,\ldots,x_k),\ w \in G$$

Conjecture. A random walk on $\Delta_k(G,N)$ provides a fast black box for N.

The Andrews-Curtis Conjecture (1965):

$\Delta_k(F_k, F_k)$ is connected

Myasnikov: $\Delta_k(F_k^{(m)}, F_k^{(m)})$ is connected for the free solvable group $F_k^{(m)}$.

Myasnikov & Myasnikov: Some potential counterexamples (originating in topology) are killed by application of **genetic algorithms**, say, in $F = \langle x, y \rangle$,

$$(x^2y^{-3}, xyxy^{-1}x^{-1}y^{-1}) \sim (x, y)$$

(example by Akbulut and Kirbi, 1985).

Genetic Algorithms

A less technical example: solving equations in a free group (Bormotov-Myasnikov and B-Booth).

- An *equation* in variable x over the free group

  $$F_k = \langle a_1, \ldots, a_k \rangle$$

  is a word

  $$w(x, a_1, \ldots, a_k)$$

  from the free product $\langle x \rangle * F_k$.

- $u \in F_k$ is a *solution* if

  $$w(u, a_1, \ldots, a_k) = 1.$$

- *Population* $\{u\}$ is a finite set of approximate solutions.
- *Fitness function* measures the quality of an approximation u.

  In a naive approach, it is the length

  $$l(w(u, a_1, \ldots, a_k))$$

  of the word $w(u)$ after all cancellations.
- **B-Booth**: A population of fitness functions.

Survival of the fittest

- Start with a random population $\{u\}$.
- Aim at finding an element u of fitness 0 (an exact solution).
- *Breeding*: given u, v, their *child* is the concatenation of some beginning segment of u with an end segment of v.
- Fitter individuals participate in breeding more frequently than less fit ones.
- *Mutation:* insertion or deletion random letters a_i at or from random positions.
- Regularly cull less fit individuals.

Playing God. The rules of selection of breeding pairs, deletion unfit individuals, frequencies of mutations are chosen, by trial and error, for better performance of the algorithm.

Playing Darwin. A potential more sophisticated way of fine tuning the evolution:

Run a co-evolution of a population of solutions and population of selection parameters, like a co-evolution of flowers and bees.

B-Booth: An example of convergence of co-evolution to a deterministic algorithm.

It was first discovered that genetic algorithms do solve equations in free groups;

and only later a theoretical explanation started to emerge.

It appears that

the existence of an efficient genetic algorithm for a group theoretic problem

suggests the

existence of a good deterministic algorithm.

Killing counterexamples to Andrews-Curtis: a more technical version of the same idea.

- A genetic version algorithm to Andrews-Curtis is exhausted.
- A counterexample is more likely, but genetic algorithms cannot produce a counterexample.
- Can a counterexample to Andrews-Curtis be found at the level of finite groups?

Finitary AC Conjecture

B, Lubotzky & Myasnikov: In a finite group G, the connected components of $\Delta_k(G, G)$ are those inherited from $G/[G, G]$.

- No easy way to refute the AC conjecture using finite groups.

Let $G = \langle S \rangle$ and $N \lhd G$.

Restricted Andrews–Curtis graph $\overline{\Delta}_k(G, N)$:

the same vertices as in $\Delta_k(G, N)$:

$$\left\{ (h_1, \ldots, h_k) \mid \langle h_1^G, \ldots, h_k^G \rangle = N \right\}.$$

Two vertices are connected by one of the edges:

$$(\ldots, x_i, \ldots, x_j, \ldots) \longrightarrow (\ldots, x_i x_j^{\pm 1}, \ldots,), \; i \neq j$$

$$(\ldots, x_i, \ldots, x_j, \ldots) \longrightarrow (\ldots, x_j^{\pm 1} x_i, \ldots), \; i \neq j$$

$$(\ldots, x_i, \ldots) \longrightarrow (\ldots, x_i^s, \ldots), \; s \in S$$

$$(\ldots, x_i, \ldots) \longrightarrow (\ldots, x_i^{-1}, \ldots).$$

Problem. Are $\overline{\Delta}_k(G, N)$ expanders?

- The **"YES"** answer would explain a good practical performance of the AC algorithm for generation random elements of normal subgroups.
- **Related question:** does the group $AC_k(F_k)$ generated by the (reduced) Andrews-Curtis transformations of the free group F_k has Kazhdan's Property (T)?

What about random elements in infinite groups?

$\boxed{\text{Later in my lectures}}$