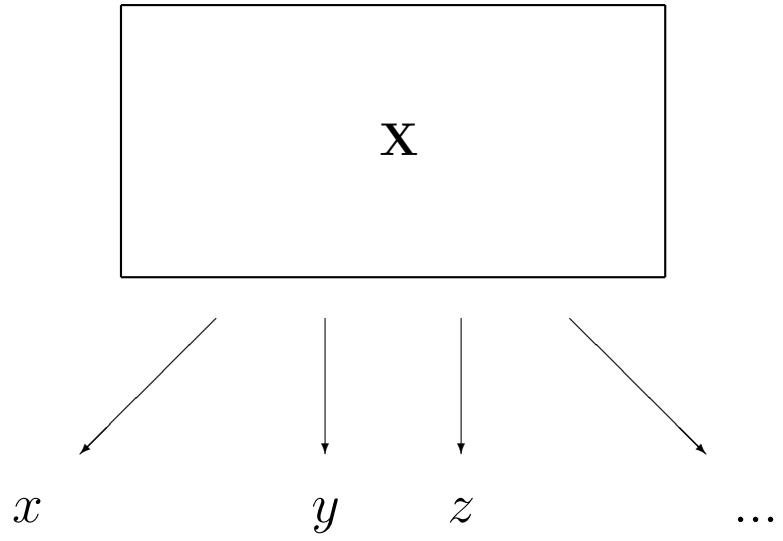
The Andrews-Curtis Conjecture and Finite Groups

Joint work with C. Bates, A. Lubotsky and A. G. Myasnikov

Alexandre Borovik

Newcastle, 29 June 2004

Black Box Group



random, independent, uniformly distributed elements

random, independent, uniformly distributed elements

given as $\Downarrow$

random, independent, uniformly distributed elements

given as

- permutations, ⇓

random, independent, uniformly distributed elements

given as

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

random, independent, uniformly distributed elements

given as

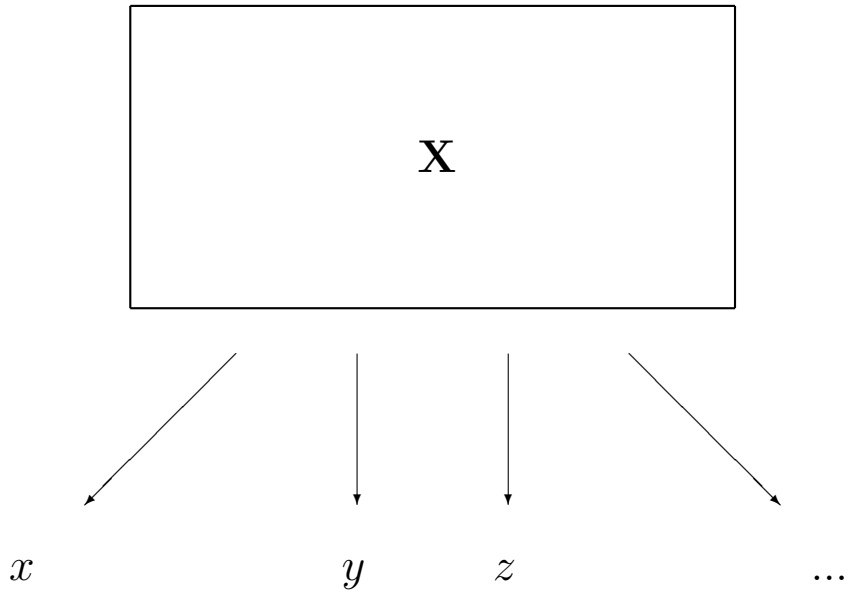
- permutations, or
- matrices in $GL_n(q)$,
- ... $\Downarrow$

random, independent, uniformly distributed elements

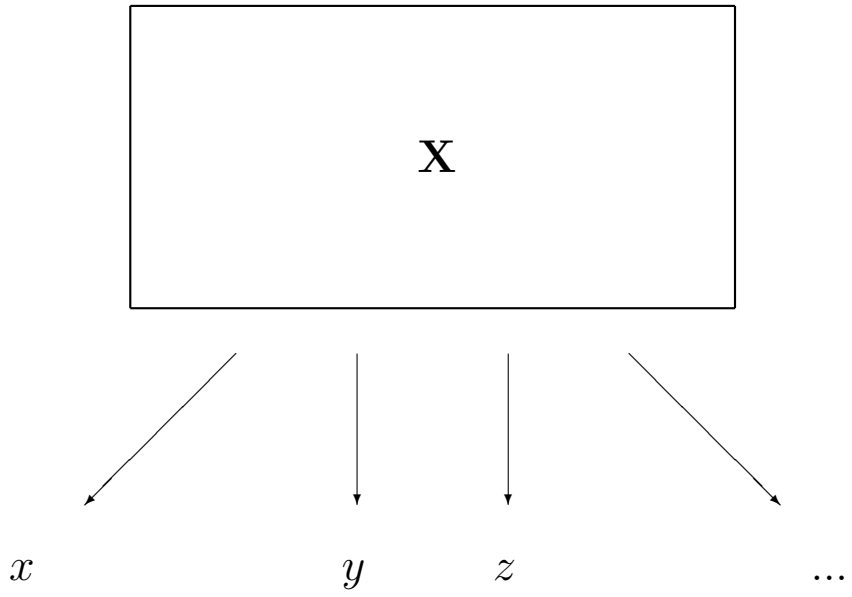
given as

- permutations, or
- matrices in $GL_n(q)$,
- ...

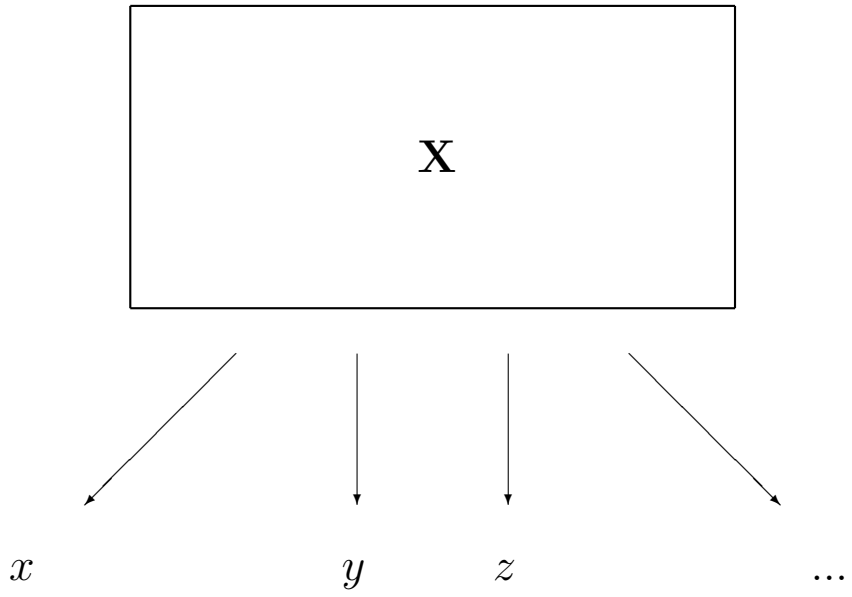
"Format": $n^2 \log q$



- We can compare: $x = y$? $\Downarrow$



- multiply, invert: $x \cdot y, \quad x^{-1}$ $\Downarrow$



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

Aim: determine $\mathbf{X}$

Recognition of black box is highly technical and uses CFSG.

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

Generation of random elements,

Leedham-Green et al.: ⇓

Generation of random elements,

Leedham-Green et al.:

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

graph with edges:

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

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

$\Downarrow$

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 $\log |G|$.

$\Downarrow$

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 $\Gamma_k(G)$

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

$$\Downarrow$$

Lubotzky–Pak:

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

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

Conjecture. For $k \geqslant 4$, $Aut\, F_k$ has (T). $\Downarrow$

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

Structural theory of black box groups

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

Structural theory of black box groups

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

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

$$\Downarrow$$

Structural theory of black box groups

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

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

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

$$\Downarrow$$

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 $N \lhd G$ $\Downarrow$

Andrews–Curtis graph for $N \lhd G$

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

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:

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

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

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

$\Downarrow$

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:

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

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

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

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 $\Downarrow$

The Andrews-Curtis Conjecture (1965):

$\triangle_k(F_k, F_k)$ is connected

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

The Andrews-Curtis Conjecture (1965):

$\triangle_k(F_k, F_k)$ is connected

Myasnikov: $\triangle_k(F_k^{(m)}, F_k^{(m)})$ 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).

Finitary AC Conjecture

- Can a counterexample to Andrews-Curtis be found at the level of finite groups?

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

Finitary AC Conjecture

- Can a counterexample to Andrews-Curtis be found at the level of finite groups?

Theorem (B, Lubotzky & Myasnikov): In a finite group G, the connected components of $\triangle_k(G, G)$ 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? $\Downarrow$

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. $\Downarrow$

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)?

Groups generated by Nielsen moves

G a finite group.

FG_n the free group with n free generators $x_1, \ldots, x_n$ in the variety generated by G.

$\mathrm{NilFree}(G) < \mathrm{Aut}(FG_n)$ is generated by all Nielsen moves

$$\begin{aligned} L_{ij}^{\pm} &: (x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_i, \ldots, x_i^{\pm 1} x_j, \ldots, x_n) \\ R_{ij}^{\pm} &: (x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_i, \ldots, x_j x_i^{\pm 1}, \ldots, x_n) \\ \mathrm{Inv}_k &: (x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_k^{-1}, \ldots, x_n) \end{aligned}$$

$\mathrm{Nil}^{+}\mathrm{Free}(G) = \left\langle L_{ij}^{\pm}, R_{ij}^{\pm} \right\rangle$

K the intersection of the kernels of all surjective homomorphisms $FG_n \longrightarrow G$

$\mathrm{Space}_n(G) = FG_n/K$.

$$\mathrm{NilFree}(G) \longrightarrow \mathrm{Aut}(\mathrm{Space}_n(G));$$

$GL_n(G)$ image of $\mathrm{NilFree}(G)$ in $\mathrm{Aut}(\mathrm{Space}_n(G))$

$SL_n(G)$ image of $\mathrm{Nil}^+\mathrm{Free}(G)$ in $\mathrm{Aut}(\mathrm{Space}_n(G))$

If $G = \mathbb{Z}/p\mathbb{Z}$ then $\mathrm{Space}_n(G) \simeq (\mathbb{Z}/p\mathbb{Z})^n$ and

$$SL_n(G) \simeq SL_n(\mathbb{F}_p).$$

Nielsen moves are transvections.

What can be said about $SL_n(G)$?

- If G is a solvable group, is it true that simple non-abelian composition factors of $SL_n(G)$ are groups $SL_k(p)$ for primes p dividing $|G/[G,G]|$ and appropriate dimensions k?

Non-abelian simple groups G.

$\mathrm{Space}_n(G)$ is the direct product of copies of G:

$$\mathrm{Space}_2(\mathrm{Alt}_5) \simeq \mathrm{Alt}_5^{19}$$

$SL_n(G)$ permutes the copies of G in $\mathrm{Space}_n(G)$.

A computer-friendly way to find the action (for small G).

- $\mathcal{G}_k(G)$ is the set of all k-tuples of elements of G which generate G.
- $\mathcal{H}_k(G)$ is the factor set of $\mathcal{G}_k(G)$ under the action of $\mathrm{Aut}(G)$.
- The Nielsen moves act on $\mathcal{H}_k(G)$ and generate a subgroup of $\mathrm{Sym}(\mathcal{H}_k(G))$; we denote it $\mathrm{Nie}_k(G)$.

Conjecture The restriction of $\mathrm{Nie}_k(G)$ to an orbit on $\mathcal{H}_k$ is the full symmetric or alternating group on this orbit.

Some experimental results (Chris Bates)

$\mathbf{Alt_5}$, rank 2

$|\mathrm{Alt}_5| = 60$

$H = \mathrm{Nie}_2(\mathrm{Alt}_5)$ acts on $\Omega = \mathcal{H}_2(\mathrm{Alt}_5)$ of cardinality 19.

Two orbits, of size 9 and 10.

The restrictions of H are Alt_9 and Sym_{10}.

$\mathbf{Alt_5}$, rank 3

$|\mathrm{Alt}_5| = 60$

The group $H = \mathrm{Nie}_3(\mathrm{Alt}_5)$ acts on $\Omega = \mathcal{H}_3(\mathrm{Alt}_5)$ of cardinality 1668 **transitively**

and is in fact isomorphic to Alt_{1668}.

$\mathbf{Alt_6}$, rank 2

$|\mathrm{Alt}_6| = 360$

$H = \mathrm{Nie}_2(\mathrm{Alt}_6)$ acts on $\Omega = \mathcal{H}_2(\mathrm{Alt}_6)$ of cardinality 53.

Four orbits of size 10, 12, 15 and 16.

The restrictions are Sym_{10}, Sym_{12}, Sym_{15} and Alt_{16}.

$\mathbf{L_3(2)}$, rank 2

$|L_3(2)| = 168$.

$H = \mathrm{Nie}_2(L_3(2))$ acts on $\Omega = \mathcal{H}_2(L_3(2))$ of cardinality 57.

Four orbits of size 7, 16, 16 and 18.

The restrictions of H are Sym_7, Alt_{16}, Alt_{16} and Sym_{18}.

S$L_2(8)$, **rank** 2

$H = \mathrm{Nie}_2(L_2(8))$ acts on $\Omega = \mathcal{H}_2(L_2(8))$ of cardinality 142.

Three orbits of size 18, 54, and 70.

The restrictions of H are Sym_{18}, Sym_{54} and Sym_{70}.

If G is simple, any tuple in

$$\Omega = G \times \cdots \times G \setminus \{(1, \ldots, 1)\}$$

generates G as a normal subgroup.

Conjecture

- The Andrews-Curtis moves generate the full symmetric or alternating group on Ω.

Root and parabolic subgroups

With every root $\rho = \epsilon_i - \epsilon_j$ of the root system

$$\Phi_{A_{n-1}} = \{\, \epsilon_i - \epsilon_j \mid i, j = 1, \ldots, n,\ i \neq j \,\}$$

of type A_{n-1} one can associate the *root subgroup*

$$U_\rho(G) = U_{ij}(G) = \left\langle L^{\pm}_{i,j}, R^{\pm}_{i,j} \right\rangle$$

$$U_{ij}(G) \simeq G \circ G$$

(central product of two copies of G).

$U_{ij}(\mathbb{Z}/p\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}$, in agreement with the standard notation for linear algebraic groups.

Unitriangular and triangular subgroups

$$\begin{aligned} UT_n^+(G) &= \langle\, U_{ij}(G) \mid i < j \,\rangle \\ &= \left\langle L_{ij}^{\pm}, R_{ij}^{\pm} \mid i < j \right\rangle \\ T_n^+(G) &= \left\langle L_{ij}^{\pm}, R_{ij}^{\pm}, \mathrm{Inv}_k \mid i < j \right\rangle \end{aligned}$$

- What is the intersection of **opposite** triangular subgroups

$$T_n^+(G) \cap T_n^-(G)?$$

Diagonal subgroup

For $g \in G$,

$$D_k(g) : (g_1, \ldots, g_n) \mapsto (g_1, \ldots, g_k^g, \ldots, g_n)$$
$$\mathrm{Inv}_k : (g_1, \ldots, g_n) \mapsto (g_1, \ldots, g_k^{-1}, \ldots, g_n)$$

$$\mathrm{Diag}_n(G) = \langle \mathrm{Inv}_k, D_k(g) \mid g \in G \rangle$$

The Andrews-Curtis group

$$AC_n(G) = \langle \mathrm{NielFree}_n(G), \mathrm{Diag}_n(G) \rangle$$

acts on $\Delta_n(G, G)$

Weyl group

$W = \mathrm{Sym}_n$ acting by permutation of components in $(g_1, \ldots, g_n)$.

Borel subgroup

$$B = B_n(G) = \langle UT_n(G), \mathrm{Diag}_n(G) \rangle$$

Monomial subgroup

$$N = \langle \mathrm{Diag}_n(G), W \rangle$$

(B, N) looks like a formal "non-commutative" analogue of a BN-pair in $AC_n(G)$.