The Andrews-Curtis Conjecture and Black Box Groups

Alexandre V. Borovik* Evgenii I. Khukhro†
Alexei G. Myasnikov‡

31 October 2001

Primary 20E05, secondary 60B15

Abstract

The paper discusses the Andrews-Curtis graph $\Delta_k(G, N)$ of a normal subgroup N in a group G. The vertices of the graph are k-tuples of elements in N which generate N as a normal subgroup; two vertices are connected if one them can be obtained from another by certain elementary transformations. This object appears naturally in the theory of black box finite groups and in the Andrews-Curtis conjecture in algebraic topology [3].

We suggest an approach to the Andrews-Curtis conjecture based on the study of Andrews-Curtis graphs of finite groups, discuss properties of Andrews-Curtis graphs of some classes of finite groups and results of computer experiments with generation of random elements of finite groups by random walks on their Andrews-Curtis graphs.

1 Introduction

The concept of a *black box group* is a formalisation of a probabilistic approach to computational problems of finite group theory. For example, given two square matrices x and y of size, say, 100 by 100 over a finite field, it is unrealistic to list all elements in the group X generated by x and y and determine the isomorphism class of X by inspection. But this can often be done, with an arbitrarily small probability of error, by treating X as a black box group, that

*Supported by the Royal Society The Leverhulme Trust Senior Research Fellowship.

†Supported by the Russian Foundation for Basic Research, grant no. 99-01-00576, and by a grant of Russian Ministry for Education in fundamental research no. E00-1.0-77.

‡Partially supported by LMS Scheme 4 grant 4523 and by NSF grant DMS-9973233

is, by studying a sample of random products of the generators x and y. The explosive growth of the theory of black box groups in recent years is reflected in numerous publications (see, for example, the survey paper [25] on the computational matrix group project) and the fundamental work [23]), and algorithms implemented in the software packages GAP [19] and MAGMA [10]. A critical discussion of the concept of black box group can be found in [6], while [7] contains a detailed survey of the subject.

In this paper, we look at the problem of generating random elements from a normal subgroup of the black box groups. The underlying structure, a version of the product replacement graph, has rather unexpectedly happened to be the Andrews–Curtis graph which appears in a certain group-theoretic problem of algebraic topology.

We set the scene in Section 2 where we briefly survey the known results about the product replacement algorithm, and in Section 3, where we introduce the Andrews–Curtis graph. If G is a group (not necessary finite) and $N \lhd G$, then the *Andrews–Curtis graph* $\Delta_k(G, N)$ is the graph whose vertices are k-tuples of elements in N which generate N as a normal subgroup:

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

Two vertices are connected by an edge if one of them is obtained from another by one of the moves:

$$\begin{aligned}
(x_1, \dots, x_i, \dots, x_j, \dots, x_k) &\longrightarrow (x_1, \dots, x_i x_j^{\pm 1}, \dots, x_k),\ i \neq j \\
(x_1, \dots, x_i, \dots, x_j, \dots, x_k) &\longrightarrow (x_1, \dots, x_j^{\pm 1} x_i, \dots, x_k),\ i \neq j \\
(x_1, \dots, x_i, \dots, x_k) &\longrightarrow (x_1, \dots, x_i^w, \dots, x_k),\ w \in G \\
(x_1, \dots, x_i, \dots, x_k) &\longrightarrow (x_1, \dots, x_i^{-1}, \dots, x_k).
\end{aligned}$$

The well-known Andrews–Curtis Conjecture provides the main source of motivation for the paper:

> *For a free group F_k of rank $k \geqslant 2$, the Andrews–Curtis graph $\Delta_k(F_k, F_k)$ is connected.*

The main goal of the paper is to suggest a possible approach to construction of a counterexample to the Andrews–Curtis conjecture using finite groups (Section 6). To that end, we need a good understanding of the Andrews–Curtis graphs of finite groups. In Section 5.2, we derive bounds for the diameters of the Andrews-Curtis graphs $\Delta_k(G, G)$ of finite simple groups G. Section 5.4 contains a detailed study of the Andrews-Curtis graphs of finite soluble groups. In particular, we give a fairly complete description of the connected components of the graphs $\Delta_k(G, G)$ for finite nilpotent and soluble groups G (Theorems 5.14 and 5.12).

In Section 4 we return to the black box group setting and use random walks on $\Delta_k(G, N)$ for generating pseudorandom elements of a normal subgroup N of a black box group G and discuss the practical performance of our algorithm. The Andrews-Curtis graph has the following apparent advantages over the commonly used product replacements graph $\Gamma_k(N)$ (it described in Section 2). The fact that the diameter $\operatorname{diam}(\Delta_k(G, N))$ is much smaller than that of $\Gamma_k(N)$ suggests the possibility that the mixing time of a random walk on $\Delta_k(G, N)$ is smaller than the mixing time of a random walk on $\Gamma_k(N)$. The vertices of $\Delta_k(G, N)$ are all tuples in $N^k \setminus (1, \dots, 1)$, hence the sample of elements of N obtained by taking random components of random generating tuples (vertices) in $\Delta_k(G, N)$ is not biased.

2 The Product Replacement Algorithm

2.1 A brief survey

A problem which we immediately encounter when dealing with black box groups is how to construct a good black box for the subgroup generated by given elements. For example, given a group generated by a collection of matrices,

$$\begin{aligned} X &\leqslant GL_N(\mathbb{F}_q), \\ X &= \langle x_1, \dots, x_k \rangle \end{aligned}$$

how can we produce (almost) uniformly distributed independent random elements from X? The commonly used solution is the *product replacement algorithm* (PRA) [13].

Denote by $\Gamma_k(X)$ the graph whose vertices are generating k-tuples of elements in X and edges are given by the following *Nielsen transformations* [30]:

$$\begin{aligned} (x_1, \dots, x_i, \dots, x_k) &\longrightarrow (x_1, \dots, x_j^{\pm 1} x_i, \dots, x_k) \\ (x_1, \dots, x_i, \dots, x_k) &\longrightarrow (x_1, \dots, x_i x_j^{\pm 1}, \dots, x_k), \end{aligned}$$

where $i \neq j$. Sometimes it is more convenient to consider the extended graph $\tilde{\Gamma}_k(X)$ which has extra edges corresponding to the transformations

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

The recipe for production of random elements from X is deceptively simple: walk randomly over this graph and select random components x_i. The detailed discussion of theoretical aspects of this algorithm can be found in Igor Pak's survey [35]. Pak [36] has also shown that, if k is sufficiently big, the mixing time for a random walk on $\Gamma_k(X)$ is polynomial in k and $\log |X|$. Here, *mixing*

time t_{mix} for a random walk on a graph Γ is the minimal number of steps such that after these steps

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

At the intuitive level, this means that the distribution of the end points of random walks on Γ is sufficiently close to the uniform distribution.

The graph $\Gamma_k(X)$ is still a very mysterious object. Notice, in particular, that, in general, the graph $\Gamma_k(G)$ is not connected. However, an elementary argument, due to Babai, shows that $\Gamma_k(G)$ is connected for $k > 2\log_2|G|$. In that case the diameter $d(\Gamma_k(G))$ can be bounded as

$$d(\Gamma_k(G)) < C\cdot\log^2|G|.$$

The following very natural question is still open.

Conjecture 1 *If G is a finite simple group, the graph $\Gamma_k(G)$ is connected for $k \geqslant 3$.*

Observe, that if we denote by $d(G)$ the minimal number of generators for G, then for *every finitely generated group* G and every $k \geq d(G)+1$ the graph $\tilde{\Gamma}_k(G)$ is connected if and only if the graph $\Gamma_k(G)$ is connected ([35]).

A conceptual explanation of the good properties of the product replacement algorithm is provided by the remarkable observation by Lubotzky and Pak.

Fact 2.1 (Lubotzky and Pak [29]) *If* $\operatorname{Aut}F_k$ *satisfies Kazhdan property* (T)*, then mixing time* t_{mix} *of a random walk on a component of* $\Gamma_k(G)$ *is bounded as*

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

Thus the issue is reduced to the long standing conjecture:

Conjecture 2 *For $k \geqslant 4$,* $\operatorname{Aut}F_k$ *has* (T).

Following [24], we say that a topological group G satisfies the Kazhdan (T)-property if, for some compact set $Q \subset G$,

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

where ρ runs over all unitary representations of G without fixed non-zero vectors. In our context, $\operatorname{Aut}F_k$ is endowed with the discreet topology.

Summarizing our brief discussion of PRA it worthwhile to mention here that despite on computer experiments which show a good overall performance of PRA still there are two major theoretical obstacles when running PRA:

(O1) Non-connectivity of the graph $\Gamma_k(G)$;

(O2) The bias in the output of PRA.

It appears that the both obstacles can be removed by taking k large enough [35]. But then this increases the size of the generating set thus affecting the performance of PRA.

2.2 Normal subgroups of black box groups

Assume that we know that some elements $y_1, \dots, y_k$ of a black box group X belong to a proper normal subgroup of X.

Question 3 *How one can construct a good black box for the normal closure*

$$Y = \langle y_1^X, \dots, y_k^X \rangle ?$$

One possibility is to run a random walk on the Cayley graph for Y with respect to the union of the conjugacy classes

$$y_1^X \cup \dots \cup y_k^X$$

as the generating set for Y.

Notice, that if we know that Y is a simple group then a deep result by Liebeck and Shalev [28, Corollary 1.14] asserts that, for a finite simple group G and a conjugacy class $C \subset G$, the mixing time of the random walk on the Cayley graph $\mathsf{Cayley}(G, C)$ is at most $c \log^3 |G| / \log^2 |C|$.

There are two remarks in order here:

- As numerous experiments showed, in general, PRA performs much better then any standard random walk on a Cayley graph of the subgroup N ([35]);
- Even though the mixing time of the PRA is polynomial (in cardinality of the generating set and $\log_2 |Y|$), it is not a priori clear how many random elements y_i^x one has to take to form a generating set of Y.

These observations (not to mention the general obstacles (O1) and (O2)) encourage one to look for other methods for constructing black box generator for normal subgroups of black box groups. In the next section we wish to discuss a modification of a product replacement algorithm whose practical performance as a black box generator for normal subgroups is better than a random walk or PRA with respect to the generating set $y_1^X \cup \dots \cup y_k^X$.

3 Andrews–Curtis graphs

Let G be a group and $N \lhd G$. Denote by $V_k(G, N)$ the set of all k-tuples of elements in N which generate N as a normal subgroup of G:

$$V_k(G, N) = \left\{ (h_1, \dots, h_k) \in G^k \mid \langle h_1^G, \dots, h_k^G \rangle = N \right\}.$$

Of course, if the group N is simple then $V_k(G,N) = N^k \setminus \{(1,\dots,1)\}$.

We define the *Andrews–Curtis graph* (or *AC-graph*) $\Delta_k(G,N)$ as the graph with the set of vertices $V_k(G,N)$ and such that two vertices are connected by an edge if one of them is obtained from another by one of the following moves (*elementary Andrews–Curtis transformations*, or *AC-transformations*):

$$(x_1,\dots,x_i,\dots,x_k) \longrightarrow (x_1,\dots,x_i x_j^{\pm 1},\dots,x_k),\ i \neq j,$$

$$(x_1,\dots,x_i,\dots,x_k) \longrightarrow (x_1,\dots,x_j^{\pm 1} x_i,\dots,x_k),\ i \neq j,$$

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

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

Notice that the moves are invertible and thus give rise to a non-oriented graph.

Sometimes it is convenient to consider a modification of the graph $\Delta_k(G,N)$. Namely, if A is a given finite set of generators for G then the graph $\bar{\Delta}_k(G,N,A)$ has the same set of vertices $V_k(G,N)$ which are connected by the same edges as above, provided only that $w \in A$. In this case, the number of edges adjacent to a given vertex is finite (even if the group G is infinite).

Observe also, that if the group G is abelian then $\Delta_k(G,N) = \tilde{\Gamma}_k(N)$. Moreover, if $Ab(G)$ is abelianization of G, i.e., $Ab(G) = G/[G,G]$, then the canonical epimorphism $G \to Ab(G)$ induces an adjacency-preserving map of graphs

$$\Delta_k(G,N) \to \tilde{\Gamma}_k(Ab(G)).$$

The name and initial motivation to study graphs $\Delta_k(G,G)$ comes from the Andrews-Curtis Conjecture (1965) (AC-conjecture):

Conjecture 4 (Andrews and Curtis [3]) *For $k \geqslant 2$, the Andrews–Curtis graph $\Delta_k(F_k,F_k)$ is connected.*

Obviously, for every group G the graph $\Delta_k(G,G)$ is connected if and only if the graph $\bar{\Delta}_k(G,G,S)$ is connected for some (or any) generating set S of G.

There is an extensive literature on the subject, see for example, [2, 12, 22]. Still virtually nothing is known about the properties of the Andrews–Curtis graph for free groups. Some potential counterexamples to the AC-conjecture (originated in group theory and topology) were recently killed by application of *genetic algorithms* [32], [33]. But the most formidable stand untouched.

One of the possible approaches to the AC-conjecture is based on the study of Andrews-Curtis graphs of quotients of F_k which are "close" to F_k. This is one of the few known positive results on connectivity of Andrews-Curtis graphs of relatively-free groups:

Fact 3.1 (A. G. Myasnikov [31]) *For the free soluble group $F_n^{(m)}$ of class m and all $k \geqslant n$, the Andrews–Curtis graph $\Delta_k(F_n^{(m)}, F_n^{(m)})$ is connected.*

In Section 6 we suggest a possible line of attack at this problem which involves the study of the Andrews–Curtis graphs $\Delta_k(G, G)$ for finite groups G.

4 Random walks on Andrews–Curtis graphs

4.1 AC-replacement algorithm

In this section we discuss random walks on $\Delta_k(G, N)$ as an alternative approach to black box generators of elements from a normal subgroup N of a group G.

Let G be a finite group and $N \lhd G$. If the graph $\Delta_k(G, N)$ is connected then a nearest neighbour random walk on this graph is an irreducible aperiodic Markov chain. Hence by Perron-Frobenius theory it has uniform equilibrium distribution.

This suggest the following modification of the PRA which we call AC-replacement algorithm ($ACR_k(G, N)$): run a nearest neighbour random walk on $\Delta_k(G, N)$ for t steps and return a random component of the tuple in the stopping state.

Conjecture 5 *Let G be a black box group and $N \lhd G$. The AC-replacement algorithm $ACR_k(G, N)$ provides a 'good' black box for N (at least for some k).*

In practice, a modification of the process, when the the last changed component of the generating tuple (say, $x_i x_j^{\pm 1}$) is multiplied into the cumulative product x, appears to be more effective:

- Initialise $x := 1$.
- Repeat
  - Select random $i \neq j$ in $\{ 1, \dots, k \}$.
  - * With equal probabilities, replace $x_i := x_i x_j^{\pm 1}$ or $x_i := x_j^{\pm 1} x_i$, or
    * produce random $w \in G$ and replace
    $$x_i := x_i (x_j^w)^{\pm 1} \text{ or } x_i := (x_j^w)^{\pm 1} x_i.$$
  - Multiply x_i into x:
    $$x := x \cdot x_i.$$
- Use x as the running output of a black box for N.

Using results on Markov chains, Leedham-Green and O'Brien [26] had shown that the distribution of the values of the cumulative product A converges exponentially to the uniform distribution on N. However, the issue of explicit estimates is open and represents a formidable problem.

In the next section we report on some computer experiments which support the conjecture above.

4.2 Generation of random elements in simple normal subgroups: computer experiments

Here we give a brief discussion of some computer experiments related to the normal subgroups of black box groups.

We run only a limited number of experiments, concentrating on the generation of the alternating group Alt_n as a normal subgroup of Sym_n by very short elements, for example, by the involution (12)(34) or by a 3-cycle (123). The two series of experiments were run, correspondingly, by the first author in GAP [19] and by Alexei D. Myasnikov (City College, New York) using bespoke C++ code. We looked at the distribution of numbers of cycles in the random permutation produced by

- the random walk on the Andrews-Curtis graph $\Delta_k(\mathrm{Sym}_n, \mathrm{Alt}_n)$,
- by the standard product replacement algorithm,
- and by a random walk on the Cayley graph $\mathsf{Cayley}(\mathrm{Alt}_n, x^{\mathrm{Sym}_n})$.

This particular criterion was chosen because of the importance of permutations with small number of cycles in black box recognition algorithms for symmetric groups [11].

We used in our experiments the AC-replacement algorithm (ACR) with and without the cumulative product, as described in Section 3.

Our experiments with alternating groups of degrees varying from 10 to 100 have shown that when the generator is "small", a very good convergence of the sample distribution to the uniform distribution was achieved after $k \cdot n \cdot [\log_2 n]$ steps of the algorithm, even if we worked with a very short generating tuple, $k = 2$, 3 or 5.

The degree of convergence was measured by comparing the distribution of the numbers of cycles in the cycle decomposition of a permutation x produced by the AC-replacement algorithm with the theoretical distribution (easily computable from the Stirling numbers of the first kind), and also by comparing the distribution of the values 1^x with the uniform distribution on the set $\{1, \dots, n\}$. In both cases we used the χ^2 criterion with the significance level 95%.

The performance of the ACR algorithm was, as a rule, better than a random walk on the Cayley graph with respect to a conjugacy class of the generator.

Also, the use of the cumulative product significantly improved performance of the algorithm.

The standard product replacement algorithm has shown a very good performance when the generating tuple was sufficiently long, or when the initial generating tuple $(g_1, \dots, g_k)$ was chosen at random.

However, the ACR algorithm has shown robustness with respect to choice of very small generators. This property is valuable in certain applications, when

one should expect to deal with the initial generating tuple which is not representative of the 'average' elements of the normal subgroup. For example, computations with centralizers of involutions of the type done in [1, 9] require computation of normal subgroups generated by involutions.

A discussion of similar experiments can be found in [8].

5 Andrews–Curtis graphs of finite groups

5.1 General bounds

We show here that if k is large enough then the AC-graph $\Delta_k(G, G)$ of a finite group G is connected. The proof is easy and similar to the analogous result for the graph $\Gamma_k(G)$ (though estimates are better).

Let $nd(G)$ be the minimal number of elements needed to generate G as a normal subgroup. Let $nd_m(G)$ be the maximal size of a minimal set of normal generators of G (Y is a minimal set of normal generators for G if $\langle Y^G\rangle = G$, but $\langle Y_0^G\rangle \neq G$ for every proper subset Y_0 of Y).

Proposition 5.1 *Let G be a finite group G. If $k \geq nd(G) + nd_m(G)$ then the graph $\Delta_k(G, G)$ is connected.*

Proof. Let $n = nd(G)$, $n_m = nd_m(G)$, and $k \geq n + n_m$. Denote by $V_t(G)$ the set of all t-tuples which generate G as a normal subgroup. Fix a tuple $h = (h_1, \ldots, h_n) \in V_n(G)$. Then k-tuple $h(k) = (h_1, \ldots, h_n, 1, \ldots, 1)$ is in $V_k(G)$. Now if $g = (g_1, \ldots, g_k) \in V_k(G)$, then there are n_m components of g, say $g_{n+1}, \ldots, g_k$, such that $(g_{n+1}, \ldots, g_k) \in V_{n_m}(G)$. It follows, that g is connected in $\Delta_k(G, G)$ to $(h_1, \ldots, h_n, g_{n+1}, \ldots, g_k)$. Obviously, the latter one is connected to $h(k)$. Hence any tuple $g \in V_k(G)$ is connected in $\Delta_k(G, G)$ to $h(k)$, so the whole graph is connected. □

5.2 Andrews–Curtis graphs of finite simple groups

In this section we give good and easy estimates (modulo known hard results) of diameters of AC-graphs of finite simple groups.

Theorem 5.2 *If G is a finite simple group and $k \geqslant 2$ then the graph $\Delta_k(G, G)$ is connected and*

$$\operatorname{diam}\left(\Delta_k(G, G)\right) < c \cdot k \cdot \log |G|$$

for some constant c.

This is a very crude estimate; the proof of the theorem contains many possible directions for improvement, see Proposition 5.3 below.

Proof. If G is a finite simple group, then the *covering number* $\mathrm{cn}(G)$ is defined as

$$\mathrm{cn}(G) = \min\{\, n \mid C^n = G \text{ for every conjugacy class } C \subset G \,\}.$$

The *Ore constant* $\mathrm{or}(G)$ is defined as

$$\mathrm{or}(G) = \min\{\, n \mid C^n = G \text{ for some conjugacy class } C \subset G \,\}.$$

The prominent Ore-Thompson Conjecture asserts that $\mathrm{or}(G) = 2$ for all finite simple groups G.

The theorem follows from a simpler proposition.

Proposition 5.3 *If G is a finite simple group and $k \geqslant 2$ then $\Delta_k(G, G)$ is connected and*

$$\mathrm{diam}\,(\Delta(G, G)) \leqslant 4(k \cdot \mathrm{or}(G) + \mathrm{cn}(G)).$$

Proof of Proposition 5.3. Set $d = \mathrm{or}(G)$. Let $\mathsf{x} = (x_1, 1, \dots, 1)$ be a vertex in $\Delta_k(G, G)$ with x_1 chosen from the conjugacy class C such that $C^d = G$. We shall prove that x can be connected to an arbitrary vertex $\mathsf{y} = (y_1, \dots, y_k)$ of $\Delta_k(G, G)$.

Indeed, since $y_i = x_1^{w_1} \cdots x_1^{w_d}$ for some $w_j \in G$, we get, after application to the tuple $(x_1, \dots, x_k)$ of $d(k-1)$ pairs of moves of the form (below $w_0 = 1$):

$$\begin{aligned} (z_1, \dots, z_k) &\longrightarrow (z_1^{w_{i-1}^{-1} w_i}, z_2, \dots, z_k),\ i = 1, 2, \dots, d \\ (z_1, \dots, z_k) &\longrightarrow (z_1, \dots, z_i z_1, \dots, z_k) \end{aligned}$$

the tuple $(x_1^w, y_2, \dots, y_k)$. If one of the y_i, $i = 2, \dots, k$, is not the identity, we can write $x_1^{-w} y_1$ as the product $x_1^{-w} y_1 = y_i^{v_1} \cdots y_i^{v_e}$ for $e \leqslant \mathrm{cn}(G)$, and get the tuple y after e pairs of moves of the form (below $v_0 = 1$):

$$\begin{aligned} (z_1, \dots, z_k) &\longrightarrow (z_1, \dots, z_i^{v_{j-1}^{-1} v_j}, \dots, z_k),\ j = 1, 2, \dots, e \\ (z_1, \dots, z_k) &\longrightarrow (z_1 z_i, z_2, \dots, z_k) \end{aligned}$$

and the correction

$$(z_1, \dots, z_k) \longrightarrow (z_1, \dots, z_i^{v_e^{-1}}, \dots, z_k).$$

If, however, all $y_i = 1$, $i = 2, \dots, k$, then $y_1 \neq 1$. Arguing as before, $2d + 1$ moves will suffice to make $(x_1, x_1^{-1} y_1, y_3, \dots, y_k) = (x_1, x_1^{-1} y_1, 1, \dots, 1)$ from $(x_1, 1, \dots, 1)$, one extra move to make $(y_1, x_1^{-1} y_1, y_3, \dots, y_k)$, and at most $2\mathrm{cn}(G) + 1$ moves to replace $x_1^{-1} y_1$ by $y_2 = 1$.

Hence the vertex x can be connected to y by a path of at most

$$\max\{\, 2\mathrm{or}(G)(k-1) + 2\mathrm{cn}(G) + 1,\ 2\mathrm{or}(G) + 1 + 2\mathrm{cn}(G) + 1 \,\} \leqslant 2k\mathrm{or}(G) + 2\mathrm{cn}(G)$$

edges, and the proposition follows. □

To complete the proof of the theorem, we need to list some of the known estimates for the covering numbers of finite simple groups. They show, in particular, that there is considerable scope for improvement of our rather crude estimates.

(a) If G is a Chevalley or twisted Chevalley group of Lie rank $\operatorname{rank} G$ then

$$\operatorname{cn}(G) < d \cdot \operatorname{rank} G$$

for some constant d which does not depend on G (Ellers, Gordeev and Herzog [18]).

(b) In the case of $PSL_n(q)$, $q \geqslant 4$, $n \geqslant 3$, there is a better bound

$$\operatorname{cn}(PSL_n(q)) = n$$

(Lev [27]), while

$$\operatorname{cn}(PSL_2(q)) = 3$$

for all $q \geqslant 4$ (Arad, Chillag and Morgan [4]).

(c) For the alternating groups,

$$\begin{aligned} \operatorname{cn}(\mathrm{Alt}_n) &= \left[\frac{n}{2}\right], \quad n \geqslant 6, \\ \operatorname{cn}(\mathrm{Alt}_5) &= 3 \end{aligned}$$

(Dvir [16]).

(d) Covering numbers of sporadic groups do not influence our asymptotic results. However, it worth mentioning that they are known (Zisser [40]).

In all these cases $\operatorname{cn}(G) < c \log |G|$. Since, obviously, $\operatorname{or}(G) \leqslant \operatorname{cn}(G)$, the theorem follows. □ □

Modulo the Ore-Thompson Conjecture the estimate of Proposition 5.3 takes the form

$$\operatorname{diam}\left(\Delta_k(G, G)\right) \leqslant 8k + 4\operatorname{cn}(G).$$

Notice that the Ore-Thompson Conjecture is true for all Chevalley groups $G(q)$ for $q \geqslant 8$ (Ellers and Gordeev [17]).

Also notice that since a simple group N is isomorphically embedded into its automorphism group, we have the obvious inequality

$$\operatorname{diam}\left(\Delta_k(G, N)\right) \leqslant \operatorname{diam}\left(\Delta_k(N, N)\right)$$

for every group G which contains N as a normal subgroup.

For the purpose of generating pseudorandom elements in a simple normal subgroup N of the group G, the Andrews-Curtis graph has the following apparent advantages over the product replacements graph $\Gamma_k(N)$. The fact that

the diameter diam $(\Delta_k(G,N))$ is much smaller than that of $\Gamma_k(N)$ suggests the possibility that the mixing time of a random walk on $\Delta_k(G,N)$ is smaller than the mixing time of a random walk on $\Gamma_k(N)$. The vertices of $\Delta_k(G,N)$ are all tuples in $N^k \setminus (1,\dots,1)$, hence the sample of elements of N obtained by taking random components of random generating tuples (vertices) in $\Delta_k(G,N)$ is not biased.

5.3 Gaschuetz's lemma for normal generation

Notice that an epimorphism $G \longrightarrow H$ of groups induces an adjacency-preserving map of graphs $\Delta_k(G,G) \longrightarrow \Delta_k(H,H)$. It follows that the preimage of every connected component of $\Delta_k(H,H)$ is the union of some connected components of $\Delta_k(G,G)$.

An earlier version of the following statement was proven by the authors and then improved by V. D. Mazurov.

Proposition 5.4 (V. D. Mazurov) *If a finite group G is generated as a normal subgroup by k elements (that is,*

$$G = \langle h_1^G, \dots, h_k^G \rangle$$

for some $h_1, \dots, h_k \in G$) and the images $\bar{g}_1, \dots, \bar{g}_k$ of some elements $g_1, \dots, g_k$ in the factor group G/M for some normal subgroup $M \lhd G$ generate G/M as a normal subgroup,

$$G/M = \langle \bar{g}_1^{G/M}, \dots, \bar{g}_k^{G/M} \rangle$$

then there exist elements $m_1, \dots, m_k$ in M such that

$$G = \langle (g_1 m_1)^G, \dots, (g_k m_k)^G \rangle.$$

Proof. The proof is based on the following classical result:

Fact 5.5 (Gaschuetz [20]) *If a finite group G is generated by k elements and the images of some elements $g_1, \dots, g_k$ in the factor group G/M for some normal subgroup $M \lhd G$ generate G/M, then there exist elements $m_1, \dots, m_k$ in M such that $\langle g_1 m_1, \dots, g_k m_k \rangle = G$.*

In a minimal counter-example to Proposition 5.4, M is a minimal normal subgroup. Let $H = \langle g_1, \dots, g_k \rangle_n$ (where $\langle\ \rangle_n$ denotes the generation as a normal subgroup in G). Then $H \cap M = 1$ and $G = H \times M$, so M is simple. If M is non-abelian then, for $1 \neq m \in M$, $G = \langle g_1 m, \dots, g_k \rangle_n$, so M is abelian and intersects $[G,G] = [H,H]$ trivially. It is obvious that $G/[H,H]M = \langle g_1, \dots, g_k \rangle [H,H]M$. By Gaschütz lemma (Fact 5.5), $G/[H,H] = \langle g_1 m_1, \dots, g_k m_k \rangle [H,H]$ for some $m_1, \dots, m_k$ from M. These $m_1, \dots, m_k$ are required elements. □

As an immediate corollary we have the following covering property of Andrews–Curtis graphs.

Corollary 5.6 *If G is a finite group normally generated by k elements and $M \lhd G$ then the canonical map*

$$\Delta_k(G,G) \longrightarrow \Delta_k(G/M, G/M)$$

is surjective.

If the canonical map $\Delta_k(G,G) \longrightarrow \Delta_k(H,H)$ is surjective we shall say that the graph $\Delta_k(G,G)$ *covers* the graph $\Delta_k(H,H)$.

5.4 The Andrews-Curtis graphs of finite soluble groups

It is easy to see that the graph $\Delta_k(G,G)$ is not necessary connected. Indeed, notice that if G is an abelian group then $\Delta_k(G,G) = \tilde{\Gamma}_k(G)$. Therefore the following fact is also applicable to the Andrews-Curtis graphs of abelian groups.

Fact 5.7 *Let A be a finite abelian group represented as*

$$A \simeq \mathbb{Z}_{e_1} \times \cdots \times \mathbb{Z}_{e_r},$$

where $e_1 \mid e_2 \mid \ldots \mid e_r$, Then

(i) (Neumann and Neumann [34]) *$\Gamma_k(A)$ is connected if $k > r$.*

(ii) (Diaconis and Graham [14]) *Γ_r has $\varphi(e_1)$ components of equal size.*

Here $\varphi(n)$ is the Euler function, i.e. the number of positive integers smaller than n and coprime to n.

However, we shall show in this section that abelian factor groups is the only obstacle to the connectedness of the Andrews-Curtis graph of finite soluble groups.

Lemma 5.8 *Let G be a soluble (not necessary finite) group. A subset $Y \subset G$ generates G as a normal subgroup if and only if Y generates G modulo $[G,G]$, i.e., the canonical image of Y generates the abelianisation $Ab(G) = G/[G,G]$.*

Proof Let $H = \langle Y^G \rangle \lhd G$. Suppose that c is the derived length of G and $G^{(c)}$ is the last (non-trivial) term of the derived series of G. By induction on c we may assume that $G = HG^{(c)}$. Now

$$G/H = HG^{(c)}/H \simeq G^{(c)}/H \cap G^{(c)}$$

which shows that G/H is abelian. Hence $[G,G] \leq H$. Therefore $H = G$, as required. □

Corollary 5.9 *If G is a finite soluble group generated as a normal subgroup by k elements than the canonical map*

$$\Delta_k(G,G) \longrightarrow \Gamma_k(G/[G,G], G/[G,G])$$

is surjective.

Lemma 5.8 allows one to compute the probability $\psi_k(G)$ that k uniformly and independently chosen elements in G generate G as a normal subgroup, i.e.,

$$\psi_k(G) = \frac{|V_k(G,G)|}{|G|^k}.$$

Observe that if G is a finite abelian group then $\psi_k(G)$ is just the probability that k elements from G generate G.

Corollary 5.10 *Let G be a finite soluble group. Then*

$$\psi_k(G) = \psi_k(Ab(G)).$$

We can now analyse the behaviour of Andrews-Curtis graphs of finite soluble groups.

Proposition 5.11 *Suppose that a finite soluble group G is generated by k elements $x_1, \dots, x_k$. Then for any $f_i \in [G,G]$ the k-tuple $(x_1, \dots, x_k)$ is connected by Andrews–Curtis transformations to $(x_1 f_1, \dots, x_k f_k)$.*

Proof. This is effectively a word-by-word reproduction of the argument from [31]. We use induction on the derived length of G. Let A be the last non-trivial term of the derived series of G. By the induction hypothesis applied to the images of the x_i and the $x_i f_i$ the corresponding k-tuples in G/A are equivalent. By [31, Property 1] this implies that $(x_1 f_1, \dots, x_k f_k)$ is equivalent (in G) to $(x_1 a_1, \dots, x_k a_k)$ for some $a_i \in A$. It remains to connect $(x_1 a_1, \dots, x_k a_k)$ with $(x_1, \dots, x_k)$ by Andrews–Curtis transformations. This is done in a process of successive "elimination" of the factors a_i. At each step the system of generators x_i of the group G is replaced by another one by some Nielsen transformations. Let A_1 be the normal closure in G of the elements $a_1, \dots, a_{k-1}$ and let the bar denote the images in G/A_1. Then $(\bar{x}_1\bar{a}_1, \dots, \bar{x}_k\bar{a}_k) = (\bar{x}_1, \dots, \bar{x}_{k-1}, \bar{x}_k\bar{a}_k)$. Since the $\bar{x}_i$ generate $\overline{G}$, by [31, Property 2] $(\bar{x}_1, \dots, \bar{x}_{k-1}, \bar{x}_k\bar{a}_k)$ is connected to $(\bar{x}_1, \dots, \bar{x}_{k-1}, \bar{x}_k)$ by a chain of Andrews–Curtis transformations applied only to the last component. Lifting these transformations to G we obtain that $(x_1 a_1, \dots, x_k a_k)$ is equivalent to $(x_1 a_1, \dots, x_{k-1} a_{k-1}, x_k a'_k)$, where $a'_k \in A_1$. We write $a'_k = a_{j_1}^{g_1} \cdots a_{j_l}^{g_l}$, where $1 \leqslant j_s \leqslant k-1$ and the g_s are some elements of G. Then we successively kill all the factors $a_{j_s}^{g_s}$ in the last component at the expense of changing x_n by some Nielsen transformations. Namely, by [31,

Property 4] $(x_1a_1, \dots, x_ka'_k)$ is equivalent to $(x_1a_1, \dots, x_{j_l}a_{j_l}^{g_l}, \dots, x_ka'_k)$. Then we apply Andrews–Curtis transformations to the last component to get

$$(x_1a_1, \dots, x_{j_l}a_{j_l}^{g_l}, \dots, x_ka'_k(a_{j_l}^{-1})^{g_l}x_{j_l}^{-1}) = (x_1a_1, \dots, x_kx_{j_l}^{-1}a_{j_1}^{g'_1} \cdots a_{j_{l-1}}^{g'_{l-1}}),$$

where $g'_s = g_s^{x_{j_l}^{-1}}$. The number of "$a^g$-factors" in the last component is now smaller, although the generator x_k is "replaced" by $x_kx_{j_k}^{-1}$. After finitely many such steps we arrive at $(x_1a_1, \dots, x_{k-1}a_{k-1}, x'_k)$, where x'_k is a result of Nielsen transformations. We have thus got rid of the a-factor in the last component. This process can now be repeated with A_1 generated by fewer elements, although for a new system of generators of G obtained from the x_i by Nielsen transformations. It is of course important that at each step we are dealing with a k-tuple of the form $(x'_1a_1, \dots, x'_ka_k)$, where the x'_i are generators of G. To use formally an induction argument, one can each time simply rearrange the components of the k-tuple, which can be done by the Andres–Curtis transformations, so that some initial segment of components increasing in length is free of a-factors. The last step of this process is also covered by this argument, when [31, Property 2] is applied as above with $A_1 = 1$. Finally we shall arrive at an equivalent k-tuple $(x'_1, \dots, x'_k)$ obtained from $(x_1, \dots, x_k)$ by Nielsen transformations. Reversing the chain of these Nielsen transformations we arrive at $(x_1, \dots, x_k)$. Thus, $(x_1a_1, \dots, x_ka_k)$ and therefore $(x_1f_1, \dots, x_kf_k)$ is equivalent to $(x_1, \dots, x_k)$. The proposition is proved. □

In Proposition 5.11, it would be interesting to replace 'generated by k elements' by 'generated as a normal subgroup by k elements':

Question 6 *Suppose that a finite soluble group G is generated as a normal subgroup by k elements $x_1, \dots, x_k$. Is it true that for any $f_i \in [G, G]$ the k-tuple $(x_1, \dots, x_k)$ is connected by Andrews–Curtis transformations to $(x_1f_1, \dots, x_kf_k)$?*

Theorem 5.12 *Suppose that a finite soluble group G can be generated by k elements. Then the preimages in G of the connected components of the Andrews–Curtis k-tuple graph of $G/[G, G]$ are all connected. In particular, the graph $\Delta_{k+1}(G, G)$ is connected.*

Proof. Let $(u_1, \dots, u_k)$ and $(v_1, \dots, v_k)$ be two k-tuples of elements of G (each generating G modulo $[G, G]$) that are equivalent modulo $[G, G]$. Then $(u_1, \dots, u_k)$ is equivalent in G to $(v_1f_1, \dots, v_kf_k)$ for some $f_i \in [G, G]$. Since G is k-generated, by Gaschütz' lemma there are elements $h_i \in [G, G]$ such that the elements $v_1h_1, \dots, v_kh_k$ generate G. By Proposition 5.11 the k-tuples $(v_1, \dots, v_k)$ and $(v_1h_1, \dots, v_kh_k)$ are equivalent, as well as the k-tuples $(v_1h_1, \dots, v_kh_k)$ and $(v_1f_1, \dots, v_kf_k)$. By transitivity hence $(u_1, \dots, u_k)$ and $(v_1, \dots, v_k)$ are equivalent, as required. Since the factor group $G/[G, G]$ is k-generated, the graph

$\Delta_{k+1}(G/[G,G], G/[G,G])$ is connected by Fact 5.7, and the second assertion also follows. □

One can compare this result with the following observation about soluble groups.

Fact 5.13 (Dunwoody [15], see also [35, Theorem 2.36]) *Let G be a finite soluble group generated by k elements. Then $\Gamma_{k+1}(G)$ is connected.*

Theorem 5.12 is especially nice in the case of nilpotent groups. A well-known fact about nilpotent groups states that if A is a subgroup of a nilpotent group G such that $A[G,G] = G$, then $A = G$. It follows that a tuple of elements generates G as a normal subgroup if and only if it generates it as a group. Applying Theorem 5.12, we immediately have

Theorem 5.14 *Suppose that G is a finite nilpotent group. Then the pre-images in G of the connected components of the Andrews–Curtis graph of $G/[G,G]$ are all connected.*

Remarks. In fact, an argument in [31] states that the tuples $(g_1, \dots, g_k)$ and $(g_1, \dots, g_{k-1}, g_k f)$ for $f \in [G,G]$ are connected by Andrews–Curtis transformations in any group $G = \langle g_1, \dots, g_k \rangle$. In the above case of G being nilpotent there is also an alternative computation based on using more of commutator calculus, which may be more efficient from computational viewpoint.

6 The Andrews-Curtis Conjecture: an approach via unsoluble finite groups

6.1 Disconnected Andrews-Curtis graphs

A possible way to confirm a counterexample to the Andrews-Curtis Conjecture starts with one of the suggested potential counterexamples, that is, words $u = u(x,y)$ and $v = v(x,y)$ which generate the free group $F_2 = \langle x, y \rangle$ of rank two, and which are suspected of not being connected to x and y by a sequence of Andrews-Curtis moves. One can take a finite group G with more than one connected component of $\Delta_2(G,G)$ and consider the map

$$\begin{array}{rcl} \omega : \Delta_2(G,G) & \longrightarrow & \Delta_2(G,G) \\ (x,y) & \mapsto & (u(x,y), v(x,y)). \end{array}$$

If ω maps a vertex (x,y) to a vertex which belongs to a different component of $\Delta_2(G,G)$, then the pairs (x,y) and $(u(x,y), v(x,y))$ obviously constitute a counterexample to the Andrews-Curtis Conjecture. Of course, the first candidate for

the map ω should come from the simplest possible potential counterexample to the AC-conjecture. The following pair

$$(x^3y^{-4}, xyxy^{-1}x^{-1}y^{-1}) \tag{1}$$

occurs in the second presentation in the series of potential counterexamples proposed by Akbulut and Kirby [2]. The total length of these words is equal to 13. Note that all pairs (u, v) which generate F_2 as a normal subgroup and have the total length $|u| + |v| \leq 12$ satisfy the AC-conjecture [33]. So the potential counterexample (1) has the minimal possible length. Moreover, recently, Havas and Ramsay proved that every pair of elements in F_2 which generates F_2 as a normal subgroup and has the total length 13 is AC-equivalent either to (x, y) or to (1) [21]. This shows that the map

$$\omega : (x, y) \mapsto (x^3y^{-4}, xyxy^{-1}x^{-1}y^{-1})$$

should be of prime interest here.

However, in view of Myasnikov's result on the Andrews-Curtis graphs of free soluble groups (Fact 3.1), we should not expect to find a counterexample to the Andrews-Curtis Conjecture among finite soluble groups.

For that reason it would be interesting to study the Andrews-Curtis graph for finite *unsoluble* groups.

Perfect groups. Recall that a group G is called *perfect* if it coincides with its commutator, $G = [G, G]$.

Question 7 *Is it true that, for a perfect finite group G, the Andrews–Curtis graph $\Delta = \Delta_k(G, G)$ is connected?*

More generally, is it true that the preimage in $\Delta_k(G, G)$ of every connected component of $\Delta_k(G/[G, G], G/[G, G])$ is connected?

In the case of a simple finite group G the answer is obviously 'yes'. Moreover, a slightly more general result is true.

Lemma 6.1 (Sukru Yalcinkaya) *If a group G has a unique maximal normal subgroup M then $\Delta_k(G, G)$ is connected for every $k \geqslant 2$.*

Proof. Notice that every element $x \in G \setminus M$ generates G as a normal subgroup, and vice versa. Therefore the vertices of $\Delta_k(G, G)$ are all k-tuples $(x_1, \ldots, x_k)$ such that at least one of x_i does not belong to M. Now any two vertices can be obviously connected by the Andrews–Curtis moves. □

The positive answer to Question 7 would implicitly suggest that the Andrews-Curtis Conjecture is true. However, the connectedness of the Andrews–Curtis graphs is not yet the end of the story, see Question 12 below.

Question 8 *Let K and L be normal subgroups of a finite group G and $K \cap L = 1$. Assume that the Andrews–Curtis graphs $\Delta_k(G/K, G/K)$ and $\Delta_l(G/L, G/L)$ are connected. Is it true that $\Delta_{k+l}(G, G)$ is connected?*

In more general terms, how do connected components of $\Delta_m(G, G)$ relate to connected components of $\Delta_k(G/K, G/K)$ and $\Delta_l(G/L, G/L)$?

The first part of the question is likely to be easy.

Non-perfect groups. If the preimage Γ of a connected component from $\Delta_2(G/[G,G], G/[G,G]))$ is disconnected, it would be very interesting to look at the map

$$\omega : (x, y) \mapsto (u(x, y), v(x, y))$$

on Γ. Notice that since the images $\bar{u}$ and $\bar{v}$ of $u(x, y)$ and $v(x, y)$ generate the factor group $A = F_2/[F_2, F_2]$ of the free group $F_2 = \langle x, y\rangle$ modulo the commutator, the determinant $\det(\tilde{u}, \tilde{v})$ of the matrix representing $\tilde{u}, \tilde{v}$ in the basis $\tilde{x}, \tilde{y}$ is ± 1. Hence the image $(\bar{u}, \bar{v})$ of $\omega(x, y)$ belongs to the same connected component of $\Delta_2(G/[G,G], G/[G,G])$ as $(\bar{x}, \bar{y})$, and $\omega(\Gamma) \subseteq \Gamma$.

Question 9 *Does the map ω preserve the connected components of Γ?*

The negative answer to this question, of course, provides a counterexample to the Andrews–Curtis Conjecture. So far this gives only a one way approach to the problem. It would be interesting to see if there exists a two-way reduction of the Andrews–Curtis Conjecture to questions about Andrews–Curtis graphs of finite groups. In particular, we would like to mention the following conjecture.

Conjecture 10 *If the normal generators x, y and $u(x, y), v(x, y)$ of F_2 are not connected by Andrews–Curtis transformations, then there exists a finite factor group G where $(\bar{x}, \bar{y})$ and $(u(\bar{x}, \bar{y}), v(\bar{x}, \bar{y})$ belong to different connected components of $\Delta_2(G, G)$.*

6.2 An alternative approach to construction of counterexamples

As we have already mentioned, good connection properties of the Andrews–Curtis graphs of finite groups do not yet herald the end of attempts to construct a counterexample to the Andrews–Curtis Conjecture by means of finite group theory. We can also try an alternative approach.

Notice that if the normal generators (x, y) and $u(x, y), v(x, y)$ of F_2 are connected by d Andrews–Curtis transformations, then the same is true for an arbitrary finite group. Therefore we come to the following question.

Question 11 *Does there exists a series of finite groups $\{G_n\}$ such that the path distance d_n in $\Delta_2(G_n, G_n)$ between the pairs $(\bar{x}, \bar{y})$ and $(u(\bar{x}, \bar{y}), v(\bar{x}, \bar{y}))$ is unbounded?*

Question 12 *Assuming that the Andrews–Curtis Conjecture is false and the normal generators x, y and $u(x,y), v(x,y)$ of F_2 are not connected by Andrews–Curtis transformations, is it true that there exists a series of finite factor groups $\{G_n\}$ such that if d_n is the path distance in $\Delta_2(G_n, G_n)$ between the pairs $(\bar{x}, \bar{y})$ and $(u(\bar{x}, \bar{y}), v(\bar{x}, \bar{y}))$ then the sequence $\{d_n\}$ is unbounded?*

Of course, similar conjectures can be formulated for arbitrary lengths k of k-tuples of normal generators.

Notice, however, that the free group F_n is residually $\mathcal{S}$ for every infinite set $\mathcal{S}$ of pairwise nonisomorphic finite nonabelian simple groups [37, 38, 39], that is, for each $g \in F_n$, $g \neq 1$, there is an epimorphism (depending on g) from F_n onto a group in $\mathcal{S}$ such that the image of g is not 1. This means, for example, that F_n is residually Chev_n for the class Chev_n of all finite Chevalley groups of rank $\leqslant n$, while these groups have uniformly bounded diameters of their Andrews–Curtis graphs (Section 5.2).

Therefore Questions 11 and 12 might happen to be hard to resolve. However, their versions for *restricted Andrews–Curtis* graphs are more likely to have positive solutions and seem to be more accessible for a study by means of computer experiments.

6.3 Restricted Andrews-Curtis graphs

Let G be a group generated by a set S and $N \lhd G$. We define the *restricted Andrews–Curtis graph* $\bar{\Delta}_k(G, N, S)$ as the graph with the same vertices as in $\Delta_k(G, N)$, that is, k-tuples of elements in N which generate N as a normal subgroup:

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

Two vertices are connected by an edge if one of them is obtained from another by one of the moves:

$$\begin{aligned}
(x_1, \dots, x_i, \dots, x_j, \dots, x_k) &\longrightarrow (x_1, \dots, x_i x_j^{\pm 1}, \dots, x_k),\ i \neq j \\
(x_1, \dots, x_i, \dots, x_j, \dots, x_k) &\longrightarrow (x_1, \dots, x_j^{\pm 1} x_i, \dots, x_k),\ i \neq j \\
(x_1, \dots, x_i, \dots, x_k) &\longrightarrow (x_1, \dots, x_i^s, \dots, x_k),\ s \in S \\
(x_1, \dots, x_i, \dots, x_k) &\longrightarrow (x_1, \dots, x_i^{-1}, \dots, x_k).
\end{aligned}$$

Thus $\bar{\Delta}_k(G, N, S)$ is a subgraph of $\Delta_k(G, N)$ whose edges correspond to Nielsen moves, inversions, and to conjugation by generators $s \in S$ rather than arbitrary elements $w \in G$.

Obviously, the graphs $\bar{\Delta}_k(G, N, S)$ and $\Delta_k(G, N)$ have the same connected components. For finite groups G, the graph $\bar{\Delta}_k(G, N, S)$ has much large diameter than $\Delta_k(G, N)$. Of course, we have the obvious estimate

$$\operatorname{diam} \bar{\Delta}_k(G, N, S) \leqslant \operatorname{diam} \Delta_k(G, N) \cdot \operatorname{diam} \mathsf{Cayley}(\mathsf{G}, \mathsf{S}),$$

where $\mathsf{Cayley}(\mathsf{G},\mathsf{S})$ is the Cayley graph of the group G with respect to the generating set S.

Question 13 *Find better bounds for the diameter of the restricted Andrews–Curtis graph $\bar{\Delta}_k(G,N,S)$ in the case of finite simple groups $G=N$ and 'natural' sets of generators.*

Notice that if the normal generators (x,y) and $u(x,y),v(x,y)$ of F_2 are connected by d edges in the restricted Andrews–Curtis graph of F_2 with respect to some generating set $\{a,b\}$ of F_2, then the same is true for an arbitrary finite group. Therefore we come to the following analogues of Questions 11 and 12.

Question 14 *Does there exist a series of finite groups $\{G_n\}$ with generators x_n,y_n such that the path distance d_n in $\bar{\Delta}_2(G_n,G_n,\{x_n,y_n\})$ between the pairs $(x_n,\ y_n)$ and $(u(x_n,y_n),v(x_n,y_n))$ is unbounded?*

Question 15 *Assume that the Andrews–Curtis Conjecture is false and the normal generators $u(x,y),v(x,y)$ of the free group F_2 are not connected by Andrews–Curtis transformations to the free generators x and y. Is it true that there exists a series of finite factor groups $\{G_n\}$ of F_2 such that if d_n is the path distance in $\bar{\Delta}_2(G_n,G_n,\{\bar{x},\bar{y}\})$ between the pairs $(\bar{x},\bar{y})$ and $(u(\bar{x},\bar{y}),v(\bar{x},\bar{y}))$ then the sequence $\{d_n\}$ is unbounded?*

It would be interesting to try to run computer experiments with the restricted Andrews–Curtis graphs of finite simple groups as an attempt to analise their metric properties. Taking, for example, the transvections

$$x=\begin{pmatrix}1&0\\2&1\end{pmatrix}\ \text{ and }\ y=\begin{pmatrix}1&2\\0&1\end{pmatrix}$$

in the group $G_q=SL_2(\mathbb{F}_q)$ for small values of q, is it feasible to compute the path distance d_q in $\bar{\Delta}_2(G_q,G_q,(x,y)$ from (x,y) to $(x^3y^{-4},xyxy^{-1}x^{-1}y^{-1})$? Might it happen that a geodesic path found in $SL_2(\mathbb{F}_q)$ can be lifted to the free group

$$\left\langle\begin{pmatrix}1&0\\2&1\end{pmatrix},\begin{pmatrix}1&2\\0&1\end{pmatrix}\right\rangle\leqslant SL_2(\mathbb{Z})?$$

However, even if the growth of d_q is detected in a small sample of computationally accessible graphs, we still encounter a possibly very difficult problem of theoretical analysis of metric properties of (restricted) Andrews–Curtis graphs of arbitrary big size.

6.4 Expanders

The following result by Lubotzky and Pak is intimately related to their theorem (Fact 2.1).

Fact 6.2 [29] *If $Aut\, F_k$ has property (T) and G is a finite group then every connected component of $\Gamma_k(G)$ is an ε-expander for some ε which depends only on k.*

Here, a graph Γ is an *ε-expander* if, for every set of vertices $B \subset \Gamma$ which is less than half of Γ, $|B| < \frac{1}{2}|\Gamma|$, has sufficiently many 'new' neighbours:

$$\left| \left\{ \begin{array}{c} \text{vertices connected} \\ \text{to } B, \text{ but not in } B \end{array} \right\} \right| \geqslant \varepsilon \cdot |B|.$$

We would like to mention, in passing, the following question.

Question 16 *Do the connected components of the graphs $\bar{\Delta}(G, N, S)$ for normal subgroups N of finite groups G form a family of expanders?*

Acknowledgement

The authors thank Robert Gilman who was at the origins of this project and contributed many important ideas, Victor D. Mazurov, who proved Proposition 5.4, and Alex D. Myasnikov who run numerous computer experiments. We also thank Sukru Yalcinkaya for an useful observation which became Lemma 6.1.

References

[1] C. Altseimer and A. Borovik, 'Probabilistic recognition of orthogonal and symplectic groups', in *Groups and Computation III* (W. Kantor and A. Seress, eds.), de Gruyter, Berlin, 2001, pp. 1–20.

[2] S. Akbut and R. Kirby, 'A potential smooth counterexample in dimension 4 to the Poincare conjecture, the Schoenflies conjecture, and the Andrews-Curtis conjecture', *Topology* 24 (1985), 375–390.

[3] J. J. Andrews and M. L. Curtis, 'Free groups and handlebodies', *Proc. Amer. Math. Soc.* 16 (1965), 192–195.

[4] Z. Arad, D. Chillag and G. Morgan, 'Groups with a small covering number', Chapter 4 in *Products of conjugacy classes in groups* (Z. Arad and M. Herzog, eds.), Lect. Notes Math. 1112, 1985.

[5] L. Babai, 'Local expansion of vertex-transitive graphs and random generation in finite groups', *Proc. ACM Symp. on Theory of Computing* 1991, pp. 164–174.

[6] L. Babai, 'Randomization in group algorithms: conceptual questions', *Groups and Computations II*, (eds L. Finkelstein and W. Kantor), DIMACS: Series in Discrete Mathematics and Theoretical Computer Science 28 (1997), 1–17.

[7] L. Babai and R. Beals, 'A polynomial-time theory of black box groups', *Groups St Andrews 1997 in Bath I*, *London Math. Soc. Lect. Notes Ser.* 260, Cambridge University Press (1999), pp. 30-64.

[8] A. Baddeley, C. R. Leedham-Green, A. C. Niemeyer and M. Frith, 'Measuring the performance of random element generators in large algebraic structures', in preparation.

[9] A. V. Borovik, 'Orthogonal and symplectic black box groups, revisited', math.GR/0110234.

[10] W. Bosma, J. Cannon and C. Playoust, 'The Magma algebra system', in *Computational algebra and number theory* (*London, 1993*), *J. Symbolic Computation* 24 (1997), 235–265.

[11] S. Bratus and I. Pak, 'Fast constructive recognition of a gray box group isomorphic to S_n or A_n using Goldbach's Conjecture', *J. Symbolic Computation*, 29 (2000), 33-57.

[12] R. G. Burns and O. Macedonska, 'Balanced presentations of the trivial group', *Bull. London Math. Soc.* 25 (1993), 513–526.

[13] F. Celler, C. Leedham-Green, S. Murray, A. Niemeyer and E. O'Brien, 'Generating random elements of a finite group', *Comm. Algebra* 23 (1995), 4931–4948.

[14] P. Diaconis and R. Graham, 'The graph of generating sets of an abelian group', *Colloq. Math.* 80 (1999), 31–38.

[15] M. J. Dunwoody, 'Nielsen transformations', in *Computational Problems in Abstract Algebra*, Pergamon Press, Oxford, 1970, pp. 45–46.

[16] Y. Dvir, 'Covering properties of permutation groups', Chapter 3 in *Products of Conjugacy Classes in Groups,* (Z. Arad and M. Herzog, eds.), Lect. Notes Math. 1112 (1985).

[17] E. W. Ellers and N. Gordeev, 'On the conjectures of J. Thompson and O. Ore'. *Trans. Amer. Math. Soc.* 350 (1998), No. 9, 3657–3671.

[18] E. W. Ellers, N. Gordeev and M. Herzog, 'Covering numbers for Chevalley groups', *Israel J. Math.* 111 (1999), 339-372.

[19] 'GAP, a system for computational discrete algebra', Lehrstuhl D fur Mathematik RTWTH, Templergraben 64, D 52056 Aachen, Germany.

[20] W. Gaschuetz 'Zu einem von B. H. und H. Neumann gestellten Problem', *Math. Nachr.* 14 (1956), 249–252.

[21] G. Havas and C. Ramsay, 'Breadth-first search and the Andrews-Curtis conjecture', preprint.

[22] C. Hog-Angeloni and W. Metzler, 'The Andrews-Curtis conjecture and its generalizations', in *Two-dimensional Topology and Combinatorial Group Theory*, London Math. Soc. Lect. Notes Ser. 197, Cambridge University Press (1993), pp. 365–380.

[23] W. Kantor and A. Seress, 'Black box classical groups', *Memoirs Amer. Math. Soc.* 149, No. 708, Amer. Math. Soc., Providence, RI, 2000.

[24] D. A. Kazhdan, 'On the connection of the dual space of a group with the structure of its closed subgroups', *Funkcional. Anal. i Prilozh.* 1 (1967), 71–74.

[25] C. R. Leedham-Green, 'The computational matrix project', in *Groups and Computation III* (W. Kantor and A. Seress, eds.), de Gruyter, Berlin, 2001, pp. 229-247.

[26] C. Leedham-Green and E. O'Brien, 'Recognising tensor-induced matrix groups', submitted.

[27] A. Lev, 'The covering number of the group $PSL_n(F)$', *J. Algebra* 182 (1996), 60–84.

[28] M. W. Liebeck and A. Shalev, 'Diameters of finite simple groups: sharp bounds and applications', preprint.

[29] A. Lubotzky and I. Pak, 'The product replacement algorithm and Kazhdan's property (T)', *J. Amer. Math. Soc.* 14 (2001), 347–363.

[30] W. Magnus, A. Karras and D. Solitar, *Combinatorial Group Theory*, Interscience Publishers, New York a. o., 1966.

[31] A. G. Myasnikov, 'Extended Nielsen transformations and the trivial group', *Mat. Zametki* 35 (1984), 491–495 (in Russian).

[32] A. D. Myasnikov, 'Genetic algorithms and the Andrews-Curtis conjecture', *Int. J. Algebra Comput.* 9 (1999), 671–686.

[33] A. D. Myasnikov and A. G. Myasnikov, 'Balanced presentations of the trivial group on two generators and the Andrews-Curtis conjecture', in *Groups and Computation III* (W. Kantor and A. Seress, eds.), de Gruyter, Berlin, 2001, pp. 257–264.

[34] B. H. Neumann and H. Neumann, 'Zwei Klassen charaktersticher Untergruppen und ihre Faktorgruppen', *Math. Nachr.* 4 (1951), 106–125.

[35] I. Pak, 'What do we know about the product replacement algorithm', in *Groups and Computation III* (W. Kantor and A. Seress, eds.), DeGruyter, Berlin, 2001, pp. 301–348.

[36] I. Pak, 'The product replacement algorithm is polynomial', preprint.

[37] T. S. Weigel, 'Residual properties of free groups', *J. Algebra*, 160 (1993), 16–41.

[38] T. S. Weigel, 'Residual properties of free groups', II, *Comm. Algebra*, 20 (1992), 1395–1425.

[39] T. S. Weigel, 'Residual properties of free groups', III, *Israel J. Math.* 77 (1992), 65–81.

[40] I. Zisser, 'The covering numbers of the sporadic simple groups', *Israel J. Math.* 67 (1989), 217–224.

Alexandre V. Borovik, Department of Mathematics, UMIST, PO Box 88, Manchester M60 1QD, United Kingdom
borovik@umist.ac.uk
http://www.ma.umist.ac.uk/avb/

Evgenii I. Khukhro, Institute of Mathematics, Novosibirsk-90, 630090, Russia
khukhro@cardiff.ac.uk

Alexei G. Myasnikov, Department of Mathematics, The City College of New York, New York, NY 10031, USA
alexeim@att.net
http://home.att.net/~alexeim/index.htm