The Finitary Andrews-Curtis Conjecture

Alexandre V. Borovik Alexander Lubotzky
Alexei G. Myasnikov

12 June 2003

To Slava Grigorchuk as a token of our friendship.

Abstract

The well known Andrews-Curtis Conjecture [2] is still open. In this paper, we establish its finite version by describing precisely the connected components of the Andrews-Curtis graphs of finite groups. This finite version has independent importance for computational group theory. It also resolves a question asked in [5] and shows that a computation in finite groups cannot lead to a counterexample to the classical conjecture, as suggested in [5].

1 Andrews-Curtis graphs

Let G be a group and G^k be the set of all k-tuples of elements of G.

The following transformations of the set G^k are called *elementary Nielsen transformations* (*or moves*):

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

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

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

Elementary Nielsen moves transform generating tuples of G into generating tuples. These moves together with the transformations

(4) $(x_1, \dots, x_i, \dots, x_k) \longrightarrow (x_1, \dots, x_i^w, \dots, x_k),\ w \in S \cup S^{-1} \subset G,$

where S is a fixed subset of G, form a set of *elementary Andrews-Curtis transformations relative to* S (or, shortly, AC_S-moves). If $S = G$ then AC-moves transform n-generating tuples (i.e., tuples which generate G as a normal subgroup) into n-generating tuples. We say that two k-tuples U and V are AC_S-equivalent, and write $U \sim_S V$, if there is a finite sequence of AC_S-moves which transforms U into V. Clearly, $\sim_S$ is an equivalence relation on the set G^k of

k-tuples of elements from G. In the case when $S = G$ we omit S in the notations and refer to AC_S-moves simply as to AC-moves.

We slightly change notation from that of [5]. For a subset $Y \subset G$ we denote by $gp_G(Y)$ the normal closure of Y in G, by $d(G)$ the minimal number of generators of G, and by $d_G(G)$ the minimal number of normal generators of G. Now, $d_G(G)$ coincides with $nd(G)$ of [5].

Let $N_k(G)$, $k \geqslant d_G(G)$, be the set of all k-tuples of elements in G which generate G as a normal subgroup:

$$N_k(G) = \{\, (g_1, \ldots, g_k) \mid gp_G(g_1, \ldots, g_k) = G \,\} .$$

Then the *Andrews–Curtis graph* $\Delta_k^S(G)$ of the group G with respect to a given subset $S \subset G$ is the graph whose vertices are k-tuples from $N_k(G)$ and such that two vertices are connected by an edge if one of them is obtained from another by an elementary AC_S-transformation. Again, if $S = G$ then we refer to $\Delta_k^G(G)$ as to the Andrews-Curtis graph of G and denote it by $\Delta_k(G)$. Clearly, if S is a generating set of G then the graph $\Delta_k^S(G)$ is connected if and only if the graph $\Delta_k(G)$ is connected. Observe, that if S is finite then $\Delta_k^S(G)$ is a regular graph of finite degree.

The famous Andrews-Curtis conjecture [2] can be stated in the following way.

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

There are some doubts whether this well known old conjecture is true. Indeed, Akbulut and Kirby [1] suggested a series of potential counterexamples for $k = 2$:

$$(u, v_n) = (xyxy^{-1}x^{-1}y^{-1}, x^n y^{-(n+1)}), \quad n \geqslant 2. \tag{1}$$

In [5], it has been suggested that one may be able to confirm one of these potential counterexamples by showing that for some homomorphism $\phi : F_2 \to G$ into a finite group G the pairs (u^ϕ, v_n^ϕ) and (x^ϕ, y^ϕ) lie in different connected components of $\Delta_2(G)$. Notice that in view of [15] the group G in the counterexample cannot be soluble.

Our main result describes the connected components of the Andrews-Curtis graph of a finite group. As a corollary we show that (u^ϕ, v_n^ϕ) and (x^ϕ, y^ϕ) lie in the same connected components of $\Delta_2(G)$ for every finite group G and any homomorphism $\phi : F_2 \to G$, thus resolving the question from [5].

Theorem 1.1 *Let G be a finite group and $k \geqslant \max\{d_G(G), 2\}$. Then two tuples U, V from $N_k(G)$ are AC-equivalent if and only if they are AC-equivalent in the abelianisation $\mathrm{Ab}(G) = G/[G,G]$, i.e., the connected components of the AC-graph $\Delta_k(G)$ are precisely the preimages of the connected components of the AC-graph $\Delta_k(\mathrm{Ab}(G))$.*

Notice that, for the abelian group $A = \mathrm{Ab}(G)$, a normal generating set is just a generating set and the non-trivial Andrews-Curtis transformations are

Nielsen moves (1)–(3). Therefore the vertices of $\Delta_k(A)$ are the same as these of the *product replacement graph* $\Gamma_k(A)$ [7, 17]: they are all generating k-tuples of A. The only difference between $\Gamma_k(A)$ and $\Delta_k(A)$ is that the former has edges defined only by 'transvections' (1)–(2), while in the latter the inversion of components (3) is also allowed. The connected components of product replacements graphs $\Gamma_k(A)$ for finite abelian groups A have been described by Diaconis and Graham [7]; a slight modification of their proof leads to the following observation

Fact 1.2 (Diaconis and Graham [7]) *Let A be a finite abelian group and*

$$A = Z_1 \times \cdots \times Z_d$$

its canonical decomposition into a direct product of cyclic groups such that $|Z_i|$ divides $|Z_j|$ for $i < j$. Then

(a) *If $k > d$ then $\Delta_k(A)$ is connected.*

(b) *If $k = d \geqslant 2$, fix generators $z_1, \ldots, z_d$ of the subgroups $Z_1, \ldots, Z_d$, correspondingly. Let $m = |Z_1|$. Then $\Delta_d(A)$ has $\phi(m)/2$ connected components (here $\phi(n)$ is the Euler function). Each of these components has a representative of the form*

$$(z_1^\lambda, z_2, \ldots, z_d), \quad \lambda \in (\mathbb{Z}/m\mathbb{Z})^*.$$

Two tuples

$$(z_1^\lambda, z_2, \ldots, z_d) \text{ and } (z_1^\mu, z_2, \ldots, z_d), \quad \lambda, \mu \in (\mathbb{Z}/m\mathbb{Z})^*,$$

belong to the same connected component if and only if $\lambda = \pm\mu$.

Taken together, Theorem 1.1 and Fact 1.2 give a complete description of components of the Andrews-Curttis graph $\Delta_k(G)$ of a finite group G.

Notice that in an abelian group A

$$\begin{array}{rcl} (xyxy^{-1}x^{-1}y^{-1}, x^n y^{-(n+1)}) & \sim & (xy^{-1}, x^n y^{-(n+1)}) \\ & \sim & (xy^{-1}, x^{n-1} y^{-n}) \\ & \vdots & \\ & \sim & (yx^{-1}, y^{-1}) \\ & \sim & (x, y) \end{array}$$

so for every homomorphism $\phi : F_2 \to G$ as above the images (u^ϕ, v_n^ϕ) and (x^ϕ, y^ϕ) are AC equivalent in the abelianisation of G, hence they lie in the same connected component of $\Delta_2(G)$.

The following corollary of Theorem 1.1 leaves no hope of finding an counterexample to the Andrews-Curtis conjecture by looking at the connected components of the Andrews-Curtis graphs of finite groups.

Corollary 1.3 *For any $k \geqslant 2$, and any epimorphism $\phi : F_k \to G$ onto a finite group G, the image of $\Delta_k(F_k)$ in $\Delta_k(G)$ is connected.*

One may try to reject the AC-conjecture by testing AC-equivalence of the tuples (u, v_n) and (x, y) in the *infinite* quotients of the group F_2. To this end we introduce the following definition.

> **Definition:** *We say that a group G satisfies the* generalised Andrews-Curtis conjecture *if for any $k \geqslant \max\{\, d_G(G), 2\,\}$ tuples $U, V \in N_k(G)$ are AC-equivalent in G if and only if their images are AC-equivalent in the abelianisation* $\mathrm{Ab}(G)$.

> **Problem:** *Find a group G which does not satisfy the generalised Andrews-Curtis conjecture.*

It will be interesting to look, for example, at the Grigorchuk group [8, 9]. It is a finitely generated residually finite 2-group G which is just-infinite, that is, every normal subgroup has finite index. Therefore the generalised Andrews-Curtis conjecture holds in every proper factor group of G by Theorem 1.1. What might be also relevant, the conjugacy problem in the Grigorchuk group is solvable [13, 18, 3]. This makes the Grigorchuk group a very interesting testing ground for the generalised Andrews-Curtis conjecture.

2 Relativised Andrews-Curtis graphs and black-box groups

Following [5], we also introduce a relativised version of the Andrews-Curtis transformations of the set G^k for the situation when G admits some fixed group of operators Ω (that is, a group Ω which acts on G by automorphisms); we shall say in this situation that G is an Ω-*group*[1]. In that case, we view the group G as a subgroup of the natural semidirect product $G \cdot \Omega$ of G and Ω. In particular, the set of $AC_{G\Omega}$-moves is defined and the set G^k is invariant under these moves. In particular, if N is a normal subgroup of G, we view N as a G-subgroup in the sense of this definition. As we shall soon see, $AC_{G\Omega}$-moves appear in the product replacement algorithm for generating pseudo-random elements of a normal subgroup in a black box finite group.

For a subset $Y \subset G$ of an Ω-group G we denote by $gp_{G\Omega}(Y)$ the normal closure of Y in $G \cdot \Omega$, and by $d_{G\Omega}(G)$ the minimal number of normal generators of G as a normal subgroup of $G \cdot \Omega$.

Let $N_k(G, \Omega)$, $k \geqslant d_{G\Omega}(G)$, be the set of all k-tuples of elements in G which generate G as a normal Ω-subgroup:

$$N_k(G, \Omega) = \{\, (g_1, \ldots, g_k) \mid gp_{G \cdot \Omega}(g_1, \ldots, g_k) = G \,\}\,.$$

[1] We shall use the terms Ω-subgroup, normal Ω-subgroup, Ω-simple Ω-subgroup, etc. in their obvious meaning.

Then the *relativised Andrews–Curtis graph* $\Delta_k^\Omega(G)$ of the group G is the graph whose vertices are k-tuples from $N_k(G,\Omega)$ and such that two vertices are connected by an edge if one of them is obtained from another by an elementary $AC_{G\Omega}$-transformation.

A *black box group* G is a finite group with a device ('oracle') which produces its (pseudo)random (almost) uniformly distributed elements; this concept is of crucial importance for computational group theory, see [10]. If the group G is given by generators, the so-called *product replacement algorithm* [6, 17] provides a very efficient and practical way of producing random elements from G; see [14] for a likely theoretical explanation of this (still largely empirical) phenomenon in terms of the (conjectural) Kazhdan's property (T) [11] for the group of automorphisms of the free group F_k for $k > 4$. In the important case of generation of random elements in a normal subgroup G of a black box group Ω, the following simple procedure is a modification of the product replacement algorithm: start with the given tuple $U \in N_k(G,\Omega)$, walk randomly over the graph $\Delta_k^\Omega(G)$ (using the 'oracle' for Ω for generating random $AC_{G\Omega}$-moves and return randomly chosen components v_i of vertices V on your way. See [4, 5, 12] for a more detailed discussion of this algorithm, as well as its further enhancements.

Therefore the understanding of the structure—and ergodic properties—of the Andrews-Curtis graphs $\Delta_k^\Omega(G)$ is of some importance for the theory of black box groups.

The following results are concerned with the connectivity of the relativised Andrews-Curtis graphs of finite groups.

Theorem 2.1 *Let G be a finite Ω-group which is perfect as an abstract group, $G = [G,G]$. Then the graph $\Delta_k^\Omega(G)$ is connected for every $k \geqslant 2$.*

Of course, this result can be immediately reformulated for normal subgroups of finite groups:

Corollary 2.2 *Let G be a finite group and $N \lhd G$ a perfect normal subgroup. Then the graph $\Delta_k^G(N)$ is connected for every $k \geqslant 2$.*

We would like to record another immediate corollary of Theorem 2.1.

Corollary 2.3 *Let G be a perfect finite group, $g_1,\dots,g_k$, $k \geqslant 2$ generate G as a normal subgroup and $\phi : F_k \longrightarrow G$ an epimorphism. Then there exist $f_1,\dots,f_k \in F_k$ such that $\phi(f_i) = g_i$, $i = 1,\dots,k$, and $f_1,\dots,f_k$ generate F_k as a normal subgroup.*

Note that if we take $g_1,\dots,g_k$ as a set of generators for G, then in general we cannot pull them back to a set $f_1,\dots,f_k$ of generators for F_k, an example can be found in $G = \mathrm{Alt}_5$, the alternating group on 5 letters [16].

In case of non-perfect finite groups we prove the following theorem.

Theorem 2.4 *Let G be a finite Ω-group. Then the graph $\Delta_k^\Omega(G)$ is connected for every $k \geqslant d_{G\Omega}(G) + 1$.*

Note this is not true for $k = d_{G\Omega}(G)$, e.g. for when G is abelian.

Corollary 2.5 *Let G be a finite group and $N \lhd G$ a normal subgroup. Then the graph $\Delta_k^G(N)$ is connected for every $k \geqslant d_G(N) + 1$.*

These results lead us to state the following conjecture.

> **Relativised Finitary AC-Conjecture:** *Let G be a finite Ω-group and $k = d_{G\Omega}(G) \geqslant 2$. Then two tuples U, V from $N_k(G, \Omega)$ are $AC_{G\Omega}$-equivalent if and only if they are $AC_{\Omega Ab(G)}$-equivalent in the abelianisation $\mathrm{Ab}(G) = G/[G,G]$, i.e., the connected components of the graph $\Delta_k^\Omega(G)$ are precisely the preimages of the connected components of the graph $\Delta_k^\Omega(\mathrm{Ab}(G))$.*

Theorem 1.1 confirms the conjecture when $G = \Omega$.

3 Elementary properties of AC-transformations

Let G be an Ω-group. From now on for tuples $U, V \in G^k$ we write $U \sim_G V$, or simply $U \sim V$, if the tuples U, V are $AC_{G\Omega}$-equivalent in G.

Lemma 3.1 *Let G be an Ω-group, N a normal Ω-subgroup of G, and $\phi : G \to G/N$ the canonical epimorphism. Suppose $(u_1, \dots, u_k)$ and $(v_1, \dots, v_k)$ are two k-tuples of elements from G. If*

$$(u_1^\phi, \dots, u_k^\phi) \sim_{G/N} (v_1^\phi, \dots, v_k^\phi)$$

then there are elements $m_1, \dots, m_k \in N$ such that

$$(u_1, \dots, u_k) \sim_G (v_1 m_1, \dots, v_k m_k).$$

Moreover, one can use the same system of elementary transformations (after replacing conjugations by elements $gN \in G/N$ by conjugations by elements $g \in G$) .

Proof. Straightforward. □

Lemma 3.2 *Let G be an Ω-group. If $(w_1, \dots, w_k) \in G^k$ then for every i and every element $g \in gp_{G\Omega}(w_1, \dots, w_{i-1}, w_{i+1}, \dots, w_k)$*

$$(w_1, \dots, w_k) \;\sim_G\; (w_1, \dots, w_i g, \dots, w_k).$$

Proof. Obvious. □

4 The N-Frattini subgroup and semisimple decompositions

Definition 1 *Let G be an Ω-group. The N-Frattini subgroup of G is the intersection of all proper maximal normal Ω-subgroups of G, if such exist, and the group G, otherwise. We denote it by $W(G)$.*

Observe, that if G has a non-trivial finite Ω-quotient then $W(G) \neq G$.

An element g in an Ω-group G is called *non-N-generating* if for every subset $Y \subset G$ if $gp_G(Y \cup \{g\}) = G$ then $gp_G(Y) = G$.

Lemma 4.1

(1) *The set of all non-N-generating elements of an Ω-group G coincides with $W(G)$.*

(2) *A tuple $U = (u_1, \ldots, u_k)$ generates G as a normal Ω-subgroup if and only if the images $(\bar{u}_1, \ldots, \bar{u}_k)$ of elements $u_1, \ldots, u_k$ in $\bar{G} = G/W(G)$ generate $\bar{G}$ as normal Ω-subgroup.*

(3) *$G/W(G)$ is an Ω-subgroup of an (unrestricted) Cartesian product of Ω-simple Ω-groups (that is, Ω-groups which do not have proper non-trivial normal Ω-subgroups).*

(4) *As an abstract group, $G/W(G)$ is a subgroup of an (unrestricted) Cartesian product of characteristically simple groups. In particular, if G is finite then $G/W(G)$ is a product of simple groups.*

Proof. (1) and (2) are similar to the standard proof for the analogous property of the Frattini subgroup.

To prove (3) let N_i, $i \in I$, be the set of all maximal proper normal Ω-subgroups of G. The canonical epimorphisms $G \to G/N_i = G_i$ give rise to a homomorphism $\phi : G \to \overline{\prod}_{i \in I} G_i$ of G into the unrestricted Cartesian product of Ω-groups G_i. Clearly, $\ker \phi = W(G)$. So $G/W(G)$ is an Ω-subgroup of the Cartesian product of Ω-simple Ω-groups G_i.

To prove (4) it suffices to notice that $G_i = G/N_i$ has no Ω-invariant normal subgroups, hence is characteristically simple. □

To study the quotient $G/W(G)$ we need to recall a few definitions. Let

$$G = \prod_{i \in I} G_i$$

be a direct product of Ω-groups. Elements $g \in G$ are functions $g : I \to \bigcup G_i$ such that $g(i) \in G_i$ and with finite support $supp(g) = \{i \in I \mid g_i \neq 1\}$. By $\pi_i : G \to G_i$ we denote the canonical projection $\pi_i(g) = g(i)$, we also denote $\pi_i(g) = g_i$. Sometimes we identify the group G_i with its image in G under the canonical embedding $\lambda_i : G_i \to G$ such that $\pi_i(\lambda_i(g)) = g$ and $\pi_j(\lambda_i(g)) = 1$ for $j \neq i$.

An embedding (and we can always assume it is an inclusion) of an Ω-group H into the Ω-group G

$$\phi : H \hookrightarrow \prod_{i \in I} G_i \tag{2}$$

is called a *subdirect decomposition* of H if $\pi_i(H) = G_i$ for each i (here H is viewed as a subgroup of G). The subdirect decomposition (2) is termed *minimal* if $H \cap G_i \neq \{1\}$ for any $i = 1, \ldots, n$, where both G_i and H are viewed as subgroups of G. It is easy to see that given a subdirect decomposition of H one can obtain a minimal one by deleting non-essential factors (using Zorn's lemma).

Definition 2 *An Ω-group G admits a finite semisimple decomposition if $W(G) \neq G$ and $G/W(G)$ is a finite direct product of Ω-simple Ω-groups.*

The following lemma shows that any minimal subdirect decomposition into simple groups is, in fact, a direct decomposition.

Lemma 4.2 *Let $\phi : G \to \prod_{i \in I} G_i$ be a minimal subdirect decomposition of an Ω-group G into Ω-simple Ω-groups G_i, $i \in I$. Then $G = \prod_{i \in I} G_i$.*

Proof. Let $K_i = G \cap G_i$, $i \in I$. It suffices to show that $K_i = G_i$. Indeed, in this event $G \geqslant \prod_{i \in I} G_i$ and hence $G = \prod_{i \in I} G_i$..

Fix an arbitrary $i \in I$. Since ϕ is minimal there exists a non-trivial $g_i \in K_i$. For an arbitrary $x_i \in G_i$ there exists an element $x \in G$ such that $\pi_i(x) = x_i$. It follows that $g_i^x = g_i^{x_i} \in K_i$. Hence $K_i \geqslant gp_{G_i \Omega}(g_i) = G_i$, as required. □

Lemma 4.3 *If an Ω-group G has a finite semisimple decomposition then it is unique (up to a permutation of factors).*

Proof. Obvious. □

Obviously, an Ω-group G admits a finite semisimple decomposition if and only if $W(G)$ is intersection of finitely many maximal normal Ω-subgroups of G. This implies the following lemma.

Lemma 4.4 *A finite Ω-group admits a finite semisimple decomposition.*

5 Connectivity of Andrews-Curtis graphs of perfect finite groups

Recall that a group G is called perfect if $[G, G] = G$.

Lemma 5.1 *Let an Ω-group G admits a finite semisimple decomposition:*

$$G/W(G) = G_1 \times \cdots \times G_k.$$

Then G is perfect if and only if all Ω-simple Ω-groups G_i are non-abelian.

Proof. Obvious. □

We need the following notations to study normal generating tuples in an Ω-group G admitting finite semisimple decomposition. If $g \in \prod_{i \in I} G_i$ then by $supp(g)$ we denote the set of all indices i such that $\pi_i(g) \neq 1$.

Lemma 5.2 *Let $G = \prod_{i \in I} G_i$ be a finite product of Ω-simple non-abelian Ω-groups. If $g \in G$ then $gp_{G\Omega}(g) \geqslant G_i$ for any $i \in supp(g)$.*

Proof. If $g \in G$ and $g_i = \pi_i(g) \neq 1$, then there exists $x_i \in G_i\Omega$ with $[g_i, x_i] \neq 1$. Hence $1 \neq [g, x_i] = [g_i, x_i] \in gp_{G\Omega}(g) \cap G_i$. Since G_i is Ω-simple it coincides with the nontrivial normal Ω-subgroup $gp_{G\Omega}(g) \cap G_i$, as required. □

Let $G/W(G) = \prod_{i \in I} G_i$ be the canonical semisimple decomposition of an Ω-group G. For an element $g \in G$ by $\bar{g}$ we denote the canonical image $gW(G)$ of g in $G/W(G)$ and by $supp(g)$ we denote the support $supp(\bar{g})$ of $\bar{g}$. □

Lemma 5.3 *Let G be a finite perfect Ω-group and $G/W(G) = \prod_{i \in I} G_i$ be its canonical semisimple decomposition. Then a finite set of elements $g_1, \ldots, g_m \in G$ generates G as a normal Ω-subgroup if and only if*

$$supp(g_1) \cup \cdots \cup supp(g_m) = I.$$

Proof. It follows from Lemma 5.2 and Lemma 4.1. □

Proof of Theorem 2.1. We can now prove Theorem 2.1 which settles the Relativised Finitary AC-Conjecture in affirmative for finite perfect Ω-groups.

Let G be a finite perfect Ω-group, $\overline{G} = G/W(G)$, and $\overline{G} = \prod_{i \in I} G_i$ be its canonical semisimple decomposition. Fix an arbitrary $k \geqslant 2$.

Claim 1. Let $U = (u_1, \ldots, u_k) \in N_k(G, \Omega)$. Then there exists an element $g \in G$ with $supp(g) = I$ such that

$$(u_1, \ldots, u_k) \sim_G (g, u_2, \ldots, u_k).$$

Indeed, by Lemma 4.1 the tuple U generates G as a normal subgroup if and only if its image $\overline{U}$ generates $\overline{G}$ as a normal subgroup. Lemma 3.1 shows that it suffices to prove the claim for the Ω-group $\overline{G}$ (recall that $supp(g) = supp(\bar{g})$). So we can assume that $G = \prod_{i \in I} G_i$. Since $U \in N_k(G, \Omega)$, Lemma 5.3 implies that

$$supp(u_1) \cup \cdots \cup supp(u_k) = I.$$

Let $i \in I$ and $i \notin supp(u_1)$. Then there exists an index j such that $i \in supp(u_j)$. By Lemma 5.2, $gp_{G\Omega}(u_j) \geqslant G_i$. So there exists a non-trivial $h \in gp_{G\Omega}(u_j)$ with $supp(h) = \{i\}$. By Lemma 3.2, $U \sim (u_1 h, u_2, \ldots, u_k) = U^*$ and $supp(u_1 h) = supp(u_1) \cup \{i\}$. Now the claim follows by induction on the cardinality of $I \setminus supp(u_1)$. In fact, one can bound the number of elementary AC-moves needed in Claim 1. Indeed, since G_i is non-abelian Ω-simple there exists an element $x \in G\Omega$ such that $u_j^x \neq u_j$. Then the element h above can be taken in the form $h = u_j^x u_j^{-1}$, and only four moves are needed to transform U into U^*. This proves the claim.

Claim 2. Every k-tuple $U_1 = (g, u_2, \ldots, u_k)$ with $supp(g) = I$ is AC-equivalent to a tuple $U_2 = (g, 1, \ldots, 1)$.

By Lemma 5.3 g generates G as a normal Ω-subgroup. Now the claim follows from Lemma 3.2.

Claim 3. Every two k-tuples $U_2 = (g, 1, \ldots, 1)$ and $U_3 = (h, 1, \ldots, 1)$ from $N_k(G, \Omega)$ are AC-equivalent.

Indeed, U_2 is AC-equivalent to $(g, 1, \ldots, 1, g)$. By Lemma 3.2 the former one is AC-equivalent to $(h, \ldots, 1, g)$, which is AC-equivalent to $(h, 1, \ldots, 1)$, as required.

The theorem follows from Claims 1, 2, and 3. □

6 Arbitrary finite groups

Lemma 6.1 *Let*

$$G = G_1 \times \cdots \times G_s \times A \tag{3}$$

be a direct decomposition of an Ω-group G into a product of non-abelian Ω-simple Ω-groups $G_i, i = 1, \ldots s$, and an abelian Ω-group A. Then, assuming $G \neq 1$,

$$d_{G\Omega}(G) = \max\{d_{A\Omega}(A), 1\}.$$

Proof. Put $S(G) = G_1 \times \cdots \times G_s$. Since A is a quotient of G then $d_{G\Omega}(G) \geqslant d_{A\Omega}(A)$. Therefore, $d_{G\Omega}(G) \geqslant \max\{d_{A\Omega}(A), 1\}$. On the other hand, if g generates $S(G)$ as a normal Ω-subgroup (such g exists by Lemma 5.3) and $a_1, \ldots, a_{d_\Omega(A)}$ generate A then we claim that the tuple of elements from G:

$$(ga_1, a_2, \ldots, a_{d_\Omega(A)})$$

generates G as a normal Ω-subgroup. Indeed, let $g = g_1 \cdots g_s$ with $1 \neq g_i \in G_i$. Since G_i is non-abelian then g_i is not central in G_i and hence there exists $h_i \in G_i$ such that $[g_i, h_i] \neq 1$. It follows that if $h = h_1 \ldots h_s$ then $[g, h] \neq 1$ and $supp([g, h]) = \{1, \ldots, n\}$. In particular, $[g, h]$ belongs to $N = gp_{G\Omega}(ga_1, a_2, \ldots, a_{d_\Omega(A)})$ and generates $S(G)$ as a normal Ω-subgroup. Therefore, $S(G) \subset N$ and hence $a_1, \ldots, a_{d_\Omega(A)} \in N$, which implies that $G = N$. This shows that $d_{G\Omega}(G) = \max\{d_\Omega(A), 1\}$, as required.

Proof of Theorem 2.4. Let G be a minimal counterexample to the statement of the theorem. Then G is not perfect. G is also non-abelian by Fact 1.2. Put $t = d_{G\Omega}(G)$ and $k \geqslant t + 1$. Let M be a minimal non-trivial normal Ω-subgroup of G. It follows that $M \neq G$, and the theorem holds for the Ω-group $\overline{G} = G/M$. Obviously, $k > d_{G\Omega}(G) \geqslant d_{\bar{G}\Omega}(\overline{G})$, hence the AC-graph $\Delta_k^\Omega(\overline{G})$ is connected. Fix any tuple $(z_1, \ldots, z_t) \in N_t(G, \Omega)$. If $(y_1, \ldots, y_k)$ is an arbitrary tuple from $N_k(G, \Omega)$ then the k-tuples $(\bar{y}_1, \ldots, \bar{y}_k)$ and $(\bar{z}_1, \ldots, \bar{z}_t, 1, \ldots, 1)$ are

AC-equivalent in $\overline{G}$. Hence by Lemma 3.1 there are elements $m_1, \ldots, m_k \in M$ such that

$$(y_1, \ldots, y_k) \sim (z_1 m_1, \ldots, z_t m_t, m_{t+1}, \ldots, m_k).$$

We may assume that one of the elements $m_{t+1}, \ldots, m_k$ in distinct from 1, say $m_k \neq 1$. Indeed, if $m_{t+1} = \ldots = m_k = 1$ then the elements $z_1 m_1, \ldots, z_t m_t$ generate G as a normal Ω-subgroup, hence applying AC-transformations we can get any non-trivial element from M in the place of m_k. Since M is a minimal normal Ω-subgroup of G it follows that M is the $G\Omega$-normal closure of m_k in G, in particular, every m_i is a product of conjugates of $m_k^{\pm 1}$. Applying AC-transformations we can get rid of all elements m_i, $i = 1, \ldots, m_t$, in the tuple above. Hence,

$$(z_1 m_1, \ldots, z_t m_t, m_{t+1}, \ldots, m_k) \sim (z_1, \ldots, z_t, 1, \ldots, 1, m_k).$$

But $(z_1, \ldots, z_t) \in N_t(G, \Omega)$, hence

$$(z_1, \ldots, z_t, 1, \ldots, m_k) \sim (z_1, \ldots, z_t, 1, \ldots, 1).$$

We showed that any k-tuple $(y_1, \ldots, y_k) \in N_k(G, \Omega)$ is AC-equivalent to the fixed tuple $(z_1, \ldots, z_t, 1, \ldots, 1)$. So the AC-graph $\Delta_k^\Omega(G)$ is connected and G is not a counterexample. This proves the theorem. □

7 Proof of Theorem 1.1

We denote by $\tilde{g}$ the image of $g \in G$ in the abelinisation $\mathrm{Ab}(G) = G/[G, G]$.

We systematically, and without specific references, use elementary properties of Andrews-Curtis transformations, Lemmas 3.1 and 3.2.

Suppose Theorem 1.1 is false. Consider a counterexample G of minimal order for a given $k \geqslant d_G(G)$. For a given k-tuple $(g_1, \ldots, g_k) \in N_k(G)$ we denote by $\mathcal{C}(g_1, \ldots, g_k)$ the set

$$\{(h_1, \ldots, h_k) \in N_k(G) \mid (\tilde{g}_1, \ldots, \tilde{g}_k) \sim (\tilde{h}_1, \ldots, \tilde{h}_k) \;\&\; (g_1, \ldots, g_k) \not\sim (h_1, \ldots, h_k)\}$$

Put

$$\mathcal{D} = \{(g_1, \ldots, g_k) \in N_k(G) \mid \mathcal{C}(g_1, \ldots, g_k) \neq \emptyset\}.$$

Then the set $\mathcal{D}$ is not empty. Consider the following subset of $\mathcal{D}$:

$$\mathcal{E} = \{(g_1, \ldots, g_k) \in \mathcal{D} \mid |gp_G(g_2, \ldots, g_k)| \text{ is minimal possible}\}.$$

Finally, consider the subset $\mathcal{F}$ of $\mathcal{E}$:

$$\mathcal{F} = \{(g_1, \ldots, g_k) \in \mathcal{E} \mid \; |gp_G(g_1)| \text{ is minimal possible }\}$$

In order to prove the theorem it suffices to show that G is abelian.

Fix an arbitrary tuple $(g_1, \ldots, g_k) \in \mathcal{F}$ and an arbitrary tuple $(h_1, \ldots, h_k) \in \mathcal{C}(g_1, \ldots, g_k)$. Denote $G_1 = gp_G(g_1)$ and $G_2 = gp_G(g_2, \ldots, g_k)$.

The following series of claims provides various inductive arguments which will be in use later.

Notice that the minimal choice of g_1 and $g_2, \dots, g_k$ can be reformulated as

Claim 1.1 *Let* $f_1 \in G_1$, $f_2, \dots, f_k \in G_2$ *such that* $(f_1, f_2, \dots, f_k) \in \mathcal{C}(g_1, \dots, g_k)$. *Then*

$$gp_G(f_1) = G_1 \text{ and } gp_G(f_2, \dots, f_k) = G_2.$$

Claim 1.2 *Let* $f_1 \in G$, $f_2, \dots, f_k \in G_2$ *such that* $(f_1, f_2, \dots, f_k) \in \mathcal{C}(g_1, \dots, g_k)$. *Then*

$$gp_G(f_2, \dots, f_k) = G_2.$$

Claim 1.3 *Let* M *be a non-trivial normal subgroup of* G. *Then*

$$(h_1, \dots, h_k) \sim (g_1 m_1, \dots, g_{k-1} m_{k-1}, g_k m_k)$$

for some $m_1, \dots, m_k \in M$.

Indeed, obviously

$$(h_1 M, \dots, h_k M), (g_1 M, \dots, g_k M) \in N_k(G/M).$$

Moreover, since

$$(\tilde{g}_1, \dots, \tilde{g}_k) \sim (\tilde{h}_1, \dots, \tilde{h}_k)$$

there exists a sequence of AC-moves $t_1, \dots, t_n$ (where each t_i is one of the transformations (1)–(4), with the specified values of w in the case of transformations (4)) and elements $c_1, \dots, c_k \in [G, G]$ such that

$$(h_1, \dots, h_k) t_1 \cdots t_k = (g_1 c_1, \dots, g_k c_k)$$

Therefore

$$(h_1 M, \dots, h_k M) t_1 \cdots t_k = (g_1 c_1 M, \dots, g_k c_k M)$$

Since $c_i M \in [G/M, G/M]$ for every $i = 1, \dots, k$ this shows that the images of the tuples $(h_1 M, \dots, h_k M)$ and $(g_1 M, \dots, g_k M)$ are AC-equivalent in the abelianisation $Ab(G/M)$. Now the claim follows from the fact that $|G/M| < |G|$ and the assumption that G is the minimal possible counterexample.

The following claim says that the set $\mathcal{C}(g_1, \dots, g_k)$ is closed under $\sim$.

Claim 1.4 *If* $(e_1, \dots, e_k) \in \mathcal{C}(g_1, \dots, g_k)$ *and* $(f_1, \dots, f_k) \sim (e_1, \dots, e_k)$ *then* $(f_1, \dots, f_k) \in \mathcal{C}(g_1, \dots, g_k)$

Now we study the group G in a series of claims.

Claim 2. $G = G_1 \times G_2$.

Indeed, it suffices to show that $G_1 \cap G_2 = 1$. Assume the contrary, then $M = G_1 \cap G_2 \neq 1$ and by Claim 1.3

$$(h_1, \ldots, h_k) \sim (g_1 m_1, \ldots, g_{k-1} m_{k-1}, g_k m_k)$$

for some $m_1, \ldots, m_k \in M$. By Claim 1.4

$$(g_1 m_1, \ldots, g_{k-1} m_{k-1}, g_k m_k) \in \mathcal{C}(g_1, \ldots, g_k)$$

By Claim 1.1,

$$gp_G(g_1 m_1) = G_1, \quad gp_G(g_2 m_2, \ldots, g_k m_k) = G_2$$

and we can represent the elements $m_2, \ldots, m_k \in G_1 \cap G_2$ as products of conjugates of $g_1 m_1$, therefore deducing that

$$(g_1 m_1, g_2 m_2 \ldots, g_k m_k) \sim (g_1 m_1, g_2, \ldots, g_k).$$

Since $m_1 \in gp_G(g_2, \ldots, g_k\rangle$, we conclude that

$$(g_1 m_1, g_2, \ldots, g_k) \sim (g_1, g_2, \ldots, g_k),$$

and therefore

$$(h_1, \ldots, h_k) \sim (g_1, \ldots, g_k),$$

a contradiction. This proves the claim. □

CLAIM 3. $[G_2, G_2] = 1$. *In particular,* $G_2 \leqslant Z(G)$.

Indeed, assume the contrary. Then $M = [G_2, G_2] \neq 1$ and by Claim 1.3

$$(h_1, \ldots, h_k) \sim (g_1 m_1, \ldots, g_k m_k), \quad m_1, \ldots, m_k \in M \leqslant G_2.$$

By virtue of Claims 1.4 and 1.2, $gp_G(g_2 m_2, \ldots, g_k m_k) = G_2$ and hence $m_1 \in gp_G(g_2 m_2, \ldots, g_k m_k)$. It follows that

$$(g_1 m_1, g_2 m_2, \ldots, g_k m_k) \sim (g_1, g_2 m_2 \ldots, g_k m_k).$$

Therefore it will be enough to prove

$$(g_1, g_2 m_2, \ldots, g_k m_k) \sim (g_1, g_2, \ldots, g_k).$$

We proceed as follows, systematically using the fact that $g_2, \ldots, g_k$ and all their conjugates commute with all the conjugates of g_1.

We start with a series of Nielsen moves which lead to

$$\begin{aligned} (g_1, g_2 m_2 \ldots, g_k m_k) &\sim (g_1,\, g_1 \cdot g_2 m_2, g_3 m_3, \ldots, g_k m_k) \\ &\sim (g_1 \cdot m_2,\, g_1 g_2 m_2, g_3 m_3, \ldots, g_k m_k). \end{aligned}$$

The last transformation is the key for the whole proof and requires some explanation. Since m_2 belongs to

$$[G_2, G_2] = [gp_G(g_2 m_2, \ldots, g_k m_k), gp_G(g_2 m_2, \ldots, g_k m_k)],$$

m_2 can be expressed as a word

$$w(x_2, \dots, x_k) = (x_{i_1}^{f_1})^{\varepsilon_1} \cdots (x_{i_l}^{f_l})^{\varepsilon_l}$$

where $x_i = g_i m_i$, $i = 2, \dots, k$, $f_j \in G$ and the word w is balanced for each variable x_i, that is, for each $h = 2, \dots, k$, the sum of exponents for each x_h is zero:

$$\sum_{i_j = h} \varepsilon_j = 0.$$

Moreover, since $G = G_1 \times G_2$, we can choose $f_j \in G_2$, whence commuting with $g_1 \in G_1$. Therefore

$$w(g_1 x_2, x_3, \dots, x_k) = w(x_2, x_3, \dots, x_k)$$

and

$$w(g_1 g_2 m_2, g_3 m_3, \dots, g_k m_k) = m_2.$$

Hence, by several consecutive multiplications by appropriate conjugates of $g_1 g_2 m_2$ and $g_i m_i$, $i = 3, \dots, k$, we can produce the factor m_2 in the leftmost position in the tuple. We now continue:

$$\begin{aligned}(g_1 m_2,\, g_1 g_2 m_2, g_3 m_3, \dots, g_k m_k) &\sim (g_1 m_2,\, g_1 g_2 m_2 \cdot (g_1 m_2)^{-1}, g_3 m_3, \dots, g_k m_k) \\ &= (g_1 m_2,\, g_2, g_3 m_3, \dots, g_k m_k).\end{aligned}$$

Again by Claims 1.4 and 1.2 $G_2 = gp_G(g_2, g_3 m_3, \dots, g_k m_k\rangle$. Since $m_2 \in G_2$,

$$(g_1 m_2,\, g_2, g_3 m_3, \dots, g_k m_k) \sim (g_1,\, g_2,\, g_3 m_3, \dots, g_k m_k).$$

Next we want to kill m_3. Present m_3 as a balanced word in $g_2, g_3 m_3, \dots, g_k m_k$ conjugated by elements $f_i \in G_2$. Note that they all commute with g_1. As before,

$$m_3 = w(g_2, g_1 g_3 m_3, g_4 m_4, \dots, g_k m_k)$$

(and, actually, $m_3 = w(g_2, y_3, \dots, y_k)$ where y_i are arbitrarily chosen from $g_i m_i$ or $g_1 g_i m_i$, $i = 3, \dots, k$.).

Thus we have:

$$\begin{aligned}(g_1,\, g_2, g_3 m_3, \dots, g_k m_k) &\sim (g_1, g_2, g_1 g_3 m_3, g_4 m_4, \dots, g_1 g_k m_k) \\ &\sim (g_1 m_3, g_2, g_1 g_3 m_3, g_4 m_4, \dots, g_k m_k) \\ &\sim (g_1 m_3, g_2, g_3, g_4 m_4, \dots, g_k m_k) \\ &\sim (g_1, g_2, g_3, g_4 m_4, \dots, g_k m_k)\end{aligned}$$

(the last transformation uses the fact that $gp_G(g_2, g_3, g_4 m_4, \dots, g_k m_k) = G_2$ by Claims 1.4 and 1.2).

One can easily observe that we can continue this argument in a similar way until we come to $(g_1, g_2, \dots, g_k)$ - contradiction, which completes the proof of the claim. □

Claim 4.
$$[G_1, G_1] = 1.$$

Let $[G_1, G_1] \neq 1$. For a proof, take a minimal non-trivial normal subgroup M of G which lies in $[G_1, G_1]$. Again, by Claim 1.3, we conclude that

$$(h_1, \dots, h_k) \sim (g_1m_1, g_2m_2, \dots, g_km_k)$$

for some $m_1, \dots, m_k \in M$. We assume first that $M \leqslant gp_G(g_1m_1)$. Then

$$(g_1m_1, g_2m_2 \dots, g_km_k) \quad \sim \quad (g_1m_1, g_2, \dots, g_k)$$

and $gp_G(g_1m_1) = gp_G(g_1)$ by Claims 1.4 and 1.1. In particular,

$$M \leqslant [gp_G(g_1m_1), gp_G(g_1m_1)] = [gp_G(g_2g_1m_1), gp_G(g_2g_1m_1)],$$

where the last equality follows from the observation that $g_2 \in Z(G)$. We shall use this in further transformations:

$$\begin{aligned}(g_1m_1, g_2, \dots, g_k) &\sim (g_1m_1, g_2g_1m_1, g_3, \dots, g_k)\\ &\sim (g_1, g_2g_1m_1, g_3, \dots, g_k)\\ &\sim (g_1, g_2, g_3, \dots, g_k).\end{aligned}$$

This shows that $(h_1, \dots, h_k) \sim (g_1, \dots, g_k)$ - contradiction. Therefore we can assume that $M \not\subseteq gp_G(g_1m_1)$ and hence $M \cap gp_G(g_1m_1) = 1$. We claim that not all of the elements $m_2, \dots, m_k$, are trivial. Otherwise

$$(h_1, \dots, h_k) \sim (g_1m_1, g_2, \dots, g_k),$$

and we can repeat the previous argument and come to a contradiction. So we assume, with out loss of generality, that $m_2 \neq 1$.

If M is non-abelian then

$$M = [M, M] = [gp_G(m_2), gp_G(m_2)] = [gp_G(g_2m_2), gp_G(g_2m_2)]$$

and

$$\begin{aligned}(g_1m_1, g_2m_2, g_3m_3, \dots, g_km_k) &\sim (g_1, g_2m_2, g_3m_3, \dots, g_km_k)\\ &\sim (g_1, g_2, g_3, \dots, g_k);\end{aligned}$$

we use in the last transformation that $gp_G(g_1) = G_1 \geqslant M$.

Therefore we can assume that M is abelian. Since $M \cap gp_G(g_1m_1) = 1$ we conclude that $[M, gp_G(g_1m_1)] = 1$. But then $[M, gp_G(g_1)] = 1$. In particular, $M \leqslant Z(G)$ and the subgroup $[gp_G(g_1m_1), gp_G(g_1m_1)] = [gp_G(g_1), gp_G(g_1)]$ contains M. But this is a contradiction with $M \cap gp_G(g_1m_1) = 1$. This proves the claim. □

Final contradiction. Claims 3 and 4 now yield that G is abelian, as required. □ □

References

[1] 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.

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

[3] L. Bartholdi, R. I. Grigorchuk and Z. Sunik, 'Branch groups', in *Handbook of Algebra*, vol. 3 (M. Hazelwinkel, ed.), 2003.

[4] A. V. Borovik, 'Centralisers of involutions in black box groups', *Computational and Statistical Group Theory* (R. Gilman et al., eds.), Contemporary Mathematics 298 (2002), 7–20; math.GR/0110233.

[5] A. V. Borovik, E. I. Khukhro, A. G. Myasnikov, 'The Andrews-Curtis Conjecture and black box groups', to appear in *Int. J. Algebra and Computation.*

[6] 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.

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

[8] R. I. Grigorchuk,'Degrees of growth of finitely generated groups and the theory of invariant means', *Math. USSR – Izv.* 25, 2 (1985), 259–300.

[9] R. I. Grigorchuk, 'Just infinite branch groups', in *New Horizons in pro-p-groups* (M. P. F. du Sautoy, D. Segal and A. Shalev, eds.), Birkhäuser, Boston, 2000, 121–179.

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

[11] 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.

[12] C. R. Leedham-Green and S. H. Murray, 'Variants of product replacement', *Computational and statistical group theory* (R. Gilman et al., eds.), Contemp. Math., 298 (2002), 97–104.

[13] Y. G. Leonov, 'The conjugacy problem in a class of 2-groups', *Mat. Zametki* 64 4 (1998), 573—583.

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

[15] A. G. Myasnikov, 'Extended Nielsen transformations and the trivial group', *Math. Notes* 35 (1984) no. 3–4, 258–261.

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

[17] 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.

[18] A. V. Rozhkov, 'The conjugacy problem in an automorphism group of an infinite tree', *Mat. Zametki* 64 4 (1998), 592–597.

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/
Alexander Lubotzky, Department of Mathematics, Hebrew University, Givat Ram, Jerusalem 91904, Israel; alexlub@math.huji.ac.il
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