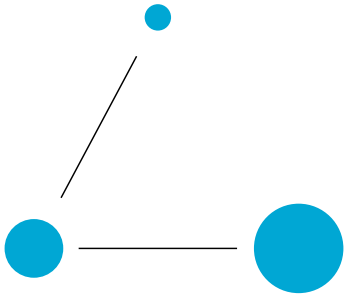
Annales Henri Lebesgue
5 (2022) 73-92



ANNALES
HENRI LEBESGUE

PAUL-HENRY LEEMANN

MIKAEL DE LA SALLE

CAYLEY GRAPHS WITH FEW AUTOMORPHISMS: THE CASE OF INFINITE GROUPS

GROUPES DE CAYLEY AVEC PEU D'AUTOMORPHISMES : LE CAS DES GROUPES INFINIS

Abstract. — We characterize the finitely generated groups that admit a Cayley graph whose only automorphisms are the translations, confirming a conjecture by Watkins from 1976. The proof relies on random walk techniques. As a consequence, every finitely generated group admits a Cayley graph with countable automorphism group. We also treat the case of directed graphs.

Résumé. — Nous caractérisons les groupes de type fini qui admettent un graphe de Cayley dont les seuls automorphismes sont les translations. Cela confirme une conjecture de Watkins

Keywords: GRR, DRR, ORR, Cayley graph, automorphisms of graphs, generalized dihedral group, generalized dicyclic group, regular automorphism group.
2020 *Mathematics Subject Classification:* 53C28, 53C26, 32Q45.
DOI: `https://doi.org/10.5802/ahl.118`
(*) The first author was supported by Swiss National Fund for Scientific Research Grant No. 200021_188578. The second author's research was supported by the ANR projects AGIRA (ANR-16-CE40-0022) and ANCG (ANR-19-CE40-0002-01). Part of this work was performed within the framework of the LABEX MILYON (ANR-10-LABX-0070) of Université de Lyon, within the program "Investissements d'Avenir" (ANR-11-IDEX-0007) operated by the French National Research Agency (ANR).

formulée en 1976. Les preuves reposent sur des méthodes de marches aléatoires. Une conséquence des résultats est que tout groupe de type fini admet un graphe de Cayley dont le groupe d'automorphismes est dénombrable. Nous obtenons des résultats similaires pour les graphes dirigés.

1. Introduction

Given a group G and a symmetric generating set $S \subseteq G \setminus \{1\}$, the Cayley graph $\mathrm{Cay}(G, S)$ is the simple unoriented graph with vertex set G and an edge between g and h precisely when $g^{-1}h \in S$. By construction, the action by left-multiplication of G on itself induces an action of the group on its Cayley graph, which is free and vertex-transitive.

We are here interested in the question to decide when S can be chosen so that these are all the automorphisms of $\mathrm{Cay}(G, S)$, or equivalently the automorphism group of the graph acts freely and transitively on the vertex set. The main result of this paper is

THEOREM 1.1. — *Every finitely generated group G that is not virtually abelian admits a finite degree Cayley graph whose automorphism group is not larger than G acting by left-translation.*

A Cayley graph of G whose automorphism group acts freely on its vertex set is called a *graphical regular representation*, or GRR.

The main result in [LS21] is similar to Theorem 1.1, but with the assumption of not being virtually abelian replaced by having an element of infinite (or sufficiently large) order and being non-abelian and non-generalized dicyclic (see Section 2 for definitions). Combining both results, we obtain that the infinite finitely generated groups that do not admit a GRR are precisely the abelian and the generalized dicyclic groups.

Together with the results from [ERS70, God81, Het76, Imr69, Imr75, IW76, NW72, Wat71, Wat72, Wat74] that treated the case of finite groups[(1)], we obtain the following result. The equivalence between (1) and (3) confirms Watkin's conjecture [Wat76].

COROLLARY 1.2. — *For a finitely generated group G, the following are equivalent:*

(1) *G admits a* GRR*,*
(2) *G admits a finite degree* GRR*,*
(3) *G does not belong to the following list:*
   - *the non-trivial abelian groups different from $\mathbf{Z}/2\mathbf{Z}$ and $(\mathbf{Z}/2\mathbf{Z})^n$ for $n \geqslant 5$,*
   - *the generalized dicyclic groups,*
   - *the following 10 finite groups of cardinality at most 32[(2)]: the dihedral groups of order $6, 8, 10$, the alternating group A_4, the products $Q_8 \times \mathbf{Z}/3\mathbf{Z}$*

[(1)] We refer to the introduction of [LS21] and the references therein for a more detailed exposition of the work on finite groups.

[(2)] with GAP IDs respectively $[6,1], [8,3], [10,1], [12,3], [24,11], [32,26], [16,13], [16,6], [18,4], [27,3]$. The first digit in the GAP ID is the order of the group, and the second is the label of the group

and $Q_8 \times \mathbf{Z}/4\mathbf{Z}$ (for Q_8 the quaternion group) and the four groups given by the presentations

$$\left\langle a, b, c \middle| a^2 = b^2 = c^2 = 1, abc = bca = cab \right\rangle,$$
$$\left\langle a, b \middle| a^8 = b^2 = 1, b^{-1}ab = a^5 \right\rangle,$$
$$\left\langle a, b, c \middle| a^3 = b^3 = c^2 = (ac)^2 = (bc)^2 = 1, ab = ba \right\rangle,$$
$$\left\langle a, b, c \middle| a^3 = b^3 = c^3 = 1, ac = ca, bc = cb, b^{-1}ab = ac \right\rangle.$$

1.1. Consequences

Another consequence of our result is the following fact, which was a motivation of the second-named author for [LS21] and the present work, see [ST19]. This solves a conjecture raised in [ST19].

COROLLARY 1.3. — *Every finitely generated group admits a finite degree Cayley graph whose automorphism group is countable.*

Recall the classical fact that the topology of pointwise convergence on vertices turns the automorphism group of a finite degree graph into a locally compact metrizable group: a sequence $(\phi_n)_n$ of automorphisms converges to ϕ if and only if for every x, $\phi_n(x) = \phi(x)$ for all but finitely many n. For this topology the stabilizer of a vertex is a compact subgroup, and therefore either finite or uncountable. Therefore Corollary 1.3 can be equivalently phrased as *Every finitely generated group admits a finite degree Cayley graph whose automorphism group is discrete* (equivalently *has finite stabilizers*).

Corollary 1.3 has interesting graph-theoretical consequences, that we now explain. Following [Ben13, Geo17, ST19], given two graphs X and Y and a positive integer R, we say that Y is *R-locally X* if every ball of radius R in Y appears as a ball of radius R in X. A graph X is *local to global rigid* (LG-rigid) if there is $R > 0$ such that any graph that is R-locally X is covered by X.

COROLLARY 1.4. — *Every finitely presented group admits a finite degree Cayley graph that is LG-rigid.*

The existence of a *LG*-rigid finite degree Cayley graph is actually equivalent to finite presentability, as a non finitely presented group cannot admit LG-rigid Cayley graphs, see [ST19].

1.2. About the proof

Theorem 1.1 is only new for groups with bounded exponents: the case of groups with elements of infinite (or arbitrarily large) order was covered in [LS21]. We have

in GAP's numbering of groups of that order. For example, the last group in the list is of order 27, and is the third in GAP's list of groups of order 27. It is also isomorphic to the free Burnside group $B(2, 3)$.

therefore concentrated our efforts for finitely generated torsion groups, but the proof that we finally managed to obtain turned out to apply without much more efforts in the generality of Theorem 1.1.

The proof relies partly on the results from [LS21], and partly on new ideas involving random walks on groups. In particular we use some recent results by Tointon [Toi20] on the probability that two independent realizations of the random walk commute. Necessary background of group theory is presented in Section 2. We discuss the needed contributions from [LS21] in Section 3. The new aspects, including random walk reminders are presented in Section 4. In the small Section 5, we deduce the main theorem and its corollaries, and then in Section 6 we discuss a conjecture that would significantly simplify our proofs. Finally, in Section 7 we briefly discuss some directed variants of the GRR problem.

Acknowledgements

Both authors thank the anonymous referees for their useful comments and suggestions.

2. Group theory background

This short section sets the group theoretical notation and terminology and contains some standard group theory results that will be used later. It can be safely skipped by most readers.

We start with a definition used in the introduction.

Definition 2.1. — *A* generalized dicyclic group *is a non-abelian group with an abelian subgroup A of index 2 and an element x not in A such that $x^4 = 1$ and $xax^{-1} = a^{-1}$ for all $a \in A$.*

A group is said to be of *exponent* n if every element satisfies $g^n = 1$, and of *bounded exponent* if it is of exponent n for some integer n. It is known that finitely generated groups of exponent n are finite if $n \in \{1, 2, 3, 4, 6\}$, but can be infinite for large n, see [Rob95, 14.2].

We shall denote the index of a subgroup H of G by $|G : H|$.

If A is a subset of a group G, the *centralizer* of A in G is the subgroup denoted $C_G(A)$ of elements of G commuting with every element of A. The centralizer of G in G is the *center* $Z(G)$ of G. If $g \in G$, we write $C_G(s)$ for $C_G(\{s\})$.

In the following, by *group property* we mean of property P that a group G can have ("G is P") or not ("G is not P").

Definition 2.2. — *If P and Q are two group properties, we say that a group G is:*

- *P-by-Q if it admits a normal subgroup N that is P such that the quotient group G/N is Q,*
- *locally P if every finitely generated subgroup of G is P,*
- *virtually P if G admits a finite index subgroup H that is P.*

Observe that a locally finite group G is finitely generated if and only if it is finite.

A group G is 2-*nilpotent* (or nilpotent of class $\leqslant 2$) if it is an extension $1 \to N \to G \to K \to 1$ of abelian groups N, K with $N \leqslant Z(G)$.

We will use later the following elementary fact:

LEMMA 2.3. — *If $1 \to N \to G \to K \to 1$ is an extension with K virtually abelian and $|G : C_G(N)| < \infty$, then G is virtually 2-nilpotent.*

Proof. — If $K_1 < K$ is abelian with finite index, then the intersection of the preimage of K_1 in G with the centralizer $C_G(N)$ of N in G is the intersection of two finite index subgroups of G and therefore has finite index in G. It is clearly 2-nilpotent. □

We also need the following folklore variant:

LEMMA 2.4. — *If a finitely generated group is finite-by-(virtually abelian), then it is virtually abelian.*

Proof. — A finite-by-(virtually abelian) group G_0 contains a finite index finite-by-abelian group G (the preimage in G_0 of the finite index abelian subgroup in the quotient). So let $1 \to N \to G \to K \to 1$ with N finite and K abelian. Let $g \in G$. Since K is abelian, the conjugacy class of g is contained in gN and is thus finite; equivalently $C_G(g)$ has finite index in G. If G_0 is finitely generated, then so is G. If S is a finite generating set of G, the center of G is equal to $\cap_{g \in S} C_G(g)$ and therefore is an abelian subgroup of finite index in G. This proves that G, and hence G_0, is virtually abelian. □

We will make use of the following lemma which is due to Dicman, see for example [Rob95, 14.5.7].

LEMMA 2.5 (Dicman's Lemma). — *Let G be a group and $X \subseteq G$ be a finite subset that is invariant by conjugation by elements of G and such that every $g \in X$ is of finite order. Then the normal subgroup $\langle X \rangle^G$ is finite.*

3. Constructing Cayley graphs with few automorphisms

We follow the same general strategy for constructing Cayley graphs with few automorphisms as the one initiated in [ST19] and later developed in [LS21]. There are two independent steps.

The first step consists in finding a finite symmetric generating set S_1 of G in which the only knowledge of the *colour* $\{g^{-1}h, h^{-1}g\} \subseteq S_1$ of every edge $\{g, h\}$ allows us to reconstruct the orientation of every edge. To say it in formulas, following [LS21] let us say that the pair (G, S_1) is *orientation-rigid* if the only permutations ϕ of G such that $\phi(gs) \in \{\phi(g)s, \phi(g)s^{-1}\}$ for every $g \in G$ and $s \in S_1$ are the left-translations by elements of G.

The second step is, given a finite symmetric generating set $S_1 \subseteq G$, to find another finite symmetric generating set $S_1 \subseteq S_2$ such that every automorphism ϕ of $\mathrm{Cay}(G, S_2)$ induces a colour-preserving automorphism of $\mathrm{Cay}(G, S_1)$, that is satisfies $\phi(gs) \in \{\phi(g)s, \phi(g)s^{-1}\}$ for every $g \in G$ and $s \in S_1$.

Clearly, if we are able to perform both steps and we apply the second step for S_1 that is orientation-rigid, then we obtain a Cayley graph $\mathrm{Cay}(G, S_2)$ in which the only automorphisms are the translations.

For the first step, there is nothing new to do, as we know exactly which groups admit an orientation-rigid pair (G, S_1) with S_1 generating. The following is a portion of [LS21, Theorem 7].

THEOREM 3.1. — *Let G be a finitely generated group that is neither abelian [with an element of order greater than 2] nor generalized dicyclic, and $S_0 \subseteq G \setminus \{1\}$ be a finite symmetric generating set. Then (G, S_1) is orientation-rigid where $S_1 = (S_0 \cup S_0^2 \cup S_0^3) \setminus \{1\}$.*

So all the new work lies in the second step. As in [LS21, ST19], the main tool to recognize the colour of the edges is by *counting triangles*. If S is a finite symmetric subset of a group G, we denote by $\mathrm{N}_3(s, S)$ the number of triangles in the Cayley graph $\mathrm{Cay}(G, S)$ containing both vertices 1 and s:

$$\mathrm{N}_3(s, S) \coloneqq |S \cap sS| \cdot \mathbf{1}_{s \in S}.$$

The relevance of this is the following easy observation that automorphisms preserve the number of triangles of a given edge: if ϕ is an automorphism of $\mathrm{Cay}(G, s)$, then for every $g, h \in G$,

$$\mathrm{N}_3\left(g^{-1}h, S\right) = \mathrm{N}_3\left(\phi(g)^{-1}\phi(h), S\right).$$

Clearly, $\mathrm{N}_3(s, S) = \mathrm{N}_3(s^{-1}, S)$, so counting triangles can never do more than recover the colour of edges. But if $s \in S$ is such that the only elements t of S such that $\mathrm{N}_3(s, S) = \mathrm{N}_3(t, S)$ are s and s^{-1}, then the automorphism group of $\mathrm{Cay}(G, S)$ preserves the colour of every edge corresponding to s. Our main new technical result is the following.

PROPOSITION 3.2. — *Let G be a finitely generated group that is not virtually abelian and $S \subset G \setminus \{1\}$ be a finite generating set. Then there exists a finite symmetric generating set $S \subseteq \widetilde{S} \subset G \setminus \{1\}$ of size bounded by $2|S|(|S| + 14)$ such that for all $s \in S$ and $t \in \widetilde{S}$, if $\mathrm{N}_3(s, \widetilde{S}) = \mathrm{N}_3(t, \widetilde{S})$ then $t = s$ or $t = s^{-1}$.*

Moreover, $\widetilde{S} \setminus S$ does not have elements of order 2.

The next section is devoted to the proof of the above Proposition.

4. Squares and random walks

The aim of this section is to prove Proposition 3.2. We start with some discussions on the *square map* $\mathrm{sq}\colon G \to G$ defined by $\mathrm{sq}(g) = g^2$, which will play an important role in our work. The main result of this section is Proposition 4.4, that will be proved using random walks.

4.1. On the squares in finitely generated groups

In our previous work, [LS21], we restricted our attention on groups G with an element of "big" (possibly infinite) order. In other words, we asked G to have a "big" cyclic subgroup C. The main advantage of this hypothesis is the fact that in cyclic groups $\mathrm{sq}^{-1}(g)$ consist of at most 2 elements and therefore, for any finite subset F of G the set $\mathrm{sq}^{-1}(F) \cap C$ is finite of size at most $2|F|$. In order to generalize results from [LS21] to arbitrary infinite finitely generated groups, we first need to establish some facts on the map sq and on its fibers. We begin our analysis of the map sq by showing that infinite finitely generated groups contains infinitely many squares.

As a first consequence of Dicman's Lemma 2.5, we obtain the following

LEMMA 4.1. — *Let n be a fixed integer in $\{1, 2, 3, 4, 6\}$. If G is an infinite finitely generated group, then $\{g^2 \mid g \in G, g^n \neq 1\}$ is infinite.*

Proof. — By contradiction, suppose that the set $X = \{g^2 \mid g \in G, g^n \neq 1\}$ is finite. This set is invariant by conjugation and, since it is finite, contains only elements of finite order. Hence by Dicman's Lemma, it generates a finite normal subgroup N. But then G/N is an infinite finitely generated group in which every element satisfies $g^n = 1$ or $g^2 = 1$, so is of exponent $n' = n$ if n is even and $n' = 2n$ is n is odd. In both cases, $n' \in \{1, 2, 3, 4, 6\}$, so the free Burnside group $B(m, n')$ being finite (see for example [Rob95, 14.2]), the group G/N is finite, which is the desired contradiction. □

COROLLARY 4.2. — *Let G be a finitely generated group. Then G is infinite if and only if* $\mathrm{sq}(G)$ *is infinite.*

The following elementary lemma will be useful.

LEMMA 4.3. — *Let a, b, s be elements of a group. If $a^2 = b^2$ and $(sa)^2 = (sb)^2$, then $[ab^{-1}, s] = 1$.*

Proof. — We have

$$ab^{-1}s = ab^{-2}s^{-1}(sb)^2b^{-1} = aa^{-2}s^{-1}(sa)^2b^{-1} = sab^{-1}.$$ □

We now state our main new contribution, which can be seen as a much stronger form of Corollary 4.2, for finitely generated groups that are not virtually abelian. The next result roughly asserts that, in such a group, not even the half of the elements can have finitely many squares.

PROPOSITION 4.4. — *Let G be a finitely generated group that is not virtually abelian. Then for every $s \in G$ and $F \subset G$ finite there are infinitely many $g \in G \setminus (\mathrm{sq}^{-1}(F) \cup s\,\mathrm{sq}^{-1}(F))$ such that*

$$\begin{cases} g^{-1}sg \notin F & \text{if } C_G(s) \text{ is locally finite} \\ g^{-1}sg = s & \text{otherwise.} \end{cases}$$

The fact that G is not virtually abelian is essential in the proposition. For example, the result is not true for the infinite dihedral group $G = \mathbf{Z}/2\mathbf{Z} * \mathbf{Z}/2\mathbf{Z}$. Indeed, if s is one of the generators of the free factors, then $G = \mathrm{sq}^{-1}(1) \cup s\,\mathrm{sq}^{-1}(1)$. Another

example is provided by a generalized dicyclic group G: if $x \in G$ is an element of order 4 such that the conjugation by x induces the inverse on an index 2 abelian subgroup A, then $G = \mathrm{sq}^{-1}(x^2) \cup x\,\mathrm{sq}^{-1}(x^2)$. This example shows that F does not necessarily contain the identity.

The proof of this proposition will rely on the following lemma, which strengthens Neumann's lemma [Neu54, Lemma 4.1].

LEMMA 4.5. — *Let G be a finitely generated group, $s \in G$ and $H_1, \ldots, H_m$ be subgroups of G and $a_1, \ldots, a_m \in G$. Assume that*

$$G = \mathrm{sq}^{-1}(1) \cup s\,\mathrm{sq}^{-1}(1) \cup a_1H_1 \cup \ldots \cup a_mH_m. \tag{4.1}$$

Let $\alpha := \sum_{i=1}^{m} \frac{1}{|G:H_i|}$ denote the sum of the inverses of the indices of H_i, with the standard convention $\frac{1}{\infty} = 0$.

1. *If $\alpha < \frac{3-\sqrt{5}}{4} \simeq 0.19$, then either G is virtually abelian, or the conjugacy class of s^2 is finite of cardinality less than $\frac{4}{(3-\sqrt{5}-4\alpha)^2}$.*
2. *If s is an involution, and $\alpha < \frac{(1-\alpha)^3}{24}$ (eg $\alpha \leqslant 0.035$), then G is virtually abelian.*

The proof of the Proposition 4.4 will only use the lemma in the case when the H_i all have infinite indices, i.e. when $\alpha = 0$, but we find this quantitative form amusing.

We will prove the above lemma in the next subsection. Let us first explain how the proposition follows.

Proof of Proposition 4.4. — Let G be a finitely generated group. Suppose that there exists $s \in G$ and $F \subset G$ finite such that there are only finitely many $g \in G \setminus (\mathrm{sq}^{-1}(F) \cup s\,\mathrm{sq}^{-1}(F))$ such that

$$\begin{cases} g^{-1}sg \notin F & \text{if } C_G(s) \text{ is locally finite} \\ g^{-1}sg = s & \text{otherwise.} \end{cases}$$

We will show that such a group is virtually abelian. We will do that in several steps. First we will show that $C_G(s)$ is locally finite. Then by multiple reductions we will prove that G is virtually 2-nilpotent and finally that G is in fact virtually abelian.

4.1.1. $C_G(s)$ is locally finite.

Suppose that $C_G(s)$ is not locally finite. By Corollary 4.2, $C_G(s)$ has infinitely many squares. This implies that $C_G(s) \setminus (\mathrm{sq}^{-1}(F) \cup s\,\mathrm{sq}^{-1}(F))$ is infinite for any finite subset $F \subset G$, as otherwise this would imply that all but finitely many $g \in C_G(s)$ satisfy $g^2 \in F$ or $g^2 = s^2(s^{-1}g)^2 \in s^2F$, i.e. $C_G(s)$ has finitely many squares.

4.1.2.

We know that $C_G(s)$ is locally finite. By assumption, there exist finite subsets $E, F \subset G$ such that

$$G = \mathrm{sq}^{-1}(F) \cup s\,\mathrm{sq}^{-1}(F) \cup C_G(s)E. \tag{4.2}$$

We will now prove that G is virtually 2-nilpotent.

4.1.3. Reduction to $F = \{1\}$

Let $F_1 \subseteq F$ be the subset of elements with finite conjugacy class (the intersection of F with the FC-center of G).

The set of $g \in G$ such that $g(F \setminus F_1)g^{-1} \cap F \neq \emptyset$ is a finite union of cosets of the groups $C_G(f)$ for $f \in F \setminus F_1$. So it is a finite union of cosets of infinite-index subgroups. By Neumann's lemma [Neu54, Lemma 4.1], this finite union is a strict subset of G, and there is $g_0 \in G$ such that $g_0(F \setminus F_1)g_0^{-1} \cap F = \emptyset$. For such a g_0 and for every $h \in \mathrm{sq}^{-1}(F \setminus F_1)$ we have $g_0 h g_0^{-1} \notin \mathrm{sq}^{-1}(F)$, so $g_0 h g_0^{-1} \in s\,\mathrm{sq}^{-1}(F) \cup C_G(s)E$. This implies that, on $g_0\,\mathrm{sq}^{-1}(F \setminus F_1)g_0^{-1} \setminus C_G(s)E$, both maps $g \mapsto g^2$ and $g \mapsto (s^{-1}g)^2$ take finitely many values, so by Lemma 4.3 we obtain

$$g_0\,\mathrm{sq}^{-1}(F \setminus F_1)g_0^{-1} \setminus C_G(s)E \subseteq C_G(s)E_1$$

for some finite set E_1, or equivalently

$$\mathrm{sq}^{-1}(F \setminus F_1) \subseteq g_0^{-1}C_G(s)(E \cup E_1)g_0.$$

In particular, we deduce from (4.2) that

$$G = \mathrm{sq}^{-1}(F_1) \cup s\,\mathrm{sq}^{-1}(F_1) \cup AC_G(s)B$$

for some finite subsets $A, B \subset G$.

Denote by N the subgroup generated by the finite set $F_1^G := \cup_{g \in G} g F_1 g^{-1}$. Then N is normal, and its centralizer in G, which is the intersection of the centralizers of f for $f \in F_1^G$, is a finite intersection of finite index subgroups, so has finite index.

Let $G' = G/N$, and s', A', B', H' be the images of $s, A, B, C_G(s)$ in G' respectively. In the quotient, the previous equation becomes

$$G' = \mathrm{sq}^{-1}(1) \cup s'\,\mathrm{sq}^{-1}(1) \cup A'H'B'. \tag{4.3}$$

By Lemma 2.3, either G is virtually 2-nilpotent and we are done, or G' is not virtually abelian. We can therefore suppose that G' is not virtually abelian and hence infinite.

4.1.4. Reduction to $s'^2 = 1$

Observe that H', the image of the locally finite group $C_G(s)$ in the quotient G/N, is locally finite, so it cannot have finite index since G' is finitely generated and infinite and so are its finite index subgroups. We deduce by (1) in Lemma 4.5 that s'^2 has finite conjugacy class. Moreover, $C_G(s)$ being locally finite, s'^2 has finite order. By Dicman's Lemma, the normal subgroup M generated by s'^2 is finite. Let $\widetilde{G} := G'/M$. Then $\widetilde{G} = \mathrm{sq}^{-1}(1) \cup \tilde{s}\,\mathrm{sq}^{-1}(1) \cup \widetilde{A}\widetilde{H}\widetilde{B}$ with $\tilde{s}^2 = 1$, $\widetilde{H}$ an infinite index subgroup and $\widetilde{A}$ and $\widetilde{B}$ finite subsets.

4.1.5. The group G is virtually 2-nilpotent

By a direct application of (2) in Lemma 4.5, we obtain that $\widetilde{G}$ is virtually abelian. This implies that G' is finite-by-(virtually abelian) and, since it is finitely generated, virtually abelian (see Lemma 2.4). This is the desired contradiction.

4.1.6. The group G is virtually abelian

We already know that G is finitely generated and virtually 2-nilpotent. Let H be a finite index subgroup of G that is 2-nilpotent.

By definition, the derived subgroup $\langle ghg^{-1}h^{-1} \mid g, h \in H\rangle$ of H is contained in the center of H. Since H is nilpotent, we also know that the subset of torsion elements is a subgroup of H (see for example [Rob95, 5.2.7]) and that all subgroups of H, and also of G, are finitely generated (see for example [Rob95, 5.4.6]). In particular, since $C_G(s)$ is locally finite, it is finite. By (4.2), this implies that there exists a finite $F' \subset G$ such that

$$G = \mathrm{sq}^{-1}(F') \cup s\,\mathrm{sq}^{-1}(F').$$

We claim that there exists $n \in \mathbf{N}$ such that $sg^n s^{-1} = g^{-n}$ for every g in G. Indeed, let $n \coloneqq \mathrm{lcm}\{k \mid 1 \leqslant k \leqslant 3|F|\}$. Then if g has order at most $3|F'|$ we have $g^n = 1$ and the desired identity holds. On the other hand, let g be of order at least $3|F'|+1$. For such a g, there exists at most $2|F'|$ integers $1 \leqslant k \leqslant 3|F'|+1$ such that g^{2k} is in F'. Therefore, there is at least $|F'|+1$ integers $1 \leqslant k \leqslant 3|F'|+1$ with $(sg^k)^2 \in F'$. By the pigeonhole principle, we have $1 \leqslant k \neq l \leqslant 3|F'|+1$, which is less than the order of g, such that $(sg^k)^2 = (sg^l)^2$ and hence $sg^{k-l}s^{-1} = g^{-(k-l)}$ and the desired identity holds. For every $g, h \in G$, we have

$$\begin{aligned}(g^n h^n)^n = s\,(g^n h^n)^{-n}\,s^{-1} &= \left(sg^n s^{-1} sh^n s^{-1}\right)^{-n} \\ &= \left(g^{-n}h^{-n}\right)^{-n} = (h^n g^n)^n\,.\end{aligned} \tag{4.4}$$

When $g, h \in H$, $a \coloneqq [g^n, h^n]$ belongs to the center of H, so (4.4) shows that $a^n = 1$. The subgroup $K < Z(H)$ of elements of the center that are of finite order is finite. In the quotient H/K, the subgroup H' generated by $\{g^n \mid g \in H/K\}$ is abelian. Moreover, the quotient $(H/K)/H'$ is a finitely generated nilpotent group of exponent n, so is finite (see for example [Rob95, 5.2.18]). This implies that H, and therefore also G, is virtually abelian. □

4.2. Random walks and proof of Lemma 4.5

The proof of Lemma 4.5 will use random walk techniques, and in particular the recent result of Tointon [Toi20] generalizing to infinite groups a classical result by P. Neumann [Neu89] roughly saying: *a finite group in which the probability that two randomly chosen elements commute is large is almost abelian.* We fix a symmetric probability measure μ on G whose support is finite, generates G and contains the identity. In particular, in this subsection G will always be a finitely generated group. Let g_n and g'_n be two independent realizations of the random walk on G given by μ, that is two independent random variables with distribution μ^{*n}, the n^{th} convolution power of μ. We will use two facts. The first is very easy[(3)] and asserts that if H is a subgroup of G and $a \in G$, then

[(3)] The law of a *reversible* aperiodic transitive random walk on a set V equidistributes if V is finite, and converges $\sigma(\ell_1(V), c_0(V))$ to 0 if V is infinite.

$$\lim_n \mathbf{P}(g_n \in aH) = \frac{1}{|G:H|}. \tag{4.5}$$

In particular, if H has infinite index, $\lim_n \mathbf{P}(g_n \in aH) = 0$. Actually, more is known: the above convergence is uniform in a and H. In the vocabulary of [Toi20], μ^{*n} *measures indices uniformly*, see [Toi20, Theorem 1.11]. To illustrate the power of random walks on groups, observe that (4.5) allows to give a transparent proof (for finitely generated groups) of Neumann's lemma: if $G = a_1H_1 \cup \ldots a_mH_m$ is a finite union of cosets of subgroups, then we have

$$\sum_{i=1}^{m} \frac{1}{|G:H_i|} = \lim_n \sum_{i=1}^{m} \mathbf{P}\left(g_n \in a_iH_i\right) \geqslant \lim_n \mathbf{P}\left(g_n \in \cup_i a_iH_i\right) = 1.$$

The second fact we will use, [Toi20, Theorem 1.9], asserts that, whenever G is not virtually abelian

$$\lim_n \mathbf{P}\left(g_n \text{ and } g_n' \text{ commute}\right) = 0. \tag{4.6}$$

We start with an easy consequence of (4.6), that we will use in the proof. It is natural to expect that the result holds with $\frac{\sqrt{5}-1}{2}$ replaced by an arbitrary positive number, see Section 6.

Lemma 4.6. — *If* $\liminf_n \mathbf{P}(g_n^2 = 1) > \frac{\sqrt{5}-1}{2}$, *then* G *is virtually abelian.*

Proof. — Denote $c_n \coloneqq \mathbf{P}(g_n^2 = 1)$. Observe that

$$\begin{aligned}\mathbf{P}\left(g_n^2 = {g_n'}^2 = (g_ng_n')^2 = 1\right) &= \mathbf{P}\left(g_n^2 = {g_n'}^2 = 1\right) - \mathbf{P}\left(g_n^2 = {g_n'}^2 = 1 \neq (g_ng_n')^2\right)\\ &\geqslant \mathbf{P}\left(g_n^2 = {g_n'}^2 = 1\right) - \mathbf{P}\left((g_ng_n')^2 \neq 1\right)\\ &= c_n^2 - (1 - c_{2n})\,.\end{aligned}$$

In the last line, we used that g_ng_n' is distributed as g_{2n}.

So, if $c = \liminf_n c_n$, we obtain

$$\liminf_n \mathbf{P}\left(g_n^2 = {g_n'}^2 = (g_ng_n')^2 = 1\right) \geqslant c^2 + c - 1,$$

which is positive if and only if $c > \frac{\sqrt{5}-1}{2}$. To conclude using (4.6), it remains to observe that $g_n^2 = {g_n'}^2 = (g_ng_n')^2 = 1$ implies that g_n and g_n' commute. □

We now proceed to prove Lemma 4.5.

Proof of Lemma 4.5(1). — Let G, s, m, H_i, a_i satisfying (4.1).

Assume that $\alpha < \frac{3-\sqrt{5}}{4}$.

By (4.1), for every $g \in G$ such that $g^2 \neq 1$, we have

$$(sg)^2 = 1 \quad \text{or} \quad sg \in a_1H_1 \cup \ldots \cup a_mH_m$$

and

$$\left(s^{-1}g\right)^2 = 1 \quad \text{or} \quad g \in a_1H_1 \cup \ldots \cup a_mH_m.$$

In particular, if $g^2 \neq 1$ and $g \notin \{1, s^{-1}\}(a_1 H_1 \cup \ldots \cup a_m H_m)$, we have $(sg)^2 = (s^{-1}g)^2 = 1$, which implies

$$g^{-1}s^2 g = \left(g^{-1}s\right)(sg) = \left(s^{-1}g\right)\left(g^{-1}s^{-1}\right) = s^{-2}.$$

Therefore we obtain

$$\mathbf{P}\left(g_n^{-1}s^2 g_n = s^{-2}\right) \geqslant \mathbf{P}\left(g_n^2 \neq 1 \text{ and } g_n \notin \left\{1, s^{-1}\right\}(a_1 H_1 \cup \ldots \cup a_m H_m)\right).$$

If $c := \liminf_n \mathbf{P}(g_n^2 = 1) > \frac{\sqrt{5}-1}{2}$, we know by Lemma 4.6 that G is virtually abelian. So we can as well assume that $c \leqslant \frac{\sqrt{5}-1}{2}$. By (4.5) we can bound

$$\limsup_n \mathbf{P}\left(g_n^{-1}s^2 g_n = s^{-2}\right) \geqslant 1 - c - 2\sum_{i=1}^{m} \frac{1}{|G : H_i|} \geqslant \frac{3 - \sqrt{5} - 4\alpha}{2}.$$

Observe that $\frac{3-\sqrt{5}-4\alpha}{2} > 0$ by our assumption on α. Now, if $g_n^{-1}s^2 g_n = s^{-2}$ and ${g'_n}^{-1}s^2 g'_n = s^{-2}$, then $g_n g'_n$ and s^2 commute, or equivalently $g_n g'_n \in C_G(s^2)$. Therefore, since $g_n g'_n$ is distributed as g_{2n}, we obtain

$$\limsup_n \mathbf{P}\left(g_{2n} \in C_G\left(s^2\right)\right) \geqslant \left(\frac{3 - \sqrt{5} - 4\alpha}{2}\right)^2.$$

By (4.5), the left-hand side is equal to $\frac{1}{|G:C_G(s^2)|}$ and the claim is proven. □

Proof of Lemma 4.5(2). — Let G, s, m, H_i, a_i satisfying (4.1), with $s^2 = 1$ and $\alpha < \frac{(1-\alpha)^3}{24}$.

Our main goal will be to prove that two randomly chosen elements of G (for well-chosen probability measures on G that are not exactly random walks but mixtures of random walks) commute with non-vanishing probability. By [Toi20], we will deduce that G is *virtually abelian*. We proceed by contradiction, and assume that G is not virtually abelian.

The element s having order 2, we can as well assume that the probability measure μ is s-left-invariant, that is it satisfies $\mu(sg) = \mu(g)$ for every $g \in G$. By (4.1) and (4.5), we know that

$$\liminf_n \mathbf{P}\left(g_n \in \mathrm{sq}^{-1}(1) \cup s\,\mathrm{sq}^{-1}(1)\right) \geqslant 1 - \alpha.$$

By the s-invariance of μ, $\mathbf{P}(g_n \in \mathrm{sq}^{-1}(1)) = \mathbf{P}(g_n \in s\,\mathrm{sq}^{-1}(1))$,so $\liminf_n \mathbf{P}(g_n^2 = 1) \geqslant \frac{1-\alpha}{2}$.

As before, since $g^2 = h^2 = (gh)^2$ implies that g and h commute, (4.6) implies that

$$\lim_n \mathbf{P}\left(g_n^2 = {g'_n}^2 = (g_n g'_n)^2 = 1\right) = 0.$$

On the other hand, $g_n g'_n$ being distributed as g_{2n}, we have

$$\liminf_n \mathbf{P}\left((g_n g'_n)^2 = 1 \text{ or } (sg_n g'_n)^2 = 1\right) \geqslant 1 - \alpha.$$

Let now $g_n^{(1)}, g_n^{(2)}$ and $g_n^{(3)}$ be three independent copies of the random walk on G given by μ. Let A_n be the event

$$A_n = \left\{\forall\, 1 \leqslant i \neq j \leqslant 3, \left(g_n^{(i)}\right)^2 = 1 \quad \text{and} \quad \left(sg_n^{(i)} g_n^{(j)}\right)^2 = 1\right\}.$$

It follows from the preceding discussion that the difference of $\{\forall\ 1 \leqslant i \leqslant 3, (g_n^{(i)})^2 = 1\}$ and A_n has probability $\leqslant 3\alpha + o(1)$, so

$$\liminf_n \mathbf{P}(A_n) \geqslant \liminf_n \mathbf{P}\left(\forall\ 1 \leqslant i \leqslant 3, \left(g_n^{(i)}\right)^2 = 1\right) - 3\alpha \geqslant \frac{(1-\alpha)^3}{8} - 3\alpha.$$

This is strictly positive by assumption.

But on A_n, for every $1 \leqslant i, j \leqslant 3$, we have

$$sg_n^{(i)}g_n^{(j)}s^{-1} = \left(g_n^{(i)}g_n^{(j)}\right)^{-1} = g_n^{(j)}g_n^{(i)}$$

and therefore

$$\left(sg_n^{(1)}\right)g_n^{(2)}g_n^{(3)}\left(sg_n^{(1)}\right)^{-1} = sg_n^{(1)}g_n^{(2)}s^{-1}sg_n^{(3)}g_n^{(1)}s^{-1} = g_n^{(2)}g_n^{(1)}g_n^{(1)}g_n^{(3)} = g_n^{(2)}g_n^{(3)}.$$

To say it differently, $sg_n^{(1)}$ commutes with $g_n^{(2)}g_n^{(3)}$. We deduce

$$\mathbf{P}\left(\left[sg_n^{(1)}, g_n^{(2)}g_n^{(3)}\right] = 1\right) \geqslant \mathbf{P}(A_n).$$

Using that μ is s-invariant, $sg_n^{(1)}$ is distributed as $g_n^{(1)}$ and

$$\mathbf{P}\left(\left[g_n^{(1)}, g_n^{(2)}g_n^{(3)}\right] = 1\right) = \mathbf{P}\left(\left[sg_n^{(1)}, g_n^{(2)}g_n^{(3)}\right] = 1\right).$$

We can rewrite this as

$$\liminf_n \mu^{*n} \otimes \mu^{*2n}\left(\{(g,h) \in G \times G \mid [g,h] = 1\}\right) > 0.$$

Denote by ν_n the probability $\frac{1}{2}(\mu^{*n} + \mu^{*2n})$. We clearly have $\nu_n \otimes \nu_n \geqslant \frac{1}{4}(\mu^{*n} \otimes \mu^{*2n})$, so

$$\liminf_n \nu_n \otimes \nu_n\Big(\{(g,h) \in G | [g,h] = 1\}\Big) > 0.$$

On the other hand, it follows from [Toi20, Theorem 1.11] that the sequences of measures μ^{*n} and μ^{*2n} (and therefore also ν_n) measure index uniformly, hence the preceding is a contradiction with [Toi20, Theorem 1.9]. So our starting assumption that G is not virtually abelian is absurd. This concludes the proof of the Lemma 4.5. □

4.3. Counting triangles

We now state and prove a lemma on the augmentation of the number of triangles (in Cayley graphs of G) containing some $s_0 \in G$. It complements results of [ST19, Lemma 9.2] and [LS21, Lemma 31] which where valid for groups with elements of infinite (respectively very large) order. The conclusion of Lemma 4.7 is also cleaner than in [LS21, ST19].

LEMMA 4.7. — *Let G be a finitely generated group that is not virtually abelian, and let $S \subset G \setminus \{1\}$ be a finite symmetric generating set.*

Then for each s_0 in S, there exists $S \subset S' \subset G$ a finite symmetric generating set such that

(1) *$\Delta := S' \setminus S$ has at most 4 elements;*
(2) *Δ does not contain elements of order at most 2;*
(3) *$\Delta \cap \{s^2 \mid s \in S\} = \emptyset$;*

(4) $\mathrm{N}_3(s, S') \leqslant 6$ *for all* $s \in \Delta$*;*
(5) $\mathrm{N}_3(s, S') = \mathrm{N}_3(s, S)$ *for all* $s \in S \setminus \{s_0, s_0^{-1}\}$*;*
(6) *the value of* $\mathrm{N}_3(s_0, S') - \mathrm{N}_3(s_0, S)$ *is equal to*

$$\begin{cases} 1 & \text{if } s_0^2 \neq 1 \text{ and } C_G(s_0) \text{ is locally finite,} \\ 2 & \text{if } s_0^2 = 1 \text{ and } C_G(s_0) \text{ is locally finite,} \\ 2 & \text{if } s_0^2 \neq 1 \text{ and } C_G(s_0) \text{ is not locally finite,} \\ 4 & \text{if } s_0^2 = 1 \text{ and } C_G(s_0) \text{ is not locally finite.} \end{cases}$$

Proof. — Let g be an element of G and $\Delta_g \coloneqq \{g, g^{-1}, s_0^{-1}g, g^{-1}s_0\}$. We will show that there exists some g in G such that $S' = S'_g \coloneqq S \cup \Delta_g$ works. Observe that for all g, the set S'_g satisfies Condition 1 of the lemma, and that it satisfies 2 if and only if $g^2 \neq 1$ and $(s_0^{-1}g)^2 \neq 1$, or equivalently $g \notin \mathrm{sq}^{-1}(1) \cup s_0\,\mathrm{sq}^{-1}(1)$.

We first restrict our attention to elements g such that the following two conditions hold

$$|g|_S \geqslant 3 \tag{4.7}$$

$$\left|s_0^{-1}g\right|_S \geqslant 3 \tag{4.8}$$

where $|g|_S$ is the word length of g relative to the generating set S.

Since S is finite, the number of $g \in G$ such that one of the conditions (4.7)-(4.8) do not hold is finite. Also, for a g satisfying Conditions (4.7) and (4.8) the intersection $\Delta_g \cap S$ is empty and Condition (3) is automatically satisfied. Moreover, in the Cayley graph of G relative to S'_g, a triangle with a side labelled by $s \in \Delta_g$ has at least another side labelled by an element of Δ_g, otherwise s would have S-length at most 2. This implies that any edge labelled by $s \in \Delta_g$ belongs to at most 6 triangles in $\mathrm{Cay}(G, S')$, which is Condition (4). Indeed, if one edge e is labelled by $s \in \Delta_g$, there are at most three possibilities to put an edge labelled by $t \in \Delta_g \setminus \{s^{-1}\}$ at each extremity of e, thus giving a maximum number of $2 \cdot 3 = 6$ triangles containing e. This also shows that for any $s \in S$ we have

$$\mathrm{N}_3\left(s, S'_g\right) - \mathrm{N}_3(s, S) = \left|\left\{t \in \Delta_g \,\middle|\, s^{-1}t \in \Delta_g\right\}\right| = |\Delta_g \cap s\Delta_g| \ .$$

We now turn our attention on the set $\Delta_g \cap s\Delta_g$. Its cardinality is equal to the number of pairs $(u, v) \in \Delta_g$ such that $u = sv$. By replacing u and v by the words $g, g^{-1}, s_0^{-1}g$ and $g^{-1}s_0$, this gives us 16 equations in the group. Among these 16 equations, 4 imply that $s = 1$. The 12 remaining equations for elements of $\Delta_g \cap s\Delta_g$ are shown in Table 4.1.

In particular, if g is as in the conclusion of Proposition 4.4 for $F = S \cup s_0 S \cup s_0^{-1} S$ and $s = s_0$, we see that only the first two lines in this Table occur if $C_G(s_0)$ is locally finite, and only the first four occur otherwise. This implies Condition (5). Also, Condition 2 holds in this case since 1 belongs to $s_0^{-1}S \subseteq F$, and Condition (6) is automatically satisfied. The fact that there are infinitely many g in the conclusion of Proposition 4.4 imply that we can find such g satisfying also conditions (4.7)-(4.8). □

We are now ready to prove Proposition 3.2.

Table 4.1. Possible elements of $\Delta_g \cap s\Delta_g$, where $\mathrm{sq}(g) = g^2$.

Possible elements of $\Delta_g \cap s\Delta_g$	Occurs if
$g = ss_0^{-1}g$	$s = s_0$
$s_0^{-1}g = sg$	$s = s_0^{-1}$
$g^{-1}s_0 = sg^{-1}$	$s = g^{-1}s_0g$
$g^{-1} = sg^{-1}s_0$	$s = g^{-1}s_0^{-1}g$
$g = sg^{-1}$	$\mathrm{sq}(g) = s$
$g^{-1} = sg$	$\mathrm{sq}(g) = s^{-1}$
$s_0^{-1}g = sg^{-1}$	$\mathrm{sq}(g) = s_0s$
$g^{-1} = ss_0^{-1}g$	$\mathrm{sq}(g) = s_0s^{-1}$
$g = sg^{-1}s_0$	$\mathrm{sq}\left(s_0^{-1}g\right) = s_0^{-1}s$
$g^{-1}s_0 = sg$	$\mathrm{sq}\left(s_0^{-1}g\right) = s_0^{-1}s^{-1}$
$s_0^{-1}g = sg^{-1}s_0$	$\mathrm{sq}\left(s_0^{-1}g\right) = s$
$g^{-1}s_0 = ss_0^{-1}g$	$\mathrm{sq}\left(s_0^{-1}g\right) = s^{-1}$

Proof of Proposition 3.2. — The proof will be by successive applications of Lemma 4.7. To prove the proposition, it is enough that all elements of S belong to at least 7 $\widetilde{S}$-triangles (to distinguish them from the newly added elements which will belong to at most 6 $\widetilde{S}$-triangles) and that the numbers $\mathrm{N}_3(s^{\pm 1}, \widetilde{S})$ for s in S are all distinct.

Let $S_0 = S \cup S^{-1}$, so that $|S_0| \leqslant 2|S|$. Let $s_1, \ldots, s_n$ be any enumeration of the elements of S. Apply successively Lemma 4.7 at most 7 times with s_1, to get a set S_1 containing S and such that $\mathrm{N}_3(s_1, S_1)$ is larger than 7. Then, applying Lemma 4.7 for s_2 at most 8 times, we can bring $\mathrm{N}_3(s_2, S_2)$ to another value $\geqslant 7$. Doing the same for each element of S, we finally obtain a set $\widetilde{S}$ as in the lemma, after a total number of $\leqslant 7 + 8 + \cdots + (|S| + 6) = |S|(|S| + 13)/2$ successive applications of Lemma 4.7. At the end, we have

$$\left|\widetilde{S}\right| \leqslant |S_0| + 4\frac{|S|(|S| + 13)}{2} \leqslant 2|S|(|S| + 14). \qquad \square$$

5. Proofs of the main results

We collect here for completeness the straightforward proofs of the results from the introduction.

Proof of Theorem 1.1. — Let G be as in Theorem 1.1, and S_0 be a finite generating set. Let $S_1 = (S_0 \cup S_0^2 \cup S_0^3) \setminus \{1\}$, and S_2 be the generating set $\widetilde{S}$ given by Proposition 3.2 for $S = S_1$. By Proposition 3.2 and the discussion preceding it, every automorphism of $\mathrm{Cay}(G, S_2)$ preserves the S_1-colours: $\phi(gs) \in \{\phi(g)s, \phi(g)s^{-1}\}$ for

every $g \in G$ and $s \in S_1$. By Theorem 3.1, ϕ is a left-translation by an element of G. □

Proof of Corollary 1.2. — If G is finite, the equivalence is the content of [God81]. We can assume that G is infinite and finitely generated. The implication (2) $\Longrightarrow$ (1) is obvious, and the implication (1) $\Longrightarrow$ (3) is known and very easy, see [Wat71]. For the reader's convenience, we recall the argument. If an infinite finitely generated group G is either abelian or generalized dicyclic then there is a nontrivial permutation ϕ of G satisfying $\phi(gh) \in \{\phi(g)h, \phi(g)h^{-1}\}$ for every $g, h \in G$: take for ϕ the inverse map if G is abelian, and the map that is the identity on A and the inverse on $G \setminus A$ if G is generalized dicyclic and x, A are as in Definition 2.1. In particular, ϕ induces an automorphism of every Cayley graph of G, different from a translation. Observe that this argument even rules out the existence of a non-locally finite GRR.

We have to justify (3) $\Longrightarrow$ (2). If G is not virtually abelian, then (2) is the conclusion of Theorem 1.1. Otherwise, G admits an element of infinite order (a torsion abelian finitely generated group is finite), and [LS21, Theorem 2] applies and proves (2). □

Proof of Corollary 1.3. — If G is not virtually abelian, this is a particular case of Theorem 1.1. Otherwise, as explained in the proof of Corollary 1.2, G has an element of infinite order and [ST19, Theorem J] applies. □

Proof of Corollary 1.4. — Combine Corollary 1.3 with [ST19, Theorem E]. □

6. A conjecture on the squares of a random walk

We mentionned before Lemma 4.6 that we expect that the following conjecture holds.

Conjecture 6.1. — *Let G be a finitely generated group that is not virtually abelian, μ be a symmetric probability measure on G with finite and generating support containing the identity, and (g_n) a realization of the random walk on G given by μ. Then*

$$\forall\, a \in G, \lim_n \mathbf{P}\left(g_n^2 = a\right) = 0. \tag{6.1}$$

Better, there should be a function $f : (0,1] \to \mathbf{N}$ such that, in a group G, if

$$\exists\, a \in G, \limsup_n \mathbf{P}\left(g_n^2 = a\right) \geqslant \varepsilon,$$

then G admits an abelian subgroup of index $\leqslant f(\varepsilon)$. This is known to be true for finite groups [Man18, Man94].

The main case of the conjecture is when $a = 1$: indeed with similar methods as the reduction to $F = \{1\}$ in the proof of Proposition 4.4, one can show that the case $a = 1$ in Conjecture 6.1 implies the full conjecture for G not virtually 2-nilpotent.

Let us mention here that this conjecture would allow to greatly simplify our proofs, as it would imply immediately the following variant of Proposition 4.4, which also implies the main Theorem 1.1 by the same argument.

LEMMA 6.2. — *If Conjecture 6.1 holds for G, then for every $s \in G$ and $F \subset G$ finite there are infinitely many $g \in G \setminus (\mathrm{sq}^{-1}(F) \cup s\,\mathrm{sq}^{-1}(F))$ such that*

$$\begin{cases} g^{-1}sg \notin F & \text{if } C_G(s) \text{ has infinite index in } G \\ g^{-1}sg = s & \text{otherwise.} \end{cases}$$

Proof. — We prove the stronger fact that the probability that $g = g_n$ satisfies the conclusion of the lemma is $1 - o(1)$ when $|G : C_G(s)| = \infty$, and $\frac{1}{|G:C_G(s)|} - o(1)$ otherwise.

It follows from (6.1) that

$$\lim_n \mathbf{P}\left(g_n \in \mathrm{sq}^{-1}(F)\right) = 0.$$

It also implies that

$$\lim_n \mathbf{P}\left(g_n \in s\,\mathrm{sq}^{-1}(F)\right) = 0. \tag{6.2}$$

To justify this, we need to introduce an independant copy $(g'_n)_{n\geqslant 0}$ of the random walk (g_n). Since the support of μ is symmetric and generates G, there is a k such that $\mathbf{P}(g'_k = s^{-1}) > 0$. So using that g_{n+k} is distributed as $g'_k g_n$, we obtain

$$\begin{aligned} \mathbf{P}\left(g_{n+k} \in \mathrm{sq}^{-1}(F)\right) &\geqslant \mathbf{P}\left(s^{-1}g_n \in \mathrm{sq}^{-1}(F) \quad \text{and} \quad g'_k = s^{-1}\right) \\ &= \mathbf{P}\left(g_n \in s\,\mathrm{sq}^{-1}(F)\right)\mathbf{P}\left(g'_k = s^{-1}\right). \end{aligned}$$

This proves (6.2). Moreover, it follows from (4.5) that

$$\begin{cases} \lim_n \mathbf{P}\left(g_n^{-1}sg_n \notin F\right) = 1 & \text{if } |G : C_G(s)| = \infty \\ \lim_n \mathbf{P}\left(g_n^{-1}sg_n = s\right) = \frac{1}{|G:C_G(s)|} & \text{otherwise.} \end{cases}$$

The conclusion follows. □

7. Directed and oriented graphs

A natural variation of Cayley graphs is the concept of *Cayley digraph* (directed graph). Given a group G and a (not necessarily symmetric) generating set $S \subseteq G\setminus\{1\}$, the Cayley digraph $\overrightarrow{\mathrm{Cay}}(G, S)$ is the digraph with vertex set G and with an arc (directed edge) from g to h if and only if $g^{-1}h \in S$.

A Cayley digraph $\overrightarrow{\mathrm{Cay}}(G, S)$ of G whose automorphism group acts freely on its vertex set is called a *digraphical regular representation*, or DRR. If moreover $\overrightarrow{\mathrm{Cay}}(G, S)$ has no bigons (that is if $S \cap S^{-1} = \emptyset$) then we speak of an *oriented graphical regular representation*, or ORR.

We have the directed equivalent of Corollary 1.2:

PROPOSITION 7.1. — *For a finitely generated group G, the following are equivalent:*

(1) *G admits a* DRR*,*
(2) *G admits a finite degree* DRR*,*

(3) *G is neither the quaternion group Q_8, nor any of $(\mathbf{Z}/2\mathbf{Z})^2$, $(\mathbf{Z}/2\mathbf{Z})^3$, $(\mathbf{Z}/2\mathbf{Z})^4$, $(\mathbf{Z}/3\mathbf{Z})^2$.*

Proof. — If G is finite, the equivalence is the content of [Bab80]. We can assume that G is infinite and finitely generated. The implication (2) $\implies$ (1) is obvious, and the implication (1) $\implies$ (3) is empty for infinite groups. We have to justify (3) $\implies$ (2).

Let S be a finite generating set of G. Using Proposition 3.2 and [LS21, Lemma 32] we obtain a finite generating set $S \subseteq \widetilde{S} \subset G$ such that for all $s \in S$ and $t \in \widetilde{S}$, if $\mathrm{N}_3(s, \widetilde{S}) = \mathrm{N}_3(t, \widetilde{S})$ then $t = s$ or $t = s^{-1}$. By [LS21, Lemma 5] and [LS21, Proposition 6] there exists a generating set $T \subseteq \widetilde{S}$ such that $\overrightarrow{\mathrm{Cay}}(G, T)$ is a DRR. Moreover, $T \cap T^{-1}$ consist only of elements of order 2. □

Observe that the equivalence of (1) and (3) was the content of [Bab78, Bab80].

We will conclude with the oriented equivalent of Corollary 1.2 and thus answer [Bab80, Problem 2.7]. Recall that a generalized dihedral group G is the semi-direct product $A \rtimes \mathbf{Z}/2\mathbf{Z}$ where A is an abelian group and $\mathbf{Z}/2\mathbf{Z}$ acts on A by inversion.

Proposition 7.2. — *For a finitely generated group G, the following are equivalent:*

(1) *G admits an* ORR*,*
(2) *G admits a finite degree* ORR*,*
(3) *G does not belong to the following list:*
- *the non-trivial generalized dihedral groups,*
- *the following 11 finite groups of cardinality at most 64: Q_8, $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/4\mathbf{Z} \times (\mathbf{Z}/2\mathbf{Z})^2$, $\mathbf{Z}/4\mathbf{Z} \times (\mathbf{Z}/2\mathbf{Z})^3$, $\mathbf{Z}/4\mathbf{Z} \times (\mathbf{Z}/2\mathbf{Z})^4$, $(\mathbf{Z}/3\mathbf{Z})^2$, $\mathbf{Z}/3\mathbf{Z} \times (\mathbf{Z}/2\mathbf{Z})^3$, $D_4 \circ D_4$ (the central product of two dihedral groups of order 8, which has order 32) and the three groups (of respective orders 16, 16 and 32) given by the presentations*

$$\left\langle a, b \,\middle|\, a^4 = b^4 = (ab)^2 = \left(ab^{-1}\right)^2 = 1 \right\rangle,$$

$$\left\langle a, b, c \,\middle|\, a^4 = b^4 = c^4 = (ba)^2 = \left(ba^{-1}\right)^2 = (bc)^2 = \left(bc^{-1}\right)^2 = 1 \right.$$
$$\left. a^2c^{-2} = a^2b^{-2} = cac^{-1}a^{-1} = 1 \right\rangle,$$

$$\left\langle a, b, c \,\middle|\, a^4 = b^4 = c^4 = (ab)^2 = \left(ab^{-1}\right)^2 = (ac)^2 = \left(ac^{-1}\right)^2 = 1 \right.$$
$$\left. (bc)^2 = \left(bc^{-1}\right)^2 = a^2b^2c^2 = 1 \right\rangle.$$

Proof. — If G is finite, the equivalence is the content of [MS18], while every generating set of a generalized dihedral group contains an element of order 2 (namely any element not in A). Once again, we have to justify (3) $\implies$ (2) for G infinite.

Let G be a finitely generated group which is not generalized dihedral. Then by [Bab78, Proposition 5.2] there exists a finite generating set S of G without elements of order 2. Then the generating set $\widetilde{S}$ given by Proposition 3.2 and [LS21, Lemma 32] has also no elements of order 2. This implies that for T given by [LS21, Lemma 5] and [LS21, Proposition 6] the DRR $\overrightarrow{\mathrm{Cay}}(G, T)$ is actually an ORR. □

BIBLIOGRAPHY

[Bab78] László Babai, *Infinite digraphs with given regular automorphism groups*, J. Comb. Theory **25** (1978), no. 1, 26–46. ↑90

[Bab80] ———, *Finite digraphs with given regular automorphism groups*, Period. Math. Hung. **11** (1980), no. 4, 257–270. ↑90

[Ben13] Itai Benjamini, *Coarse geometry and randomness*, Lecture Notes in Mathematics, vol. 2100, Springer, 2013, Lecture notes from the 41st Probability Summer School held in Saint-Flour, 2011. Chapter 5 is due to Nicolas Curien, Chapter 12 was written by Ariel Yadin, and Chapter 13 is joint work with Gady Kozma, École d'Été de Probabilités de Saint-Flour. ↑75

[ERS70] Pál Erdős, Alfréd Rényi, and Vera Túran Sós, *Combinatorial theory and its applications. I-III. Proceedings of a colloqium, Balatonfüred, 1969*, Colloquia Mathematica Societatis János Bolyai, vol. 4, North-Holland, 1970. ↑74

[Geo17] Agelos Georgakopoulos, *On covers of graphs by Cayley graphs*, Eur. J. Comb. **64** (2017), 57–65. ↑75

[God81] Christopher D. Godsil, *GRRs for nonsolvable groups*, Algebraic methods in graph theory, Vol. I, II (Szeged, 1978), Colloquia Mathematica Societatis János Bolyai, vol. 25, North-Holland, 1981, pp. 221–239. ↑74, 88

[Het76] D. Hetzel, *Über reguläre graphische Darstellung von auflösbaren Gruppen*, Ph.D. thesis, Technische Universität Berlin, Deutschland, 1976. ↑74

[Imr69] Wilfried Imrich, *Graphen mit transitiver Automorphismengruppe*, Monatsh. Math. **73** (1969), 341–347. ↑74

[Imr75] ———, *On graphs with regular groups*, J. Comb. Theory **19** (1975), no. 2, 174–180. ↑74

[IW76] Wilfried Imrich and Mark E. Watkins, *On automorphism groups of Cayley graphs*, Period. Math. Hung. **7** (1976), no. 3-4, 243–258. ↑74

[LS21] Paul-Henry Leemann and Mikael de la Salle, *Cayley graphs with few automorphisms*, J. Algebr. Comb. **53** (2021), no. 4, 1117–1146. ↑74, 75, 76, 77, 78, 79, 85, 88, 90

[Man94] Avinoam Mann, *Finite groups containing many involutions*, Proc. Am. Math. Soc. **122** (1994), no. 2, 383–385. ↑88

[Man18] ———, *Groups satisfying identities with high probability*, Int. J. Algebra Comput. **28** (2018), no. 8, 1575–1584. ↑88

[MS18] Joy Morris and Pablo Spiga, *Classification of finite groups that admit an oriented regular representation*, Bull. Lond. Math. Soc. **50** (2018), no. 5, 811–831. ↑90

[Neu54] Bernhard H. Neumann, *Groups covered by permutable subsets*, J. Lond. Math. Soc. **29** (1954), 236–248. ↑80, 81

[Neu89] Peter M. Neumann, *Two combinatorial problems in group theory*, Bull. Lond. Math. Soc. **21** (1989), no. 5, 456–458. ↑82

[NW72] Lewis A. Nowitz and Mark E. Watkins, *Graphical regular representations of non-abelian groups. I, II*, Can. J. Math. **24** (1972), 993–1018. ↑74

[Rob95] Derek J. S. Robinson, *A course in the theory of groups*, second ed., Graduate Texts in Mathematics, vol. 80, Springer, 1995. ↑76, 77, 79, 82

[ST19] Mikael de la Salle and Romain Tessera, *Characterizing a vertex-transitive graph by a large ball*, J. Topol. **12** (2019), no. 3, 705–743. ↑75, 77, 78, 85, 88

[Toi20] Matthew C. H. Tointon, *Commuting probabilities of infinite groups*, J. Lond. Math. Soc. **101** (2020), no. 3, 1280–1297. ↑76, 82, 83, 84, 85

[Wat71] Mark E. Watkins, *On the action of non-Abelian groups on graphs*, J. Comb. Theory **11** (1971), 95–104. ↑74, 88

[Wat72] ———, *On graphical regular representations of $C_n \times Q$*, Graph Theory Appl., Proc. Conf. Western Michigan Univ. 1972, Lecture Notes in Mathematics, vol. 303, Springer, 1972, pp. 305–311. ↑74

[Wat74] ———, *Graphical regular representations of alternating, symmetric, and miscellaneous small groups*, Aequationes Math. **11** (1974), 40–50. ↑74

[Wat76] ———, *Graphical regular representations of free products of groups*, J. Comb. Theory **21** (1976), no. 1, 47–56. ↑74

Manuscript received on 26th October 2020,
accepted on 1st June 2021.

Recommended by Editor I. Benjamini.

This journal is a member of Centre Mersenne.

Paul-Henry LEEMANN
Université de Neuchâtel,
Institut de mathématiques,
11 Rue Emile-Argand
2000 Neuchâtel (Suisse)
paul-henry.leemann@unine.ch

Mikael DE LA SALLE
CNRS, Université de Lyon,
Univ Claude Bernard Lyon 1
Institut Camille Jordan
43 blvd. du 11 novembre 1918
69622 Villeurbanne (France)
delasalle@math.univ-lyon1.fr