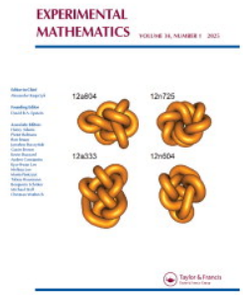

Experimental Mathematics

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/uexm20

Finite Groups with Geodetic Cayley Graphs

Murray Elder, Adam Piggott, Florian Stober, Alexander Thumm & Armin Weiß

To cite this article: Murray Elder, Adam Piggott, Florian Stober, Alexander Thumm & Armin Weiß (07 May 2025): Finite Groups with Geodetic Cayley Graphs, Experimental Mathematics, DOI: 10.1080/10586458.2025.2486403

To link to this article: https://doi.org/10.1080/10586458.2025.2486403

Published online: 07 May 2025.

EXPERIMENTAL MATHEMATICS
2025, VOL. 00, NO. 0, 1–24
https://doi.org/10.1080/10586458.2025.2486403

Taylor & Francis
Taylor & Francis Group

Finite Groups with Geodetic Cayley Graphs

Murray Elder[a], Adam Piggott[b], Florian Stober[c], Alexander Thumm[d], and Armin Weiß[c]

[a]School of Mathematical and Physical Sciences, University of Technology Sydney, Broadway NSW, Australia; [b]Mathematical Sciences Institute, Australian National University, Canberra, ACT, Australia; [c]Institut für Formale Methoden der Informatik, Universität Stuttgart, Stuttgart, Germany; [d]Department für Elektrotechnik und Informatik, Universität Siegen, Siegen, Germany

ABSTRACT

A connected undirected graph is called *geodetic* if for every pair of vertices there is a unique shortest path connecting them. It has been conjectured that for finite groups, the only geodetic Cayley graphs are odd cycles and complete graphs. In this article we present a series of theoretical results which contribute to a computer search verifying this conjecture for all groups of size up to 1024. The conjecture is also verified for several infinite families of groups including dihedral and some families of nilpotent groups. Two key results which enable the computer search to reach as far as it does are: if the center of a group has even order, then the conjecture holds (this eliminates all 2-groups from our computer search); if a Cayley graph is geodetic then there are bounds relating the size of the group, generating set and center (which significantly cuts down the number of generating sets which must be searched).

KEYWORDS
Geodetic graph; geodetic group; finite group; Cayley graph; group center

2020 MATHEMATICS SUBJECT CLASSIFICATION:
05C12; 05C25; 20F05

1. Introduction

Cayley graphs form an important subclass of vertex-transitive and regular graphs. The undirected Cayley graph of a group G with respect to a generating set Σ is the connected graph on vertex set $V = G$ and edge set E, where $\{g, h\} \in E$ if and only if there is a generator $a \in \Sigma$ such that $ga = h$. Besides being an important tool in combinatorial group theory, there are also interesting graph-theoretic questions about Cayley graphs. One example which has been much studied is the longstanding conjecture that every finite undirected Cayley graph that is not the complete graph on two vertices has a Hamiltonian cycle (see for example [26]).

A connected undirected graph $\Gamma = (V, E)$ is called *geodetic* if for any pair $u, v \in V$, the shortest path from u to v is unique. Research on geodetic graphs began in 1962, when Ore posed the problem of classifying all such graphs [25]. This goal has been achieved so far for planar geodetic graphs, and geodetic graphs of diameter two [33, 34]; yet, after decades of active research, a full classification of finite geodetic graphs has not been attained (for some recent developments, see for example [14, 17, 35]).

In 1997, Shapiro [32] asked whether each finitely generated group that admits a geodetic Cayley graph with respect to some finite generating set is *plain*, that is, isomorphic to the free product of finitely many finite groups and finitely many copies of $\mathbb{Z}$. It is well known and not hard to see that the converse holds: each plain group admits a geodetic Cayley graph (with respect to the generating set consisting of each non-trivial element of each finite factor, and a cyclic generator for each $\mathbb{Z}$ factor). Recently, significant progress has been made on this question and variants of it [11–13, 21] (see also the paragraph below on related work).

For any group, the Cayley graph with respect to the generating set consisting of every non-trivial element is the complete graph, which is geodetic. For cyclic groups of odd order, there is a second possibility: taking an arbitrary single generator, the Cayley graph is an odd cycle, which is also geodetic. The question we study here is whether there is any other possibility. In a 2017 PhD thesis [15], Federici conjectured that among the finite groups, there is none.

Conjecture A. [15, Conjecture 6] *Every finite geodetic Cayley graph is either a cycle of odd length or a complete graph.*

We say that a group satisfies Conjecture A if all its possible Cayley graphs satisfy Conjecture A. In this paper we report on a systematic computer experiment which confirms the conjecture for a significant number of groups.

Theorem B. *All groups of size up to 1024 satisfy Conjecture A.*

We also show that all groups of even order up to 2014, all simple groups of order up to 5000, and the symmetric group S_7 satisfy Conjecture A. Given that there are approximately 49.5 billion groups of order at most 1024, and each group of order n has 2^{n-1} potential generating sets, a naive computer search could not possibly achieve the result in Theorem B. Instead, our computer search

CONTACT Murray Elder murrayelder@gmail.com School of Mathematical and Physical Sciences, University of Technology Sydney, Broadway NSW 2007, Australia.

relies on a series of theoretical results concerning finite groups and when they can admit geodetic Cayley graphs. Some of these results confirm the conjecture for infinite families of groups, as summarized by the following.

Theorem C. *A finite group G satisfies Conjecture A if any one of the following conditions holds.*

(1) The center $Z(G)$ of G has even order (Theorem 3.12).
(2) The group G contains an abelian subgroup of index two (Theorem 5.4).
(3) The group G is nilpotent and its order does not have certain small divisors depending on the nilpotency class of G (see Theorem 5.9 for the precise statement).
(4) The group G has large commutativity degree (Theorem 5.14).

This cuts down the number of groups which need to be considered enormously, from 49.5 billion to 3197. In fact, just excluding abelian groups and groups with even-order center leaves 4734 groups of order at most 1024. We note that Conjecture A was shown to be satisfied by all abelian groups by Georgakopoulos as reported in [15, Proposition 10].

A second key theoretical result is the following, which provides an upper bound on the number of generating sets that the search must consider for each group.

Theorem D. *Let G be a finite group with generating set Σ such that the Cayley graph $\mathrm{Cay}(G, \Sigma)$ is a counterexample to Conjecture A, i.e., it is geodetic but neither complete nor a cycle. Then $|\Sigma| < 1.07\sqrt{|G|}$.*

Article organization. Section 2 sets our notation for groups and graphs, and provides some preliminary results about geodetic graphs. Theorems C and D are proved via a series of results presented in Sections 3–5. In Section 6 we give details of the implementation of our computer program. We use GAP [18] and its small group (SmallGrp) library [2] to enumerate the groups and check which of them are already covered by Theorem C. Then we apply an exhaustive search to check whether there is any geodetic generating set for any of the remaining groups. This exhaustive search crucially relies on several pruning methods based on variants of Theorem D and other theoretical results developed in Sections 3 and 4. The code is available at

https://osf.io/9ay6s/?view_only=37e18301e4e74e12bfe4e07b90b924c0.

Related work. As noted above, the first mention of Conjecture A that we are aware of is in the 2017 thesis of Federici [15], where the conjecture is proved for abelian groups and where it is shown that the Cayley graph of a semidirect product $C_m \rtimes C_n$ with C_n acting faithfully on C_m with respect to the "standard" generating set is not geodetic. Notice that for both m and n sufficiently large, this class of groups turns out to be one of the most difficult cases for our computer search (see Section 6.5). Besides this result, Federici proves some helpful lemmas for general geodetic Cayley graphs and runs computer experiments (unfortunately undocumented) which do not find any geodetic Cayley graphs except the obvious ones.

In 2022 Che [6] programmed an exhaustive computer search as part of an undergraduate project supervised by Alexey Talambutsa establishing Conjecture A for subgroups of the symmetric group S_4. Moreover, for

- all subgroups of S_6 with generating sets of size five,
- all subgroups of S_7 with generating sets of size four,
- all subgroups of S_9 with generating sets of size three,
- all subgroups of S_{10} with generating sets of size two,

Che showed that none of the corresponding Cayley graphs except complete ones and odd cycles are geodetic. For the source code, see https://gitlab.com/andr0901/kayley-geodesics. Be aware that restricting the number of generators to five or less is a strong restriction. (Note that by contrast, Theorem B verifies all generating sets for S_6, and Theorem 6.7 below verifies all generating sets for S_7. The groups S_9 and S_{10} are beyond our scope.)

A geodetic Cayley graph for a group corresponds to an inverse-closed confluent length-reducing rewriting system [12], yielding a connection between a geometric property (being geodetic) and formal languages. Monadic rewriting systems are special cases of length-reducing rewriting systems, and a result that is similar to Conjecture A is known for monadic rewriting systems: the only normalized finite confluent monadic rewriting systems for finite groups are those that correspond to complete Cayley graphs, or those that correspond to directed cycles for cyclic groups [27, Corollary 3.13]. As discussed in [12], it is an interesting open problem to classify the groups presented by inverse-closed finite convergent length-reducing rewriting systems. One reason to pursue new examples of finite geodetic Cayley graphs is that, by a simple construction that corresponds to the free product of groups, they immediately give new examples of infinite geodetic Cayley graphs.

In [13] Townsend and the first two authors generalize the concept of a geodetic graph to graphs which have at most k different geodesics between any pair of vertices for some constant k, which they call *k-geodetic*, and study properties of groups which admit k-geodetic Cayley graphs. While the main focus in [13] is on infinite groups, [13, Example 1.1] gives examples of Cayley graphs of finite groups that are k-geodetic but not $(k-1)$-geodetic or complete for $k \geq 2$. The easiest such examples are cyclic groups of even order with a non-complete 2-geodetic Cayley graph as well as a complete bipartite Cayley graph.

A graph is called *strongly geodetic* if for every pair of vertices there is at most *one* non-backtracking path connecting them that has length at most the diameter of the graph [4]. Clearly, all strongly geodetic graphs are geodetic. By [4, Theorem 1] the class of strongly

geodetic regular graphs coincides with the class of so-called *Moore graphs*, which also have been thoroughly studied in graph theory (for a definition see [20] or the survey paper [24]). Moreover, by [1, 8] the Moore graphs are completely classified: cycles of odd length, complete graphs, the Petersen graph, Hoffman-Singleton graph, and potentially hypothesized graphs (not known to exist) with 3250 vertices and degree 57. Of these, only the cycles and the complete graphs are Cayley graphs [5, 24] (we provide an alternative proof of this fact in Corollary 3.15). Hence, Conjecture A is true if we replace "geodetic" with "strongly geodetic".

2. Preliminaries

2.1. Groups and words

Throughout this article, we only consider finite groups. We write these multiplicatively, mostly omitting the binary operation altogether, and denote their identity element by 1. As usual, we write $[g,h] = g^{-1}h^{-1}gh$ for the *commutator* of two elements g, h of a group G. The *center* of G is the subgroup $Z(G) = \{g \in G \mid [g,h] = 1 \text{ for all } h \in G\}$. Two elements $g, g' \in G$ are *conjugate* if $g' = h^{-1}gh$ $(=: g^h)$ for some $h \in G$. Given $g \in G$ and $H \subseteq G$, we write $g^H = \{g^h \mid h \in H\}$.

We denote by $\mathrm{ord}(g)$ the *order* of $g \in G$, i.e., the smallest positive integer n with $g^n = 1$. The *order* (number of elements) of the group G is denoted by $|G|$, and the *exponent* of G by $\exp(G)$, i.e., the smallest positive integer n such that $g^n = 1$ for all $g \in G$. We denote the trivial group by 1.

For a subset $X \subseteq G$, we write $\langle X \rangle$ for the subgroup generated by X. It consists of those group elements that can be written as words over the alphabet $\Sigma = X \cup X^{-1}$. We denote the set of all such words by Σ^*. Given words $v, w \in \Sigma^*$, we write $v = w$ with the meaning that v and w evaluate to the same group element in G, whereas $v \equiv w$ denotes equality of words.

A subset $\Sigma \subseteq G$ with $\langle \Sigma \rangle = G$ is called a *generating set* of G. Throughout, we assume that all generating sets satisfy $1 \notin \Sigma$ and are *symmetric*, i.e., $a \in \Sigma$ implies $a^{-1} \in \Sigma$. We sometimes represent the inverse a^{-1} of a generator $a \in \Sigma$ by $\overline{a}$ to emphasize that it is a single letter.

The length of a word $w = a_1 \cdots a_n \in \Sigma^*$ (with $a_i \in \Sigma$) is denoted by $|w| = n$. We denote the set of words over Σ of length n by Σ^n. A word $w \in \Sigma^*$ is called a *geodesic* for (or representing) a group element $g \in G$ if $w = g$ and w is shortest among all words with that property. The geodesic length of $g \in G$ is defined as the length of a geodesic word representing g. If g admits a unique geodesic, we denote its geodesic by $\mathrm{geod}(g)$.

We use the following notation for specific groups. C_n is the cyclic group of order n, D_{2n} the dihedral group of order $2n$, and S_n (resp. A_n) the symmetric (resp. alternating) group on n elements. A direct product is denoted by $\times$ and a *semidirect product* by $\rtimes$, where $G = N \rtimes H$ means that N is a normal subgroup of G and H a subgroup of G such that $G = NH$ and $N \cap H = 1$. Notice that $G/N \cong H$ in this case. Be aware that, if we are given only N and H, then writing $G = N \rtimes H$ does not completely define G – instead we need to also specify a homomorphism from H to the automorphism group of N describing the action $(h, n) \mapsto hnh^{-1}$ of H on N (in other words H acts on N via automorphisms).

2.2. Graphs and Cayley graphs

We consider only *undirected finite simple graphs* $\Gamma = (V, E)$ where $E \subseteq \binom{V}{2}$. The *Cayley graph* $\mathrm{Cay}(G, \Sigma) = (V, E)$ of a group G (with respect to a generating set $\Sigma \subseteq G$) is defined by $V = G$ and $E = \{\{g, ga\} \mid g \in G, a \in \Sigma\}$. In other literature the *directed* Cayley graph is often considered; however, throughout this paper $\mathrm{Cay}(G, \Sigma)$ is undirected (and contains no loops) due to the above assumptions on Σ. Note that G acts on $\mathrm{Cay}(G, \Sigma)$ by left multiplication, i.e., $g.v = gv$ and $g.\{h, ha\} = \{gh, gha\}$. In particular, $\mathrm{Cay}(G, \Sigma)$ is vertex-transitive. The Cayley graph is connected because Σ generates G. In fact, it is biconnected for every finite group G with $G \neq 1$ and $G \ncong C_2$ [36, Theorem 3]. The degree of each vertex is $|\Sigma|$.

Given a graph $\Gamma = (V, E)$, a *path* of length n from $v_0 \in V$ to $v_n \in V$ in Γ is a sequence $v_0, \ldots, v_n$ of vertices (not necessarily distinct) with $\{v_{i-1}, v_i\} \in E$ for all $1 \leq i \leq n$. A *cycle* is a path of length at least 3 with $v_i = v_j$ if and only if $\{i, j\} = \{0, n\}$. The *distance* $d(u, v)$ between vertices u and v is defined as the length of a shortest path (*geodesic*) connecting u and v. The *diameter* of Γ is $\max\{d(u, v) \mid u, v \in V\}$. Moreover, given $v \in V$ and $H \subseteq V$, we define $d(v, H) = \min\{d(v, h) \mid h \in H\}$ to be the distance of v to H, $\mathcal{N}(v) = \{u \mid \{u, v\} \in E\}$ to be the neighborhood of v, and $\mathcal{N}(H) = \bigcup_{h \in H} \mathcal{N}(h) \setminus H$ to be the neighborhood of $H \subseteq V$.

A subset $H \subseteq V$ is called a *clique* (resp. *independent set*) if $\{u, v\} \in E$ (resp. $\{u, v\} \notin E$) for all $u, v \in H$ with $u \neq v$. A graph $\Gamma = (V, E)$ is called *complete* if V is a clique; it is called a *cycle* if the entire graph is a cycle as defined above.

2.3. Geodetic graphs

Definition 2.1. *A graph is* geodetic *if each pair of vertices is connected by a unique geodesic.*

The following equivalent definition using even cycles is due to Stemple and Watkins.

Lemma 2.2. [34, Theorem 2] *A connected graph Γ is geodetic if and only if Γ contains no even cycle $x_0, \ldots, x_{2n} = x_0$ with $n \geq 2$ such that $d(x_i, x_{i+n}) = n$ for all $0 \leq i \leq n$.*

An important special case are cycles of length four or six, the conditions under which those can exist are described in [33]. Of these we recall some basic facts on 4-cycles.

Lemma 2.3. *[33, Theorem 3.3] Suppose that $\Gamma = (V, E)$ is a geodetic graph. Then the vertices of every cycle v_0, v_1, v_2, v_3, v_0 of length four in Γ induce a complete subgraph.*

Remark 2.4. *Throughout, we use Lemma 2.3 in the following way without giving further reference. If Σ is a generating set of a group G such that the corresponding Cayley graph is geodetic and $a, b, c, d \in \Sigma$ with $a \neq c$ and $ab = cd \neq 1$, then $ab, cd, c^{-1}a, bd^{-1} \in \Sigma$ (since $1, a, ab, c, 1$ is a cycle of length 4).*

Lemma 2.5. [33, Theorem 3.5] *Let $\Gamma = (V, E)$ be a geodetic graph and $C \subseteq V$ be a clique in Γ. If $v \in V$ is adjacent to at least two distinct vertices in C, then $C \cup \{v\}$ is a clique.*

Lemma 2.6. *Let $\Gamma = (V, E)$ be a geodetic graph. Then the neighbors of any vertex $v \in V$ can be partitioned into a set of disjoint cliques.*

Proof. Assume for contradiction that $x, y, z \in \mathcal{N}(v)$ with $\{x, y\} \in E$, $\{y, z\} \in E$ but $\{x, z\} \notin E$. Then there are two geodesics from x to z (one via v and one via y), contradicting Γ being geodetic. □

After fixing a starting point in a Cayley graph $\mathrm{Cay}(G, \Sigma)$ (for instance the vertex corresponding to the identity element 1), paths starting at 1 are in bijection with words $w \in \Sigma^*$ (recall that we always assume the generating set $\Sigma \subseteq G$ to be symmetric). This allows us to denote paths by words in Σ^* rather than vertex sequences and leads to the following observation.

Observation 2.7. *The Cayley graph $\mathrm{Cay}(G, \Sigma)$ of a group G is geodetic if and only if each element $g \in G$ is represented by a unique geodesic $w \in \Sigma^*$, with the identity element represented by the empty word $\varepsilon \in \Sigma^*$.*

3. Structure of geodetic Cayley graphs

3.1. Complete subgroups

Definition 3.1. *Let G be a group with generating set Σ. We call $H \leq G$ a* complete subgroup *(with respect to Σ) if $H \setminus \{1\} \subseteq \Sigma$ or, equivalently, if $H \subseteq G$ induces a complete subgraph of $\mathrm{Cay}(G, \Sigma)$.*

Lemma 3.2. *Let $\Gamma = \mathrm{Cay}(G, \Sigma)$ be geodetic and let $C \subseteq G$ be a maximal clique of Γ with $1 \in C$.*

(1) Then $g^{-1}C = C$ or $g^{-1}C \cap C = \{1\}$ for each $g \in C$.
(2) If C is the only maximal clique C' with $1 \in C'$ and $|C'| = |C|$, then C is closed under inversion.

Proof. Recall that multiplying by a group element on the left induces an isomorphism. Since $1 \in g^{-1}C \cap C$ for each $g \in C$, the first statement follows from Lemma 2.5. For the second statement, note that we have shown that $g^{-1}C = C$ holds for each $g \in C$ by uniqueness of C. As such, $g^{-1} \in g^{-1}C = C$. □

Note that, in the second case of the previous lemma, where C is the only maximal clique of its size, C is not only closed under inversion, it is also a subgroup. We prove a more general statement.

Lemma 3.3. *Let $\Gamma = \mathrm{Cay}(G, \Sigma)$ be geodetic. If $X \subseteq G$ is a clique of Γ with $1 \in X$ and such that X is closed under inversion, then $\langle X \rangle$ is a complete subgroup.*

Proof. Let $C \subseteq G$ be a maximal clique containing X. If $g \in X \setminus \{1\}$, then $\{g^{-1}, 1, g\} \in C$ so $\{g^{-1}, 1\} \in g^{-1}C$. Hence $g^{-1}C \cap C \neq \{1\}$ and so $g^{-1}C = C$ by Lemma 3.2. Thus for any $g \in X$ we have $C = g(g^{-1}C) = gC$. By induction, assume products of i elements of X lie in C which holds for $i = 1$. Then $g_1 \dots g_{i+1} \in g_1 C = C$. This shows that $\langle X \rangle \subseteq C$ so $\langle X \rangle$ is a clique. □

We observe that the second item of Lemmas 3.2 and 3.3 together imply [15, Lemma 14] of Federici.

Lemma 3.4. *Let $\mathrm{Cay}(G, \Sigma)$ be geodetic and let $H_1, H_2 \leq G$ be complete subgroups. If $H_1 \cap H_2 \neq 1$ then $\langle H_1, H_2 \rangle$ is also a complete subgroup of G.*

Proof. Under these assumptions $H_1 \cup H_2$ is a clique (Lemma 2.5). Since $1 \in H_1 \cup H_2$ and $H_1 \cup H_2$ is closed under inversion, $\langle H_1, H_2 \rangle$ is a clique by Lemma 3.3. □

Lemma 3.5. *Let $\Gamma = (V, E)$ be a biconnected vertex-transitive non-complete geodetic graph and let $C \subseteq V$ be a clique of Γ of size k. Then there is an independent set $I \subseteq \mathcal{N}(C)$ of size $k^2 - k$.*

Proof. By [19, Corollary 1] every biconnected non-complete geodetic graph containing a clique of size k also contains the star graph $K_{1,k}$ as an induced subgraph. In other words, there exists a vertex $v \in V$ with an independent set of size k in its neighborhood $\mathcal{N}(v)$. As Γ is vertex-transitive, for every vertex $v \in V$ there is an independent set $I(v) \subseteq \mathcal{N}(v)$ of size k.

Fix a maximal clique $\tilde{C}$ of Γ with $C \subseteq \tilde{C}$ and set $\tilde{I}(v) \coloneqq I(v) \setminus \tilde{C}$. Note that $\tilde{I}(v) \subseteq \mathcal{N}(C)$. Since an independent set can contain at most one vertex of any given clique, we have $|\tilde{I}(v)| \geq |I(v)| - 1 = k - 1$.

We claim that $\tilde{I}(u) \cap \tilde{I}(v) = \emptyset$ for distinct $u, v \in C$. If there were a vertex $x \in \tilde{I}(u) \cap \tilde{I}(v)$, then we would have $x \in \tilde{C}$ by Lemma 2.5, because x is adjacent to two vertices in $\tilde{C}$. That contradicts the definition of $\tilde{I}$, which excludes vertices in $\tilde{C}$.

Let $I \coloneqq \bigcup_{v \in C} \tilde{I}(v) \subseteq \mathcal{N}(C)$ and observe that $|I| \geq k(k-1) = k^2 - k$, as the union is disjoint. It remains to show that I is indeed an independent set. Assume there are $x, y \in I$ with $\{x, y\} \in E$. By definition of I there are $u, v \in C$ such that $x \in \tilde{I}(u)$ and $y \in \tilde{I}(v)$. We must have $u \neq v$, as $\tilde{I}(u)$ is an independent set. Now we have a 4-cycle u, x, y, v. By Lemma 2.3 this implies the existence of the edge $\{u, y\}$. Now y is a neighbor of both u and v. That implies $y \in \tilde{C}$ by Lemma 2.5, a contradiction with the definition of $\tilde{I}(v)$. □

Proposition 3.6. *Let $\Gamma = \mathrm{Cay}(G, \Sigma)$ be a geodetic but not complete Cayley graph. If $H \leq G$ is a complete subgroup with respect to Σ, then $|G| \geq |H|^3 - |H|^2 + |H|$.*

Proof. By Lemma 3.5 there is an independent set of size $|H|^2 - |H|$ in the neighborhood of H which does not contain any vertex of H. We now look at the left cosets of H. Each such coset is a clique of Γ. Thus, each coset can contain at most one point of the independent set. Since H itself does not contain any point of the independent set, the index of H is at least $|H|^2 - |H| + 1$. Hence, $|G| = |G : H|\,|H| \geq |H|^3 - |H|^2 + |H|$. □

3.2. Conjugacy classes and elements of order two

Lemma 3.7 (Conjugacy class of generators). *Let G be a group with geodetic Cayley graph $\mathrm{Cay}(G, \Sigma)$ and $H \leq G$ such that $H = \langle H \cap \Sigma \rangle$. If $x^H \subseteq \Sigma$ for some $x \in \Sigma$, then $H \cap \Sigma = \{x^{\pm 1}\}$ or H is a complete subgroup. In particular, if $x^G \subseteq \Sigma$ for some $x \in G$, then $\mathrm{Cay}(G, \Sigma)$ satisfies Conjecture A.*

Proof. If $y \in H \cap \Sigma$ with $y \neq x^{\pm 1}$, then $x^y \in \Sigma$ and, therefore, $yx^y = xy \in \Sigma$ as this element cannot have length zero or two. We also have $x^{-1}y \in \Sigma$ and $yx^{\pm 1} \in \Sigma$ by symmetry.

If $H \cap \Sigma \neq \{x^{\pm 1}\}$, then there exists $y \in H \cap \Sigma$ with $y \neq x^{\pm 1}$. We will show that every $uv \in G$ with $u, v \in H \cap \Sigma$ has length at most one. If $u \notin \{x^{\pm 1}\}$ and $v \in \{x^{\pm 1}\}$, or vice versa, then this follows from the argument above. Otherwise, first consider the case that $u, v \notin \{x^{\pm 1}\}$ and define $u' \coloneqq ux$ and $v' \coloneqq \bar{x}v$. As $u' = ux = x^{\bar{u}}u$, we have $u' \in \Sigma$ and likewise $v' \in \Sigma$. Since $uv = u'v'$, it follows that $uv \in \Sigma$. If $u, v \in \{x^{\pm 1}\}$, we set $u' \coloneqq uy$ and $v' \coloneqq y^{-1}v$ and by the same argument conclude that $uv \in \Sigma$.

Finally, if $x^G \subseteq \Sigma$, then either $\Sigma = G \cap \Sigma = \{x^{\pm 1}\}$ or G is a complete subgroup of itself (or both in case $G \cong C_2$ or $G \cong C_3$). In the first case, $G = \langle x^{\pm 1} \rangle$ is a cyclic group. If, moreover, $|G| > 2$, then $\mathrm{Cay}(G, \Sigma)$ is a cycle of length $|G|$, which has to be odd as an even cycle is not geodetic. Otherwise as well as in the second case, $\mathrm{Cay}(G, \Sigma)$ is complete. □

The above lemma may seem technical but is extremely useful, for example, as demonstrated by the following consequences. For the first of these, note that $x^G = \{x\}$ whenever $x \in Z(G)$.

Corollary 3.8 (Generator in center). *If $Z(G) \cap \Sigma \neq \emptyset$, then $\mathrm{Cay}(G, \Sigma)$ satisfies Conjecture A.*

From this we obtain the following result first shown by Georgakopoulos and presented in [15].

Corollary 3.9. [15, Proposition 10] *If G is a finite abelian group, then G satisfies Conjecture A.*

Proof. This is immediate from Corollary 3.8 since $G = Z(G)$. □

Note that Lemma 3.7 can also be applied to deduce the completeness of a subgroup. A simple example of such an application is as follows. (Another example of this kind can be found in Lemma 6.5 and both of these observations are used to facilitate our computer search.)

Corollary 3.10 (Commuting generators). *Let $\mathrm{Cay}(G, \Sigma)$ be geodetic and $x, y \in \Sigma$. If $xy = yx$ and $y \neq x^{\pm 1}$, then $\langle x, y \rangle \leq G$ is a complete subgroup.*

Proof. Apply Lemma 3.7 with $H = \langle x, y \rangle$. □

If a group has an element of order two we have the following.

Lemma 3.11 (Order-two elements). *Let G be a group with generating set Σ such that the Cayley graph is geodetic. Let $g \in G$ be an element of order two. Then the geodesic for g is of the form*

$$(w_1 \cdots w_\ell) \cdot w_{\ell+1} \cdot (\overline{w_\ell} \cdots \overline{w_1})$$

of length $2\ell + 1$ where $\ell \in \mathbb{N}$ and $w_i \in \Sigma$ for each $1 \leq i \leq \ell + 1$. In particular, Σ contains an element of order two conjugate to g, namely $w_{\ell+1}$.

Proof. Let $w_1 \cdots w_k \in \Sigma^*$ be a geodesic for g. We have $g = g^{-1}$ and thus $w_1 \cdots w_k = \overline{w_k} \cdots \overline{w_1}$. Hence, we have two paths of length k that lead from 1 to g. Since $\mathrm{Cay}(G, \Sigma)$ is geodetic, g must have a unique geodesic, i.e., the two paths must coincide; hence, $w_i = \overline{w_{k-i+1}}$ for $i \in \{1, \ldots, k\}$.

If k is even, then $g = (w_1 \cdots w_{k/2}) \cdot (w_{k/2+1} \cdots w_k) \equiv (w_1 \cdots w_{k/2}) \cdot (\overline{w_{k/2}} \cdots \overline{w_1}) = 1$, contradicting the assumption that g is of order two. Thus, $k = 2\ell + 1$ must be odd and we obtain the equation

$$\begin{aligned} g &= (w_1 \cdots w_\ell) \cdot w_{\ell+1} \cdot (w_{\ell+2} \cdots w_k) \\ &\equiv (w_1 \cdots w_\ell) \cdot w_{\ell+1} \cdot (\overline{w_\ell} \cdots \overline{w_1}). \end{aligned}$$

Hence, g is conjugate to $w_{\ell+1} \in \Sigma$ and $w_{\ell+1} = \overline{w_{\ell+1}}$, proving the lemma. □

The above results lead to the following observation which turns out to be extremely useful in any computer search, since it shows that every 2-group immediately satisfies Conjecture A.

Theorem 3.12 (Even order center). *Let G be a group such that $Z(G)$ is of even order. Then the only geodetic Cayley graph of G is the complete graph.*

Proof. Assume we have a geodetic Cayley graph of G. By Lemma 3.11, the generating set Σ must contain at least one element of each conjugacy class of elements of order two in G. Since $Z(G)$ is of even order it must contain an element g of order two. As g is in the center of the group, it is not conjugate to any other elements. Hence, $g \in \Sigma$ and by Corollary 3.8, the Cayley graph is either complete, or an odd cycle. Since G contains an even order subgroup, G itself has even order. Therefore, the Cayley graph cannot be an odd cycle, so it must a be complete graph. □

Remark 3.13. *All but* 4734 *groups of the approximately* 49.5 *billion groups of order at most* 1024 *are covered by the combination of Theorem 3.12 and Corollary 3.9.*

3.3. Cayley graphs of diameter two

Proposition 3.14. *If G is of even order, then G has no geodetic Cayley graph of diameter two.*

Proof. Assume that $\Gamma = \mathrm{Cay}(G, \Sigma)$ is a geodetic Cayley graph of diameter two and $|G|$ is even. Since $|G|$ is even, G has elements of order two. Since Γ is geodetic and has diameter two, each such element is contained in Σ by Lemma 3.11. But then Σ contains an entire conjugacy class. By Lemma 3.7, the graph Γ would therefore have to be complete or a cycle, both of which are absurd. □

This affords a short elementary proof of the (well-known) fact that the Moore graphs of diameter two, other than C_5, are not Cayley graphs (see [5, Theorem 3.13], [24, 29]).

Corollary 3.15. *The Petersen graph, the Hoffman-Singleton graph, and all of the hypothetical Moore graphs of degree* 57 *and diameter two are not Cayley graphs.*

Proof. As each graph has an even number of vertices and diameter two, this follows from Proposition 3.14. □

In order to prove the next lemma, we recall the following definition. A graph Γ is called *strongly regular* with parameters (δ, λ, μ) if every vertex has degree δ, any two adjacent vertices share exactly λ neighbors, and any two non-adjacent vertices have exactly μ neighbors in common. A necessary condition for a graph with ν vertices to be strongly regular with parameters (δ, λ, μ) is the equation $(\nu - \delta - 1)\mu = \delta(\delta - \lambda - 1)$. Clearly, every strongly regular graph with parameter $\mu = 1$ is geodetic and has diameter two, and in this case the above condition becomes

$$\nu = \delta(\delta - \lambda) + 1. \tag{1}$$

Lemma 3.16. *If $\Gamma = \mathrm{Cay}(G, \Sigma)$ is geodetic and has diameter two and $|G| < 2025$, then Γ is the cycle C_5.*

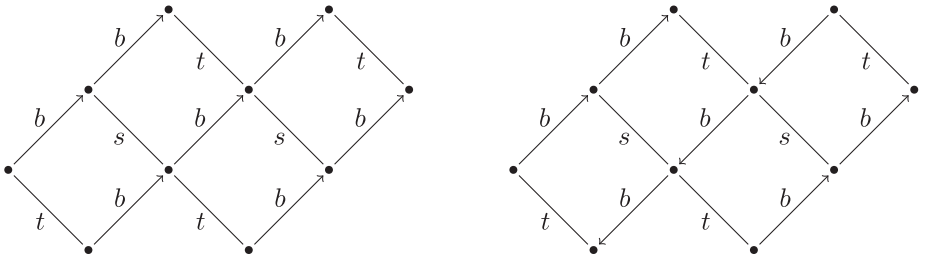

Figure 1. The situation in the proof of Lemma 3.17. Note that s, t have order two, so edges labeled s, t are drawn as undirected.

Proof. From [22, 33] (see also [3, Theorem 1]), we have that every geodetic graph of diameter two falls into one of the following classes: block graphs joining all cliques in one vertex, biconnected graphs with exactly two different vertex degrees, and strongly regular graphs with parameter $\mu = 1$.

Among these, the strongly regular graphs are the only regular graphs. If the parameter λ is zero, then Γ is a Moore graph. The Moore graphs of diameter two are the cycle C_5, the Petersen graph, the Hoffman-Singleton graph and hypothetical graphs of degree 57 [1, 8]. Hence, by Corollary 3.15, only C_5 remains.

Deutsch and Fischer [10] showed that if $\lambda > 0$, then we have $\lambda > 1$ and either $(\delta, \lambda) = (21, 2)$ or

$$\delta \geq (\lambda + 1)(\lambda + 13) \tag{2}$$

[10, Theorem 4.1 and Corollary]. By the Handshake Lemma, an odd degree is only possible for a group of even order and hence is excluded by Proposition 3.14. This excludes the case $(21, 2)$. For the second case, if $\lambda \geq 3$, then Equations (1) and (2) yield $|G| = \delta(\delta - \lambda) + 1 \geq \lambda^4 + 27\lambda^3 + 208\lambda^2 + 351\lambda + 170 \geq 3905$. For $\lambda = 2$ we obtain $\delta \geq 45$. Again, δ must be even; hence, $\delta \geq 46$ and $\delta - \lambda \geq 44$. Applying these bounds to Equation (1), we obtain $|G| = \delta(\delta - \lambda) + 1 \geq 46 \cdot 44 + 1 = 2025$. □

We note that an alternative proof of Lemma 3.16 with a bound of 1300 has been provided to us by Filippo Prandina, which relies on a database by Brouwer[1] of strongly regular graphs.

3.4. Central elements

Lemma 3.17. *Let* $\mathrm{Cay}(G, \Sigma)$ *be geodetic and* $b, t \in \Sigma$. *Suppose that* $b^2 \neq 1$, $t^2 = 1$, *and* $b^2 t = tb^{\pm 2}$. *Then the subgroup* $\langle b, t\rangle \leq G$ *is complete with respect to* Σ.

Proof. If $bt = tb^{\pm 1}$, then the statement follows from Lemma 3.7, so assume that $bt \neq tb^{\pm 1}$ holds. As $bbt = tbb$ or $bbt = t\overline{bb}$, we have $s \coloneqq bt\overline{b} = \overline{b}tb$ or $s \coloneqq btb = \overline{b}t\overline{b}$, respectively. In particular, there are two words of length three representing s; thus there must be a shorter one. Moreover, since s has order two, its geodesic must have odd length. Hence, $s \in \Sigma$. The situation is as shown in Figure 1.

Let $H \coloneqq \langle b, t, s\rangle = \langle H \cap \Sigma\rangle \leq G$. One may verify by straightforward computations (conjugating st by $b, \bar{b}, s, t$) that $(st)^H = \{st, ts\} \subseteq \Sigma$. The statement then follows using Lemma 3.7. □

Lemma 3.18. *Let* $\mathrm{Cay}(G, \Sigma)$ *be geodetic. If there exists some* $b \in \Sigma$ *with* $b^2 \neq 1$ *and* $(b^2)^G \subseteq \{b^{\pm 2}\}$, *then* $\mathrm{Cay}(G, \Sigma)$ *is an odd cycle or a complete graph.*

Proof. Suppose first, that $(b^2)^G = \{b^2\}$ and thus $b^2 \in Z(G)$. Then either $b \in Z(G)$ or $b \notin Z(G)$. In the first case, the statement follows immediately from Corollary 3.8. In the second case, $|G : Z(G)|$ is even; hence so is $|G|$. As such, there exists an element of order two in G. In fact, there even exists $t \in \Sigma$ with $t^2 = 1$ by Lemma 3.11. We then obtain $(b^2)^G \subseteq \Sigma$ from Lemma 3.17. The statement now follows from Corollary 3.8.

Finally, suppose that $(b^2)^G = \{b^{\pm 2}\}$ has two elements. Then $\left|G : C_G(b^2)\right| = 2$ and, as before, there thus exists some $t \in \Sigma$ with $t^2 = 1$. The statement follows from Lemmas 3.17 and 3.7. □

Lemma 3.19 (Flat coset). *Let* G *be a group with generating set* Σ *such that the Cayley graph is geodetic. If* $w \in \Sigma^m$ *is a geodesic of length* m *and* $a \in \Sigma$ *such that* $aw = wa$ *and* $w \neq a^{\pm m}$, *then each* $h \in w\langle a\rangle$ *has a geodesic of length at most* m. *Moreover, if* $w \notin \langle a\rangle$, *then each* $h \in w\langle a\rangle$ *has a geodesic of length exactly* m.

Proof. We denote by w_i the geodesic of wa^i. Let r be the order of a in G. Observe that $w_0 = w_r$.

[1] https://aeb.win.tue.nl/graphs/srg/srgtab.html

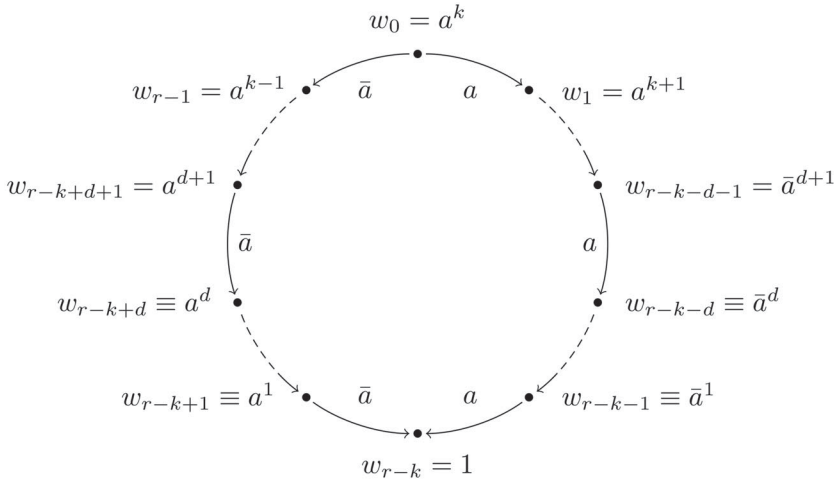

Figure 2. The coset $w\langle a\rangle$ in the case $w = a^k$ in the proof of Lemma 3.19.

First, we prove the lemma for the case $w \notin \langle a\rangle$. In this case, aw_i and w_ia are two different words, as otherwise $w \in \langle a\rangle$. Both aw_i and w_ia are of length $|w_i| + 1$ representing wa^{i+1}. Thus, there must be a shorter word, implying that $|w_{i+1}| \leq |w_i|$. Therefore, $m = |w_r| \leq \cdots \leq |w_i| \leq \cdots \leq |w_0| = m$, and we conclude $|w_i| = m$ for all i.

Second, we consider the case $w = a^k$. The proof of this case is illustrated in Figure 2. Recall that w_i is the geodesic for $wa^i = a^{i+k}$. Observe that, because the geodesic of a^k has length m, we must have $m \leq k$. In fact, because $w \neq a^{\pm m}$, we have $m < k$. Using the same argument, we also have $m < r - k$. We prove by induction on i that $|w_i| \leq m$. For $w_0 = w_r = w$ this obviously holds.

If $0 < i \leq r - k$, then we have two words, $w_{i-1}a$ and aw_{i-1} of length $|w_{i-1}| + 1$ for $a^{i+k} = w_i$. To prove that the two words are different, we show $w_{i-1} \neq a^{|w_{i-1}|}$: If w_{i-1} were a power of a, then $w_{i-1} = a^{i+k-1}$. That is impossible, as $|w_{i-1}| \leq m < k \leq i + k - 1$. Thus, the geodesic w_i has length at most $|w_{i-1}| \leq m$.

For $r - k < i < r$, we also use induction on decreasing values of i, multiplying with $\bar{a}$. Now $w_r = w$ is the base case for the induction. Assuming the statement holds for $i + 1$, the two words $w_{i+1}\bar{a}$ and $\bar{a}w_{i+1}$ both correspond to the group element $a^{i+k} = w_i$. To prove that the two words are different, we show $w_{i+1} \neq \bar{a}^{|w_{i+1}|}$: If w_{i+1} were a power of $\bar{a}$, then $w_{i+1} = \bar{a}^{2r-k-i-1}$ leading to the contradiction $2r - k - i - 1 \geq r - k > m \geq |w_{i+1}|$. Therefore, we must have $|w_i| \leq |w_{i+1}| \leq m$. □

The second case of the proof, where $w = a^k$ is illustrated in Figure 2. One can observe the two inductions, starting at w, one multiplying with a, the other multiplying with $\bar{a}$ covering the entire subgroup. Before arriving at 1 we encounter small powers of a, respectively $\bar{a}$. In fact, there is an integer $d \leq |w|$, such that a^i and $\bar{a}^i$ are geodesic for $0 \leq i \leq d$, but for $j > d$ the words a^j and $\bar{a}^j$ are not geodesics. By applying Lemma 3.19 to the geodesic of a^{d+1}, which has length d, we obtain $d = m$. This proves the following.

Corollary 3.20. *Let* $\mathrm{Cay}(G, \Sigma)$ *be a counterexample to Conjecture A and let* $a \in \Sigma$. *Then there is an integer* $m \in \mathbb{N}$ *such that* $a^{\pm i}$ *is a geodesic if* $i \leq m$ *and each element in the set* $\langle a\rangle \setminus \{a^{\pm i} \mid 0 \leq i \leq m\}$ *has a geodesic of length exactly* m.

Lemma 3.21 (Geodesics for central elements are powers of generators). *Let* G *be a group with geodetic Cayley graph* $\mathrm{Cay}(G, \Sigma)$, *and let* $z \in Z(G) \setminus \{1\}$. *Then the unique geodesic of* z *is* a^k *for some* $a \in \Sigma$ *and* $k \geq 1$.

Proof. Let $w_1 \cdots w_k \in \Sigma^*$ be a geodesic for z. As z is in the center we have

$$w_1w_2 \cdots w_k = z = z^{w_1} = w_2 \cdots w_kw_1.$$

Now we have two words of length k representing z. There cannot be a shorter word, as we chose $w_1 \cdots w_k$ to be a geodesic. The Cayley graph is geodetic, so the words must coincide: we obtain $w_1 = w_2 = \cdots = w_k$. □

Theorem 3.22 (Geodesics for central elements are powers with the same exponent). *Let* $G \neq 1$ *be a group with geodetic Cayley graph* $\mathrm{Cay}(G, \Sigma)$ *and* $\Sigma \cap Z(G) = \emptyset$. *Then, there is an integer* $k \geq 3$ *such that for each* $z \in Z(G) \setminus \{1\}$ *there exists an element* $c_z \in \Sigma$ *such that* c_z^k *is the geodesic for* z. *Moreover,* k *divides* $|G : Z(G)|$.

In light of this theorem, we make the following definitions for a non-cyclic geodetic Cayley graph $\mathrm{Cay}(G, \Sigma)$ with $G \neq 1$ and $\Sigma \cap Z(G) = \emptyset$. If $k \geq 3, z \in Z(G) \setminus \{1\}$ and $c_z \in \Sigma$ are as in Theorem 3.22,

(1) c_z is called a *central root*
(2) k is called the *length of central geodesics*
(3) a geodesic between two central elements is called a *central geodesic*, and is necessarily labeled by c_z^k for some central root c_z.

Observe that if $\Sigma \cap Z(G) \neq \emptyset$, then $k = 1$, as in this case the Cayley graph is complete by Corollary 3.8.

Proof. We know by Lemma 3.21 that the geodesic of every element in the center is a power of a generator. We first show that no two central elements can have a geodesic that is a power of the same generator (note that a generator and its inverse is allowed and will happen). Let b^k be a geodesic representing a central element and assume that k is minimal so that b^k is central. Let g be a generator different to $b^{\pm 1}$ (such a generator must exist, otherwise G would be a cyclic group, but then $b \in Z(G)$). By Lemma 3.19 the elements $b^k g$ and $b^k \bar{g}$ both have a geodesic of length at most k, which we write as $(b^k g)$ and $(b^k \bar{g})$. Now $(b^k g)(b^k \bar{g})$ is a word of length at most $2k$ representing the central element b^{2k}. Thus, b^{2k} is not a geodesic. Assume there is some $i \geq 1$ such that b^{k+i} is a geodesic of a central element. This implies that b^i is a geodesic of a central element. By minimality of k we conclude $i \geq k$. It follows that no power of b other than b^k is a geodesic for a non-trivial central element. In particular, the order of $b \cdot Z(G)$ in $G/Z(G)$ is k and, thus, k divides $|G : Z(G)|$.

Next we show that the geodesics of all non-trivial central elements have the same length. For a central element and its inverse this is obvious. Assume there are $c, d \in \Sigma$ with $c \notin \{d, \bar{d}\}$ and $k, \ell \geq 1$ such that c^k and d^ℓ both are geodesics representing different central elements. Note that $c^k \neq \bar{d}^\ell$ because both are geodesics. Now assume for a contradiction that $k \neq \ell$, w. l. o. g. $k < \ell$. Lemma 3.19 tells us that $c^k d^\ell \in c^k \langle d \rangle$ has a geodesic u of length $|u| = m \leq k$. But $c^k d^\ell$ is also in the center (and non-trivial), so $u = f^m$ for some $f \in \Sigma$. Applying Lemma 3.19 again to $d^\ell = f^m c^{-k} \in f^m \langle c \rangle$, we obtain a geodesic v of length at most $m \leq k < \ell$, contradicting d^ℓ being a geodesic.

It remains to show, that no central element has a geodesic of length two. In that case the Cayley graph would be cyclic or complete by Lemma 3.18, contradicting $\Sigma \cap Z(G) = \emptyset$. □

From Theorem 3.22 and Corollary 3.8, we immediately obtain the following corollary.

Corollary 3.23. *If $\Gamma = Cay(G, \Sigma)$ is geodetic and has diameter two and $Z(G) \neq 1$, then Γ is the cycle C_5.*

Lemma 3.24. *Let $\mathrm{Cay}(G, \Sigma)$ be geodetic. If there is an element $z \in Z(G)$, with $\mathrm{ord}(z) \geq 4$, then the length of central geodesics must be odd.*

Proof. Let $m = \mathrm{ord}(z)$. If m is even, then the statement follows from Theorem 3.12. Thus from here on we assume that m is odd and $m \geq 5$. Assume that b^{2k} is the geodesic for z. Let y be the geodesic for $z^{(m-1)/2}$. By Theorem 3.22 it has length $2k$. As $m \geq 5$, we have $y \neq b^{\pm 2k}$. Note that $t = b^{km} = y b^k$. By Lemma 3.19, the element $t \in y\langle b \rangle$ has length at most $|y| = 2k$. Clearly $t^2 = b^{2km} = 1$. If $t = 1$, then $y = t b^{-k} = \bar{b}^k$, contradicting $2k$ being the length of the central geodesics. It follows that t has order two, thus by Lemma 3.11 it must have odd length, that is, the length of t is at most $2k - 1$. Applying Lemma 3.19 to $y = t\bar{b}^k \in t\langle b \rangle$ we obtain the contradiction $|y| \leq |t| = 2k - 1$. □

4. Bounds on the size of generating sets

In this section we establish bounds on the possible sizes of those generating sets which result in a geodetic Cayley graph that is a counterexample to Conjecture A. To obtain these, we study the structure and size of balls of radius one and two in such a graph, as well as the positional relationships of central geodesics.

Let $\mathrm{Cay}(G, \Sigma)$ be an arbitrary geodetic Cayley graph. Throughout, we denote the r-ball in $\mathrm{Cay}(G, \Sigma)$ centered at a vertex $g \in G$ by $\mathcal{B}_r(g) \coloneqq \{h \in G \mid d(g, h) \leq r\}$. As Cayley graphs are vertex-transitive, all balls of the same radius r are isomorphic subgraphs of $\mathrm{Cay}(G, \Sigma)$.

We begin by analyzing the structure of one-balls. By Lemma 2.6 the neighbors of any $g \in G$ can be partitioned into a set of disjoint cliques. We denote by m the number of these disjoint cliques and by $\delta_1 \leq \delta_2 \leq \ldots \leq \delta_m$ their sizes. Clearly, $\delta \coloneqq \sum_{i=1}^m \delta_i$ is the degree of $\mathrm{Cay}(G, \Sigma)$ and thus $\delta = |\Sigma|$.

Lemma 4.1. *Let $\mathrm{Cay}(G, \Sigma)$ be a counterexample to Conjecture A. Then $m \geq 1 + \delta_m \geq 1 + \delta/m$ and $m \geq 3$.*

Proof. The Cayley graph $\mathrm{Cay}(G, \Sigma)$ contains a clique of size $\delta_m + 1$. By [19, Corollary 1] the neighborhood of some and, hence, of every vertex contains an independent set of size $\delta_m + 1$. Thus $m \geq \delta_m + 1$ by definition of m. The second inequality follows from $\delta = \sum_{i=1}^m \delta_i \leq \sum_{i=1}^m \delta_m = m\delta_m$.

For the final inequality, note that $m \leq 1$ holds if and only if $\mathrm{Cay}(G, \Sigma)$ is complete. If $m = 2$, then $\mathrm{Cay}(G, \Sigma)$ is a cycle. Neither can be a counterexample to Conjecture A. As such, $m \geq 3$. □

We define the function α, which will take an important role as parameter for the size of a two-ball in $\mathrm{Cay}(G, \Sigma)$ as follows:

$$\alpha(m_0) \coloneqq \frac{3m_0 - 4}{2m_0 - 2}.$$

Lemma 4.2. *Let* $\mathrm{Cay}(G,\Sigma)$ *be a counterexample to Conjecture A and let* $\alpha = \alpha(m)$. *Then, for every* $g \in G$, *the size of the two-ball centered at* g *satisfies*

$$\left|\mathcal{B}_2(g)\right| = 1 + \delta + \delta^2 - \sum_{i=1}^{m} \delta_i^2 \geq 1 + \delta + \tfrac{1}{2}\alpha\delta^2.$$

Proof. Every vertex at distance one from g which is contained in a clique of size δ_i has $\delta - \delta_i$ neighbors at distance two from g. As each vertex at distance two from g has a unique neighbor at distance one from g, we obtain the equality

$$\left|\mathcal{B}_2(g)\right| = 1 + \delta + \sum_{i=1}^{m} \delta_i(\delta - \delta_i) = 1 + \delta + \delta^2 - \sum_{i=1}^{m} \delta_i^2.$$

We then apply the reversed Cauchy-Schwarz inequality due to Pólya and Szegö. [28, pp. 57, 213–214] with the bounds $1 \leq \delta_i \leq m-1$ obtained in Lemma 4.1. This yields

$$m\sum_{i=1}^{m} \delta_i^2 = \left(\sum_{i=1}^{m} 1^2\right) \cdot \left(\sum_{i=1}^{m} \delta_i^2\right) \leq \frac{1}{4}\frac{m^2}{m-1}\left(\sum_{i=1}^{m} \delta_i\right)^2 = \frac{1}{4}\frac{m^2}{m-1}\delta^2,$$

from which the claimed inequality follows. □

Lemma 4.3. *Let* $g, h \in G$. *If* $d(g,h) \geq 3$, *then* $\left|\mathcal{B}_2(g) \cap \mathcal{B}_2(h)\right| \leq 2\delta - 1$.

Proof. Let h' be the vertex preceding h on the geodesic path from g to h. Then $\mathcal{B}_2(g) \cap \mathcal{B}_1(h) \subseteq \{h'\}$ by uniqueness of geodesics. Hence, $\left|\mathcal{B}_2(g) \cap \mathcal{B}_1(h')\right| \leq \left|\mathcal{B}_1(h') \setminus \{h\}\right| = \delta$. If $h'' \in \mathcal{N}(h) \setminus \{h'\}$, then $d(g,h'') \geq 3$, which implies $\left|\mathcal{B}_2(g) \cap \mathcal{B}_1(h'')\right| \leq 1$. In total, we obtain $\left|\mathcal{B}_2(g) \cap \mathcal{B}_2(h)\right| \leq 2\delta - 1$. □

We now have all the tools necessary to prove the main result of this section.

Theorem 4.4. *Let* $\mathrm{Cay}(G,\Sigma)$ *be a counterexample to Conjecture A of diameter at least three. Then* $\alpha_0 |\Sigma|^2 < |G|$ *holds for all* $\alpha_0 = \alpha(m_0)$ *such that* $m_0 \geq 3$ *is any integer with* $\frac{1}{2}(m_0-1)(3m_0-4)(m_0-2)^2 < |G|$.

Recall that the assumption on the diameter is satisfied whenever G has nontrivial center (Corollary 3.23), even order (Proposition 3.14), or order at most 2025 (Lemma 3.16). In case $\mathrm{Cay}(G,\Sigma)$ has diameter two, we obtain a similar but weaker bound as follows. As in the proof of Lemma 3.16, we have $|\Sigma| \geq (\lambda+1)(\lambda+13)$ for some $\lambda \geq 2$ as well as $|\Sigma| \geq 46$. The former yields the inequality

$$\lambda \leq \frac{\sqrt{144 + 4|\Sigma|} - 14}{2} \leq \frac{\sqrt{144} + \sqrt{4|\Sigma|} - 14}{2} = \sqrt{|\Sigma|} - 1.$$

Then $|G| = |\Sigma|^2 - \lambda|\Sigma| + 1 > |\Sigma|^2 - |\Sigma|\sqrt{|\Sigma|} + |\Sigma|$ by Equation (1) and using the above. Since $|\Sigma| \geq 46$, a direct computation shows that $\beta_0|\Sigma|^2 < |G|$ where $\beta_0 = \frac{47}{46} - \frac{1}{\sqrt{46}} \approx 0.874$ giving the bound in Theorem D.

Remark 4.5. *Before proceeding with the proof, we note that the factor* $\alpha_0 = \alpha(m_0)$ *is monotonically increasing in* m_0. *The choice* $m_0 = 3$ *is always valid for a counterexample to Conjecture A and yields* $\alpha_0 = \frac{5}{4}$. *On the other hand,* $\alpha_0 \to \frac{3}{2}$ *as* $m_0 \to \infty$. *Moreover, as a byproduct of our computer experiments, we obtain* a posteriori *that the conclusion of Theorem 4.4 holds with* $\alpha_0 = \frac{7}{5}$, *after verifying that Conjecture A holds for every group of order at most* 560 *(see Theorem B), we set* $m_0 = 6$.

We use a combination of the bound obtained in Theorem 4.4, as well as other ones discussed hereafter, in our computer experiments. This results in a massive reduction in the number of generating sets we have to consider. In order to make these bounds as tight as possible, we choose the maximal value m_0 *that is permitted for the group currently under examination. For some groups, we also employ Theorem 3.22 to establish an improved lower bound on the diameter which, in turn, allows us to replace Lemma 4.3 with a better estimate.*

Proof. For the sake of deriving a contradiction, we assume that $\alpha_0 |\Sigma|^2 \geq |G|$. We also continue to employ the notation established above. In particular, the previous inequality becomes $\alpha_0\delta^2 \geq |G|$, and Lemma 4.1 then yields $\alpha_0(m^2-m)^2 \geq \alpha_0\delta^2 \geq |G|$. We cannot have $m < m_0$, for otherwise

$$\tfrac{1}{2}(m_0-1)(3m_0-4)(m_0-2)^2 = \alpha_0\big((m_0-1)^2 - (m_0-1)\big)^2 \geq \alpha_0(m^2-m)^2 \geq |G|$$

which contradicts the choice of m_0. Hence $m \geq m_0$ and, therefore, also $\alpha = \alpha(m) \geq \alpha(m_0) = \alpha_0$.

Finally, recall that $\mathrm{Cay}(G,\Sigma)$ has diameter at least three by assumption. Hence there exist elements $g, h \in G$ with $d(g,h) = 3$. Using Lemmas 4.2 and 4.3 we arrive at

$$\left|\mathcal{B}_2(g) \cup \mathcal{B}_2(h)\right| = \underbrace{\left|\mathcal{B}_2(g)\right| + |\mathcal{B}_2(h)|}_{\geq 2+2\delta+\alpha\delta^2} - \underbrace{\left|\mathcal{B}_2(g) \cap \mathcal{B}_2(h)\right|}_{\leq 2\delta-1} \geq 3 + \alpha\delta^2 \geq 3 + \alpha_0\delta^2 \geq 3 + |G|\,.$$

As such, $|G| \geq \left|\mathcal{B}_2(g) \cup \mathcal{B}_2(h)\right| \geq |G| + 3 > |G|$, which is the desired contradiction. □

Corollary 4.6. *Let* $\mathrm{Cay}(G,\Sigma)$ *be a counterexample to Conjecture A. Then* $\alpha_0\big(|Z(G)|-1\big)^2 < |G|$.

Proof. This follows from Theorem 4.4, as $|\Sigma| \geq |Z(G)|-1$ by Theorem 3.22 and Corollary 3.8. Note that we can assume that $Z(G) \neq 1$; Corollary 3.23 then excludes the case that Cay(G, Σ) has diameter two. □

In Theorem 4.4 we have used two balls of radius two centered at vertices at distance three from each other to give a lower bound to the size of the group. In cases where the group has a non-trivial center, we can improve upon this. By Theorem 3.22, the distance between any two central elements is at least three. Using a subset of these as centers of balls of radius two, and Lemma 4.3 to bound the size of pairwise intersections, we arrive at the following.

Theorem 4.7. *Let* $\mathrm{Cay}(G,\Sigma)$ *be a counterexample to Conjecture A. Then the inequality*

$$\tfrac{1}{2}\alpha_0 z_0\,|\Sigma|^2 - z_0(z_0-2)\,|\Sigma| + \tfrac{1}{2}z_0(z_0+1) \leq |G|\,, \tag{3}$$

where $\alpha_0 = \alpha(m_0)$ *holds for all integers* z_0 *with* $1 \leq z_0 \leq |Z(G)|$ *and all lower bounds* m_0 *on the number* $m \geq m_0$ *of maximal cliques in the neighborhood* $\mathcal{N}(1)$ *of* $1 \in G$.

Proof. Choose a set of z_0 central elements, say $Z_0 \subseteq Z(G)$. By Lemmas 4.2 and 4.3,

$$|G| \geq \Big|\bigcup_{g\in Z_0}\mathcal{B}_2(g)\Big| \geq \sum_{g\in Z_0}\big|\mathcal{B}_2(g)\big| - \sum_{\substack{g,h\in Z_0\\ g\neq h}}\big|\mathcal{B}_2(g)\cap\mathcal{B}_2(h)\big| \geq z_0\big(1+\delta+\tfrac{1}{2}\alpha\delta^2\big) - \binom{z_0}{2}(2\delta-1)$$

with $\alpha \geq \alpha_0$. (Recall that $\delta = |\Sigma|$.) Expanding the rightmost expression yields the stated inequality. □

Note that in Theorem 4.7 we have a family of inequalities, parameterized by the number z_0 of central elements used for placing the two-balls. For groups with a small center, the best lower bound is achieved by $z_0 = |Z(G)|$. However, if the center is large enough, then at some point it is no longer beneficial to place more balls, due to the way we approximate the intersection. The best lower bound is obtained for $z_0 \approx \frac{1}{4}\alpha_0\delta$. Based on this observation we obtain the following bound on the center.

Corollary 4.8. *Let* $\mathrm{Cay}(G,\Sigma)$ *be a counterexample to Conjecture A. Then* $\frac{1}{16}\alpha_0^2\big(|Z(G)|-1\big)^3 \leq |G|$.

Proof. If $|Z(G)| = 1$, then the statement holds. If $|Z(G)| > 1$, the inequality is derived from Theorem 4.7 by setting $z_0 = \big\lceil \frac{1}{4}\alpha_0\big(|Z(G)|-1\big)\big\rceil$:

$$\begin{aligned}
|G| &\geq (\tfrac{1}{2}\alpha_0\delta - z_0)z_0\delta + 2z_0\delta\\
&\geq (\tfrac{1}{2}\alpha_0\delta - \tfrac{1}{4}\alpha_0(Z(G)-1)-1)z_0\delta + 2z_0\delta\\
&\geq (\tfrac{1}{2}\alpha_0\delta - \tfrac{1}{4}\alpha_0(Z(G)-1))z_0\delta\\
&\geq \tfrac{1}{16}\alpha_0^2(Z(G)-1)^3.
\end{aligned}$$

The first inequality follows directly from equation (3) by dropping the terms not containing $\delta = |\Sigma|$, which are all positive. The second inequality uses $z_0 = \big\lceil \frac{1}{4}\alpha_0\big(|Z(G)|-1\big)\big\rceil \leq \frac{1}{4}\alpha_0\big(|Z(G)|-1\big)+1$. The third inequality is obtained by dropping the term $2z_0\delta - z_0\delta \geq 0$. Finally we use the inequalities $z_0 \geq \frac{1}{4}\alpha_0\big(|Z(G)|-1\big)$ and $\delta \geq |Z(G)|-1$ to obtain the desired statement. □

To obtain the result above, we placed two-balls on central elements. If the central elements are sufficiently far apart, then we can show an even stronger bound, by placing the two-balls along the central geodesics (geodesics connecting the central elements). Recall that by Theorem 3.22 central geodesics all have the same length k. We begin with the following lower bound on the distance between two vertices on two different central geodesics.

Lemma 4.9. *Let* $\mathrm{Cay}(G,\Sigma)$ *be a counterexample to Conjecture A with* $Z(G) \neq 1$. *Let* g *be a vertex on a central geodesic with endpoints* y_1 *and* y_2. *Let* h *be a vertex on a different central geodesic with endpoints* z_1 *and* z_2. *Then* $d(g,h) \geq \max\{i,j\}$, *where* $i = \min\{d(y_1,g), d(y_2,g)\}$ *and* $j = \min\{d(z_1,h), d(z_2,g)\}$.

Proof. Let k be the length of the central geodesics. As g and h lie on different central geodesics, at most one pair of the vertices $\{y_1,y_2,z_1,z_2\}$ may coincide. We choose $y \in \{y_1,y_2\}$, $z \in \{z_1,z_2\}$ and $a,b \in \Sigma$ such that $\{y_1,y_2\} = \{y, ya^k\}$, $\{z_1,z_2\} = \{z, zb^k\}$, and if any of the four endpoints coincide, then $ya^k = zb^k$. A consequence of this choice is $y \neq z$, $y \neq zb^k$, $d(y,g) \leq k-i$, and $d(z,h) \leq k-j$.

We claim that $d(y,h) \geq k$. Let w be the geodesic of $y^{-1}h$. Observe that $y^{-1}h$ commutes with b, as it is the product of the central element $y^{-1}z$ with a power of b. In the case that $w \neq b^{\pm m}$ where $m = |w|$, by Lemma 3.19, the geodesic of $y^{-1}z \in y^{-1}h\,\langle b\rangle$ has length at most m, that is $k = d(1,y^{-1}z) \leq m = d(1,y^{-1}h)$. We obtain the desired statement $d(y,h) \geq k$ using vertex transitivity. In the case

that $w = b^{\pm m}$, assume for a contradiction that $m < k$. Then $y^{-1}h = b^{\pm m}$ is on the central geodesic between 1 and $b^{\pm k}$. By vertex transitivity, h is on the central geodesic between y and $yb^{\pm k}$. Thus $y \in \{z, zb^k\}$ contradicting the choice of y.

From the triangle inequality $d(y,h) \leq d(y,g) + d(g,h)$ we obtain $d(g,h) \geq d(y,h) - d(y,g) \geq k - (k-i) = i$. Similarly, using $d(z,g) \leq d(z,h) + d(h,g)$, we obtain $d(g,h) \geq j$. □

Multiple disjoint balls of radius two can be placed along each central geodesic if its length permits. However, we will only give an explicit bound for the simplest case, placing a single such ball in the middle of each central geodesic.

Proposition 4.10. *Let* $\mathrm{Cay}(G,\Sigma)$ *be a counterexample to Conjecture A. If* $3 \nmid |G|$ *and* $5,7 \nmid |G : Z(G)|$, *then* $\frac{1}{4}\alpha_0\big(|Z(G)|-1\big)^4 < |G|$.

Proof. If $|Z(G)| = 1$, then clearly the statement is true. By Theorem 3.12 the order of $Z(G)$ is odd. With our assumption $3 \nmid |G|$, there must be an element of order at least 5 in the center. Thus, the length k of central geodesics must be odd by Lemma 3.24. As $5,7 \nmid |G : Z(G)|$ we have $k \geq 11$.

There are $\frac{1}{2}|Z(G)|\big(|Z(G)|-1\big)$ distinct pairs of central elements, and thus, that many central geodesics. We place a two-ball on the middle of each central geodesic. The intersection between any pair of two-balls is trivial, as the distance between any two of their center points is at least 5 by Lemma 4.9. Thus we obtain

$$\begin{aligned} |G| &\geq \tfrac{1}{2}|Z(G)|\big(|Z(G)|-1\big)|\mathcal{B}_2(1)| \\ &> \tfrac{1}{2}\big(|Z(G)|-1\big)^2\big(\tfrac{1}{2}\alpha\delta^2+\delta+1\big) \\ &> \tfrac{1}{4}\alpha\big(|Z(G)|-1\big)^2\delta^2. \end{aligned}$$

Using the inequality $\delta \geq |Z(G)| - 1$ yields the desired bound. □

5. Further cases: dihedral, nilpotent, groups with large commutativity degree

In this section we show that further large families of groups satisfy Conjecture A by combining results from Section 3 with more detailed knowledge about finite group theory and insights gleaned from the computer search.

We first consider groups that have an abelian subgroup of index two (which is necessarily normal); these include the dihedral groups. Pushing this to index three presents more challenges; so for that case we are able to prove the conjecture only in the two important special cases when the subgroup is not normal or when the center is trivial. For nilpotent groups we can prove the conjecture holds in all groups of class two except for a particular subfamily (see Proposition 5.13), and in groups of any class provided certain numerical conditions are satisfied (see Theorem 5.9). Each of these families of groups in some sense is close to abelian, which is emphasized by the fact that these classes cover all groups with a high *commutativity degree* (see Theorem 5.14).

5.1. Abelian subgroups of index two

Lemma 5.1. *Let* G *be a group and* $1 < N < G$ *with* $|G : N| = 2$. *If* $\mathrm{Cay}(G,\Sigma)$ *is geodetic, then* $N \cap \Sigma \neq \emptyset$.

Proof. If $\Sigma \cap N = \emptyset$, then every word $w \in \Sigma^*$ representing $1 \in G$ has even length. Hence, all cycles in $\mathrm{Cay}(G,\Sigma)$ must have even length. But then $\mathrm{Cay}(G,\Sigma)$ cannot be geodetic (see Lemma 2.2). □

Theorem 5.2. *Let* $\phi : A \to A$ *be an order-two automorphism of an abelian group* $A = \langle X \mid R\rangle$. *Let*

$$D_{A,\phi} \coloneqq A \rtimes_\phi C_2 = \langle X \cup \{t\} \mid R \cup \{t^2, txt(\phi(x))^{-1};\, x \in X\}\rangle$$

be the corresponding semidirect product. Then the only geodetic Cayley graph of the generalized dihedral group $D_{A,\phi}$ *is the complete graph.*

Proof. Assume that $\mathrm{Cay}(D_{A,\phi},\Sigma)$ is geodetic but not complete (in particular, $Z(D_{A,\phi}) \cap \Sigma = \emptyset$ by Corollary 3.8). Since $\mathrm{ord}(t) = 2$, the generating set Σ contains a conjugate of t by Lemma 3.11. Upon replacing Σ with a suitable conjugate if necessary, we may therefore assume that $t \in \Sigma$.

As $|D_{A,\phi} : A| = 2$, there exists some $x \in A \cap \Sigma$ by Lemma 5.1. If $\phi(x) \in \{x^{\pm 1}\}$, then $x^{D_{A,\phi}} \subseteq \{x^{\pm 1}\} \subseteq \Sigma$. Since $\Sigma \neq \{x^{\pm 1}\}$, Lemma 3.7 implies that $\mathrm{Cay}(D_{A,\phi},\Sigma)$ is complete. Thus $\phi(x) \notin \{x^{\pm 1}\}$. Note that $\phi(x)x$ commutes with t as $t\phi(x)x = ttxtx = xtxtt = x\phi(x)t = \phi(x)xt$ as $x, \phi(x) \in A$. Hence $\phi(x)x \in Z(D_{A,\phi}) \setminus \{1\}$.

By Theorem 3.22, there exists $y \in \Sigma$ such that $\phi(x)x = y^k$ with $k \geq 3$ and, therefore, with $k = 3$ by uniqueness of geodesics (since $\phi(x)x = txtx$). Thus, in particular, the length of central geodesics is three. Now, suppose that $z \in \Sigma$ with $z^3 \in Z(D_{A,\phi})$. Then $z \in A$, for otherwise $z^3 \notin A$ (since A has index 2) which would contradict the assumption that $z^3 \in Z(D_{A,\phi}) \leq A$. In particular, this shows that $y \in \Sigma \cap A$.

Next, we argue that we can find an element $z \in \Sigma \cap A$ with $z \notin \{y^{\pm 1}\}$. If so, then y and z commute; hence $z^{\langle y \rangle} = \{z\} \subseteq \Sigma$ and then we can apply Lemma 3.7 to show that $\langle y \rangle$ is complete. However, this implies $y^3 \in \Sigma$ and thus $Z(D_{A,\phi}) \cap \Sigma \neq \emptyset$; contradicting the assumption that $Z(G) \cap \Sigma = \emptyset$.

Firstly, suppose that $y = x$, then $x^3 = y^3 = \phi(x)x$ and thus $\phi(x) = x^2$. We obtain the contradiction $y^3 = x^3 = \bar{x}x^4 = \bar{x}\phi(\phi(x)) = \bar{x}x = 1$. Next, suppose that $y = x^{-1}$ holds. Then $x^{-3} = y^3 = \phi(x)x$ and thus $\phi(x) = x^{-4}$, or equivalently $\phi(y) = y^{-4}$. Then $\phi(\phi(y)) = \phi(y^{-4}) = y^{16}$ and since ϕ is order two, this means $y = y^{16}$ so $y^{15} = 1$. This means the order of y is either 3, 5, or 15. It cannot be 3 since y^3 is a non-trivial element of the center. If $y^5 = 1$, then $y = y^{-4} = \phi(y) \in Z(D_{A,\phi})$ and so $Z(D_{A,\phi}) \cap \Sigma \neq \emptyset$ and we are done. Thus $\mathrm{ord}(y) = 15$. We then have $y^6 \in Z(D_{A,\phi}) \setminus \{1\}$ and $y^6 \notin \{y^{\pm 3}\}$. Thus $y^6 = z^3$ for some $z \in \Sigma \cap A$ with $z \notin \{y^{\pm 1}\}$. Lastly if $y \neq x^{\pm 1}$ then $z \coloneqq x$ satisfies our requirements. Thus we have found an element $z \in \Sigma \cap A$ with $z \notin \{y^{\pm 1}\}$ which by the above paragraph shows that the Cayley graph is complete, contradicting our assumption. □

Corollary 5.3. *The only geodetic Cayley graph of a dihedral group is the complete graph.*

We will now reduce the general case, of admitting an abelian subgroup of index two, to the situation discussed in Theorem 5.2. In other words, we will prove the following.

Theorem 5.4. *Let G be a group. If there exists an abelian subgroup $A \leq G$ such that $|G : A| = 2$, then the only geodetic Cayley graph of G is the complete graph.*

Our reduction will rely on a certain relationship between the structure of the group G and the parity of the order of A as well as that of $Z(G)$. Part of this relationship is captured by the following observation (with $p = 2$). It will be used again (with $p = 3$) in Section 5.2.

Lemma 5.5. *Let G be a group and $A \trianglelefteq G$ a normal abelian subgroup of prime index $|G : A| = p$. If $g \in G \setminus A$, then $g^p \in Z(G) \cap A$. Moreover, if $p \nmid |A|$, then there exists some $\tilde{g} \in G \setminus A$ with $\tilde{g}^p = 1$.*

Proof. The image of any given $g \in G \setminus A$ in the quotient $G/A \cong C_p$ has order p and, as such, $g^p \in A$. In particular, g^p commutes with every element $a \in A$ and, clearly, g^p also commutes with g. We have $\langle A, g \rangle = G$ since $A \leq G$ is a maximal subgroup (its index is prime) and $g \in G \setminus A$. Therefore, the element g^p commutes with all elements of G, i.e., $g^p \in Z(G)$ as claimed. Lastly, since p divides $|G| = |G : A|\,|A|$, there exists an element $\tilde{g} \in G$ of order p by Cauchy's theorem. If $p \nmid |A|$, then $\tilde{g} \notin A$ by Lagrange's theorem. □

Proof of Theorem 5.4. If $|Z(G)|$ is even, then Theorem 3.12 applies, so assume $|Z(G)|$ is odd. We claim that $|A|$ is odd as well. Suppose otherwise. Then there exists some $a \in A$ with $\mathrm{ord}(a) = 2$. Note that we cannot have $a \in Z(G)$ for $|Z(G)|$ is odd. Let $g \in G \setminus A$ and consider $\tilde{a} \coloneqq a^g a \in A$. Clearly, $a^g \neq a$ for otherwise we would have $a \in Z(G)$. Therefore, $\tilde{a} \neq 1$. Since $\tilde{a}^2 = 1$, we conclude that $\mathrm{ord}(\tilde{a}) = 2$. Moreover $\tilde{a}^g = a^{gg} a^g = a a^g = a^g a = \tilde{a}$ since $g^2 \in Z(G)$ by Lemma 5.5. But then we conclude that $\tilde{a} \in Z(G)$ and, therefore, $|Z(G)|$ would have to be even.

Finally, since $|A|$ is odd, there exists $t \in G \setminus A$ with $t^2 = 1$ by Lemma 5.5. Consider the automorphism $\phi \colon A \to A$ with $\phi(a) = a^t$. It satisfies $\phi^2 = \mathrm{id}$ and $\phi \neq \mathrm{id}$ since $t^2 = 1$ and $t \notin Z(G)$, respectively. As such, it has order two and we can apply Theorem 5.2. □

5.2. Abelian subgroups of index three

For an index 3 abelian subgroup $A \leq G$ we are able to show that Conjecture A holds for two cases: first if A is not normal and second if the center of G is trivial.

The general intuition is that, if a group has a lot of commuting elements (as it does when it contains an abelian subgroup of small index), then all of its Cayley graphs will need to have a lot of squares. However, we can only manage to make this precise with particular hypotheses. In Section 5.4 we investigate this intuition further.

Lemma 5.6. *Let G be a group and suppose that there exists an abelian subgroup $A \leq G$ such that $|G : A| = 3$ and A is not normal in G. Then the only geodetic Cayley graph of G is the complete graph.*

Proof. Let $A^g \leq G$ be a conjugate subgroup with $A \neq A^g$. Then $\langle A, A^g \rangle = G$ since A is a maximal subgroup of G (as its index is prime). Moreover, we observe that $A \cap A^g \subseteq Z(G)$ as every element of $A \cap A^g$ commutes with every element of $\langle A, A^g \rangle$.

Now consider the action of G by left-multiplication on the set of cosets G/A. It gives rise to a homomorphism $\rho \colon G \to S_3$ with $\mathrm{Ker}(\rho) = \{h \in G \mid hgA = gA \text{ for all } g \in G\} = \bigcap_{g \in G} A^g \leq Z(G)$. The ρ-preimage of $C_3 \leq S_3$ is an abelian subgroup $\rho^{-1}(C_3) \leq G$, as it is an extension of $\mathrm{Ker}(\rho) \leq Z(G)$ by a cyclic group.

Since $|G : \rho^{-1}(C_3)| = 2$ as ρ is surjective, the statement now follows from Theorem 5.4. □

Remark 5.7. *In the situation described in Lemma 5.6, we have $|G : Z(G)| = 6$. In Corollary 4.6 we have proved an inequality relating the size of the center and the size of the group, which in the case at hand gives us the bound $|G| < 36$ (assuming that G violates Conjecture A,*

we have $\frac{5}{4}(|Z(G)|-1)^2 < |G| = 6\,|Z(G)|$ *which, since* $|Z(G)|$ *is necessarily odd by Theorem 3.12, implies that* $|Z(G)| < 6$ *and thus* $|G| < 36$*). These groups can be checked by a computer search.*

We note that this alternative proof can be adapted, so as to cover groups with an abelian but not *normal subgroup of index* 5 *or* 7 *(the center of such a group has index at most* 20 *or* 42 *and, thus, by Corollary 4.8 we need only consider such groups with order at most* 300 *and* 840*, respectively).*

The other case is that G contains a normal abelian subgroup of index three. For this we can make progress when we restrict to the case where the center is trivial.

Theorem 5.8. *Let* G *be a group with* $Z(G) = 1$ *and suppose that there exists an abelian subgroup* $A \leq G$ *such that* $|G : A| = 3$*. Then the only geodetic Cayley graph of* G *is the complete graph.*

Proof. Assume that $\mathrm{Cay}(G, \Sigma)$ is geodetic but not complete. By Lemma 5.6, A is a normal subgroup of G. Note that we then have $\mathrm{ord}(\psi) = 3$ for each $\psi \in G \backslash A$ by Lemma 5.5 and our assumption on $Z(G)$. In order to derive a contradiction, we establish two claims regarding the conjugacy classes of elements of A with specific geodesics, in particular, elements of the set $C \coloneqq \{g \in A \mid \mathrm{geod}(g) \equiv \psi_1\psi_2 \text{ with } \psi_1, \psi_2 \in \Sigma \setminus A\}$.

Claim (1). If $x \in \Sigma \cap A$*, then* $x^G = \{x, \psi_1\psi_2, \psi_2\psi_1\}$ *for some* $\psi_1, \psi_2 \in \Sigma \setminus A$ *with* $\psi_1\psi_2, \psi_2\psi_1 \in C$*.*

Since $A \leq G$ is a maximal subgroup, there exists some $\psi \in \Sigma \setminus A$. Because $G = A \cdot \{1, \psi, \psi^{-1}\}$, we know that $x^G = \{x, \psi^{-1}x\psi, \psi x\psi^{-1}\}$. We also note that $\psi x\psi x\psi x = (\psi x)^3 = 1$ as $\psi x \in G \setminus A$. Therefore, the element $\psi x\psi = x^{-1}\psi^{-1}x^{-1}$ has length at most two. In turn, we conclude that both of the elements $\psi^{-1}x\psi = \psi(\psi x\psi)$ and $\psi x\psi^{-1} = (\psi x\psi)\psi$ have length at most two.

If one of these elements, $\psi^{-1}x\psi$ say, had length one, then, so would $x\psi$ and $\psi^{-1}x$ by Lemma 2.3; hence, so would $\psi(x\psi) = x^{-1}(\psi^{-1}x^{-1})$ and $(\psi^{-1}x)\psi^{-1} = (x^{-1}\psi)x^{-1}$; hence, so would ψx and $x\psi^{-1}$. It follows that the other element $(\psi x)\psi^{-1} = \psi(x\psi^{-1})$ would also have length one. But then all elements of the conjugacy class x^G would have length one, i.e., $x^G \subseteq \Sigma$. This contradicts Lemma 3.7.

Next, we assume that $\mathrm{geod}(\psi^{-1}x\psi) \equiv y_1y_2$ with $y_1, y_2 \in \Sigma \cap A$. This implies $y_1, y_2 \in \{x^{\pm 1}\}$, for otherwise $\langle \Sigma \cap A \rangle \leq G$ is a complete subgroup by Lemma 3.7 and thus y_1y_2 has length one. If $\psi^{-1}x\psi = x^{\pm 2}$, then either $\psi x\psi^{-1} = \psi_1\psi_2 \in C$ or, for the same reason as above, $\psi x\psi^{-1} = x^{\mp 2}$.

In the second case, x is conjugate to x^{-1} by transitivity of conjugacy. Since x is the only element of length one in x^G, this implies $x = x^{-1}$. But then $\psi^{-1}x\psi = x^{\pm 2} = 1$, which is absurd.

In the first case, i.e., $x^G = \{x, \tilde{x}, \psi_1\psi_2\}$ where $\tilde{x} = x^{\pm 2}$, we have $\psi^{-1}x\psi = \tilde{x} = x^{\pm 2}$ and, hence, $x = x^{\pm 8}$ as $\psi^3 = 1$. If $\psi^{-1}x\psi = x^{-2}$, then $x^9 = 1$ and thus $\psi^{-1}x^3\psi = x^{-6} = x^3 \in Z(G)$. But this implies $x^3 = 1$ and, therefore, $x^{-2} = x \in \Sigma$; a contradiction. In the case $\psi^{-1}x\psi = x^2$, we first observe that $\psi_2\psi_1 = x$. Indeed, $\psi_2\psi_1$ is conjugate to x and cannot equal x^2 or $\psi_1\psi_2$ by uniqueness of geodesics. Using this, we obtain $\psi_2 x\psi_2^{-1} = x^2$ since $\psi_2(\psi_1\psi_2)\psi_2^{-1} = x$ and ψ_2 has order three. Now $\psi_1 x = \psi_2^{-1}\psi_2\psi_1 x = \psi_2^{-1}x^2 = \psi_2^{-1}\psi_2 x\psi_2^{-1} = x\psi_2^{-1} \in \Sigma$, since it has two expressions of length two. But then the same is true for $x^2 = \psi_2(\psi_1 x)$; hence $x^2 \in \Sigma$, which contradicts our assumption that x^2 has length two.

The only remaining possibility is that $\mathrm{geod}(\psi^{-1}x\psi) \equiv \psi_1\psi_2$ and, hence, $\mathrm{geod}(\psi x\psi^{-1}) \equiv \psi_2\psi_1$ for some $\psi_1, \psi_2 \in \Sigma \setminus A$. This establishes Claim (1).

Claim (2). If $\psi_1, \psi_2 \in \Sigma \setminus A$ *with* $g = \psi_1\psi_2 \in C$*, then for some* $x \in \Sigma \cap A$

$$g^G = \{x, \psi_1\psi_2, \psi_2\psi_1\} \quad \text{or} \quad g^G = \{x^2, \psi_1\psi_2, \psi_2\psi_1\}.$$

Clearly, $\psi_1\psi_2$ and $\psi_2\psi_1$ are distinct elements of g^G. Moreover, $\psi_2\psi_1$ also has length two by Claim (1). The third element of g^G is $h \coloneqq \psi_1^{-1}\psi_2\psi_1^{-1} = \psi_2^{-1}\psi_1\psi_2^{-1}$, which therefore has length at most two. The claim is trivial if h has length one. Suppose that h has length two and $\mathrm{geod}(h) \equiv \psi_1'\psi_2'$ with $\psi_1', \psi_2' \in \Sigma \setminus A$. Clearly, $\psi_2'\psi_1' \neq \psi_1'\psi_2'$ and $\psi_2'\psi_1' \in g^G$. Moreover, $\psi_2'\psi_1'$ also has length two by what we have just shown. It follows that $\{\psi_1', \psi_2'\} = \{\psi_1, \psi_2\}$, which is clearly impossible.

If $\mathrm{geod}(h) \equiv y_1y_2$ with $y_1, y_2 \in \Sigma \cap A$, then $y_1 = y_2$ by uniqueness of geodesics and the fact that $y_1y_2 = y_2y_1$. Hence $h = x^2$ with $x = y_1 = y_2 \in \Sigma$. This completes our proof of the claim.

We finally derive the desired contradiction. To this end, recall that there exists some $\psi \in \Sigma \setminus A$. Furthermore, we cannot have $\Sigma = \{\psi^{\pm 1}\}$ for G is not cyclic. As such, we either have $\Sigma \cap A \neq \emptyset$ or there exists some $\psi' \in \Sigma \setminus A$ with $\psi' \notin \{\psi^{\pm 1}\}$. In the latter case, $\Sigma \cap A \neq \emptyset$ by Claim (2).

Now, choose some $x \in \Sigma \cap A$ and let $\psi_1, \psi_2 \in \Sigma \setminus A$ with $x^G = \{x, \psi_1\psi_2, \psi_2\psi_1\}$ as in Claim (1). We then have $x = \psi_1^{-1}\psi_2\psi_1^{-1} = \psi_2^{-1}\psi_1\psi_2^{-1}$. Let $\psi_3 \coloneqq x\psi_1 = \psi_1^{-1}\psi_2 \in \Sigma$ and observe $\psi_3 \notin \{\psi_1^{\pm 1}, \psi_2\}$. In fact, we also have $\psi_3 = \psi_1^{-1}\psi_2 \neq \psi_2^{-1}$ for otherwise $\psi_2\psi_1 = 1$. Now note that $\psi_3^{-1}\psi_2^{-1} = x$ and thus $\psi_2^{-1}\psi_3^{-1} \in x^G \setminus \{x\} = \{\psi_1\psi_2, \psi_2\psi_1\}$, which contradicts uniqueness of geodesics. □

5.3. Nilpotent groups

In every nilpotent group, certain iterated commutators evaluate to central elements. This fact, together with our results concerning central elements developed in Section 3.4, imposes restrictions on the structure of a nilpotent group with an alleged non-complete geodetic Cayley graph. For groups of nilpotency class two, we obtain further restrictions based on a more detailed analysis of the involved commutator maps; see Proposition 5.13.

Recall that a group G is *nilpotent* if $G = 1$ or $G/Z(G)$ is nilpotent. If G is nilpotent, then there exists a number s such that $[g_1, \dots, g_{s+1}] \coloneqq [[g_1, \dots, g_s], g_{s+1}] = 1$ for all $g_1, \dots, g_{s+1} \in G$. The smallest such number s is the *nilpotency class* of G. A group is nilpotent if and only if it is a direct product of p-groups; see [30, Theorem 5.2.4]. In particular, every nilpotent group of even order has even-order center.

Theorem 5.9. *Let G be a nilpotent but not cyclic group of nilpotency class s and suppose that*

$$p \nmid \frac{\exp(G)}{\exp(Z(G))}$$

for each odd prime $p < 3 \cdot 2^{s-1} - 2$. Then the only geodetic Cayley graph of G is the complete graph.

Proof. All finite nilpotent groups are direct products of p-groups. Thus, if 2 divides $|G|$, then there must be an order 2 element in the center and the statement follows from Theorem 3.12. If G is abelian, then the statement is a consequence of Corollary 3.9. We now assume that $s > 1$ and $2 \nmid |G|$, and that there exists a geodetic Cayley graph $\mathrm{Cay}(G, \Sigma)$ which is not complete.

In every finite group of nilpotency class s, by [7, Lemma 2.6], there are generators $a_1, \dots, a_s \in \Sigma$ such that $z = [a_1, a_2, \dots, a_s] \neq 1$. Further, since G is nilpotent of class s, we have $z \in Z(G)$; hence, by Corollary 3.8 and Theorem 3.22, $z = a^k$ with $a \in \Sigma$ and $k \geq 3$ equal to the order of a in the quotient group $G/Z(G)$. Since a^k is a geodesic, its length is shorter than the length of the commutator, which is $3 \cdot 2^{s-1} - 2$.

Let p be a prime divisor of $k = pr$. Then p also divides $|G : Z(G)|$, $|G|$, and $|Z(G)|$. Furthermore, p is odd and $p \leq k < 3 \cdot 2^{s-1} - 2$. Let p^n be the largest power of p dividing $\exp(Z(G))$ (note that $n \geq 1$). Let $\tilde{z} \in Z(G)$ with $\mathrm{ord}(\tilde{z}) = p^n$. Once more, $\tilde{z} = \tilde{a}^k$ for some $\tilde{a} \in \Sigma$ by Theorem 3.22. Now consider the element $b = \tilde{a}^r$ (where $k = pr$ as above). Clearly, $(b^p)^{p^n} = \tilde{z}^{p^n} = 1$. As such, $\mathrm{ord}(b) = p^{n+1}$ and, thus, p^{n+1} divides $\exp(G)$. We conclude that p divides $\exp(G)/\exp(Z(G))$, which contradicts our assumption on G. □

Remark 5.10. *The condition in Theorem 5.9 is satisfied if no odd prime $p < 3 \cdot 2^{s-1} - 2$ divides the order of G or, more generally, if p^2 does not divide $\exp(G)$ for any such prime p. If, for example, G is a nilpotent group of nilpotency class two with $9 \nmid \exp(G)$, then G satisfies Conjecture A; if G is of nilpotency class three and neither 3, 5, nor 7 divide $|G|$, then G satisfies Conjecture A.*

We now turn to the case of nilpotency class two. In the following we always assume that G is nilpotent group of nilpotency class two and that $\mathrm{Cay}(G, \Sigma)$ is a counterexample to Conjecture A. Recall that, by Theorem 3.12, this implies that $2 \nmid |G|$ and, by Theorem 5.9 (see also Remark 5.10), that $3 \mid |Z(G)|$.

Throughout, we will consider the subset $\Delta \coloneqq \{x \in \Sigma \mid x^3 \in Z(G) \setminus \{1\}\} \subseteq \Sigma$. Since $[x, y] \in Z(G) \setminus \{1\}$ for some $x, y \in \Sigma$ (see the proof of Theorem 5.9), the length of central geodesics is three according to Theorem 3.22. As such, the map $\alpha \colon G \to G$ given by $g \mapsto g^3$ induces a bijection from Δ onto $Z(G) \setminus \{1\}$. As there exists an element of order three in $Z(G)$, there exists an element of order nine in Δ; in particular, $\Delta \neq \emptyset$.

Lemma 5.11. *Let $x, y \in \Sigma$ with $x \in \Delta$ or $y \in \Delta$. Then $[x, y] = 1$ if and only if $\{x^{\pm 1}\} = \{y^{\pm 1}\}$.*

Proof. If $[x, y] = 1$ and $\{x^{\pm 1}\} \neq \{y^{\pm 1}\}$, then $\langle x, y \rangle \leq G$ is a complete subgroup by Corollary 3.10. If, furthermore, $x \in \Delta$, then $x^3 \in Z(G) \cap \Sigma$. But then $\mathrm{Cay}(G, \Sigma)$ is complete by Corollary 3.8. □

Lemma 5.12. *Let $x \in \Sigma$ and $y_1, y_2 \in \Sigma \setminus \{x^{\pm 1}\}$ with $y_1 \in \Delta$. Then $[x, y_1] = [x, y_2]$ implies $y_1 = y_2$.*

Proof. Let $z \coloneqq [x, y_1] = [x, y_2] \in Z(G)$. Then $z \neq 1$ by Lemma 5.11 and, thus, $z = a^3$ with $a \in \Delta$. Assuming $y_1 \neq y_2$, the element $xz = x^{y_1} = x^{y_2}$ has two distinct representatives of length three; therefore, it has length at most two. But then $\bar{x} = a$ by uniqueness of geodesics, as $\bar{x}(xz) = z = a^3$. In particular, this shows that $x = \bar{a} \in \Delta$ and that $x^y = xz = x^{-2}$ for $y \in \{y_1, y_2\}$.

Since $2 \nmid |G|$, the order of x cannot be even. Let $\mathrm{ord}(x) = 2k + 1$ and note that $k \geq 4$ as $x \in \Delta$. Then $(x^k)^y = x^{-2k} = x$ for $y \in \{y_1, y_2\}$. As such, $x^k = y_1 x y_1^{-1} = y_2 x y_2^{-1}$ has length at most two. Since $x^k \notin \{1, x^{\pm 1}, x^{\pm 2}\}$, we can apply Lemma 3.19 (with w being the geodesic of x^k) to conclude that all elements of the coset $x^k \langle x \rangle$ have length at most two. In particular $x^{-3} = z \in Z(G)$ has length at most two; a contradiction! □

As usual, we denote the *commutator (or derived) subgroup* of G by $G' = \langle [a, b]; a, b \in G \rangle$, and the *Frattini* subgroup of G by $\Phi(G)$, i.e., $\Phi(G)$ is the intersection of all maximal subgroups of G.

Using the above, we will now show that a nilpotent group G of class two that violates Conjecture A would have to be *special*, i.e., it would satisfy $G' = \Phi(G) = Z(G)$. In some sense, such groups are as non-abelian as possible given the constraint $G' \leq Z(G)$ imposed by G being nilpotent of class two.

Proposition 5.13. *Suppose that G is a nilpotent group of class two and a counterexample to Conjecture A. Then $\exp(G) = 9$ and $G' = \Phi(G) = Z(G) \ncong C_3$, i.e., G is a special but not extra-special 3-group.*

Proof. Suppose that $\mathrm{Cay}(G, \Sigma)$ violates Conjecture A and, as above, let $\Delta \coloneqq \{x \in \Sigma \mid x^3 \in Z(G) \setminus \{1\}\} \subseteq \Sigma$ be the set of central roots. The subgroup $H \coloneqq \langle \Delta \rangle$ clearly satisfies $H' \leq G' \leq Z(G) \leq H \leq G$. Furthermore, $H/Z(G)$ is an elementary abelian 3-group. We treat the cases $\Sigma \setminus \Delta = \emptyset$ and $\Sigma \setminus \Delta \neq \emptyset$ separately.

We first deal with the case $\Sigma \setminus \Delta = \emptyset$, i.e., $\Sigma = \Delta$ and $H = G$. As such, $G/Z(G)$ is an elementary abelian 3-group and thus so is G' (which is the image of $G/Z(G) \times G/Z(G)$ under the bilinear map induced by the commutator map). To show that $G' = Z(G)$, fix $x \in \Sigma$ and consider the homomorphism

$$\psi : G \to Z(G); \quad g \mapsto [x, g].$$

By Lemma 5.12, ψ is injective on $\Sigma \setminus \{x^{\pm 1}\}$. But then $Z(G) \setminus \psi(G)$ contains at most two elements. From $\psi(G) \neq 1$, we conclude that $\psi(G) = Z(G)$ by Lagrange's Theorem. Hence, $G' = Z(G)$. From this we conclude that $\exp(G) = 9$ and that the Frattini subgroup $\Phi(G)$ coincides with $G' = Z(G)$ (in p-groups, the Frattini subgroup is the smallest subgroup with elementary abelian quotient; hence, $G' \leq \Phi(G) \leq Z(G)$ since $G/Z(G)$ is elementary abelian). Finally, note that $|Z(G)| - 1 = |\Delta| = |\Sigma| \geq 4$ since G is not cyclic. Therefore, we can conclude that $Z(G) \ncong C_3$. This completes the proof for the case $\Sigma \setminus \Delta = \emptyset$.

We now assume that there exists an element $u \in \Sigma \setminus \Delta$ and consider the homomorphism

$$\phi : G \to Z(G); \quad g \mapsto [u, g].$$

By Lemma 5.11, $\phi(\Delta) \subseteq Z(G) \setminus \{1\}$ and, by Lemma 5.12, ϕ is injective on Δ. Since $|\Delta| = |Z(G) \setminus \{1\}|$, we then have $\phi(\Delta) = Z(G) \setminus \{1\}$ and, therefore, $\phi(H) = \mathrm{Im}(\phi) = Z(G)$. We claim that $\phi(\Sigma \setminus \Delta) = \{1\}$. Indeed, if $y_2 \in \Sigma \setminus \Delta$ would satisfy $\phi(y_2) \neq 1$, then $\phi(y_2) = \phi(y_1)$ for some $y_1 \in \Delta$. Hence, $y_1 = y_2$ by Lemma 5.12.

The homomorphism ϕ factors through the quotient $G \to G/Z(G)$ and the inclusion $G' \to Z(G)$. As such, $G' = Z(G)$ is isomorphic to a quotient of $H/Z(G)$; hence, $Z(G)$ is an elementary abelian 3-group. It follows that $\Delta \subseteq \Sigma_2$, i.e., $\mathrm{ord}(x) = 9$ for all $x \in \Delta$. On the other hand, we have $u^3 \in Z(G)$ since $[u^3, x] = [u, x]^3 = \phi(x)^3 = 1$ for each $x \in \Sigma$. This implies $u^3 = 1$ since $u \in \Sigma \setminus \Delta$. Moreover, the same holds for all $u \in \Sigma \setminus \Delta$. Since all elements of Σ have order three in the quotient $G/Z(G)$, the latter is an elementary abelian 3-group. As in the previous case, we conclude that $\exp(G) = 9$ and $G' = \Phi(G) = Z(G)$.

It remains to show that $Z(G) \ncong C_3$. By way of contradiction, let us assume that $Z(G) \cong C_3$. Then Δ consists of precisely two elements, i.e., $\Delta = \{x^{\pm 1}\}$, and $\phi(\Delta) = Z(G) \setminus \{1\} = \{x^{\pm 3}\}$. Upon replacing u by u^{-1} if necessary, we may then assume that $[x, u] = x^{-3}$. It follows that $uxu = u^2x^{-2} = u^{-1}x^{-2}$ and this element has length at most two by uniqueness of geodesics. Hence, $(uxu)u = uxu^{-1}$ also has length at most two and so does $x^3 = x^{-1}(uxu^{-1})$. But this contradicts Theorem 3.22 since $x^3 \in Z(G) \setminus \{1\}$. As such, $Z(G) \ncong C_3$. □

To further explore the applicability of Theorem 5.9 and Proposition 5.13, we have examined all non-abelian groups of order p^k with $p \in \{3, 5, 7, 11\}$ and $k \leq 7$ in GAP [18] using its SmallGrp library [2]. The results of this examination are summarized in Table 1. Note that such groups have nilpotency class $s \leq 6$. Moreover, by Theorem 5.9, every p-group of nilpotency class s with $p \geq 3 \cdot 2^{s-1} - 2$ satisfies Conjecture A; this threshold is indicated by horizontal lines in the table.

5.4. Groups with large commutativity degree

Many of our results address Conjecture A in the case of groups that are, in some sense, close to being abelian. This property can be quantified by a group G's *commutativity degree* $\mathbf{P}(G)$, which is the probability that two randomly chosen elements of G commute, i.e.,

$$\mathbf{P}(G) \coloneqq \frac{|\{(g, h) \in G \times G \mid gh = hg\}|}{|G \times G|}.$$

The interested reader is referred to the survey by Das, Nath, and Pournaki [9] for further details and historical context. We will content ourselves here with the following observation.

Table 1. The number of groups of order p^k with $k \leq 7$ and nilpotency class s covered by Theorem 5.9 and Proposition 5.13 / total number of such groups (if distinct).

p	$s \leq 1$	$s = 2$	$s = 3$	$s = 4$	$s = 5$	$s = 6$
3	45	587 / 1,926	150 / 6,362	36 / 1,386	0 / 180	0 / 6
5	45	7,256	247 / 23,073	119 / 3,382	5 / 1,227	0 / 9
7	45	26,914	255 / 76,783	131 / 8,034	60 / 2,140	15 / 198
11	45	204,912	514,627	139 / 26,882	62 / 5,170	19 / 402

Table 2. The possible structures of a non-abelian group G with $\mathbf{P}(G) > \frac{11}{32}$.

Group Structure			Applicable result
G'	$G' \cap Z(G)$	$G/Z(G)$	
C_2	C_2	C_2^{2r} $(r \geq 1)$	Theorem 3.12
C_3	1	S_3	Theorem 5.4
C_2^2 or C_4	C_2	D_8	Theorem 3.12
C_2^2	C_2^2	C_2^3 or C_2^4	Theorem 3.12
C_3	C_3	C_3^2	Proposition 5.13
C_5	1	D_{10}	Theorem 5.4
C_6	C_2	$S_3 \times C_2$ or $C_3 \rtimes C_4$	Theorem 3.12

Theorem 5.14. *Conjecture A holds for every group G with $\mathbf{P}(G) > \frac{11}{32}$.*

Proof. For abelian groups, this follows from Corollary 3.9 (see also [15]). If G is non-abelian and $\mathbf{P}(G) > \frac{11}{32}$, then according to Rusin [31, p. 246] the structure of G must be as indicated in Table 2.

In most of these cases, $Z(G)$ contains a subgroup isomorphic to C_2; hence, Theorem 3.12 applies. If $G/Z(G) \cong S_3$ or $G/Z(G) \cong D_{10}$, then G contains an abelian subgroup of index two corresponding to $C_3 \leq S_3$ or $C_5 \leq D_{10}$ in $G/Z(G)$, respectively. As such, we can apply Theorem 5.4. In the remaining case, i.e., if $C_3 \cong G' \leq Z(G)$, then G is covered by Corollary 5.13. □

6. Experiments

We now turn to the exhaustive computer search to check which groups of order up to 1024, as well as all even orders up to 2014 and all non-abelian finite simple groups up to order 5000, have a generating set that yields a geodetic Cayley graph. The aim of this experiment was to either verify Conjecture A for as many group orders as possible, or to find a group and a generating set that yields a nontrivial geodetic Cayley graph, i.e., a graph that is neither complete nor an odd cycle. For our code, see

https://osf.io/9ay6s/?view_only=37e18301e4e74e12bfe4e07b90b924c0.

Improving the computer search has been a major motivation for the theoretical work in the previous sections. Important results in this regard are the bounds on the generating set discussed in Section 4 as well as the results covering entire classes of groups, the most important of which is Theorem 3.12 excluding all groups with even-order center.

In turn, the results from the computer search also influenced our theoretical work. For example, at one point in the development of our computer search algorithms, groups which were semidirect products with C_2 had a long running time. This directed our theoretical work to focus on such groups, leading to Theorem 5.4 showing that Conjecture A holds for all groups with an abelian subgroup of index two.

6.1. Overview

Our approach consists of three stages. The first is the *filtering stage* in which we identify the relevant groups which are not covered by our theoretical results, and thus need to be considered in our computer search. We realized this stage using GAP [18].

The second stage is a *preprocessing stage*, also realized in GAP, during which we compute the information required for the search and store it in a JSON file. Besides the multiplication table describing the group, the most important information computed in this stage comprises a set of *forbidden elements* and a set of *required subsets*.

Forbidden elements are elements which cannot be part of any geodetic generating set except for the complete one. A required subset is a set of elements of which each geodetic generating set needs to contain at least one. We will give more details on how we compute and use these below.

The third and final stage is the actual search, which we have implemented in Rust. Obviously, enumerating all generating sets is infeasible even for relatively small groups. For example, already for the symmetric group S_5, which has 120 elements, there are 2^{72} potential generating sets (symmetric subsets not containing the identity element). To circumvent this problem, we discard generating sets based on the theoretical results described in the previous sections. We implement this using a binary counter for enumerating generating sets, which allows us to systematically skip the respective ranges. For each of the remaining generating sets, we test whether or not the resulting Cayley graph is geodetic and report those that are.

6.2. Filtering

We used GAP [18] and its SmallGrp library [2] to obtain a list of all finite groups up to order 1024 relevant to our search. (In a second run we repeated the experiment also filtering out all odd-order groups, which we report on below.) When generating this list of groups, we ignored the following.

Table 3. Number of groups of order up to 1024 and excluding 2-groups which are caught by the different filtering steps.

Total number of groups	1,206,579
Abelian groups	2034
Groups with center of even order	1,200,151
Groups with Abelian subgroup of Index 2	989
Nilpotent groups as in Proposition 5.13	170
Nilpotent groups as in Theorem 5.9	18
Groups with Abelian Subgroup of Index 3 as in Theorem 5.8	86
Groups with large center as in Corollary 4.8 and Proposition 4.10	274
Remaining groups	3197

The filtering is performed in the same order as in the table, and each group is only counted toward the first category it matches.

- All abelian groups (Corollary 3.9).
- All groups with even-order center (Theorem 3.12).
- All groups with a large center (Corollary 4.8 and Proposition 4.10).
- All groups with abelian index-2 subgroups (Theorem 5.4).
- The groups with abelian index-3 subgroups covered by Theorem 5.8.
- The nilpotent groups covered by Theorem 5.9 and Proposition 5.13.

Note that, while there are approximately $50 \cdot 10^9$ groups up to order 1024, most of those are 2-groups, which all have an even-order center. Excluding the 2-groups there are only 1206579 groups of order at most 1024, and after excluding the groups in the above list only 3197 groups remain. We provide more details on the number of groups falling into each of the above categories in Table 3.

Remark 6.1. *The smallest group with a center larger than the bound from Corollary 4.8 is* $C_{13} \times A_4$. *Its center has order* 13 *– just above the bound, which in this case is* 12.

To find an example for Proposition 4.10, we have to look a bit further. The proposition excludes 3 as a prime divisor of the order of the group, and, 5 and 7 are excluded as prime divisors of the index of the center. The smallest group covered by Proposition 4.10 that is not already covered by Corollary 4.8 is $C_7 \times (C_{13} \rtimes C_4)$. *Its center has order 7, just larger than the bound of* 6.

During filtering we only verify those bounds on the size of the center based on Corollary 4.8 and Proposition 4.10 (with $m_0 = 3$). More precise bounds on the size of non-complete geodetic generating sets, and thus also on the size of the center, are computed within the initialization step of our search algorithm. Therein, we utilize most results of Section 4 (with optimal parameters). Due to tighter bounds, we were able to exclude an additional 240 groups from the search.

Remark 6.2. *For filtering the groups of even order up to 2014, we use the same method. However, there is one special case: the groups of order* $1536 = 3 \cdot 2^9$. *There are more than* $4 \cdot 10^8$ *of them—too many for running through the entire filtering stage. However, most of them have a normal Sylow* 3*-subgroup. Because such groups have an even-order center, they can be safely ignored by Theorem 3.12. Therefore, we only run the filtering procedure for the remaining groups, indexed* 408526598–408641062 *in the SmallGrp library.*

6.3. Preprocessing

The main objective of the preprocessing stage is to compute the forbidden elements and the required subsets of each group. As mentioned above, an element is forbidden if, whenever it is part of a geodetic generating set, the associated Cayley graph is necessarily complete. Note that, since we filter out abelian groups in the filtering stage, here we do not need to consider the possibility that the Cayley graph is an odd cycle. The set of forbidden elements comprises all elements $g \in G$ such that $h = g$ or $h = g^2$ is nontrivial and satisfies $h^G \subseteq \{h^{\pm 1}\}$; see Lemmas 3.7 and 3.18. In particular, this includes central elements (Corollary 3.8) and their square roots (Theorem 3.22).

A required subset is a set of which each geodetic generating set needs to contain at least one element. In the preprocessing we compute the following sets, which we know to be required.

- Each conjugacy class of elements of order two (Lemma 3.11).
- Each normal subgroup of index two (Lemma 5.1).
- Each complement of a maximal subgroup (as we want a generating set).

There is one other family of required subsets: the potential roots of each central element. However, since these sets are smaller, and thus their inclusion is more effective, when we know the length of central geodesics, we do not add these sets in the preprocessing stage, but later in the search algorithm.

At this stage we also take advantage of automorphisms to reduce the size of the required subsets and thus reduce the number of generating sets we need to look at. The procedure is to go through the required subsets one by one. For each, we compute the orbits of its elements under the automorphism group and select one element from each orbit. As we are interested only in symmetric generating sets, we consider the orbits of an element and its inverse as a single orbit. Continuing with the next required subset, we no longer use the full automorphism group, but only the point-wise stabilizer of the elements that were selected in the previous required subsets. This is justified by the following straight-forward observation:

Lemma 6.3. *Let $R \subseteq G$ and $Y \subseteq G$ and let $\tilde{R} \subseteq R$ be a system of representatives of $R/\operatorname{Stab}(Y)$.*[2] *Then for all $X \subseteq G$ with $R \cap X \neq \emptyset$, there exists some $\phi \in \operatorname{Stab}(Y)$ such that $\phi(X) \cap \tilde{R} \neq \emptyset$.*

In cases where the required subset contains only part of an orbit under the action of the automorphism group, we take care to select representatives that are part of the original set. This way, for each generating set that contains an element of each of the original required subsets, there is a generating set which contains at least one element of each of the smaller required subsets obtained after applying the automorphism group.

Finally, we discard required subsets that are supersets of smaller ones.

Remark 6.4. *For the finite simple groups $\mathrm{PSL}(2, q)$ with $q \in \{17, 19, 16\}$, for parallelization, we split the computation of the search algorithm into several chunks. This is implemented by generating several instances during the preprocessing stage with different required and forbidden subsets.*

6.4. The search algorithm

For a group G, we fix a subset $C \subseteq G \setminus \{1\}$ such that $\left|\{g, g^{-1}\} \cap C\right| = 1$ for each $g \in G \setminus \{1\}$. We call the elements of C *candidates*. In this way, each inverse-closed subset $\Sigma \subseteq G \setminus \{1\}$ (i.e., each potential generating set) bijectively corresponds to a *candidate set* $X = \Sigma \cap C \subseteq C$. Note that if more than half of the elements of G are of order two, then, according to Liebeck and MacHale [23], G has an abelian subgroup of index two or $Z(G)$ has even order. Since such groups were excluded during the filtering stage, we may assume at most half the elements of G have order two; hence, $|C| \leq \frac{1}{2}|G| + \frac{1}{4}|G| = \frac{3}{4}|G|$.

In the following, we identify C with the set of numbers $\{0, \ldots, |C| - 1\}$; in particular, we fix an order on C. We enumerate the potential generating sets of a group by enumerating all subsets of C in the order of a binary counter from 0 to $2^{|C|}$, where a binary number naturally corresponds to a subset of C. The main loop of our search algorithm is presented in Algorithm 1. Incrementing the binary counter is done in lines 6 to 14. In line 18 we check whether the resulting Cayley graph is geodetic and connected (TestGeodetic, for details see below). We use a stack to keep track of the current candidate set X, the corresponding increment I, and some additional information that is not displayed in Algorithm 1. During the execution of the algorithm, we maintain the following invariants of the stack (which we consider to grow upwards).

(I_1) If (X, I) is above (X', I'), then $X \supseteq X'$ and $I < I'$. Moreover, $X \cap [I', |C|] = X' \cap [I', |C|]$.
(I_2) If (X, I) is directly above (X', I'), then additionally $X \cap [I, |C|] = (X' \cap [I, |C|]) \cup \{I\}$.

We use several pruning methods to shortcut the counting process. The variable I_{next} in Algorithm 1 serves as the index of the bit to be increased next (meaning that $I_{\text{next}} = 0$ yields a usual increment by one); by increasing I_{next}, we can skip over certain values for the counter.

The pruning methods, described in detail below, rely upon

- bounds on the size of the generating set,
- the forbidden candidate array (for simplicity not included in the pseudocode Algorithm 1),
- the required subsets described above in Section 6.3 (handled in line 5 in Algorithm 1),
- saturating the generating set (FillIn),
- handling of collisions at distance 3 discovered during the check whether the Cayley graph is geodetic (HandleCollisions).

Finally, for groups of even order and groups with non-trivial center, we employ further pruning techniques during TestGeodetic and HandleCollisions.

Bounds on the number of generators

In Section 4 we developed several bounds on the size of non-complete geodetic generating sets. As Proposition 3.14 and Lemma 3.16 already cover the diameter-two case of our search, the most general such bound is due to Theorem 4.4: it gives us an upper bound of $c \cdot \sqrt{n}$ where n is the order of the group. The constant factor c is at most $2/\sqrt{5}$ but, depending on the size of the group, the factor can be even smaller. In fact, we compute the optimal bound given by Theorem 4.4 in our program. If the group has non-trivial center, we use Theorem 4.7 to obtain an even smaller bound in the order of $\sqrt[3]{n}$. We use these bounds to prune the search tree as follows:

[2] Here, by abuse of notation, we write $R/\operatorname{Stab}(Y)$ to denote the set $R/\!\sim$ where $x \sim y$ if $\phi(x) = y$ for some $\phi \in \operatorname{Stab}(Y)$.

```
procedure CheckGroup(G)
 1: (X, I) ← (∅, ∞)
 2: Stack.Push(X, I)
 3: I_next ← 0
 4: while Stack ≠ ∅ do
 5:     I_next ← max{I_next, Required(X)}
 6:     while I_next ∈ X do
 7:         I_next ← I_next + 1
 8:     if I_next ≥ |C| then
 9:         return
10:     while I_next ≥ I do
11:         (X, I) ← Stack.pop()
12:     I_last ← I
13:     (X, I) ← (X ∪ {I_next}, I_next)
14:     Stack.Push(X, I)
15:     I_next ← CheckGenSet(X, I, I_last)
```

```
procedure CheckGenSet(X, I, I_last)
16: if FillIn(X, I, I_last) fails then
17:     return I
18: T ← TestGeodetic(X)
19: if T = Geodetic then
20:     output X
21:     return 0
22: if HandleCollisions(T, X, I, I_last) fails then
23:     return I
24: else
25:     return 0
```

Algorithm 1: Outline of our search algorithm.

whenever there are too many bits set to one in the counter (i.e., $|X|$ is too big – detected either in FillIn or HandleCollisions), we increment the least-significant bit currently set to one by setting $I_{\text{next}} \leftarrow I$ (see lines 17 and 23 of Algorithm 1).

In some cases, the bound computed at this stage is impossible to satisfy and, therefore, the group possesses no geodetic generating set other than the complete one. In this way, we exclude an additional 240 (of the remaining 3197) groups from the search.

Forbidden candidates

As a first improvement, we use a bit array indicating candidates that are forbidden given the other candidates already contained in X. For each entry on the stack (stack frame) we keep a separate forbidden candidate array. Initially, the forbidden candidate array of the first stack frame comprises the forbidden candidates computed during preprocessing (Section 6.3). When creating a new stack frame, the forbidden candidates of its predecessor are copied; afterwards, additional candidates might be marked as forbidden on the new stack frame. An additional candidate can be marked as forbidden if its inclusion in X would

- lead to a generating set that is too large,
- require the inclusion of a candidate that is already forbidden, or
- violate the order in which we search through the generating sets.

These conditions are tested for during the FillIn and HandleCollisions procedures. For details we refer to the respective paragraphs below.

We use the forbidden candidate array in the FillIn and HandleCollisions procedures as well as in the counter logic. While omitted from the description in Algorithm 1 for simplicity, its incorporation is rather straightforward: whenever I_{next} is a forbidden candidate, it is incremented.

Required subsets

We incorporate the required subsets computed during the preprocessing step as detailed in Section 6.3. Whenever there is a required subset R with $R \cap X = \emptyset$, we increase I_{next} to the smallest candidate contained in R (see line 5 of Algorithm 1). This dispenses with all candidate sets in between which do not contain an element of the required subset and, thus, need not be considered.

If multiple required subsets are disjoint from X, we apply the following heuristic: choose a required subset to be satisfied first such that the smallest candidate contained in it is maximal with respect to the order on C.

It may happen that the smallest candidate of a required subset is forbidden. In this case we simply consider the smallest candidate I in the required subset that is not forbidden. If I is larger than I_{last}, the candidate of the previous stack frame, then we cannot satisfy the required subset by pushing a new stack frame without violating the order in which we search through the generating sets (Invariant (I_1)). Therefore, we assign $I_{\text{next}} \leftarrow I_{\text{last}}$ in order to skip a number of candidate sets to which we cannot add any candidate from the required subset.

Finally, we remark that further required subsets are created during the HandleCollisions procedure and at the beginning of the search for groups with nontrivial center.

Saturating the generating set (FillIn)

The most crucial improvement of our algorithm over a naïve search is based on Lemma 2.3. If $a, b, c, d \in \Sigma$ with $ab = cd \neq 1$ for a geodetic generating set $\Sigma \subseteq G$, then $(ab), (c^{-1}a) \in \Sigma$. Therefore, whenever we add a new candidate to X, we test whether a product of the newly added element(s) and some other element of the generating set Σ associated with X equals a different product of two elements of Σ. If so, we also add this product to Σ by adding the corresponding candidate to X. By repeating this we obtain a

candidate set X'. If the corresponding generating set Σ' is too large, or if X' contains a forbidden candidate, then the FillIn procedure fails and marks the current increment I as forbidden on the previous stack frame.

In order to avoid considering the same generating set multiple times, we only want to add a candidate J to X during the FillIn procedure if $J < I$; otherwise, the resulting candidate set would be considered again after incrementing the counter.

As such, if X' contains a candidate J with $I < J$, then the FillIn procedure fails and, thus, in line 17 of Algorithm 1 we set $I_{\text{next}} \leftarrow I$ skipping a number of candidate sets that would violate the search order. Moreover, if X' contains a candidate J with $I_{\text{last}} < J$, then we also mark I as forbidden on the previous stack frame, which corresponds to I_{last}. This is because introducing I as a candidate in any stack frame above the previous one would violate the second part of Invariant (I_1).

Testing whether the Cayley graph is geodetic (TestGeodetic)

As the Cayley graph is vertex-transitive, it suffices to check whether geodesics from the origin $1 \in G$ to each other vertex exist and are unique. We implemented this using a breadth-first search. If during this breadth-first search we encounter an element with two different geodesics of length three, then we record this element for later handling. We collect a certain number of such elements depending on the order of the group and other parameters such as, e.g., the order of the center and the number of elements of order two. In the case of groups with non-trivial center we implemented some further checks as detailed below.

Handling collisions at distance three (HandleCollisions)

While testing whether the Cayley graph is geodetic, we compute a list of elements which have multiple geodesics of length three. We aim to extend the generating set to a geodetic generating set. To achieve this, we need to add new generators (by adding the respective candidates) such that each element in the list either becomes a generator or can be uniquely written as a product of two generators.

Since there are many options as for which generators to add, for each of the recorded collisions, we create a temporary required subset. It remains valid until the current candidate is removed from the candidate set, i.e., the lifetime of these new required subsets is tied to the current stack frame.

The temporary required subset associated with a collision is constructed as follows. Suppose that adding a single candidate J to X would resolve the collision. Then we insert J into the required subset, unless invoking FillIn with $X' = X \cup \{J\}$ fails. For pairs of candidates whose addition would resolve the collision, we proceed similarly, but only add the larger of the two candidates to the required subset.

Finally, if all calls to FillIn fail, and thus the required subset is empty, then the call to HandleCollisions fails as we cannot resolve the collision. Crucially, if all calls to FillIn forbid the corresponding inclusion, then we also forbid I on the stack frame corresponding to I_{last}.

Modifications for groups of even order

If during TestGeodetic we find an element of order two among the collisions at distance three, then the only choice is to add the element itself to the generating set. Recall that, by Lemma 3.11, such an element cannot have a geodesic of length two. As such, we do not construct a required subset in this case (by calling HandleCollisions), but add the respective candidates directly to the candidate set instead (or possibly forbid the current increment I) and continue afterwards with FillIn.

Based on the same observation, as a further improvement for groups of even order (more precisely, for groups whose order is divisible by six) we have implemented the following. During FillIn, we check whether a generator is of order six, and thus generates a subgroup isomorphic to C_6, or whether two generators together generate a subgroup isomorphic to S_3. If so, we add all non-trivial elements of the corresponding subgroup to the generating set Σ since such a subgroup is complete with respect to any geodetic generating set as the following lemma shows.

Lemma 6.5. *Let* $\mathrm{Cay}(G, \Sigma)$ *be geodetic and* $H \leq G$ *with* $\langle H \cap \Sigma \rangle = H$. *If* $|H| = 6$, *then* H *is complete.*

Proof. Suppose that $H \cong C_6$. If we have a generator $g \in H \cap \Sigma$ of order six, then $g^3 = \overline{g}^3$ has length one by Lemma 3.11, i.e., $g^3 \in \Sigma$. It follows that $H \cap \Sigma$ always contains some element h of order two and at least one other element k which commutes with h. Hence, the subgroup $H = \langle h, k \rangle$ is complete by Corollary 3.10.

Similarly, let $g, h \in \Sigma$ generate the subgroup H isomorphic to S_3 and assume (without loss of generality) that g is of order two. If h is of order three, then we have $gh = h^{-1}g$ and, hence, $gh \in \Sigma$ and similarly $hg \in \Sigma$ and $(hg)h = h(gh) \in \Sigma$ showing that $H = \{1, g, h, gh, hg, hgh\}$ is complete. If h is of order two, then $ghg = hgh$ is of order two; hence, by Lemma 3.11, $ghg \in \Sigma$. Thus, we have an entire conjugacy class $g^H = \{g, h, ghg\}$ contained in Σ. Therefore, the subgroup $H = \langle g, h \rangle$ is complete by Lemma 3.7. □

Modifications for groups with nontrivial center

For groups with nontrivial center, we compute all possible lengths of central geodesics given by Theorem 3.22. Then we run the search repeatedly, once for each length of central geodesics. We add the corresponding central roots as required subsets and add the central roots which are too short as forbidden elements. When testing whether the Cayley graph is geodetic, we additionally check whether there are central elements with geodesics shorter than the length of central geodesics. If that happens, then the only geodetic graphs the Cayley graph can be extended to by adding more generators are graphs with a smaller length of central geodesics.

6.5. Experimental results

Our experiments were conducted on a machine with an AMD Ryzen 9 5900X CPU (12 cores, 24 threads, 3.7 GHz) and 128 GB of RAM. Running the experiments for all groups up to order 1024 took 299 hours of total CPU time, and we were able to establish

Theorem B. *All groups of size up to 1024 satisfy Conjecture A.*

With parallelization, the running time was dominated by a few "difficult" groups. See Table 4 for the running time of select groups and Figure 3 for a plot of the running time of every group of order up to 1024 compared to the group's order.

As it can be seen from Table 4 and Figure 3, our search is substantially faster for groups of even order. Therefore, for groups of even order we extended our search up to order 2014. We did not go beyond that since larger groups are not completely listed in the GAP SmallGrp library [2]. Moreover, note that, as detailed in Remark 6.2, for groups of order 1536, we had to take some special care during the filtering stage.

Theorem 6.6. *Conjecture A holds for all groups of even order at most* 2014.

In the light of Corollary 3.10 and Theorem 5.9 it seems reasonable to search for counterexamples to Conjecture A within classes of groups that are far from commutative. Thus, it is natural to consider non-abelian finite simple groups. Nevertheless, in our experiments these groups turned out to be even easier to handle than many of the other groups of even order. (Note that by the famous Feit-Thompson theorem [16] all non-abelian simple groups have even order.) Indeed, for this special case we could go further than order 2014 and succeeded to show the following.

Theorem 6.7. *Conjecture A holds for* S_7 *and for the simple groups* PSL(2, 17), A_7, PSL(2, 19), *and* PSL(2, 16). *In particular, it holds for all simple groups of order at most* 5000.

To give an indication which groups are "easy" and which are "difficult", we give an overview on some selected groups in Table 4. The table contains the following classes of groups:

- alternating and symmetric groups,
- further simple groups of order exceeding 2014,
- the five groups of order up to 1024 with the longest running time,
- different groups of order $729 = 3^6$,
- groups with the longest running time among the even groups of order up to 1024,
- groups of even order between 1026 and 2014 with the longest running time.

Note that the order of the groups certainly plays a role in the running time, but there was also a huge variance in running time for different groups of roughly the same order. For instance this can be seen very prominently for groups of order 729 in Figure 3.

There are various reasons for this difference. For example we observe an impact of the size of the center, which is to be expected given the results in Section 4. Moreover, we see the clear effect of the groups having even order: for these we have additional possibilities to generate small required subsets and we can use the improved FillIn procedure. However, also among groups of odd order and

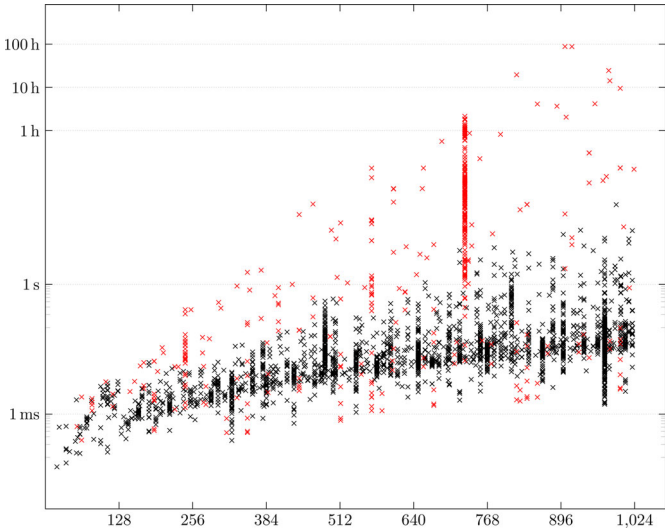

Figure 3. Running time of our computer search for all groups of order up to 1024; groups of even order are marked in black, those of odd order are marked in red.

Table 4. Experiments for selected groups including the five groups with the longest running time.

Group	Order	Index	Sets tested	Duration
A_5	60	5	31	0.3 ms
S_5	120	34	207	1.3 ms
A_6	360	118	6249	23 ms
S_6	720	763	27590	120 ms
A_7	2520	—	74,946,283	52 min
S_7	5040	—	1,059,510,737	197 min
$\mathrm{PSL}(2,17)^{\parallel}$	2448	—	123,451,769	23 min
$\mathrm{PSL}(2,16)^{\parallel}$	4080	—	4,869,673,337	13 h
$\mathrm{PSL}(2,19)^{\parallel}$	3420	—	2,696,472,513	21 h
$C_{109} \rtimes C_9$	981	3	5,683,264,056	14 h
$(C_7 \rtimes C_3) \times (C_{13} \rtimes C_3)$	819	6	8,728,959,134	19 h
$C_{89} \rtimes C_{11}$	979	1	10,178,934,027	24 h
$C_{61} \rtimes C_{15}$	915	1	43,174,839,011	87 h
$C_{43} \rtimes C_{21}$	903	1	43,967,855,355	88 h
C_9^2 extended by C_3^2	729	96	13,525	39 ms
$(C_3 \times (C_{27} \rtimes C_3)) \rtimes C_3^{\ddagger}$	729	90	11,276,468	208 s
$C_{27} \rtimes C_{27}^{\ddagger}$	729	22	10,776,997	255 s
$(C_9 \rtimes C_9) \rtimes C_9$	729	75	97,944,803	52 min
$(C_{27} \rtimes C_9) \rtimes C_3$	729	390	175,898,535	87 min
$((C_9 \times C_3) \rtimes C_3) \rtimes C_3^2$	729	399	240,194,985	128 min
$C_{31} \rtimes C_{30}$	930	1	821,601	18 s
$C_{17} \times A_5$	1020	9	1,030,890	18 s
$C_2^5 \rtimes C_{31}$	992	194	3,260,710	70 s
$C_{11} \times \mathrm{PSL}(3,2)$	1848	127	1,024,861,064	8 h
$C_{37} \rtimes C_{54}$	1998	7	1,292,527,452	13 h
$C_2^4 \rtimes (C_5 \times (C_7 \rtimes C_3))$	1680	939	1,709,925,665	14 h

The first column shows the group according to the GAP structure description, the second column displays the order of the group, the third column the index in the SmallGrp library, the fourth column the number of calls to the TestGeodetic procedure, and the final column contains the running time. The computation was parallelized for the groups $\mathrm{PSL}(2,q)$ (marked with $^{\parallel}$) according to Remark 6.4; the quantities displayed in the last two columns are cumulative. The center of the groups of order 729 is either of order three or nine (marked with ‡).

with trivial center there is a huge variation in running time. We observe that the most difficult instances are groups $C_p \rtimes C_n$ with a faithful action, p prime, and n as large as possible.

Additional statistics on our experiments may be found at

https://osf.io/9ay6s/?view_only=37e18301e4e74e12bfe4e07b90b924c0.

7. Discussion

We have shown that for several infinite classes of finite groups there are no geodetic Cayley graphs except the complete graphs. This includes all abelian groups (except cyclic groups of odd order), dihedral groups, and groups with even-order center, as well as many nilpotent groups. Moreover, we have verified by a computer search that Conjecture A holds for all groups up to order 1024, all groups of even order up to 2014, all simple groups of order up to 5000, and the symmetric group S_7.

The main open problem, of course, remains whether Conjecture A holds for all finite groups, i.e., that every geodetic Cayley graph of a finite group is either complete or a cycle of odd length. Our experiments suggest that it might be reasonable to aim for proving Conjecture A for all groups of even order.

Acknowledgments

The authors sincerely thank Alexey Talambutsa for pointing out previous work, Filippo Prandina for highlighting a mistake in a previous version, and the anonymous reviewers for their careful reading and helpful corrections, comments, and improvements to the writing of this article.

Disclosure statement

The authors report there are no competing interests to declare.

Funding

In completing this work, the first two authors were supported by Australian Research Council grant DP210100271 and the fifth author was partially supported by DFG grant WE 6835/1–2.

References

[1] Bannai, E., Ito, T. (1973). On finite Moore graphs. *J. Faculty Sci. Univ. Tokyo. Sect. 1 A, Math.* 20: 191–208. https://api.semanticscholar.org/CorpusID:118193462.
[2] Besche, H. U., Eick, B., O'Brien, E., Horn, M. (2023). SmallGrp, the GAP small groups library, Version 1.5.3. https://gap-packages.github.io/smallgrp/. Refereed GAP package.
[3] Blokhuis, A., and Brouwer, A.E. (1988). Geodetic graphs of diameter two. *Geom. Dedicata*, 25:527–533.
[4] Bosák, J., Kotzig, A., Znám, Š (1968). Strongly geodetic graphs. *J. Combin. Theory* 5: 170–176.
[5] Cameron, P. J. (1999). *Permutation Groups*. London Mathematical Society Student Texts. Cambridge: Cambridge University Press. DOI: 10.1017/CBO9780511623677.
[6] Che, A. (2022). Uniqueness of geodesics in Cayley graphs of finite groups. Technical Report.
[7] Clement, A. E., Majewicz, S., Zyman, M. (2017). *The Theory of Nilpotent Groups*. Cham: Birkhäuser/Springer.
[8] Damerell, R. M. (1973). On Moore graphs. *Math. Proc. Cambridge Philos. Soc.*, 74(2): 227–236. DOI: 10.1017/S0305004100048015.
[9] Das, A. K., Nath, R. K., Pournaki, M. R. (2013). A survey on the estimation of commutativity in finite groups. *Southeast Asian Bull. Math.* 37(2): 161–180.
[10] Deutsch, J., and Fisher, P.H. (2001). On strongly regular graphs with $\mu = 1$. European J. Combin., 22(3):303–306, Doi: 10.1006/eujc.2000.0472
[11] Eisenberg, A., Piggott, A. (2019). Gilman's conjecture. *J. Algebra* 517:167–185. DOI: 10.1016/j.jalgebra.2018.09.022.
[12] Elder, M., Piggott, A. (2022). Rewriting systems, plain groups, and geodetic graphs. *Theoret. Comput. Sci.* 903: 134–144.
[13] Elder, M., Piggott, A., Townsend, K. (2023). On k-geodetic graphs and groups. *Int. J. Algebra Comput.* 33: 1169–1182. DOI: 10.1142/S0218196723500534.
[14] Etgar, A., Linial, N. (2024). On the connectivity and diameter of geodetic graphs. *Eur. J. Combin.* 116: Paper No. 103886. DOI: 10.1016/j.ejc.2023.103886.
[15] Federici, B. (2017). Interactions between large-scale invariants in infinite graphs. Ph.D. thesis, University of Warwick. https://wrap.warwick.ac.uk/108882/.
[16] Feit, W., Thompson, J. G. (1963). Solvability of groups of odd order. *Pac. J. Math.* 13: 775–1029. http://projecteuclid.org/euclid.pjm/1103053943.
[17] Frasser, C., Vostrov, G. (2020). Geodetic graphs homeomorphic to a given geodetic graph. *Int. J. Graph Theory Appl.* 3: 13–44.
[18] The GAP Group. (2022). GAP – Groups, Algorithms, and Programming, Version 4.12.2. https://www.gap-system.org.
[19] Gorovoy , D., Zmiaikou, D. (2024). On graphs with unique geoodesics and antipodes. *Discrete Math.* 347(4): Paper No. 113864, 17. DOI: 10.1016/j.disc.2023.113864.
[20] Hoffman, A. J., Singleton, R. R. (1960). On Moore Graphs with Diameters 2 and 3. *IBM J. Res. Dev.* 4(5): 497–504. DOI: 10.1147/rd.45.0497.
[21] Hughes, S., Nairne, P. S., Spriano, D. (2024). Regularity of quasigeodesics characterises hyperbolicity. https://arxiv.org/abs/2205.08573, arXiv:2205.08573.
[22] Kantor, W.M., (1977). Moore geometries and rank 3 groups having $\mu = 1$. Quart. J. Math. Oxford Ser. (2), 28(111):309–328. Doi:10.1093/qmath/28.3.309.
[23] Liebeck, H., MacHale, D. (1972). Groups with automorphisms inverting most elements. *Math. Z.* 124(1): 51–63. DOI: 10.1007/BF01142582.
[24] Miller, M., Širáň, J. (2005). Moore graphs and beyond: a survey of the degree/diameter problem. *Electron. J. Combin.* DS14: 61.
[25] Ore, O. (1962). Theory of graphs. In: *Colloquium Publications*. Providence, RI: American Mathematical Society.
[26] Pak, I., Radoičić, R. (2009). Hamiltonian paths in Cayley graphs. *Discrete Math.* 309(17): 5501–5508. DOI: 10.1016/j.disc.2009.02.018.
[27] Piggott, A. (2015). On groups presented by monadic rewriting systems with generators of finite order. *Bull. Aust. Math. Soc.* 91(3): 426–434. DOI: 10.1017/S0004972715000015.
[28] Pólya, G., Szegö, G. (1925). *Aufgaben und Lehrsätze aus der Analysis: Erster Band: Reihen · Integralrechnung Funktionentheorie*. Grundlehren der mathematischen Wissenschaften. Berlin; Heidelberg: Springer. DOI: 10.1007/978-3-662-38381-0.
[29] Potočnik, P., Spiga, P., Verret, G. (2013). Cubic vertex-transitive graphs on up to 1280 vertices. *J. Symbolic Comput.* 50: 465–477. DOI: 10.1016/j.jsc.2012.09.002.
[30] Robinson, D. J. S. (1996). *A Course in the Theory of Groups*, volume 80 of Graduate Texts in Mathematics, 2nd ed. New York: Springer-Verlag. DOI: 10.1007/978-1-4419-8594-1.
[31] Rusin, D. J. (1979). What is the probability that two elements of a finite group commute? *Pac. J. Math.* 82(1): 237–247.
[32] Shapiro, M. (1997). Pascal's triangles in Abelian and hyperbolic groups. *J. Aust. Math. Soc.* 63(2): 281–288.
[33] Stemple, J. G. (1974). Geodetic graphs of diameter two. *J. Combin. Theory Ser. B* 17(3): 266–280.
[34] Stemple, J. G., Watkins, M. E. (1968). On planar geodetic graphs. *J. Combin. Theory* 4(2): 101–117.
[35] Stober, F., Weiß, A. (2023). Geodetic graphs: experiments and new constructions. *arXiv preprint*. arXiv:2308.08970.
[36] Watkins, M. E. (1970). Connectivity of transitive graphs. *J. Combin. Theory* 8(1): 23–29. DOI: 10.1016/S0021-9800(70)80005-9.