



HAL
open science

Cayley graphs with few automorphisms

Paul-Henry Leemann, Mikael de La Salle

► **To cite this version:**

Paul-Henry Leemann, Mikael de La Salle. Cayley graphs with few automorphisms. *Journal of Algebraic Combinatorics*, 2020, 10.1007/s10801-020-00956-1 . hal-01950331

HAL Id: hal-01950331

<https://hal.science/hal-01950331>

Submitted on 10 Dec 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Cayley graphs with few automorphisms

Paul-Henry Leemann, Mikael de la Salle

December 7, 2018

Abstract

We show that every finitely generated group G with an element of order at least $(5 \operatorname{rank}(G))^{12}$ admits a locally finite directed Cayley graph with automorphism group equal to G . If moreover G is not generalized dihedral, then the above Cayley directed graph does not have bigons. On the other hand, if G is neither generalized dicyclic nor abelian and has an element of order at least $1.41 \cdot 10^{19} \operatorname{rank}(G)^{132}$, then it admits an undirected Cayley graph with automorphism group equal to G . This extends classical results for finite groups and free products of groups. The above results are obtained as corollaries of a stronger form of rigidity which says that the rigidity of the graph can be observed in a ball of radius 2 around a vertex. This strong rigidity result also implies that the Cayley (di)graph covers very few (di)graphs. In particular, we obtain Cayley graphs of Tarski monsters which essentially do not cover other quasi-transitive graphs.

We also show that a group admits a labeled unoriented Cayley graph with automorphism group equal to itself if and only if it is neither generalized dicyclic nor abelian with an element of order greater than 2.

1 Introduction

A powerful geometric tool for the study of a finitely generated group G endowed with a finite generating set S is the (right) *Cayley graph* $\operatorname{Cay}(G, S^\pm)$. It is a labeled graph with vertices G and arcs (oriented edges) $G \times S^\pm$, where $S^\pm = S \cup S^{-1}$ and the arc (g, s) goes from g to gs and is labeled by s .

The group G naturally acts on the left on $\operatorname{Cay}(G, S^\pm)$ by multiplication. This action is transitive on the set of vertices and consists exactly of label preserving isomorphisms of the Cayley graph. Therefore, we have an embedding $G \cong \operatorname{Aut}_{\text{A lab}}(\operatorname{Cay}(G, S^\pm)) \leq \operatorname{Aut}(\operatorname{Cay}(G, S^\pm))$. Moreover, a locally finite graph is isomorphic to a Cayley graph if and only if it admits a subgroup of its automorphism group which acts regularly (freely and transitively) on the vertices, [19]. It is natural in this context to search for generating set S such that $G = \operatorname{Aut}(\operatorname{Cay}(G, S^\pm))$. Such a Cayley graph is called a *graphical regular representation*, or GRR. An easy verification (consider the inverse map) shows that abelian groups of exponent greater than 2 cannot admit GRR. As observed by Watkins, [21], generalized dicyclic groups also do not admit GRR, see Proposition 3.1 for a proof. The existence of GRR for finite groups has attracted a lot of attention in the 1970's and combined efforts of, notably, Imrich, Watkins, Nowitz, Hetzel and Godsil, [10, 6, 21, 17, 22, 23, 11, 12, 8, 7], showed that for

finite groups generalized dicyclic or abelian with an element of order greater than 2 groups as well as 13 exceptional groups (all of order at most 32, see Table 1 page 18) are the only finite groups that do not admit a GRR. Moreover, Babai and Godsil showed [4] that if G is a nilpotent non-abelian group of odd order, asymptotically almost all Cayley graphs of G are GRR. These results use deeply the fact that the groups under consideration are finite and are mostly based on "unscrewing" groups. They do not admit straightforward generalizations to infinite groups. For example, the proof of the existence of GRR uses the Feit-Thompson theorem that states that every finite group of odd order is solvable. On the other hand, Watkins showed, [24], that a free product of at least 2 and at most countably many groups has a GRR. Moreover, if the group in question is finitely generated, then the GRR in question is locally finite. Here the method used is to start with a free group and then consider quotients of it.

Our first main result states that for a finitely generated non-generalized dicyclic nor abelian group, having an element of large order is enough to guarantee the existence of a GRR (see Corollary 2.10 for a detailed statement):

Theorem 1.1. *Let G be a finitely generated group. Assume that G is not abelian, not generalized dicyclic and that G admits an element of order at least $1.41 \cdot 10^{19} \text{rank}(G)^{132}$. Then G admits a locally finite Cayley graph whose only automorphisms are the left-multiplications by elements of G .*

We hence partially recover existing results about existence of GRR for finite groups and free products and also extend it to more infinite groups. Moreover, we also show that if G has elements of arbitrary large order, then every finite generating set S is contained in a generating set T such that $\text{Cay}(G, T^\pm)$ is a GRR for G . This result can be thought as a weak form of the statement that asymptotically almost all Cayley graphs of the group are GRR.

Cayley graphs are often studied as undirected graphs, but their oriented, or directed, versions are also of interest. The (right) *directed Cayley graph* $\vec{\text{Cay}}(G, S)$ has vertex set G and arc set $G \times S$. It is a *digraphical regular representation*, or DRR, if $G \cong \text{Aut}_{\text{A lab}}(\vec{\text{Cay}}(G, S)) = \text{Aut}(\vec{\text{Cay}}(G, S))$. Since every homomorphism of $\vec{\text{Cay}}(G, S)$ naturally extends to $\text{Cay}(G, S^\pm)$, the existence of a GRR implies the existence of a DRR, but the converse does not hold. In [3], Babai showed that a finite group G admits a DRR if and only if it is neither the quaternion group Q_8 nor any of $(\mathbf{Z}/2\mathbf{Z})^2$, $(\mathbf{Z}/2\mathbf{Z})^3$, $(\mathbf{Z}/2\mathbf{Z})^4$ or $(\mathbf{Z}/3\mathbf{Z})^2$. This result is obtained by a rather general construction and the study of a few special cases; in great contrast with the existence of GRR which requires a lot of specific constructions. On the other hand, Babai also showed in [2] that every infinite group, with no restriction on generation or cardinality, admits a DRR. However the DRR's he constructed are never locally finite and the proof is rather complicated and use combinatorial set theory. Finally, in November 2018, Morris and Spiga showed in [16] that for a finite group G of cardinality n , the proportion of subsets S of G such that $\vec{\text{Cay}}(G, S)$ is a DRR goes to 1 as $n \rightarrow \infty$.

A variation of the notion of directed graphs is the notion of oriented graphs: directed graphs without bigons. For a Cayley digraph $\vec{\text{Cay}}(G, S)$, this is equivalent to the fact that $S \cap S^{-1}$ is empty. An oriented graph $\vec{\text{Cay}}(G, S)$ which is a DRR is called a *oriented regular representation* or ORR. Generalized dihedral groups do not admit a generating set without elements of order 2 and thus

cannot have ORR. For finite groups, Morris and Spiga showed, [14], that these are, alongside 11 groups of order at most 64, the only groups that do not admit ORR, answering a question posed by Babai in 1980. Their proof rely on the classification of finite simple groups.

Our methods also apply to prove that many finitely generated groups admit a DRR and an ORR (see Corollary 2.9 for a detailed statement).

Theorem 1.2. *Let G be a finitely generated group. If G contains an element of order at least $(5 \operatorname{rank}(G))^{12}$, then it has a locally finite directed Cayley graph whose only automorphisms are the left-multiplication by elements of G .*

If G is not a generalized dihedral group, then this digraph can be chosen without bigons.

In contrast with the above mentioned results, the methods we develop to prove Theorem 1.1 and 1.2 only use the finite generation of G and the existence of an element of large order (depending only on the rank of G). Moreover, we only use elementary group theory, and no structure theorems about subgroups or quotients. One strength of the method developed in this article is that it produces DRR, ORR and GRR altogether in an unified way.

Another way to study Cayley graphs is via the graphs they cover. Every subgroup $H \leq G$ gives rise to a label-preserving covering $\operatorname{Cay}(G, S^\pm) \twoheadrightarrow \operatorname{Sch}(G, H, S^\pm)$, where $\operatorname{Sch}(G, H, S^\pm)$ is the so-called (right) Schreier coset graph (also called Schreier orbital graph). All label-preserving covering from $\Gamma = \operatorname{Cay}(G, S^\pm)$ come in this way, but in general Γ may cover other graphs. In particular, in [20], the second author together with Romain Tessera proved that if G is finitely presented and contains an element of infinite order, then there exists a finite generating set S and an integer R (depending only on the rank of G) such that every graph that is R -locally isomorphic to $\operatorname{Cay}(G, S^\pm)$ is covered by it. On the other hand, the first author showed in [13] that Cayley graphs of Tarski monsters do not cover by label-preserving covering other infinite transitive graphs, hence partially answering a question of Benjamini.

In this paper, we introduce a notion of *strong graphical rigidity* for a triple (G, S, T) where $S \subseteq T$ are two finite generating set for G . Strong graphical rigidity of the triple (G, S, T) implies both that $\operatorname{Cay}(G, T^\pm)$ is a GRR and that essentially every covering $\operatorname{Cay}(G, T^\pm) \twoheadrightarrow \Delta$ preserve the labels when restricted to $\operatorname{Cay}(G, S^\pm)$. This allows us to show that for Tarski monsters there is essentially no covering $\operatorname{Cay}(G, T^\pm) \twoheadrightarrow \Delta$ with Δ transitive, see Theorem 2.12 for a precise statement. We also introduce the notion of *strong digraphical rigidity* for the triple (G, S, T) which implies the existence of a DRR for G as well as the oriented version of the covering statement.

We introduce the notion of *prerigidity* which is a weakening of the property to admit a GRR. This notion is about colour-preserving automorphisms and every prerigid graph is in particular a so called CCA (Cayley Colour Automorphism) graph. See [9, 5] for more details about CCA graphs. In Theorem 2.4 we show that a group is prerigid if and only if it is not a generalized dicyclic group nor an abelian with an element of order greater than 2 group, hence giving a geometric interpretation for these groups.

Finally, we stress out the fact that given an oracle for the word problem in G , all our proofs are constructive and when we construct T starting from S , there is an explicit bound on the cardinality of T^\pm , which depends only on the cardinality of S^\pm .

The next section contains all the necessary definitions and the statements of the main results of this paper. Section 3 contains the proof of Theorem 2.4, that is a geometric characterization of non-generalized dicyclic nor abelian with an element of order greater than 2 groups via their Cayley graphs. Then, Section 4 provides better bounds than the ones given by Theorem 2.4 for a large subclass of non-generalized dicyclic nor abelian with an element of order greater than 2 groups. Finally, Section 5 contains the proof of the existence of (strong) GRR and DRR, as well as the results about coverings.

Acknowledgements: The first author was partly supported by Swiss NSF grant P2GEP2_168302. The second author's research was supported by the ANR projects GAMME (ANR-14-CE25-0004) and AGIRA (ANR-16-CE40-0022). Part of this work was performed within the framework of the LABEX MILYON (ANR-10-LABX-0070) of Université de Lyon, within the program "Investissements d'Avenir" (ANR-11-IDEX-0007) operated by the French National Research Agency (ANR).

2 Definitions and results

2.1 Graphs

We first quickly recall the basic graph terminology we will use. More details may be found in [13]. For us, a *digraph* (or directed graph) will be a pair (V, E) together with two maps $\iota, \tau: E \rightarrow V$. V is the set of vertices, E the set of *arcs* (also called oriented edges). Every arc e has an initial vertex $\iota(e)$ and a terminal vertex $\tau(e)$. A *graph* (or undirected graph) is a digraph such that every arc e has an inverse \bar{e} satisfying $\bar{\bar{e}} = e$, $\iota(\bar{e}) = \tau(e)$ and $\tau(\bar{e}) = \iota(e)$. *Morphisms* of (di)graphs are maps that preserve the structure and isomorphisms are morphisms that are bijective on vertices and on arcs. An *edge* of a graph is a pair $\{e, \bar{e}\}$. A graph is *simple* if it has no loop (edge from v to itself) nor multiple edges (2 or more edges from v to w).

Two vertices v and w in a graph are adjacent if there is an edge between them, that is if there is an arc from v to w or equivalently from w to v . A graph is *locally finite* if every vertex has a finite number of adjacent vertices and *connected* if every two vertices v and w can be connected by a path (a sequence of adjacent vertices). A digraph is locally finite, if its underlying graph is.

Graphs are naturally metric spaces for the shortest path metric, where all edges are identified with the unit segment of the reals. The *ball* $\text{Ball}(v, r)$, is the biggest subgraph included in the closed metric ball of radius r around the vertex v . For example, if Γ is a triangle (3 vertices, 3 edges), then the ball of radius 1 around a vertex contains all 3 vertices, but only 2 edges, while the ball of radius 1.5 is Γ itself. Generally, it is always possible to assume that the radius is in $\frac{1}{2}\mathbf{Z}$. The following fact illuminates the importance of balls of radius 1 and 1.5 for coverings.

Lemma 2.1. *Let $\varphi: \Gamma \rightarrow \Delta$ be a covering between two simple graphs. The following are equivalent*

1. *For every vertex v , the restriction $\varphi: \text{Ball}(v, 1) \rightarrow \text{Ball}(\varphi(v), 1)$ is bijective,*

2. For every vertex v , the restriction $\varphi: \text{Ball}(v, 1.5) \rightarrow \text{Ball}(\varphi(v), 1.5)$ is injective.

2.2 Groups and Cayley graphs

Let G be a group and $S \subset G$ a generating set. For simplicity and clarity of the exposition, we will suppose that all our generating sets do not contain the identity element. This supposition comes at no cost, since passing from S to $S \setminus \{1\}$ has no effect on the automorphism group of the Cayley (di)graph. We will denote by $S^\pm = S \cup S^{-1}$ the symmetrization of S , where $S^{-1} = \{s^{-1} \mid s \in S\}$.

Since abelian groups of exponent greater than 2 will play an important role in the following, we begin by quickly recall two equivalent characterizations of them. For an abelian group G , the followings are equivalent: G is not isomorphic to $(\mathbf{Z}/2\mathbf{Z})^{(X)}$ for some set X and G has an element of order greater than 2. Such groups are called abelian of exponent greater than 2 or abelian but not elementary abelian 2-groups. To a pair (G, S) with G a group and S a generating set it is customary to associated the (right) Cayley graph $\text{Cay}(G, S^\pm) = (G, G \times S^\pm)$ where an arc (g, s) has initial vertex g , terminal vertex gs and is labeled by s . This graph has no multiple edge and if 1 does not belong to S it has no loop. A morphism $\varphi: \text{Cay}(G, S^\pm) \rightarrow \Delta$ is said to be an *arc-labeling preserving morphism* if when $\varphi(e) = \varphi(f)$, the two vertices e and f have the same label. Every morphism that preserves the label of arcs induces a labeling of Δ by pushforward. As said in the introduction, $G \cong \text{Aut}_{A\text{lab}}(\text{Cay}(G, S^\pm)) \leq \text{Aut}(\text{Cay}(G, S^\pm))$ and arc-labeling preserving coverings $\varphi: \text{Cay}(G, S^\pm) \rightarrow \Delta$ are in bijection with conjugacy classes of subgroups of G . Cayley digraphs $\vec{\text{Cay}}(G, S) = (G, G \times S)$ and their morphisms are defined similarly to the undirected case. As for the undirected case, $G \cong \text{Aut}_{A\text{lab}}(\vec{\text{Cay}}(G, S))$ acts freely transitively on the vertices of $\vec{\text{Cay}}(G, S)$. The *underlying graph* of $\vec{\text{Cay}}(G, S)$ is $\text{Cay}(G, S^\pm)$. Let us define $\text{Aut}_{E\text{lab}}(\vec{\text{Cay}}(G, S^\pm))$ as the group of *edge-labeling preserving automorphisms*. That is, φ is in $\text{Aut}_{E\text{lab}}(\vec{\text{Cay}}(G, S^\pm))$ if and only if for every edge $\{e, \bar{e}\}$, the set of labels of $\{\varphi(e), \varphi(\bar{e})\}$ is the same as for $\{e, \bar{e}\}$. We hence have $G = \text{Aut}_{A\text{lab}}(\vec{\text{Cay}}(G, S^\pm)) \leq \text{Aut}_{E\text{lab}}(\vec{\text{Cay}}(G, S^\pm)) \leq \text{Aut}(\vec{\text{Cay}}(G, S^\pm))$. In general, these three groups are distincts. This can be seen by looking at $G = F_n$ the free group of rank 2 and S a free generating set. Then the vertex stabilizer of 1 is trivial for $\text{Aut}_{A\text{lab}}(\vec{\text{Cay}}(G, S^\pm))$. On the other hand, for any vertex v , we have $|\text{Stab}_{\text{Aut}_{E\text{lab}}(\vec{\text{Cay}}(G, S^\pm))}(1).v| = 2^{|v|}$ while $|\text{Stab}_{\text{Aut}(\vec{\text{Cay}}(G, S^\pm))}(1).v| = (2n)^{|v|}$.

Definition 2.2. A pair (G, S) of a group with a generating system is a *pre-rigid* pair if $\text{Aut}_{E\text{lab}}(\vec{\text{Cay}}(G, S^\pm))$ acts freely transitively on the vertices of $\vec{\text{Cay}}(G, S^\pm)$, that is if $G = \text{Aut}_{E\text{lab}}(\vec{\text{Cay}}(G, S^\pm))$. The group G is *pre-rigid* if (G, G) is a prerigid pair.

The pair (G, S) is said to be a *GRR pair* if $\text{Aut}(\vec{\text{Cay}}(G, S^\pm))$ acts freely transitively on the vertices of $\vec{\text{Cay}}(G, S^\pm)$, that is if $G = \text{Aut}(\vec{\text{Cay}}(G, S^\pm))$.

Similarly, (G, S) is a *DRR pair* if $\text{Aut}(\vec{\text{Cay}}(G, S))$ acts freely transitively on the vertices of $\vec{\text{Cay}}(G, S)$, that is if $G = \text{Aut}(\vec{\text{Cay}}(G, S))$.

A triple (G, S, T) with $S \subseteq T$ two generating systems is said to be a *r-strong prerigid triple* (respectively *r-strong GRR triple*, respectively *r-strong DRR triple*) if any rooted edge-labeling preserving automorphism of the ball of radius r in $\vec{\text{Cay}}(G, T^\pm)$ (respectively any rooted automorphism of the ball in $\vec{\text{Cay}}(G, T^\pm)$, respectively in $\vec{\text{Cay}}(G, T)$) fixes pointwise the ball of radius 1 in

$\text{Cay}(G, S^\pm)$ (respectively in $\text{Cay}(G, S^\pm)$, respectively in $\vec{\text{Cay}}(G, S)$).

A DRR pair (G, S) with $S \cap S^{-1}$ empty is called an *ORR pair*, while a *r-strong ORR triple* (G, S, T) is an *r-strong DRR triple* with $T \cap T^{-1}$ empty.

ORR pair and ORR strong triple correspond to what Babai calls oriented graphs: directed graphs without bigon.

It is illuminating to reinterpret all the above definitions in term of the stabilizer of the vertex 1. Indeed, since the action of $\text{Aut}_{A\text{lab}}(\text{Cay}(G, S^\pm))$ on the vertices is transitive, then the action of a subgroup $\text{Aut}_{A\text{lab}}(\text{Cay}(G, S^\pm)) \leq A \leq \text{Aut}(\text{Cay}(G, S^\pm))$ is regular if and only if $\text{Stab}_A(1)$ is trivial. If $t > r$ and (G, S, T) is a *r-strong prerigid/GRR/DRR triple*, then it is also a *t-strong prerigid/GRR/DRR triple*. By the above observation and the fact that S is generating, a pair (G, T) is a prerigid/GRR/DRR pair if and only if there exists a (equivalently for all) generating set $S \subseteq T$ such that (G, S, T) is a ∞ -strong prerigid/GRR/DRR triple. In other words, (G, S, T) is a *r-strong prerigid/GRR/DRR triple* if (G, T) is a prerigid/GRR/DRR pair and this is witnessed by the S -ball of radius r . The following result follows from the fact that balls of radius 1 are stars.

Lemma 2.3. *A triple (G, S, T) is 1-strongly prerigid if and only if S consists only of elements of order 2.*

A triple (G, S, T) is a 1-strong GRR if and only if G is either the trivial group or the cyclic group of order 2.

A triple (G, S, T) is a 1-strong DRR if and only if $T = S$ has at most 1 element. In particular, G is cyclic.

This tells us that for general groups, the best rigidity results we can hope for are 1.5-strong (pre)rigidity. In Theorem 2.4 we show that if G is neither generalized dicyclic nor abelian of exponent greater than 2, then for any generating symmetric set S , the triple $(G, S, S^{\leq 11})$ is 1.5-strongly-prerigid. On the other hand, in Theorem 2.8 we show that for any finite generating set S , there exists T finite such that (G, S, T) is a 1.5-strong DRR, provided that G has an element of large enough (depending only on $|S|$) order. For the undirected case, we are able to provide finite T such that (G, S, T) is a 2-strong GRR triple.

Let us recall (Watkins, [21]) that (G, S) is a *Class II pair* if the group $\text{Aut}(G, S)$ of automorphisms ψ of G such that $\psi(S) = S$ is non-trivial, while G is a *Class II group* if (G, S) is a Class II pair for every symmetric generating S . The group $\text{Aut}(G, S)$ naturally injects into $\text{Stab}_{\text{Aut}(\text{Cay}(G, S^\pm))}(1)$. Then (G, S) is not a Class II pair if and only if (the image of) $\text{Aut}(G, S)$ is trivial. This is a necessary condition for (G, S) to be a GRR pair and Watkins conjectured that finite groups split into groups admitting a GRR and Class II groups. The conjecture was finally proved in 1978 by Godsil, constructing upon the works of many others, see the introduction for a list of references. Recall that G is a *generalized dicyclic group* if it is a non-abelian group, has an abelian normal subgroup A of index 2 and an element x of order 4 not in A such that $xax^{-1} = a^{-1}$ for every $a \in A$. An easy exercise shows that we always have $x^2 \in A$ of order 2. On the other hand, if A is abelian and $y \in A$ is of order 2, then it is always possible to construct a generalized dicyclic group $G = \langle A, x \rangle$ with $x^2 = y$. Watkins showed that abelian groups with an element of order greater than 2 and generalized dicyclic groups are contained in Class II groups, see also Proposition 3.1. Moreover, the result on GRR for finite groups shows that for

finite groups Class II is the union of abelian groups with an element of order greater than 2, generalized dicyclic groups and of 13 exceptional small groups.

Our first main result consists to show that prerigid groups are in fact the same as the union of abelian groups with an element of order greater than 2 and of generalized dicyclic groups, and hence a proper subclass of Class II groups. More precisely, denoting by $S^{\leq n}$ the set of non-trivial element of G of S -length at most n , that is vertices distinct from 1 in the ball or radius n in $\text{Cay}(G, S^{\pm})$, we have

Theorem 2.4. *For a group G , the following are equivalent*

1. G is neither generalized dicyclic, nor abelian with an element of order greater than 2;
2. G is prerigid;
3. for every (equivalently there exists a) generating set S , the pair $(G, S^{\leq 11})$ is prerigid;
4. for every (equivalently there exists a) generating set S , the triple $(G, S, S^{\leq 11})$ is 1.5-strongly prerigid;

There is a subclass of non-generalized dicyclic nor abelian with an element of order greater than 2 groups for which it is possible to obtain a far better bound; namely

Proposition 2.5. *Let G be a non-abelian group. Suppose that either G has no elements of order 4, or that it does not have non-trivial abelian characteristic subgroup. Then for every symmetric generating set S , there exists $\tilde{S} \leq T$ symmetric and generating such that $|\tilde{S}| = |S|$, $|T| \leq 3|S|$ and (G, \tilde{S}, T) is 1.5-strongly prerigid.*

In order to find GRR and DRR, we will make an extensive use of the notion of triangles in graphs. This is inspired by the work of the second author with R. Tessera, [20].

Definition 2.6. A *triangle* in a graph (V, E) is a subset $T \subset V$ of cardinality 3 such that for every $x \neq y \in T$ there is an edge e joining x to y . If $S \subset G$ is a finite generating set of a group and $s \in S$, we denote by $N_3(s, S)$ the number of triangles in $\text{Cay}(G, S^{\pm})$ containing the vertices 1 and s .

By regularity of $\text{Cay}(G, S^{\pm})$, we have $N_3(s, S) = N_3(s^{-1}, S)$ and for every $g \in G$ this is equal to the number of triangles containing the vertices g and gs . Since $N_3(s, S)$ is a geometric property, an automorphism of $\text{Cay}(G, S^{\pm})$ cannot send an edge labeled by s to an edge labeled by t if $N_3(s, S) \neq N_3(t, S)$. The following lemma shows the usefulness of both the notion of prerigidity and of the triangles approach.

Lemma 2.7. *Let G be a group and S a generating set. If S is such that the $N_3(s, S)$ are pairwise distincts for $s \in S$ (in particular, $S \cap S^{-1}$ consists of elements of order 2), then $\vec{\text{Cay}}(G, S)$ is a DRR for G . On the other hand, if (G, S) is a prerigid pair and all the $N_3(s^{\pm 1}, S)$ are pairwise distincts, then $\text{Cay}(G, S^{\pm})$ is a GRR for G .*

The second main theorem of this paper shows that for finitely generated groups, the existence of elements of large enough order is a sufficient condition to have a 1.5-strong DRR triple and also a 2-strong GRR triple. In particular, it implies the existence of a DRR and of a GRR for these groups. Before stating our theorem we need a little bit of notation. We note $F(n) := 2(2n^2 + 3n - 2)^2(2n^2 + 4n - 1)$ and $\check{F}(n) := 2(2n^2 + 3n - 2)^2(2n^2 + 4n) = 4(2n^2 + 3n - 2)^2(n + 2)n$ and for $S \subset G$, we denote by S^* any "antisymmetrization" of S . That is, S^* consists of a choice of one element in $\{s, s^{-1}\}$ for any $s \in S$. Equivalently, it is also a minimal subset of S^\pm for the condition $(S^*)^\pm = S^\pm$. If $S \cap S^{-1}$ consists only of elements of order 2, then it is possible to take $S^* = S$.

Theorem 2.8. *Let G be a group and S a finite generating set. If G contains an element of order at least $F(2|S^*|^2 + 28|S^*| - 4)$, then there exists a generating set T such that T^\pm contains S^\pm , has at most $2|S^*|^2 + 28|S^*|$ elements and (G, S^*, T) is a 1.5-strongly DRR triple.*

If S contains no elements of order 2 and G has an element of order at least $\check{F}(2|S^|^2 + 28|S^*| - 4)$, then there exists a generating set T such that T^\pm contains S^\pm , has at most $2|S^*|^2 + 28|S^*| = 2|S^*|^2 + 14|S^\pm|$ elements and (G, S^*, T) is a 1.5-strongly ORR triple.*

In both cases, if (G, S_0, S) is 1.5-strongly prerigid for some generating $S_0 \subseteq S$, then the triple (G, S_0, T) is a 2-strong GRR triple.

Recall that a *generalized dihedral group* is the semi-direct product $A \rtimes \mathbf{Z}/2\mathbf{Z}$ where A is abelian and $\mathbf{Z}/2\mathbf{Z}$ acts on A by inversion. In [15], Morris and Spiga showed that any finitely generated group that is not generalized dihedral admits a generating set S without elements of order 2 and with $|S| = \text{rank}(G)$. We hence obtain the following corollary.

Corollary 2.9. *Let G be a finitely generated group. If G contains an element of order at least $F(2\text{rank}(G)^2 + 28\text{rank}(G) - 4)$ then it has a DRR of valency at most $2\text{rank}(G)^2 + 28\text{rank}(G)$. If G is not a generalized dihedral group and contains an element of order at least $\check{F}(2\text{rank}(G)^2 + 28\text{rank}(G) - 4)$ then the above DRR is in fact an ORR.*

If G contains elements of arbitrary large order, then for every finite generating set S , there exists T such that T^\pm contains S^\pm , has at most $2|S^|^2 + 28|S^*|$ elements and $\vec{\text{Cay}}(G, T)$ is a DRR for G . If moreover G is not a generalized dihedral group and S has no elements of order 2, then $\vec{\text{Cay}}(G, T)$ is an ORR for G .*

Since cyclic groups always admit an ORR, it is possible in the above corollary to suppose that $\text{rank}(G) \geq 2$ and a direct computation gives $\check{F}(2\text{rank}(G)^2 + 28\text{rank}(G) - 4) \leq (5\text{rank}(G))^{12}$ as given in the introduction.

On the other hand, Theorem 2.8 together with Theorem 2.4 and Proposition 2.5 gives us

Corollary 2.10. *Let G be a non-generalized dicyclic nor abelian finitely generated group. If G contains an element of order at least $F(2^{25}\text{rank}(G)^{22} + 2^{14} \cdot 7\text{rank}(G) - 4)$, then it has a GRR of valency at most $2^{25}\text{rank}(G)^{22} + 2^{14} \cdot 7\text{rank}(G)$. If G has no elements of order 4 or no non-trivial characteristic abelian subgroup, then this bound can be lowered to $F(18\text{rank}(G)^2 + 84\text{rank}(G) - 4)$ and the GRR obtained is of valency at most $18\text{rank}(G)^2 + 84\text{rank}(G)$.*

If moreover G has elements of arbitrary large order, then for every finite generating set S , there exists $S \subset T$ such that $\text{Cay}(G, T^\pm)$ is a GRR for G with $|T|^\pm \leq 2|S^{\leq 11}|^2 + 15|S^{\leq 11}|$, or $|T| \leq \frac{9}{2}|S^\pm|^2 + 42|S^\pm|$ if G has no elements of order 4 or no non-trivial characteristic abelian subgroup.

Since G is not abelian, it is not cyclic and $\text{rank}(G) \geq 2$. A direct computation gives us $F(2^{25} \text{rank}(G)^{22} + 2^{14} \cdot 7 \text{rank}(G) - 4) \leq 1.41 \cdot 10^{19} \text{rank}(G)^{132}$ which is the bound given in the introduction.

For finitely generated groups, this subsumes the result of Watkins on free products. Indeed, free products always have elements of infinite order. On the other hand, Corollary 2.9 is partial improvement of Babai's work on infinite groups, since the DRR we obtain is locally finite. Moreover, we do not only exhibit one DRR, or GRR, for the groups in question, but we obtain some kind of asymptotic comportement. Nevertheless, in contrast with Watkins and Babai's results, we do not treat the non-finitely generated case.

It is possible to deduce from the fact that (G, S, T) is a 2-strong GRR triple informations about graph homomorphisms that are bijective on balls of radius 2, such homomorphisms are necessarily coverings. In fact, a slight modification of the proof of Theorem 2.8 yields the following result.

Proposition 2.11. *Let (G, S_0, S) be a 1.5-strong prerigid triple with S finite such that G contains an element of order at least $F(2|S^*|^2 + 28|S^*| - 4)$. Let T be the generating set given by (the proof of) Theorem 2.8 — in particular (G, S_0, T) is a 2-strong GRR triple. Then, for any covering $\psi: \text{Cay}(G, T^\pm) \rightarrow \Delta$ that is bijective on balls of radius 1.5, there exists a subgraph $\hat{\Delta}$ of Δ such that the restriction of ψ to $\text{Cay}(G, S^\pm)$ is a arc-labeling preserving covering onto $\hat{\Delta}$.*

Recall (see for example [13]) that arc-labeling preserving coverings are in bijections with conjugacy classes of subgroups of G and that turns $\hat{\Delta}$ of Proposition 2.11 into a Schreier graph of G .

Using Proposition 2.11 and Proposition 44 from [13], we obtain the following rigidity results about Cayley graphs of Tarski monsters.

Theorem 2.12. *For any $p \geq 6\,776\,965\,274\,112$ and any Tarski monster \mathcal{T}_p , there exists a symmetric generating system T of size at most 90, such that if $\psi: \text{Cay}(\mathcal{T}_p, T^\pm) \rightarrow \Delta$ is a covering that is bijective on balls of radius 1.5, then either ψ is the identity, or Δ is infinite and the action of its automorphism group on its vertices has finite orbits. In particular, if the covering is not trivial, then Δ is not transitive, and not even quasi-transitive.*

The method we use, using triangles, is not able to say anything on coverings which are not bijective on balls of radius 1.5. Nevertheless, if being bijective on 1.5 is a restriction on which kind of coverings we consider, it is a small one. Indeed, if $\varphi: \Gamma \rightarrow \Delta$ is a covering between two simple graphs (no loops, nor multiple edges), it is bijective on balls of radius $1.5 - \varepsilon$ for any $\varepsilon > 0$ and injective on balls of radius 1.5, as noted in Lemma 2.1.

Finally, we want to stress out the following facts.

Remark 2.13. In all the above results about GRR, the hypothesis of the existence of an element of large enough order is a necessary. Indeed, there exists 13 finite exceptional groups that are not generalized dicyclic nor abelian with an element of order greater than 2 (and hence prerigid) but that do not admit any GRR.

More details and lower bounds on the order may be found at the end of Section 4. Similarly, the 5 exceptional finite groups without DRR as well as the 11 finite non-generalized dihedral groups without ORR show that in these cases too the hypothesis of an element of large order is necessary.

Remark 2.14. As already said, one of the strength of our method is that the same construction give altogether GRR, DRR and ORR. Another important point is that the proof of our results gives an algorithm that take in entry a generating set of G and an oracle for the word problem in G and return (given the existence of an element of large order) a DRR, and even an ORR and a GRR when applicable.

3 Prerigid triples

The aim of this section is to show Theorem 2.4, which implies that generalized dicyclic groups and abelian groups of exponent greater than 2 are the only non-prerigid groups.

Clearly, for a group G and a symmetric generating set S , the stabilizer of 1 in $\text{Aut}_{E\text{-lab}}(\text{Cay}(G, S^\pm))$ coincides with the group $\mathcal{B}(G, S)$ of all permutations φ of G satisfying the following condition

$$\varphi(1) = 1 \text{ and } \forall g \in G, \forall s \in S, \varphi(gs) \in \varphi(g)\{s, s^{-1}\}.$$

In particular, the pair (G, S) is prerigid if and only if $\mathcal{B}(G, S)$ is trivial. On the other hand, it directly follows from the definition that if $S \subseteq T$, then $\mathcal{B}(G, T) \leq \mathcal{B}(G, S)$. In particular, if (G, S) is prerigid for some S , then G is prerigid. On the other hand, if G is a finitely generated prerigid group, then a compactness argument shows that there exists a finite generating set S such that (G, S) is prerigid. We will show that G is not generalized dicyclic nor abelian but not elementary 2 group, if and only if for every (equivalently there exists a) S symmetric generating set, $(G, S^{\leq 11})$ is prerigid, and that this is also equivalent to the similar statement for 1.5-strong prerigidity.

Similarly, the group of rooted edge-labeling preserving automorphism of the ball of radius 1.5 in $\text{Cay}(G, T^\pm)$ is isomorphic to the group $\mathcal{B}(G, T, 1.5)$ of bijections $\varphi: T \rightarrow T$ such that

$$\varphi(1) = 1 \text{ and } \forall s, t \in T, st \in T \implies \varphi(st) \in \varphi(s)\{t, t^{-1}\}.$$

We first turn our attention on generalized dicyclic groups and abelian groups.

Proposition 3.1. *If G is a generalized dicyclic group or an abelian group with a element of order at least 3, then it is not prerigid.*

Proof. We have to prove that $\mathcal{B}(G, G) \neq \{\text{Id}\}$. If G is abelian, then the inverse map $\varphi: g \rightarrow g^{-1}$ belongs to $\mathcal{B}(G, G)$. If G is of exponent greater than 2, then there is an $s \in S$ of order greater than 2, and thus $\varphi \neq \text{Id}$ ¹.

On the other hand, if $G = \langle A, x \rangle = A \sqcup xA$ is a generalized dicyclic group, then the fonction φ defined by $\varphi(a) = a$ and $\varphi(xa) = (xa)^{-1}$ for every $a \in A$ is

¹In fact, if G is abelian but not elementary 2-group, we exactly have $\mathcal{B}(G, G) = \{\text{Id}, \varphi\}$ as shown by a careful analysis of the proof of Theorem 3.11.

in $\mathcal{B}(G, G)$ and differs from the identity as x has order 4. Indeed, it is obviously a bijection and for a and b in A we have

$$\begin{aligned}\varphi(a \cdot b) &= ab = \varphi(a)b = \varphi(a)\varphi(b) \\ \varphi(a \cdot xb) &= \varphi(xa^{-1}b) = b^{-1}ax^{-1} = \varphi(a)(xb)^{-1} = \varphi(a)\varphi(xb) \\ \varphi(xa \cdot b) &= b^{-1}a^{-1}x^{-1} = \varphi(xa)b = \varphi(xa)\varphi(b) \\ \varphi(xa \cdot xb) &= \varphi(x^2a^{-1}b) = x^2a^{-1}b = \varphi(xa)(xb)^{-1} = \varphi(xa)\varphi(xb)\end{aligned}$$

Where in the last line we used that $x^3b = x^{-1}b = b^{-1}x^{-1}$. \square

In fact, this proof also shows the previously known fact, [21], that generalized dicyclic or abelian with an element of order greater than 2 groups is a subclass of Class II groups. That is, groups such that for every symmetric generating set S , there exists an automorphism ψ of G such that $\psi(S) = S$.

From Lemma 2.3 and Proposition 3.1, we deduce the following.

Lemma 3.2. *An abelian group is prerigid if and only if it is an elementary abelian 2-group. In this case, for every $S \subseteq T$ symmetric and generating, (G, S, T) is a 1-strong prerigid triple.*

In many of the following results, the quaternions group

$$Q_8 = \langle i, j, k \mid i^4 = 1, i^2 = j^2 = k^2 = ijk \rangle$$

plays a special role and we often assume that 2 given elements do not generate Q_8 . This hypothesis is necessary as shown in the following lemma than can be checked by hand or computer.

Lemma 3.3. *For every choice of $(\alpha_1, \alpha_2, \alpha_3)$ in $\{1, -1\}^3$, there exists a bijection $\varphi: Q_8 \rightarrow Q_8$ in $\mathcal{B}(Q_8, Q_8)$ such that $\varphi(i) = i^{\alpha_1}$, $\varphi(j) = j^{\alpha_2}$ and $\varphi(k) = k^{\alpha_3}$.*

We also record the two following facts about Q_8 that we will use later. The first one is a classical result and the proof is an easy exercise let to the reader. It implies that if $\langle g, h \rangle$ is isomorphic to Q_8 , then it is isomorphic to it by $i \mapsto g$ and $j \mapsto h$. The second one allows us to easily detect if $\langle g, h \rangle$ is isomorphic to Q_8 .

Lemma 3.4. *The automorphism group of Q_8 acts transitively on pairs of generators.*

Lemma 3.5. *Let $G = \langle g, h \rangle$. If $gh = hg^{-1}$ and $hg = gh^{-1}$, then G is a quotient of Q_8 . If moreover G contains an element of order greater than 2 or is not abelian, then it is isomorphic to Q_8 .*

Proof. Recall that Q_8 is also given by the following presentation

$$Q_8 = \langle i, j \mid i^4 = 1, i^2 = j^2, jij^{-1} = i^{-1} \rangle,$$

and that all proper quotient of Q_8 are elementary abelian 2-group. The equality $gh = hg^{-1}$ is equivalent to $hg^{-1}h^{-1} = g$ and thus to $hgh^{-1} = g^{-1}$. Hence, we only need to show that $g^4 = 1$ and $g^2 = h^2$. Now, $hg = gh^{-1}$ is equivalent both to $g = hgh$ and to $g = h^{-1}gh^{-1}$. We have

$$\begin{aligned}g^2 &= hg^{-1}h^{-1} \cdot hgh = h^2 \\ g^2 &= h^{-1}gh^{-1} \cdot hg^{-1}h^{-1} = h^{-2}\end{aligned}$$

which gives us both $g^2 = h^2$ and $g^4 = 1$. \square

In the sequel, we fix two symmetric generating sets $S \subseteq T$ of G , and we fix φ in $\mathcal{B}(G, T, 1.5)$.

It is possible to partition T into $A \sqcup B$, where

$$\begin{aligned} A &= \{g \in T \mid \varphi(g) = g\} \\ B &= \{g \in T \mid \varphi(g) = g^{-1} \neq g\}. \end{aligned}$$

By definition, every h in B satisfies $h^2 \neq 1$.

As a direct consequence of the definition we obtain

Lemma 3.6. *Let s be in T and n be a relative integer. If $\varphi(s) = s$ (respectively $\varphi(s) = s^{-1}$) and s^n is in T , then $\varphi(s^n) = s^n$, (respectively $\varphi(s^n) = s^{-n}$).*

Lemma 3.7. *If $g \in A$ is such that $g^2 \neq 1$, then $C_G(g) \cap T \cap gT \subseteq A$.*

Proof. Let h be an element of $C_G(g) \cap T \cap gT$. So $\varphi(h) = \varphi(g(g^{-1}h))$ belongs both to $\{h, h^{-1}\}$ and $\{h, gh^{-1}g = g^2h^{-1}\}$. So if $h \in B$, then $h^{-1} = g^2h^{-1}$, a contradiction as we assumed $g^2 \neq 1$. \square

Lemma 3.8. *Let g and h be two elements of A such that $gh \in T$. If $\langle g, h \rangle$ is not isomorphic to Q_8 , then gh is in A .*

Proof. We show that if $gh \in B$, then $\langle g, h \rangle = Q_8$. Since B is closed under inversion, we also have $h^{-1}g^{-1} \in B$. In particular, $(gh)^2 \neq 1$ and $(h^{-1}g^{-1})^2 \neq 1$. So we have $gh = \varphi(h^{-1}g^{-1}) = h^{-1}g$, or equivalently $hg = gh^{-1}$, and $h^{-1}g^{-1} = \varphi(gh) = gh^{-1}$, or equivalently $gh = hg^{-1}$. Therefore, we could apply Lemma 3.5 using the fact that gh is in B and hence of order greater than 2. \square

Lemma 3.9. *Let $g \in A$ and h in B be such that hg and $g^{-1}h$ are still in T . Then we have $hgh^{-1} = g^{-1}$. Moreover, if the subgroup $\langle g, h \rangle$ is not isomorphic to Q_8 , then the element hg is in B .*

Proof. Assume first that $hg \in A$. Then we have that hg and g^{-1} both belong to A but their product belongs to B , so by Lemma 3.8 $\langle hg, g \rangle$ (which is just $\langle h, g \rangle$) is isomorphic to Q_8 . In particular $hgh^{-1} = g^{-1}$.

Assume now that $hg \in B$. Then $\varphi(hg) = g^{-1}h^{-1} \in \{h^{-1}g, h^{-1}g^{-1}\}$. If $g^{-1}h^{-1} = h^{-1}g$, we have $hgh^{-1} = g^{-1}$ as desired. On the other hand, if $g^{-1}h^{-1} = h^{-1}g^{-1}$, then g and h commute. By Lemma 3.7, we have $g^2 = 1$ and therefore $hgh^{-1} = g = g^{-1}$. \square

Lemma 3.10. *Let $g, h \in A$ and $f \in B$ be such that*

$$\{gh, fg, g^{-1}f, fh, h^{-1}f, fgh, (gh)^{-1}f\} \subseteq T.$$

Then $ghg^{-1} \in \{h, h^{-1}\}$, with $ghg^{-1} \neq h$ if and only if $\langle g, h \rangle$ is isomorphic to Q_8 .

Proof. If $\langle g, h \rangle$ is isomorphic to Q_8 , then $ghg^{-1} = h^{-1}$ is clear. Otherwise, by Lemma 3.8 we have $gh \in A$, and applying three times Lemma 3.9 we obtain

$$h^{-1}g^{-1} = f(gh)f^{-1} = (fgf^{-1})(fhf^{-1}) = g^{-1}h^{-1}$$

and g, h commute. \square

Theorem 3.11. *Let S be a generating set in G , and let $T = S^{\leq 11}$. If (G, S, T) is not 1.5-strongly prerigid, then G is generalized dicyclic or an abelian group of exponent greater than 2.*

Proof. By Lemma 3.2, we can suppose that G is not an elementary abelian 2-group.

Let $T = S^{\leq i}$ for some i . We will see that $i = 11$ is enough to prove the theorem. For the convenience of the reader, each time we will use a preceding result, we will specify in square brackets for which values of i it is true. By hypothesis, there is a $\varphi \in \mathcal{B}(G, T, 1.5)$ and an s in S such that $\varphi(s) \neq s$. In particular, s is in $B \cap S$.

Case 1 Assume that there are $g_0, h_0 \in B \cap S$ such that $g_0 h_0 \in B$. For every $g \in A \cap S^{\leq i-2}$ we have by Lemma 3.9 that $g_0 g g_0^{-1} = h_0 g h_0^{-1} = (g_0 h_0) g (g_0 h_0)^{-1} = g^{-1}$. This implies that $g = g^{-1}$. In other words, $\varphi(g) = g^{-1}$ for every $g \in S^{\leq i-2}$.

Observe that if $g \in S^{\leq i-3}$ and $h \in S$ do not commute, then they generate Q_8 and in particular have order 4. Indeed, since $gh \in S^{\leq i-2}$, we have $gh = \varphi(h^{-1}g^{-1}) \in \{hg^{-1}, hg\}$. The equality $gh = hg$ is excluded, so we have $gh = hg^{-1}$ and $g \neq g^{-1}$. Similarly exchanging the roles of g, h we have $hg = gh^{-1}$. This implies that the $\langle g, h \rangle$ is isomorphic to Q_8 by Lemma 3.5. We can assume that G is not abelian, since otherwise there is nothing to prove. Pick a non commuting pair $(g_1, h_1) \in S \times S$. By the preceding $\langle g_1, h_1 \rangle$ is isomorphic to Q_8 , and in particular $\varepsilon := g_1^2 = h_1^2$ has order 2. Then every element a of $Z(G) \cap S^{\leq 3}$ has order 2. Indeed, $(g_1 a, h_1)$ is also a non commuting pair and by the preceding [we use $i-3 \geq 3+1$] we have $(g_1 a)^2 = h_1^2 = g_1^2$, which implies that $a^2 = 1$.

So elements of $S^{\leq 3}$ are of order 1, 2, 4, and the elements of order ≤ 2 are exactly those that belong to $Z(G)$. Observe that $g_1^2 = h_1^2$ has order 2, so belongs to $Z(G)$.

Denote by G_0 the subgroup of $Z(G)$ generated by $Z(G) \cap S^{\leq 3}$, and by G_1 the group generated by G_0, g_1 and h_1 . G_0 is an abelian 2-group, so it can be seen as a vector space over the field with two elements, which contains the non-zero vector $g_1^2 = h_1^2 = \varepsilon$. By completing this vector to a basis $\{g_1^2\} \cup \{g_x : x \in X\}$ of G_0 , G_1 is isomorphic to $Q_8 \times (\mathbf{Z}/2\mathbf{Z})^{(X)}$ for a set X . To conclude, we have to prove that $G = G_1$.

Pick $g \in S$. We shall prove that $g \in G_1$. If $g \in Z(G)$, then we have $g \in G_0$ and we are done, hence we can suppose that g is not in the center. Assume first that g commutes with g_1 , then gg_1 commutes with h_1 . Indeed, if it was not the case, then by the above [use $i-3 \geq 2$] gg_1 and h_1 generate Q_8 . But then we would have $g_1^2 = h_1^2 = (gg_1)^2 = g^2 g_1^2$ which implies $g^2 = 1$ in contradiction with the fact that g is not in $Z(G)$. Since g and g_1 commute and gg_1 commutes with h_1 , we have

$$g(g_1 h_1)g^{-1} = (gg_1)h_1g^{-1} = h_1(gg_1)g^{-1} = h_1 g_1 \neq g_1 h_1,$$

where the inequality is by the fact that g_1 and h_1 generate Q_8 . Hence g do not commute with $g_1 h_1$, which implies [use $i-3 \geq 2$]

$$g^2 = (g_1 h_1)^2 = g_1^2,$$

where we used once again that g_1 and h_1 generate Q_8 . Finally, $(gg_1)^2 = g^2 g_1^2 = g_1^4 = 1$ and therefore gg_1 belong to $Z(G) \cap S^{\leq 2}$. This implies that g^{-1} is in $g_1 G_0 \subseteq G_1$.

Similarly, if g commutes with h_1 we have $g \in G_1$. It remains to consider the case when g commutes neither with g_1 nor with h_1 . Then we have $g^2 = g_1^2 = h_1^2 = \varepsilon$ and

$$\begin{aligned} (h_1^{-1}g_1^{-1}g)^2 &= (h_1^{-1}g_1^{-1})(gh_1^{-1})(g_1^{-1}g) = \varepsilon^3(g_1^{-1}h_1^{-1})(h_1^{-1}g)(gg_1^{-1}) \\ &= \varepsilon^3g_1^{-1}h_1^{-2}g_1 = 1. \end{aligned}$$

So $h_1^{-1}g_1^{-1}g$ belongs to $Z(G) \cap S^{\leq 3}$ and $g \in G_1$.

Case 2 Assume now that for every $g, h \in B \cap S$, $gh \in A$, but that there exists $g_0, h_0 \in A \cap S^{\leq 2}$ such that $g_0h_0 \in B$. By Lemma 3.8 [$i \geq 2 + 2$], $\langle g_0, h_0 \rangle$ is isomorphic to Q_8 . Denote by G_0 the centralizer of $\langle g_0, h_0 \rangle$ in G , $\tilde{S} := G_0 \cap S^{\leq 5}$, and let G'_0 be the subgroup generated by \tilde{S} , and G_1 be the group generated by G'_0 and $\langle g_0, h_0 \rangle$. By Lemma 3.7 applied to g_0 , \tilde{S} is contained in A [use $i \geq 5 + 2$]. Since every element g of \tilde{S} commutes with g_0h_0 , it is of order 1 or 2. Otherwise, Lemma 3.7 applied to g would imply that g_0h_0 is in A [use $i \geq 5 + 4$], a contradiction. Moreover, Lemma 3.10 implies that every elements of \tilde{S} commute (remember that we have assumed that there exists $f \in B \cap S$) [use $i \geq 1(f) + 5(g) + 5(h)$]. So G'_0 is abelian and generated by element of order 2, it is a elementary 2-group. We obtain that G_1 is isomorphic to $Q_8 \times (\mathbf{Z}/2\mathbf{Z})^{(X)}$. So all we have to do is prove that $G_1 = G$.

Let $g \in S$. Since $g_0 \in A \cap S^{\leq 2}$, we have that $gg_0g^{-1} \in \{g_0, g_0^{-1}\}$ by Lemma 3.9 [$i \geq 2 + 1$] and Lemma 3.10 [$i \geq 1 + 2 + 1$]. Similarly $gh_0g^{-1} \in \{h_0, h_0^{-1}\}$. We consider all four cases.

1. $(gg_0g^{-1}, gh_0g^{-1}) = (g_0, h_0)$. Then g belongs to G'_0 and in particular to G_1 .
2. $(gg_0g^{-1}, gh_0g^{-1}) = (g_0, h_0^{-1})$. Then

$$(g_0g)h_0(g_0g)^{-1} = g_0h_0^{-1}g_0 = h_0.$$

The last equality is because $\langle g_0, h_0 \rangle$ is isomorphic to Q_8 . So $g_0g \in S^{\leq 3}$ commutes with both g_0 and h_0 and therefore belongs to G'_0 . In particular $g = g_0^{-1}(g_0g)$ belongs to G_1 .

3. $(gg_0g^{-1}, gh_0g^{-1}) = (g_0^{-1}, h_0)$. Exchanging g_0 and h_0 we deduce from the previous case that $g \in h_0^{-1}G'_0 \subseteq G_1$.
4. $(gg_0g^{-1}, gh_0g^{-1}) = (g_0^{-1}, h_0^{-1})$. Then

$$g(g_0h_0)g^{-1} = (gg_0g^{-1})(gh_0g^{-1}) = g_0^{-1}h_0^{-1} = g_0h_0,$$

where the last equality is because g_0 and h_0 generate Q_8 . So g commutes with g_0h_0 but not with h_0 , so from the second case (replacing (g_0, h_0) by (g_0h_0, h_0) which still generates Q_8), we obtain that $g_0h_0g \in S^{\leq 5}$ is in G_0 and thus in G'_0 . We then have $g \in h_0^{-1}g_0^{-1}G'_0 \subseteq G_1$.

So in each case we have $g \in G_1$. This proves that G coincides with G_1 and completes the proof of this case.

Case 3 Consider the remaining case: for every $g, h \in B \cap S$, $gh \in A$, and for every $g, h \in A \cap S^{\leq 2}$, $gh \in A$. Pick $g_0 \in B \cap S$. By Lemma 3.9 [with $i \geq 1 + 2 + 2$], we have for every $g, h \in A \cap S^{\leq 2}$,

$$h^{-1}g^{-1} = g_0(gh)g_0^{-1} = (g_0gg_0^{-1})(g_0hg_0^{-1}) = g^{-1}h^{-1}$$

Therefore the subgroup G_0 of G generated by $A \cap S^{\leq 2}$ is abelian, and for every element f of $B \cap S$, the action of f by conjugation on G_0 is the inverse map. In particular G_0 is normal; denote by $q: G \rightarrow G/G_0$ the quotient map. By definition, $q(g) = 1$ for every $g \in A \cap S$. Moreover, since $g_0^2 \in A \cap S^{\leq 2}$, the image $q(g_0)$ has order 2. Finally, every other element $g \in B \cap S$ satisfies that $g_0^{-1}g \in A \cap S^{\leq 2}$, so $q(g) = q(g_0)$. To summarize, $q(S)$ is equal to the group of order 2 $\{e, q(g_0)\}$. Since S is generating, we deduce that $q(G)$ has cardinality 2, *i.e.* that G_0 has index 2 in G . We conclude that G is generalized dicyclic. \square

We have proven that if G is a generalized dicyclic or abelian with an element of order greater than 2 group, then it is not prerigid (Proposition 3.1). This implies that for every symmetric generating S , $(G, S^{\leq 11})$ is not a prerigid pair, hence $(G, S, S^{\leq 11})$ is not a 1.5-strong prerigid triple. On the other hand, the existence of a symmetric generating set S such that $(G, S, S^{\leq 11})$ is not 1.5-strongly prerigid implies that G is generalized dicyclic or abelian with an element of order greater than 2, hence proving Theorem 2.4.

4 More on prerigidity

In the last section, we have shown that if G is not a generalized dicyclic group nor an abelian with an element of order greater than 2 group, then for every symmetric generating set S , the triple (G, S, T) is 1.5-strongly prerigid for $T = S^{\leq 11}$. The main caveat of this general method is that the size of $S^{\leq 11}$ is really big when compared to the size of S . This is important as in the hypothesis of Theorem 2.8 and Proposition 2.11 we suppose that G has an element of order at least $F(2|T|^2 + 28|T| - 4)$. In this section, we provide criterions on (G, S) which ensures that (G, \tilde{S}, T) is 1.5-strongly prerigid for some $\tilde{S} \subset T$ with $|\tilde{S}| = |S|$ and $|T| \leq 3|S|$.

4.1 General results on prerigidity

By Lemma 3.2, if G is abelian of exponent at most 2, then for every $S \subseteq T$ generating, (G, S, T) is 1-strongly prerigid. On the other hand, generalized dicyclic or abelian with an element of order greater than 2 groups are never prerigid. Therefore, we will assume in this section that G is neither abelian nor generalized dicyclic.

Proposition 4.1. *Let G be a group and S a generating set such that*

$$\forall s \in S, \begin{cases} s^2 = 1 \text{ or} \\ \exists g := g_s \in G : s^2 \neq g^2 \text{ and } sgs^{-1} \notin \{g, g^{-1}\}. \end{cases} \quad (*)$$

Let p denotes the cardinality of elements of S of order 2 and q the cardinality of elements of S of order at least 3. Then there exists $S \subseteq T$ with $|T^\pm| \leq p + 6q$ such that (G, S, T) is 1.5-strongly prerigid.

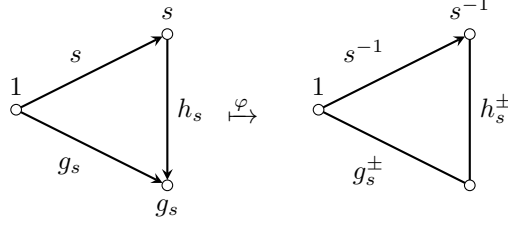


Figure 1: The action of φ on the triangle $(1, s, g_s)$.

Proof. Let T be the union of S , $\{g_s \mid s \in S \text{ of order at least } 3\}$ and $\{h_s := s^{-1}g_s \mid s \in S \text{ of order at least } 3\}$. Then T^\pm contains at most $p + 6q$ elements.

Suppose by contradiction that we have φ an edge-labeling preserving rooted automorphism of the ball of radius 1.5 in $\text{Cay}(G, T^\pm)$ that does not fix pointwise elements of S . Then we have some $s \in S$ with $\varphi(s) = s^{-1} \neq s$. In particular, s is not of order 2 and the action of φ on the triangle $(1, s, g_s)$ is depicted in Figure 1. Since we are looking at balls in a Cayley graph of G , the label of every cycle in it corresponds to a relation in G . Therefore, depending on φ , one of the following relations is true in G :

$$\begin{cases} s^{-1}h_s g_s^{-1} = 1 \\ s^{-1}h_s^{-1}g_s = 1 \\ s^{-1}h_s g_s = 1 \\ s^{-1}h_s^{-1}g_s^{-1} = 1 \end{cases}$$

which correspond respectively to

$$\begin{cases} s^2 = 1 \\ s^2 = g_s^2 \\ s g_s = g_s s \\ s g_s s^{-1} = g_s^{-1} \end{cases}$$

which contradicts our hypothesis. \square

In the rest of this section, we investigate some properties of the group G or of the pair (G, S) that imply Condition (*) on S . In this context, elements of order 4 as well as squares play an important role.

Lemma 4.2. *Let G be a group and S a generating set such that*

$$\begin{cases} \text{all elements of } S \cap Z(G) \text{ have order } 2; \\ S \text{ does not contain elements of order } 4. \end{cases} \quad (\dagger)$$

Then S satisfies Condition (). Moreover, if $hs \neq sh$, then it is possible to choose g_s in $\{sh, sh^{-1}, hs^{-1}, h^{-1}s^{-1}\}$.*

Proof. Let $s \in S$. If $s^2 = 1$, then there is nothing to do. If $s^2 \neq 1$, then by assumption $s^4 \neq 1$ and there exists $h \in G$ such that $hs \neq sh$, this implies that $h^{-1}s \neq sh^{-1}$. On the other hand, for every $k \in G$, we cannot have $k^2 = s^2$

and $(k^{-1})^2 = s^2$ together, otherwise we would have $s^4 = 1$. Suppose that $h^2 \neq s^2$ (the proof is similar for h^{-1}) and take $g_s = sh^{-1}$. By assumption on h , we have $sg_s = s \cdot sh^{-1} \neq sh^{-1} \cdot s = g_s s$. Now, if $sg_s s^{-1} = g_s^{-1}$, we have $s \cdot sh^{-1} \cdot s^{-1} = (sh^{-1})^{-1}$ and then $s^2 = h^2$ which contradicts our hypothesis. Similarly, $sg_s^{-1} s^{-1} \neq g_s$. As noted before, at least one of the square of g_s and g_s^{-1} is not equal to s^2 . We thus have proved that if $sh \neq hs$ and $s^4 \neq 1$, at least one of $\{sh^{-1}, hs^{-1}, sh, h^{-1}s^{-1}\}$ may be taken for g_s in order to verify Condition (*). \square

Corollary 4.3. *If G is such that*

$$G = \langle G \setminus (Z(G) \cup \{g \in G \mid g^4 = 1\}) \cup \{g \in G \mid g^2 = 1\} \rangle$$

then it admits a generating set S satisfying Condition (). If moreover G is finitely generated, then there exists a finite generating set S satisfying Condition (*).*

As an important corollary of Lemma 4.2, we have

Proposition 4.4. *Suppose that G is not abelian and has no elements of order 4. Then for every generating set S , there exists T of the same cardinality as S and that satisfies Condition (*).*

Proof. Since G is not abelian, every generating set S contains at least an element t outside the center and $T := (S \setminus Z(G)) \cup \{st \mid s \in S \cap Z(G)\}$ works. \square

Another way to look at Condition (*) is to forget elements of order 4 and turn our attention to squares of elements in G . The proof of the following lemma is straightforward and left to the reader.

Lemma 4.5. *Let s, g be any two elements in G such that $[s^2, g^2] \neq 1$. Then, $s^2 \neq 1$, $sg \neq gs$, $s^2 \neq g^2$ and $sgs^{-1} \neq g^{-1}$.*

Let $\text{Sq}(G)$ be the subgroup of G generated by $\{g^2 \mid g \in G\}$. This is a fully characteristic subgroup of G (invariant under all endomorphisms of G). As a corollary of the last lemma, we have

Corollary 4.6. *Let G be a group and S a generating set. If*

$$S^2 \cap Z(\text{Sq}(G)) \subseteq \{1\}. \quad (\ddagger)$$

then S satisfies Condition ().*

Since the center of a group is characteristic, we have that $Z(\text{Sq}(G))$ is an abelian and characteristic subgroup of G . This implies the followings

Proposition 4.7. *Let G be a group without non-trivial abelian characteristic subgroup (for example a non-abelian characteristically simple group). Then every generating set S satisfy Condition (*).*

We now compare the relative strength of our various prerigidity criterions, with a special attention to the 13 exceptional finite groups that are in Class II but not generalized dicyclic nor abelian with an element of order greater than 2.

1. $(\mathbf{Z}/2\mathbf{Z})^2$, $(\mathbf{Z}/2\mathbf{Z})^3$ and $(\mathbf{Z}/2\mathbf{Z})^4$ (abelian groups of exponent 2), [10];
2. $D_{2,3}$, $D_{2,4}$ and $D_{2,5}$ (dihedral groups of order 6, 8 and 10), [21];
3. A_4 (the alternating group on 4 elements), [23];
4. $H_1 = \langle a, b, c \mid a^2 = b^2 = c^2 = 1, abc = bca = cab \rangle = \text{SD}_{16}$ (the semi-dihedral group of order 16), [23];
5. $H_2 = \mathbf{Z}/8\mathbf{Z} \rtimes \mathbf{Z}/2\mathbf{Z}$, [17];
6. $H_3 = (\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}) \rtimes \mathbf{Z}/2\mathbf{Z}$, [23];
7. $H_4 = \text{UT}(3, 3) = \left\{ \left(\begin{array}{ccc|c} 1 & x & y & \\ 0 & 1 & z & \\ 0 & 0 & 1 & \end{array} \right) \mid x, y, z \in \mathbf{Z}/3\mathbf{Z} \right\}$, [17];
8. $Q_8 \times \mathbf{Z}/3\mathbf{Z}$ and $Q_8 \times \mathbf{Z}/4\mathbf{Z}$, [22].

Table 1: The 13 exceptional finite groups. All of them are neither generalized dicyclic group nor abelian of exponent greater than 2, but still do not admit any GRR.

By Lemma 4.2 and Corollary 4.6, if S satisfies (\dagger) or (\ddagger) it automatically satisfies Condition $(*)$, while by Proposition 4.1, if S satisfies $(*)$, there exists T such that (G, S, T) is a 1.5-strongly GRR triple. On the other hand, the study (see Subsection 4.2) of finite exceptional groups tell us that the converse of these statements are not always true. Indeed, $Q_8 \times \mathbf{Z}/4\mathbf{Z}$ has no generating set satisfying Condition $(*)$ (Lemma 4.8) despite being prerigid (Theorem 2.4). On the other hand, $Q_8 \times \mathbf{Z}/3\mathbf{Z}$ has no generating set satisfying (\ddagger) (Lemma 4.9), while $\{(i, 1), (j, 1)\}$ satisfies (\dagger) . Finally, if S satisfies (\ddagger) and G has at most 1 element of order 2, then S also satisfies (\dagger) . The proof is straightforward and let to the reader.

4.2 A special look at the 13 exceptional finite groups

Recall that for finite groups, there is 13 exceptional groups that are in Class II, but are not generalized dicyclic nor abelian with an element of order greater than 2. All of them have order at most 32. The study of these exceptional finite groups allows us to better understand the link between all the prerigidity criterions. These exceptional groups, as well as the corresponding references, are listed in Table 1.

Lemma 4.8. *No generating set of $Q_8 \times \mathbf{Z}/4\mathbf{Z}$ satisfies Condition $(*)$. On the other hand, all the 12 other exceptional groups have a generating set satisfying Condition (\dagger) and therefore Condition $(*)$.*

Proof. We begin by showing that all exceptional groups that aren't $Q_8 \times \mathbf{Z}/4\mathbf{Z}$ satisfy condition (\dagger) . The 3 abelian groups in the list, the dihedral groups, H_1 and H_3 are all generated by elements of order 2. On the other hand, A_4 , H_3 and H_4 are not abelian and do not have elements of order 4. Finally, for H_2 we

can take $\{(1, 0), (0, 1)\}$ for our generating set, while for $Q_8 \times \mathbf{Z}/3\mathbf{Z}$ we can take $\{(i, 1), (j, 1)\}$.

Now we turn our attention on $G = Q_8 \times \mathbf{Z}/4\mathbf{Z}$ and suppose that we have a generating set S satisfying Condition (*). Every generating set of G contains an element of the form $s = (x, \pm 1)$. Since s is not of order 2 and S satisfies Condition (*), we have some $g = g_s = (y, n) \in G$. Such a g does not commute with s and therefore, $x \neq \pm 1$, $y \neq \pm 1$ and $xy = -yx = y^{-1}x$. But in this case, $y^2 = x^2 = -1$. Since we also have $g^2 \neq s^2$, this forces n to be either 0 or 2. But then, $sgs^{-1} = (xyx^{-1}, n) = (y^{-1}, -n) = g^{-1}$ which contradicts our assumption on g . \square

Lemma 4.9. *Among the 12 finite groups that don't have a GRR but admits a generating set satisfying Condition (*), H_2 and $Q_8 \times \mathbf{Z}/3\mathbf{Z}$ are the only ones that don't admit a generating set satisfying condition (†).*

Proof. As said in the last lemma, 8 of these 12 groups are generated by elements of order 2 and hence automatically satisfy (†), while direct computations give us $Z(\text{Sq}(A_4)) = \{1\}$. For H_4 we have that $Z(\text{Sq}(H_4)) = \langle E_{1,3} \rangle$, where $E_{1,3}$ is the elementary matrix with 1 on the diagonal and one 1 in position (1, 3). It is thus possible to take $S = \{E_{1,2}, E_{2,1}, E_{1,2}E_{1,3}E_{2,1}\}$ as a generating set of H_4 .

On the other hand, the groups H_2 , and $Q_8 \times \mathbf{Z}/3\mathbf{Z}$ both have $\{1\} \neq \text{Sq}(G)$ abelian and cannot be generated by elements of order 2. \square

Finally, Theorem 2.8 and its proof give us a sufficient condition on the order of elements of a prerigid group G to ensure that G has a GRR. This condition is given in term of $\tilde{F}(|S|)$, where \tilde{F} is an explicit function and S a prerigid generating set. On the other hand, Theorem 2.4 and the existence of the finite exceptional groups show that prerigidity alone does not implies the existence of a GRR. Moreover, this can be used to give some necessary conditions on the order of elements of G to insure the existence of a GRR. In particular, we have $\tilde{F}(2) > 5$ (given by $D_{2,5}$), $\tilde{F}(3) > 8$ (given by H_1) and $\tilde{F}(6) > 12$ (given by $Q_8 \times \mathbf{Z}/3\mathbf{Z}$).

5 Strongly rigid triples

The aim of this section is to give a proof of Theorem 2.8, as well as of Proposition 2.11 and Theorem 2.12. We begin by proving two lemmas on triangles in Cayley graphs. These lemmas are strongly inspired by Lemmas 9.2 and 9.3 of [20]. The main difference is that we only require the group G to have an element of large enough order, and not necessarily of infinite order. Observe that an imprecise form of this result was already announced in [20], but without an actual proof.

Contrary to the two preceding sections, all groups in this section are finitely generated and all generating sets under considerations are finite.

5.1 The key lemmas

Lemma 5.1. *Let $S \subseteq G \setminus 1$ be a finite symmetric generating set. Suppose that G has an element of order o , with*

$$\begin{cases} o \geq 2(2|S|^2 + 3|S| - 2)^2(2|S|^2 + 2|S|) & \text{if } o \text{ is odd} \\ o \geq F(|S|) = 2(2|S|^2 + 3|S| - 2)^2(2|S|^2 + 4|S| - 1) & \text{otherwise.} \end{cases} \quad (1)$$

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

[(a)]

1. $\Delta := S' \setminus S$ has at most 4 elements;
2. $\Delta \cap \{s^2 \mid s \in S\} = \emptyset$;
3. $N_3(s, S') \leq 6$ for all $s \in \Delta$;
4. $N_3(s, S') = N_3(s, S)$ for all $s \in S \setminus \{s_0, s_0^{-1}, s_0^2, s_0^{-2}\}$;
5. the pair $(N_3(s_0, S') - N_3(s_0, S), N_3(s_0^2, S') - N_3(s_0^2, S))$ belongs to

$$\begin{cases} \{(2, 0), (4, 0)\} & \text{if } s_0 \text{ has order 2} \\ \{(1, 1), (2, 2), (3, 3)\} & \text{if } s_0 \text{ has order 3} \\ \{(1, 0), (2, 0), (2, 2)\} & \text{if } s_0 \text{ has order 4} \\ \{(1, 0), (2, 0), (2, 1)\} & \text{if } s_0 \text{ has order } \geq 5. \end{cases}$$

Moreover, the value of $(N_3(s_0, S') - N_3(s_0, S), N_3(s_0^2, S') - N_3(s_0^2, S))$ is the same for all finite generating sets S containing s_0 and s_0^2 and satisfying (1).

If s_0 is not of order 2 and G has an element of order o , with

$$\begin{cases} o \geq 2(2|S|^2 + 3|S| - 2)^2(2|S|^2 + 2|S|) & \text{if } o \text{ is odd} \\ o \geq \check{F}(|S|) = 4(2|S|^2 + 3|S| - 2)^2|S|(|S| + 2) & \text{otherwise.} \end{cases} \quad (2)$$

then it is even possible to find S' as above and such that $S' \setminus S$ contains no involution.

Proof. Let γ be the element of large order given in the hypothesis and $\Delta_n := \{\gamma^n, \gamma^{-n}, s_0^{-1}\gamma^n, \gamma^{-n}s_0\}$. We will show that there exists an n such that $S' = S'_n := S \cup \Delta_n$ works. Observe that for all n , the set S'_n satisfies Condition 1 of the lemma.

Suppose that n is such that

$$|\gamma^n|_S \geq 3 \quad (3)$$

$$|s_0^{-1}\gamma^n|_S \geq 3 \quad (4)$$

$$\gamma^{2n} \notin S \cup s_0S \quad (5)$$

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

Before going further in our analysis, we record that the number of $1 \leq n < \text{order}(\gamma)$ such that one of the conditions (3)–(5) does not hold is at most $2(|S|^2 + |S| - 1)$. Moreover, if $\text{order}(\gamma)$ is odd or if $n \leq \frac{1}{2} \text{order}(\gamma)$, then there are at most $2|S|^2 - 1$ such n . Indeed, Condition (3) means that γ^n (which is different from 1) avoids elements of length 1 or 2 and there are at most $|S|^2$ such elements. If Condition (3) holds, it implies that $s_0^{-1}\gamma^n$ is of S -length at least 2, therefore it is enough to avoid $(|S| - 1)^2$ new elements (the number of reduced S -words s_1s_2 of length 2 such that $s_0s_1s_2$ has length 3) to ensure that Condition (4) also holds. Finally, there are at most $2(2|S| - 1)$ values of $n < \text{order}(\gamma)$ such that Condition (5) fails. In fact, if $\text{order}(\gamma)$ is odd, or if $n \leq \frac{1}{2} \text{order}(\gamma)$, there is

Possible elements of $\Delta_n \cap s\Delta_n$	Occurs if
$\gamma^n = ss_0^{-1}\gamma^n$	$s = s_0$
$s_0^{-1}\gamma^n = s\gamma^n$	$s = s_0^{-1}$
$\gamma^{-n}s_0 = s\gamma^{-n}$	$s = \alpha_n(s_0)$
$\gamma^{-n} = s\gamma^{-n}s_0$	$s = \alpha_n(s_0)^{-1}$
$\gamma^{-n}s_0 = s\gamma^n$	$s = \beta_n(s_0)$
$\gamma^n = s\gamma^{-n}s_0$	$s = \beta_n(s_0)^{-1}$
$\gamma^{-n}s_0 = ss_0^{-1}\gamma^n$	$s = \beta_n(s_0)s_0$
$s_0^{-1}\gamma^n = s\gamma^{-n}s_0$	$s = (\beta_n(s_0)s_0)^{-1}$

Table 2: Possible elements of $\Delta_n \cap s\Delta_n$.

only $2|S| - 1$ values of $n < \text{order}(\gamma)$ such that Condition (5) fails. This almost gives the claim, as $|S|^2 + (|S| - 1)^2 + 2(2|S| - 1) = 2|S|^2 + 2|S| - 1$. One gains 1 by noticing that the (possible) n such that $\gamma^n = s_0$ was counted twice: once to ensure Condition (3) and once to ensure Condition (5).

Also, for an n satisfying Conditions (3) to (5), S'_n automatically satisfies Condition 2. Moreover, in the Cayley graph of G relative to S'_n , a triangle with a side labelled by $s \in \Delta_n$ has at least another side in Δ_n , otherwise s would have S -length at most 2. This implies that any $s \in \Delta_n$ belongs to at most 6 triangles in $\text{Cay}(G, S'^{\pm})$, which is Condition 3. Indeed, since the Cayley graph is simple, any triangle is uniquely determined by two edges. If one edge e is labeled by $s \in \Delta_n$, there is at most three possibilities to put an edge labeled by $s^{-1} \neq t \in \Delta_n$ at each extremities of e , thus giving a maximum number of $2 \cdot 3 = 6$ triangles containing e . This also shows that for any $s \in S$ we have

$$N_3(s, S'_n) - N_3(s, S) = |\{t \in \Delta_n \mid s^{-1}t \in \Delta_n\}| = |\Delta_n \cap s\Delta_n|$$

We now turn our attention on the set $\Delta_n \cap s\Delta_n$. Its cardinality is equal to the number of pairs $(u, v) \in \Delta_n$ such that $u = sv$. By replacing u and v by the words $\gamma^n, \gamma^{-n}, s_0^{-1}\gamma^n$ and $\gamma^{-n}s_0$, this gives us 16 equations in the group. Among these 16 equations, 4 imply that $s = 1$ and 4 that γ^{2n} belongs to $S \cup s_0S$, which is impossible if n satisfies Conditions (3) to (5). The 8 remaining equations for elements of $\Delta_n \cap s\Delta_n$ are shown in Table 2, where $\alpha_n(g) := \gamma^{-n}g\gamma^n$ and $\beta_n(g) := \gamma^{-n}g\gamma^{-n}$. Observe that α and β give two actions of $\mathbf{Z}/\text{order}(\gamma)\mathbf{Z}$ on G (viewed as a set) and that $\gamma^{-n}s_0$ (and $s_0^{-1}\gamma^n$) is an involution if and only if $\beta_n(s_0) = s_0^{-1}$. Let A , respectively B , denotes the size of the orbit of s_0 under α , respectively β and let $M < \sqrt{\frac{\text{order}(\gamma)}{2}}$ be an integer to be specified later. If $A \cdot B \leq \frac{\text{order}(\gamma)}{2}$, there exists $n \leq A \cdot B$ such that $\gamma^{-n}s_0\gamma^n = s_0 = \gamma^{-n}s_0\gamma^{-n}$ which implies that $\gamma^{2n} = 1$. But in this case we would have $2n \geq \text{order}(\gamma) \geq 2AB > 2n$ which is absurd. This implies in particular that at least one of A or B is (strictly) greater than M , leaving us with 3 cases.

Case 1 Both A and B are greater than M . If n is such that $\alpha_n(s_0), \beta_n(s_0)$ and $\beta_n(s_0)s_0$ all do not belong to S , then $\Delta_n \cap s\Delta_n$ contains at most 2 elements:

γ^n if $s = s_0$ and $s_0^{-1}\gamma^n$ if $s = s_0^{-1}$. This implies Condition 4 and that the pair $(N_3(s_0, S') - N_3(s_0, S), N_3(s_0^2, S') - N_3(s_0^2, S))$ is equal to $(2, 0)$ if s_0 has order 2, $(1, 1)$ if s_0 has order 3 and $(1, 0)$ otherwise. Moreover, neither γ^n nor $\gamma^{-n}s_0$ are involutions since $2n \leq 2M < \text{order}(\gamma)$ and $\beta_n(s_0)$ is not in S . We now prove that an n satisfying the above conditions as well as Conditions (3) to (5) always exists if M and the order of γ are large enough. Conditions (3) to (5) and the above forbid some $1 \leq n \leq M$. As already explained, since $n \leq M \leq \frac{1}{2} \text{order}(\gamma)$, Conditions (3) to (5) forbids at most $2|S|^2 - 1$ values of n . On the other hand, all the $(\alpha_n(s_0))_{n=1}^M$ are distinct and distinct from s_0 , so the condition $\alpha_n(s_0) \notin S$ forbids at most $|S| - 1$ values. The same is true for $(\beta_n(s_0))_{n=1}^M$, and the condition for $(\beta_n(s_0)s_0)_{n=1}^M$ forbids at most $|S|$ values. Therefore, if both A and B are greater than M , then the number of $n \leq M$ such that S'_n does not work is at most $2|S|^2 + 3|S| - 3$. This implies that there exists n such that the conclusion of the lemma holds as soon as $M \geq 2|S|^2 + 3|S| - 2$.

Case 2 If $A \leq M$ and $B > M$. This time we shall take $n \leq B$ such that n is a multiple of A , it satisfies Conditions (3) to (5) and both $\beta_n(s_0)$ and $\beta_n(s_0)s_0$ do not belongs to S , in particular $\gamma^{-n}s_0$ is not an involution. For such an n , the set $\Delta_n \cap s\Delta_n$ contains at most 4 elements: γ^n and $s\gamma^{-n}$ if $s = s_0$ and γ^{-n} and $s\gamma^n$ if $s = s_0^{-1}$. This implies Condition 4 and that the pair $(N_3(s_0, S') - N_3(s_0, S), N_3(s_0^2, S') - N_3(s_0^2, S))$ is equal to $(4, 0)$ if s_0 is of order 2, $(2, 2)$ if s_0 is of order 3 and $(2, 0)$ otherwise. So we are left to justify that such an n exists. As noted above, Conditions (3) to (5) forbid at most $2(|S|^2 + |S| - 1)$ values ($2|S|^2 - 1$ if $\text{order}(\gamma)$ is odd) of $1 \leq n < B$. Similarly, the conditions $\beta_n(s_0) \notin S$ and $\beta_n(s_0)s_0 \notin S$ forbid respectively at most $|S| - 1$ and $|S|$ values, so we are done if

$$\lfloor \frac{B-1}{A} \rfloor > 2|S|^2 + 4|S| - 3,$$

for example if $\frac{B}{A} \geq 2|S|^2 + 4|S| - 1$. If we want to ensure that γ^n is not an involution, we may need to forbid one more value of n and take $\frac{B}{A} \geq 2|S|^2 + 4|S|$. Since $AB \geq \frac{\text{order}(\gamma)}{2}$, we have

$$\frac{B}{A} \geq \frac{\text{order}(\gamma)}{2A^2} \geq \frac{\text{order}(\gamma)}{2M^2}$$

Therefore, there exists a n such that the conclusion of the lemma holds if $\text{order}(\gamma) \geq 2M^2(2|S|^2 + 4|S| - 1)$. If we want to ensure that Δ contains no involution, we need to take $\text{order}(\gamma) \geq 4M^2|S|(|S| + 2)$. If we know that $\text{order}(\gamma)$ is odd, then it is enough to have $\text{order}(\gamma) \geq 4M^2|S|(|S| + 1)$.

Case 3 If $A \geq M$ and $B < M$. Similarly to Case 2, we take $n < A$ a multiple of B satisfying Conditions (3) to (5) and that $\alpha_n(s_0) \notin S$. Since $\beta_n(s_0) = s_0$, $\gamma^{-n}s_0$ is an involution if and only if s_0 is an involution. Such an n exists as soon as $\text{order}(\gamma) \geq 2M^2(2|S|^2 + 3|S| - 1)$ and if moreover $\text{order}(\gamma) \geq 2M^2|S|(2|S| + 3)$ and s_0 is not of order 2 it is possible to ensure that Δ contains no involution (it is enough to have $\text{order}(\gamma) \geq 4M^2|S|(|S| + \frac{1}{2})$ if $\text{order}(\gamma)$ is odd). In this case $\Delta_n \cap s\Delta_n$ contains at most 4 elements: γ^n and $s\gamma^n$ if $s \in \{s_0, s_0^{-1}\}$, $\gamma^{-n}s_0$ if $s = s_0^2$ and $s_0^{-1}\gamma^n$ if $s = s_0^{-2}$. This implies Condition

4 and that $(N_3(s_0, S') - N_3(s_0, S), N_3(s_0^2, S') - N_3(s_0^2, S))$ is equal to $(2, 0)$ if s_0 is of order 2, $(3, 3)$ if s_0 is of order 3, $(2, 2)$ if s_0 is of order 4 and $(2, 1)$ otherwise. The only case that need explication is when s_0 is of order 4. In this case, $(N_3(s_0, S') - N_3(s_0, S), N_3(s_0^2, S') - N_3(s_0^2, S))$ is equal to $(2, 1)$ if $s_0^{-1}\gamma^n = \gamma^{-n}s_0$ and $(2, 2)$ otherwise. But since we took n as a multiple of B , we have $s_0 = \beta_n(s_0) = \gamma^{-n}s_0\gamma^{-n}$ which forbids the case $(2, 1)$.

In all of the 3 cases, we can always find an n such that the conclusion of the lemma holds as soon as $M \geq 2|S|^2 + 3|S| - 2$ and $\text{order}(\gamma) \geq 2M^2(2|S|^2 + 4|S| - 1)$ ($\text{order}(\gamma) \geq 4M^2|S|(|S| + 2)$ if we want no involutions in Δ). It is thus sufficient to have $\text{order}(\gamma) \geq 2(2|S|^2 + 3|S| - 2)^2(2|S|^2 + 4|S| - 1)$ ($4|S|(|S| + 2)(2|S|^2 + 3|S| - 2)^2$ if we want no involutions in Δ), or even $\text{order}(\gamma) \geq 4(2|S|^2 + 3|S| - 2)^2(|S|^2 + |S|)$ if $\text{order}(\gamma)$ is odd.

Moreover, by construction the value of $(N_3(s_0, S') - N_3(s_0, S), N_3(s_0^2, S') - N_3(s_0^2, S))$ only depends on A and B , which in turn depend on s_0 and γ only. \square

Recall that for $S \subset G \setminus \{1\}$ a finite symmetric set, we have

$$|S^*| = \frac{1}{2}|\{s \in S \mid s^2 \neq 1\}| + |\{s \in S \mid s^2 = 1\}|$$

the number of equivalence classes in S for the equivalence relation $s \sim t$ if $t \in \{s, s^{-1}\}$. In particular, $|S^*|$ is the size of the minimal T such that $T^\pm = S$.

Lemma 5.2. *Recall that $F(n) = 2(2n^2 + 3n - 2)^2(2n^2 + 4n - 1)$ and $\check{F}(n) = 4(2n^2 + 3n - 2)^2(n + 2)n$. Let $S \subseteq G \setminus 1$ be a finite generating set. Suppose that G has an element of order at least $F(15p + 28q + 2p^2 + 4pq + 2q^2 - 4)$ where p is the number of elements of order 2 of S and q is half the number of elements of order at least 3 of S^\pm . Then there exists a finite symmetric generating set $S \subseteq \tilde{S} \subseteq G \setminus 1$ of size bounded by $15p + 28q + 2p^2 + 4pq + 2q^2$ such that for all $s \in S$ and $t \in \tilde{S}$, if $N_3(s, \tilde{S}) = N_3(t, \tilde{S})$ then $t = s$ or $t = s^{-1}$.*

If S has no elements of order 2 and G has an element of order at least $\check{F}(2|S^|^2 + 28|S^*| - 4) = \check{F}(\frac{1}{2}|S^\pm|^2 + 14|S^\pm| - 4)$, then there exists a finite symmetric generating set $S \subseteq \tilde{S} \subseteq G \setminus 1$ with no elements of order 2, of size bounded by $\frac{1}{2}|S|^2 + 14|S|$ such that for all $s \in S$ and $t \in \tilde{S}$, if $N_3(s, \tilde{S}) = N_3(t, \tilde{S})$ then $t = s$ or $t = s^{-1}$.*

Before proving the lemma, we attire the attention of the reader that for a general S we have $15p + 28q + 2p^2 + 4pq + 2q^2 = 2|S^*|^2 + 28|S^*| - 13p = 2|S^*|^2 + 14|S^\pm| - 2q$. Depending on what is known on S , one bound may be better than the other.

Proof. To prove the first assertion, it is enough that all elements of S belong to at least 7 \tilde{S} -triangles (to distinguish them from the newly added elements which will belong to at most 6 \tilde{S} -triangles) and that the numbers $N_3(s^{\pm 1}, \tilde{S})$ for s in S are all distincts. In order to do that, we will apply several times Lemma 5.1 to elements of S in order to augment the number of triangles to which they belong. This will give us a sequence of generating sets $S^\pm = S_0 \subseteq S_1 \subseteq \dots \subseteq S_k = \tilde{S}$ where $S_{i+1} = S'_i$ and k is the total number of times we apply Lemma 5.1. Therefore, we need an element of order at least $F(|S_{k-1}|)$. On the other hand, since each application of Lemma 5.1 adds at most 4 elements, we also have

$|S_{k-1}| \leq |S^\pm| + 4(k-1)$. It is thus enough to determine k to finish the proof. Finally, we use the fact that $p+q = |S^*|$ while $p+2q = |S^\pm|$.

The proof of the second assertion is similar except for the fact that $|S^\pm| = 2q$ while $|S^*| = q$ and that we need to use the function \tilde{F} instead of the function F in Lemma 5.1 to ensure that we do not add elements of order 2 to S .

Lemma 5.1 tells us that we can augment the number of triangles to which $s \in S^\pm$ and s^{-1} belong, without changing the number of triangles for other $t \in S^\pm$, except maybe for $t \in \{s^2, s^{-2}\}$. Moreover, in doing that, the new elements we add to S^\pm belong to at most 6 triangles at the moment they are added, and they cannot belong to more than 6 later in process as they are never of the form $s^{\pm 2}$ for $s \in S$.

To be more precise, we define a directed graph (V, \vec{E}) as follows. The vertices are the equivalence classes of elements of S^\pm modulo the equivalence $s \sim t$ if $t = s$ or $t = s^{-1}$, so $|V| = |S^*| = p+q$. There is a directed edge $([s] \rightarrow [t])$ from the class of s to the class of t if $[t] \neq [s]$ and if, when applied to $s_0 = s$, the generating set S' given by Lemma 5.1 satisfies $N_3(t, S') - N_3(t, S^\pm) > 0$. Note that this implies that $[t] = [s^2]$. Moreover, by the last statement in Lemma 5.1, each time we use Lemma 5.1 with s , to go from S_i to S_{i+1} , for $t \in S_i$ we have $N_3(t, S_{i+1}) - N_3(t, S_i) = N_3(t, S') - N_3(t, S^\pm)$, which is positive if and only if $[t] = [s]$ or $([s] \rightarrow [t]) \in \vec{E}$.

An important observation at this point is that (as in every directed graph with out-degree bounded by 1) the vertex set V can be partitioned as $V = \{[s_1], \dots, [s_r]\} \sqcup C_1 \sqcup \dots \sqcup C_m$ where the C_i are cycles and $F = \{[s_1], \dots, [s_r]\}$ is a forest: there is no edge from $[s_i]$ to $[s_j]$ for $j < i$. In particular if we apply Lemma 5.1 to s_i , this will not change the value of $N_3(s_j, \cdot)$ for $j < i$.

Initialization We first need to ensure that every $s \in S^\pm$ belongs to at least 7 triangles. This can be done by applying at most $4p + 7q$ times Lemma 5.1. Indeed for every $s \in S^\pm$, each application of Lemma 5.1 adds at least 1 triangle to both s and s^{-1} if s is of order at least 3 and at least 2 triangles if s is of order 2.

The forest We then deal with the elements $s_1, \dots, s_r \in S$. Assume that, for some $1 \leq j < r$, we have constructed a finite generating set \tilde{S}_j containing S with the following two properties:

- every $s \in S$ belongs to at least 7 triangles,
- $N_3(s_i, \tilde{S}_j) \neq N_3(s_{i'}, \tilde{S}_j)$ for every $i \neq i' \leq j$.

If $N_3(s_{j+1}, \tilde{S}_j) \notin \{N_3(s_i, \tilde{S}_j) : i \leq j\}$ we can put $\tilde{S}_{j+1} = \tilde{S}_j$ and we are done for $j+1$. Otherwise, we apply Lemma 5.1 several times with s_{j+1} , until the number of triangles for s_{j+1} is different than for all s_i with $i \leq j$. The number of applications of the Lemma is necessarily bounded by j , as each application increases the number of triangles for s_{j+1} , but not for s_i with $i \leq j$. On the other hand, for $j = 1$ we have just proved the existence of such \tilde{S}_1 obtained from S after at most $4p + 7q$ applications of the lemma. So at the end, we obtain a generating set \tilde{S}_r satisfying the above property after applying in total less than $k_f := 4p + 7q + \sum_{j=0}^{r-1} j$ times Lemma 5.1.

The cycles Finally, we have to treat the cycles separately. Assume that, for some $0 \leq j < m$, we have obtained a generating set \tilde{S}_{r+j} containing \tilde{S}_r such that $N_3(\cdot, \tilde{S}_{r+j})$ is injective on $F \sqcup C_1 \sqcup \dots \sqcup C_j$.

Denote by M_j the cardinality of $F \sqcup C_1 \sqcup \dots \sqcup C_j$, and let $c_{j+1} = |C_{j+1}| = M_{j+1} - M_j$. Without loss of generality, we may suppose that $c_1 \leq \dots \leq c_m$. Let $s \in S$ such that $[s] \in C_{j+1}$. Its order is at least 5, and $C_{j+1} = \{[s], [s^2], \dots, [s^{2^{c_{j+1}-1}}]\}$, with $s^{2^{c_{j+1}}} = s^{\pm 1}$. By inspecting the conclusion 5 of Lemma 5.1 and recalling the definition of the graph (V, \vec{E}) , we observe that each application of the lemma for s increases the number of triangles for s by 2 and for s^2 by 1.

If $c_{j+1} = 2$, we apply the lemma for s until the number of triangle to which s belongs is different from the number for s^2 , and both are different from the number for each $[t] \in F \sqcup C_1 \sqcup \dots \sqcup C_j$. This requires at most $1 + 2M_j$ applications of the Lemma, because each application of the lemma increases by 2 the number of triangles for s , by 1 the number of triangles for s^2 and leaves unchanged the number for each $[t] \in F \sqcup C_1 \sqcup \dots \sqcup C_j$.

If $c_{j+1} > 2$, we first apply the lemma for $s^{2^{c_{j+1}-2}}$ until the number of triangle to which $s^{2^{c_{j+1}-1}}$ belongs is different from the number for each $[t] \in F \sqcup C_1 \sqcup \dots \sqcup C_j$ (and we do not care yet of $s^{2^{c_{j+1}-2}}$). This requires at most M_j applications. If $c_j > 3$, we then apply the lemma at most $M_j + 1$ times to $s^{2^{c_{j+1}-3}}$ to ensure that the number of triangles for $s^{2^{c_{j+1}-2}}, s^{2^{c_{j+1}-1}}$ and $[t] \in F \sqcup C_1 \sqcup \dots \sqcup C_j$ are all different. We go on, until we apply the lemma at most $M_j + c_{j+1} - 3$ times to s^2 so that that the number of triangles for $s^2, \dots, s^{2^{c_{j+1}-1}}$ and $[t] \in F \sqcup C_1 \sqcup \dots \sqcup C_j$ are all different. We then, as in the case $c_j = 2$, apply the lemma at most $1 + 2(M_j + c_{j+1} - 2) = (M_j + c_{j+1} - 2) + (M_j + c_{j+1} - 1)$ times and ensure that the number of triangles for $s, s^2, \dots, s^{2^{c_{j+1}-1}}$ and $[t] \in F \sqcup C_1 \sqcup \dots \sqcup C_j$ are all different. To summarize: given \tilde{S}_{r+j} we can construct the desired \tilde{S}_{r+j+1} by applying Lemma 5.1 at most

$$\begin{aligned} M_j + M_j + 1 + \dots + M_j + c_j - 2 + M_j + c_j - 1 &= \sum_{k=1}^{M_j + c_j - 1} k - \sum_{k=1}^{M_j - 1} k \\ &\leq \sum_{k=1}^{M_{j+1} - 1} k - \sum_{k=1}^{M_j - 1} k. \end{aligned}$$

For $j = m$, the generating set \tilde{S}_{r+m} satisfies that $N_3(\cdot, \tilde{S}_{r+m})$ is greater than 6 and injective on V , as requested. The total number of applications of Lemma 5.1 is bounded above by

$$4p + 7q + \sum_{k=1}^{|V|-1} k = 4p + 7q + \frac{1}{2}|V|(|V| - 1).$$

□

5.2 The general case

We now deduce Theorem 2.8 from Lemma 5.2, and from Theorem 2.4 for the undirected case. We firstly treat the directed case. We start with a generating

set S with p elements of order 2 and q of order at least 3. Then its symmetrization S^\pm has p elements of order 2 and at most $2q$ of order at least 3. We apply Lemma 5.2 to S^\pm and find a symmetric generating set \tilde{S} containing S^\pm such that for all $s \in S$ and $t \in \tilde{S}$, if $N_3(s, \tilde{S}) = N_3(t, \tilde{S})$ then $t = s$ or $t = s^{-1}$. Moreover, we have a bound on the size of \tilde{S} . Finally, let T be \tilde{S}^* , in particular T is minimal such that $T^\pm = \tilde{S}$. Observe that if S was "antisymmetric" ($S^* = S$), then it is possible to choose T containing S . Moreover, if S contained no elements of order 2 and G has an element of order sufficiently large, it is possible to take T with no elements of order 2. Now, we argue that (G, S^*, T) is a 1.5-strong DRR. If e is an arc labeled by s in $\text{Cay}(G, T)$, then all the triangles to which e belongs are already in the ball of radius 1.5. The condition on the number of triangles together with the antisymmetry of S^* imply that every automorphism of the ball of radius 1.5 fixes edges labeled by elements of S^* . If T has no elements of order 2 we have $T \cap T^{-1} = \emptyset$ which implies that $\text{Cay}(G, T)$ is an oriented regular representation.

For the undirected case, the triangles condition gives us, for $T^\pm = \tilde{S}$ as in the directed case, that the group $\text{Aut}(\text{Ball}(\text{Cay}(G, T^\pm), 2))$ is a subgroup of $\text{Aut}_{E\text{lab}}(\text{Ball}(\text{Cay}(G, S^\pm), 1.5))$, which fixes S_0 by the prerigidity assumption. Observe that the radius 2 in $\text{Cay}(G, T^\pm)$ is both sufficient and necessary to distinguish elements of $\text{Ball}(\text{Cay}(G, S^\pm), 1.5)$ by the aim of triangles. This finishes the proof of Theorem 2.8.

For the bounds of Corollary 2.10, we start with a generating set S of size $\text{rank}(G)$. Then $|S^{\leq 11}|$ is bounded by $2 \cdot 11$ if G is cyclic and otherwise by

$$\begin{aligned} 2|S| \sum_{i=0}^{10} (2|S| - 1)^i &= 2|S| \frac{(2|S| - 1)^{11} - 1}{2|S| - 2} \\ &\leq 2 \cdot 2^{11} \text{rank}(G)^{11}. \end{aligned}$$

If G has no elements of order 4 or no non-trivial abelian characteristic subgroup, then every generating set S satisfies condition (*) of Proposition 4.1. If we start with a S^* containing p_S elements of order 2 and q_S of order at least 3, the proof of Proposition 4.1 gives us T^* with $p_T \leq p_S + 2q_S$ elements of order 2 and $q_S \leq q_T \leq 3q_S$ elements of order at least 3 such that $p_T + q_T = p_S + 3q_S$ and $p_T + 2q_T \leq p_S + 6q_S$. In order to use Lemma 5.2 we need an element of order at least $F(15p_T + 28q_T + 2p_T^2 + 4p_Tq_T + 2q_T^2 - 4)$. By the above, we have

$$\begin{aligned} 2(p_T + q_T)^2 + 15p_T + 28q_T &= 2(p_S + 3q_S)^2 + 15(p_S + 3q_S) + 13q_T \\ &\leq 2(p_S + 3q_S)^2 + 15(p_S + 3q_S) + 39q_S \\ &= 2p_S^2 + 12p_Sq_S + 18q_S^2 + 15p_S + 84q_S \\ &\leq 18(p_S + q_S)^2 + 84(p_S + q_S) \end{aligned}$$

We now prove Proposition 2.11. So, let (G, S_0, S) be a 1.5-strong prerigid triple, T as above and $\psi: \text{Cay}(G, T^\pm) \rightarrow \Delta$ be a covering that is bijective on balls of radius 1.5. Such a covering induces an automorphism of the ball of radius 1.5: $\eta = \psi^{-1} \circ \psi|_{\text{Ball}_{\text{Cay}(G, T^\pm)}(1_G, 1.5)}$. Since ψ preserves the triangles and is defined everywhere, η is in $\text{Aut}_{E\text{lab}}(\text{Ball}_{\text{Cay}(G, S^\pm)}(1_G, 1.5))$ and hence fixes pointwise S_0 . In particular, for two arcs e and f in $\text{Cay}(G, T^\pm)$, if $\psi(e) = \psi(f)$ and e is labeled by an element of S_0^\pm , then e and f have same label. Therefore, the restriction of ψ to $\text{Cay}(G, S_0^\pm)$ is well-defined and a arc-labeling preserving covering on its image.

5.3 Tarski's monsters

Recall that a Tarski's monster, \mathcal{T}_p , of exponent p , is an infinite group such that every non-trivial proper subgroup is isomorphic to the cyclic group of order p . It follows easily from the definition that such a group is necessary of rank 2 and simple. On the other hand, the existence of such groups is a difficult problem. It was first solved by Ol'shanskiĭ in 1980, [18], showing that for every $p > 10^{75}$ there exist uncountably many non-isomorphic Tarski's monsters of exponent p . This bound was then lowered to $p \geq 1003$ by Adian and Lysënok, [1].

Let \mathcal{T}_p be a Tarski monster and $S = \{a, b\}$ be any generating set of size 2. Then the order of a and b is p . Moreover, the normalizer of a in \mathcal{T}_p is $\langle a \rangle$, the normalizer of b is $\langle b \rangle$ and $\langle b \rangle \cap \langle a \rangle = \{1\}$. In particular, (\mathcal{T}_p, S) satisfies the hypothesis of 2.12, except maybe for the existence of an element of order large enough. For p really big, it is possible to directly apply our general results, but it is possible to obtain a better bound than the general one. Indeed, $a^2 \neq b^2$ and $aba^{-1} \notin \{b, b^{-1}\}$, thus we can take $\{a, b, a^{-1}b\}^{\pm 1}$ for the set T used in the proof of Proposition 4.1. That is, (\mathcal{T}_p, S, T) is 1.5-strongly prerigid. We now need to apply Lemma 5.2 to $T = \{a, b, a^{-1}b\}^{\pm}$. All elements of this set are of order $p \geq 5$. Since all elements of T belong to at least 1 triangle and we do not have any elements of order 2, we need to apply Lemma 5.1 at most $k = 6 + (6 + 1) + (6 + 2) = 21$ times. In order to do that, and since Tarski's monsters contain only elements of odd order, we need an element of order at least $F'(6 + 4(k - 1)) = F'(86) = 6\,776\,965\,274\,112$, where $F'(n) = 2(2n^2 + 3n - 2)^2(2n^2 + 2n)$ is the bound given in Lemma 5.1 when we know that $\text{order}(\gamma)$ is odd. At the end, we obtain a symmetric generating set X of size at most $6 + 4k = 90$ such that $(\mathcal{T}_p, \{a, b\}^{\pm}, X^{\pm})$ satisfies the conclusion of Proposition 2.11.

Now, any covering $\psi: \text{Cay}(G, X^{\pm}) \rightarrow \Delta$ bijective on balls of radius 1.5 restricts to a arc-labeling preserving covering from $\text{Cay}(G, S^{\pm})$ to some $\tilde{\Delta}$. By [13], there is only three possibilities for such a covering. Either it is the identity, or $\tilde{\Delta}$ is a rose, or $\tilde{\Delta}$ is infinite with finite orbits. Since $\tilde{\Delta}$ is obtained from Δ by erasing all edges e such that $N_3(e, X)$ does not belong to $N_3(\{f \mid f \text{ is labelled by an element of } S^{\pm}\}, X)$, every automorphism of Δ restrict to an automorphism of $\tilde{\Delta}$. In particular, either ψ is the identity, or Δ is infinite with finite orbits, or Δ is rose. The last possibility is excluded by the fact that ψ is bijective on balls of radius 1.5.

References

- [1] S. I. Adian and I. G. Lysënok. Groups, all of whose proper subgroups are finite cyclic. *Izv. Akad. Nauk SSSR Ser. Mat.*, 55(5):933–990, 1991.
- [2] László Babai. Infinite digraphs with given regular automorphism groups. *J. Combin. Theory Ser. B*, 25(1):26–46, 1978.
- [3] László Babai. Finite digraphs with given regular automorphism groups. *Period. Math. Hungar.*, 11(4):257–270, 1980.
- [4] László Babai and Chris D. Godsil. On the automorphism groups of almost all Cayley graphs. *European J. Combin.*, 3(1):9–15, 1982.

- [5] Edward Dobson, Ademir Hujdurović, Klavdija Kutnar, and Joy Morris. On color-preserving automorphisms of Cayley graphs of odd square-free order. *J. Algebraic Combin.*, 45(2):407–422, 2017.
- [6] P. Erdős and A. Rényi, editors. *Combinatorial theory and its applications. I-III*. North-Holland Publishing Co., Amsterdam-London, 1970. *Colloquia Mathematica Societatis János Bolyai*, 4.
- [7] Chris D. Godsil. GRRs for nonsolvable groups. In *Algebraic methods in graph theory, Vol. I, II (Szeged, 1978)*, volume 25 of *Colloq. Math. Soc. János Bolyai*, pages 221–239. North-Holland, Amsterdam-New York, 1981.
- [8] D. Hetzel. *Über reguläre graphische Darstellung von auflösbaren Gruppen*. PhD thesis, Technische Universität Berlin, 1976.
- [9] Ademir Hujdurović, Klavdija Kutnar, and Dragan Marušič. Odd automorphisms in vertex-transitive graphs. *Ars Math. Contemp.*, 10(2):427–437, 2016.
- [10] Wilfried Imrich. Graphen mit transitiver Automorphismengruppe. *Monatsh. Math.*, 73:341–347, 1969.
- [11] Wilfried Imrich. On graphs with regular groups. *J. Combinatorial Theory Ser. B*, 19(2):174–180, 1975.
- [12] Wilfried Imrich and Mark E. Watkins. On automorphism groups of Cayley graphs. *Period. Math. Hungar.*, 7(3-4):243–258, 1976.
- [13] Paul-Henry Leemann. Schreier graphs: Transitivity and coverings. *Internat. J. Algebra Comput.*, 26(1):69–93, 2016.
- [14] Joy Morris and Pablo Spiga. Classification of finite groups that admit an oriented regular representation. *ArXiv e-prints*, July 2017.
- [15] Joy Morris and Pablo Spiga. Every finite non-solvable group admits an oriented regular representation. *J. Combin. Theory Ser. B*, 126:198–234, 2017.
- [16] Joy Morris and Pablo Spiga. Asymptotic enumeration of Cayley digraphs. *ArXiv e-prints*, page arXiv:1811.07709, November 2018.
- [17] Lewis A. Nowitz and Mark E. Watkins. Graphical regular representations of non-abelian groups. I, II. *Canad. J. Math.*, 24:993–1008; *ibid.* 24 (1972), 1009–1018, 1972.
- [18] A. Yu. Ol’shanskiĭ. An infinite group with subgroups of prime orders. *Izv. Akad. Nauk SSSR Ser. Mat.*, 44(2):309–321, 479, 1980.
- [19] Gert Sabidussi. On a class of fixed-point-free graphs. *Proc. Amer. Math. Soc.*, 9:800–804, 1958.
- [20] Mikael de la Salle and Romain Tessera. Characterizing a vertex-transitive graph by a large ball. *ArXiv e-prints*, 08 2015.
- [21] Mark E. Watkins. On the action of non-Abelian groups on graphs. *J. Combinatorial Theory Ser. B*, 11:95–104, 1971.

- [22] Mark E. Watkins. On graphical regular representations of $C_n \times Q$. pages 305–311. *Lecture Notes in Math.*, Vol. 303, 1972.
- [23] Mark E. Watkins. Graphical regular representations of alternating, symmetric, and miscellaneous small groups. *Aequationes Math.*, 11:40–50, 1974.
- [24] Mark E. Watkins. Graphical regular representations of free products of groups. *J. Combinatorial Theory Ser. B*, 21(1):47–56, 1976.