On the Finiteness of the Classifying Space for Virtually Cyclic Subgroups

Dissertation

zur
Erlangung des Doktorgrades (Dr. rer. nat.)
der
Mathematisch-Naturwissenschaftlichen Fakultät
der
Rheinischen Friedrich-Wilhelms-Universität Bonn

vorgelegt von

Timm Wilhelm von Puttkamer
aus
Frankfurt am Main

Bonn 2018

Angefertigt mit Genehmigung der Mathematisch-Naturwissenschaftlichen Fakultät
der Rheinischen Friedrich-Wilhelms-Universität Bonn

1. Gutachter: Prof. Dr. Wolfgang Lück

2. Gutachter: Prof. Dr. Ian J. Leary

Tag der Promotion: 25.06.2018

Erscheinungsjahr: 2018

Contents

Preface

In this thesis we mainly study finiteness properties of classifying spaces for families of subgroups. Let us recall that for a discrete group G and a family $\mathcal{F}$ of subgroups of G we say that a G-CW complex $E_{\mathcal{F}}(G)$ is a model for the classifying space for the family $\mathcal{F}$ if the fixed point set $(E_{\mathcal{F}}(G))^H$ is contractible if $H \in \mathcal{F}$ and empty otherwise. For example, if we choose the family consisting only of the trivial subgroup, then the corresponding classifying space is the universal cover of the Eilenberg-MacLane space $K(G,1)$. Two other important choices for families of subgroups are $\mathcal{F}in$, the family of finite subgroups, and $\mathcal{VC}yc$, the family of virtually cyclic subgroups. The corresponding classifying spaces $E_{\mathcal{F}in}(G) = \underline{E}G$ resp. $E_{\mathcal{VC}yc}(G) = \underline{\underline{E}}G$ play an important role in the formulation of the Baum-Connes resp. the Farrell-Jones conjecture. For example, the latter conjecture predicts that the algebraic K-theory of a group ring can be computed by an equivariant homology theory evaluated on the space $\underline{\underline{E}}G$. It is thus an interesting question whether a group admits a finite-dimensional or finite classifying space $\underline{\underline{E}}G$. Although there are large classes of groups which have a finite-dimensional classifying space $\underline{\underline{E}}G$, the quest of finding finite models for $\underline{\underline{E}}G$, apart from trivial examples, has proven elusive. In 2006 Juan-Pineda and Leary [JL06] formulated:

Conjecture. A group G admits a finite model for $\underline{\underline{E}}G$ if and only if G is virtually cyclic.

Juan-Pineda and Leary were able to verify their conjecture for abelian and hyperbolic groups and since then no counterexample to their conjecture has been found. One goal of this thesis lies in verifying the conjecture for an extensive class of groups. As it turns out, most proofs work by examining whether a given group has the so-called BVC property. The latter property for a group G says that there are only finitely many virtually cyclic subgroups $V_1, \ldots, V_n$ of G such that any virtually cyclic subgroup of G is conjugate to a subgroup of one of the V_i. Heuristically, this means that G has only finitely many conjugacy classes of maximal virtually cyclic subgroups. It is not hard to see that a group G has a model for $\underline{\underline{E}}G$ with finite 0-skeleton if and only if G has the BVC property. In a large part of this thesis we shall study the BVC property or rather a weaker, but more flexible variant of this property that we call $b\mathcal{VC}yc$. For a group G and a family of subgroups $\mathcal{F}$ of G, we say that G has $b\mathcal{F}$ if there are finitely many subgroups $H_1, \ldots, H_n$ of G lying in $\mathcal{F}$ such that any *cyclic* subgroup is conjugate to a subgroup of one of the H_i.

We prove that HNN extensions of finitely generated free groups and one-relator groups have $b\mathcal{VC}yc$ if and only if they are virtually cyclic, thereby resolving the aforementioned conjecture for these classes of groups. Moreover, we shall establish a connection between the $b\mathcal{VC}yc$ property and the conjugacy growth function for finitely generated groups under the assumption that cyclic subgroups are undistorted. Namely, we prove that a finitely generated group with $b\mathcal{VC}yc$ whose cyclic subgroups are undistorted has at most linear conjugacy growth. As an application we succeed in proving that finitely generated linear groups and certain CAT(0) groups have $b\mathcal{VC}yc$ only if they are virtually cyclic.

After these positive results we provide constructions of groups that elucidate some of the non-intuitive behavior of the $b\mathcal{VC}yc$ property. For example, we will construct a finitely generated torsion-free group $G = H \rtimes \mathbb{Z}$ such that G has $b\mathcal{VC}yc$ but H does not. We also provide an example of a finitely generated group with $b\mathcal{VC}yc$ that has exponential conjugacy growth, which shows that the assumption on the cyclic subgroups being undistorted is necessary in the aforementioned theorem.

For the class of residually finite groups, we will provide some evidence why the conjecture of Juan-Pineda and Leary might hold. In fact, we conjecture that a residually finite group with $b\mathcal{VC}yc$ or $b\mathcal{C}yc$ is already virtually cyclic. Since finitely generated linear and ascending HNN extensions of finitely generated free groups are residually finite, resolving this conjecture would also yield alternative proofs for these classes of groups. Suppose G is a residually finite group with $b\mathcal{C}yc$, i.e. there are n cyclic subgroups $V_1, \ldots, V_n$ of G such that any cyclic subgroup of G is conjugate to a subgroup of one of the V_i. Then any finite quotient of G has at most n conjugacy classes of maximal cyclic subgroups. We will almost classify the finite groups with only two conjugacy classes of maximal cyclic subgroups. In particular, we will show that such groups are solvable of derived length at most 4. This result implies that a residually finite group with $b\mathcal{C}yc$ as above with $n \leq 2$ is virtually cyclic.

After having studied finiteness properties of the space $\underline{\underline{E}}G$, we will provide results on the homotopy type of the quotient space $\underline{\underline{B}}G = \underline{\underline{E}}G/G$. Juan-Pineda and Leary asked whether $\underline{\underline{B}}G$ being homotopy equivalent to a finite CW complex implies that $\underline{\underline{B}}G$ is already contractible. We will answer this question affirmatively for abelian groups and poly-$\mathbb{Z}$-groups. For abelian groups we will show that $H_2(\underline{\underline{B}}G; \mathbb{Z})$ is not finitely generated unless G is locally virtually cyclic.

Finally, we study two inheritance properties for the Farrell-Jones conjecture. It is known that the Farrell-Jones conjecture has an inheritance property for finite products, i.e. if two groups G_1 and G_2 satisfy the conjecture, then so does their direct product $G_1 \times G_2$. One might ask whether a corresponding inheritance property still holds for infinite direct products. Another question, popularized by Wolfgang Lück, is, whether for any group there exists a minimal family, possibly different from the family of virtually cyclic subgroups, with respect to which the Farrell-Jones conjecture holds. We will show that these two properties, formulated suitably, actually turn out to be equivalent.

Parts of the results in the first four chapters have already been published in [vW] and [vW17] in joint work with Xiaolei Wu, sometimes with slightly different notions and proofs. For example, in this thesis we consistently work with the $b\mathcal{VC}yc$ instead of the BVC property. Also, we provide some alternative proofs e.g. for CAT(0) groups using the notion of conjugacy growth.

Acknowledgments. First and foremost I would like to thank my advisor Wolfgang Lück for his continued support and for giving me the opportunity to work on this project. I am indebted to Xiaolei Wu with whom I had numerous discussions about mathematics and who taught me a lot about carrying out a research project successfully. Moreover, I would like to thank Denis Osin for providing help in understanding some of his proofs on relatively hyperbolic groups. I am also thankful to Enrico Jabara for discussions on a proof in one of his papers.

Last but not least I want to express my gratitude towards the Bonn International Graduate School and the International Max Planck Research Schools of the Max Planck Society for their support.

1. Classifying Spaces for Families of Subgroups

In this chapter we introduce classifying spaces for families of subgroups, discuss their basic properties and highlight previous work. We recall their finiteness properties and the main conjecture due to Juan-Pineda and Leary that this thesis will come back to repeatedly.

Definition 1.0.1. A *family of subgroups* $\mathcal{F}$ of a group G is a nonempty subset of the set of all subgroups of G that is closed under conjugation and forming subgroups.

Examples 1.0.2. The following list gives some families of subgroups one commonly encounters.

- $\mathcal{T}r$: the family containing only the trivial subgroup
- $\mathcal{F}in$: the family of finite subgroups
- $\mathcal{C}yc$: the family of cyclic subgroups
- $\mathcal{VC}yc$: the family of virtually cyclic subgroups
- $\mathcal{A}ll$: the family of all subgroups

For a type of family like $\mathcal{F}in$, $\mathcal{VC}yc$, etc. we sometimes want to explicitly specify the group the family is to be taken with respect to. For example, to indicate that we consider the family of finite subgroups of the group G, we will use the notation $\mathcal{F}in(G)$.

Definition 1.0.3. Given a group G and a family $\mathcal{F}$ of subgroups of G we call a G-CW complex $E_{\mathcal{F}}(G)$ a model for the *classifying space for the family* $\mathcal{F}$ if the set of fixed points $(E_{\mathcal{F}}(G))^H$ is contractible if $H \in \mathcal{F}$ and empty otherwise.

Alternatively, the space $E_{\mathcal{F}}(G)$ can be characterized as the terminal object in the G-homotopy category of G-CW-complexes whose isotropy groups are contained in $\mathcal{F}$ (see [Lüc05, Definition 1.8]). In other words, for any G-CW-complex X whose isotropy groups lie in $\mathcal{F}$ there exists a G-map $X \to E_{\mathcal{F}}(G)$ which is unique up to G-homotopy. For any group G and any family $\mathcal{F}$ of subgroups of G there exists a classifying space $E_{\mathcal{F}}(G)$ [Lüc05, Theorem 1.9]. There are also definitions for the classifying space for a family of subgroups that are applicable if G is a topological group and not just discrete. However, since we will only deal with discrete groups, Definition 1.0.3 suffices for our purposes. It is customary to abbreviate $E_{\mathcal{F}}(G)$ by $\underline{\underline{E}}G$ for $\mathcal{F} = \mathcal{VC}yc$ the family of virtually cyclic subgroups, $\underline{E}G$ for $\mathcal{F} = \mathcal{F}in$ the family of finite subgroups and EG for $\mathcal{F} = \mathcal{T}r$ the family consisting only of the trivial subgroup. The space $\underline{E}G$ is also sometimes called the *classifying space for proper actions.*

The spaces $\underline{E}G$ resp. $\underline{\underline{E}}G$ play an important role in the formulation of the Baum-Connes resp. the Farrell-Jones conjecture. For example, the Farrell-Jones conjecture predicts that a certain G-homology theory evaluated on the space $\underline{\underline{E}}G$ computes the algebraic K-theory of a group ring of G. But classifying spaces for families have also other applications, e.g. one can sometimes compute the group homology of G by relating the spaces EG and $\underline{E}G$ and finding a nice model for the latter space.

Since any family contains the trivial subgroup, one sees from Definition 1.0.3 that any classifying space $E_{\mathcal{F}}(G)$ is necessarily contractible.

Examples 1.0.4. (1) Consider the real numbers $\mathbb{R}$ with the standard $\mathbb{Z}$-action by translations. Since this action is free, $\mathbb{R}$ is a model for $E\mathbb{Z}$. As $\mathbb{Z}$ is torsion-free, it also follows that $\underline{E}\mathbb{Z} = \mathbb{R}$.

(2) The space S^∞, equipped with the antipodal $\mathbb{Z}/2$-action, is a model for the trivial family, since S^∞ is contractible.

(3) The reals $\mathbb{R}$ are a classifying space for the family of finite subgroups of the infinite dihedral group D_∞ acting in the standard way. Any nontrivial finite subgroup of $D_\infty = \langle a, b \mid a^2 = 1, aba^{-1} = b^{-1} \rangle$ is cyclic of the form $\langle ab^n \rangle$ for some $n \in \mathbb{Z}$. The involution ab^n acts on $\mathbb{R}$ via $x \mapsto -(x+n)$ with the single fixed point $-n/2$.

(4) The space consisting of a single point is a classifying space for the family of all subgroups. For example, for G finite we have $\underline{E}G = \{\mathrm{pt}\}$ and for G virtually cyclic $\underline{\underline{E}}G = \{\mathrm{pt}\}$.

There are often quite natural models for the classifying space for proper actions. For example, a proper G-CW complex which is a complete CAT(0)-space, on which G acts by isometries is a model for $\underline{E}G$. Other models for the classifying space for proper actions are given by the Rips complex for hyperbolic groups, Teichmüller space for mapping class groups, Culler-Vogtmann Outer space for the outer automorphism group of a finitely generated free group and tree models arising from Bass-Serre theory, see also [Lüc05] for a good overview of these models.

The situation for $\underline{\underline{E}}G$ is more delicate. As an illustrative example, in the following we want to present the construction of a rather simple model of the classifying space $\underline{\underline{E}}G$ for $G = \mathbb{Z} \times \mathbb{Z}$ following [JL06] which is originally due to Lück. Note that since G is torsion-free the space $\mathbb{R}^2$ with the standard $\mathbb{Z}^2$-action is a model of minimal dimension for $EG = \underline{E}G$.

The construction of $\underline{\underline{E}}G$ proceeds as follows: Let T be a countably infinite tree with vertex set V. Let us index the maximal infinite cyclic subgroups of $\mathbb{Z} \times \mathbb{Z}$ by V, so for each $v \in V$ we have an infinite cyclic subgroup $H_v \leq \mathbb{Z} \times \mathbb{Z}$ and we let $Q_v = G/H_v \cong \mathbb{Z}$. We equip the tree T with the trivial G-action and construct a G-space X with an equivariant projection map to T as follows: Above the vertex v we take a 1-dimensional model for EQ_v (e.g. the real line $\mathbb{R}$ with its translation action by $\mathbb{Z}$). The action of G on EQ_v is induced by the quotient map $G \twoheadrightarrow Q_v$. Above each edge (v, w) of T we take the join $EQ_v * EQ_w$ of the chosen models and the map to the edge in T is induced by the projection $EQ_v \times EQ_w \times I \to I$. We are now left to show:

Proposition 1.0.5. The G-CW-complex X is a model for $\underline{\underline{E}}(\mathbb{Z} \times \mathbb{Z})$ of minimal dimension.

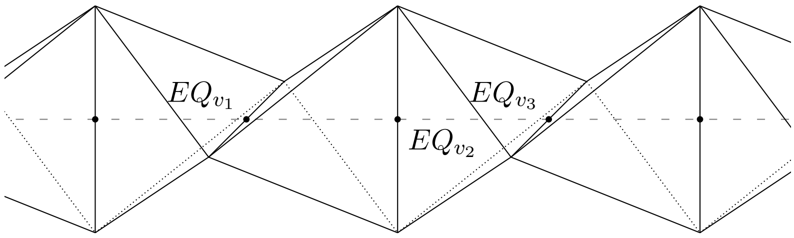

Figure 1.1.: A model for $\underline{\underline{E}}(\mathbb{Z} \times \mathbb{Z})$ with underlying tree $T = \mathbb{R}$.

Proof. We see easily that the isotropy groups of X are either H_v or $H_v \cap H_w$ for $v, w \in V$ and hence cyclic. Now, let $H \leq G$ be a virtually cyclic group. Since G is torsion-free, H is either trivial or infinite cyclic. But X is contractible, since we can first contract all classifying spaces EQ_v onto the tree T and afterwards contract T to a point. So assume that H is infinite cyclic. Then $H \leq H_v$ for a unique $v \in V$ and we see that

$$X^H = X^{H_v} = EQ_v$$

where in the last step we have used that the groups H_v are maximal infinite cyclic subgroups, so $(EQ_w)^{H_v} = \emptyset$ for $v \neq w$. Since the EQ_v are contractible, it follows that X is a model for $\underline{\underline{E}}G$.

We can describe the quotient space X/G as follows: Above each vertex v there is a copy of S^1 being a model of BQ_v and above each edge (v, w) there is a copy of S^3 being the join of BQ_v and BQ_w. Hence the integral homology groups $H_1(X/G)$ and $H_3(X/G)$ are both free abelian of infinite rank. In particular, the dimension of $\underline{\underline{E}}G$ has to be at least 3. Since X was 3-dimensional, we have already constructed a minimal model. ☐

1.1. Finiteness Properties

It is an interesting question what finiteness properties a model of a classifying space for a family of subgroups has and what the obstructions to such finiteness properties are. Let us first recall the following basic definition.

Definition 1.1.1 (Finiteness properties of G-CW-complexes)**.** A G-CW-complex X is *finite* if X has only finitely many equivariant cells. The G-CW-complex X is of *finite type* if each n-skeleton X_n is finite. It is called of *dimension at most* n if $X = X_n$ and it is called *finite-dimensional* if it is of dimension at most n for some $n \in \mathbb{N}$.

For example, for a hyperbolic group G the Rips complex provides a finite model for $\underline{E}G$ [MS02]. Also there are finite-dimensional models for $\underline{\underline{E}}G$ for G a countable elementary amenable group of finite Hirsch length [FN13; DP13].

Definition 1.1.2. Let G be a group and let $\mathcal{F}$ be a family of subgroups of G. We will denote by $\mathrm{gd}_{\mathcal{F}}(G)$ the *geometric dimension of G with respect to the family $\mathcal{F}$*, which is defined to be the infimum over the dimensions of all G-CW-models for $E_{\mathcal{F}}G$. As usual, we abbreviate $\underline{\mathrm{gd}}\, G = \mathrm{gd}_{\mathcal{F}in}\, G$ and $\underline{\underline{\mathrm{gd}}}\, G = \mathrm{gd}_{\mathcal{VC}yc}\, G$.

Lemma 1.1.3. Let G be a group and $\mathcal{F}$ a family of subgroups of G. Then there is a model for $E_{\mathcal{F}}(G)$ with a finite 0-skeleton if and only if G contains finitely many subgroups $H_1, \ldots, H_n$ in $\mathcal{F}$ such that for any $H \in \mathcal{F}$ there is some $g \in G$ so that $H^g \leq H_i$ for some i.

Proof. Suppose that $E_{\mathcal{F}}(G)$ has a finite 0-skeleton, say $\bigsqcup_{i=1}^n G/H_i$ for some $H_i \in \mathcal{F}$. Given a group $K \in \mathcal{F}$, consider the 0-dimensional G-CW-complex G/K. By the universal property of $E_{\mathcal{F}}(G)$ and the equivariant cellular approximation theorem there is a G-map from G/K to the 0-skeleton of $E_{\mathcal{F}}(G)$. Thus we have a G-map from G/K to G/H_i for some i. But this implies that K is conjugate to a subgroup of H_i. The claim follows.

Conversely, given subgroups $H_1, \ldots, H_n$ in $\mathcal{F}$ with the stated properties, we let $X_0 = \bigsqcup_{i=1}^n G/H_i$. By an equivariant version of killing homotopy groups [Lüc89, Proposition 2.3] one inductively constructs a G-CW complex X with the prescribed 0-skeleton whose fixed point sets X^H are contractible for $H \in \mathcal{F}$. □

For the family $\mathcal{F}in$ of finite subgroups Lück could completely characterize what it means for a group G to admit a model of finite type for $\underline{E}G$ in terms of group-theoretical conditions.

Theorem 1.1.4. A group G admits a model of finite type for $\underline{E}G$ if and only if the following two conditions are satisfied:

(1) The group G contains only finitely many conjugacy classes of finite subgroups.

(2) For any finite subgroup $H \leq G$ the Weyl group $W_G(H) = N_G(H)/H$ is finitely presented and of type FP_∞.

Proof. This is [Lüc00, Theorem 4.2]. □

Note that for families like $\mathcal{VC}yc$ a similar group-theoretic characterization as in Theorem 1.1.4 is not known.

Given a family of subgroups $\mathcal{F}$ of a group G and a subgroup $K \leq G$ we let $\mathcal{F} \cap K = \{H \cap K \mid H \in \mathcal{F}\}$, which is a family of subgroups of K, called the *restriction of $\mathcal{F}$ to K*.

Proposition 1.1.5 (Transitivity Principle)**.** Let G be a group and let $\mathcal{F} \subseteq \mathcal{G}$ be two families of subgroups of G.

(1) Let $n \in \mathbb{N}_0$ and suppose that for every $H \in \mathcal{G}$ there exists an n-dimensional model for $E_{\mathcal{F}\cap H}H$. Then
$$\mathrm{gd}_{\mathcal{F}}(G) \leq n + \mathrm{gd}_{\mathcal{G}}(G)\,.$$

(2) Suppose there exists a finite model for $E_{\mathcal{F}\cap H}H$ for any $H \in \mathcal{G}$ and a finite model for $E_{\mathcal{G}}G$. Then there exists a finite model for $E_{\mathcal{F}}G$. The corresponding statement is true if we replace “finite” by “finite type” everywhere.

Proof. This is [LW12, Proposition 5.1]. □

Definition 1.1.6. Let $\mathcal{F}$ be a family of subgroups. For a natural number $n \geq 1$, we say that a group G has property $n\mathcal{F}$ if there are $H_1, \ldots, H_n \in \mathcal{F}$ such that any cyclic subgroup of G is contained in a conjugate of H_i for some i. We say that G has $b\mathcal{F}$ if G has $n\mathcal{F}$ for some $n \in \mathbb{N}$. We call the subgroups H_i *witnesses* to $b\mathcal{F}$ for G and we say that the set $\{H_1, \ldots, H_n\}$ is a *witness* to $b\mathcal{F}$ for G.

The following is immediate:

Lemma 1.1.7. If $\pi\colon G \to Q$ is an epimorphism of groups and G has $b\mathcal{F}$, then Q has $b\pi_*\mathcal{F}$, where $\pi_*\mathcal{F} = \{K \leq \pi(H) \mid H \in \mathcal{F}\}$. In particular, if G has $b\mathcal{VC}yc$, then so does Q.

Lemma 1.1.8. Let G be a group and suppose $K \leq G$ is a finite index subgroup. If G has $b\mathcal{F}$, then so does K.

Proof. Let $m = [G : K]$ and let Kg_i for $1 \leq i \leq m$ be the right cosets of K in G. Furthermore let $\{H_1, \ldots, H_n\}$ be witnesses to $b\mathcal{F}$ for G. Then consider the following finite collection of subgroups of K which lie in $\mathcal{F}$:

$$\{g_i H_j g_i^{-1} \cap K \mid 1 \leq j \leq n, 1 \leq i \leq m\}$$

We claim that these constitute witnesses to $b\mathcal{F}$ for K. Let $C \leq K$ be some cyclic subgroup, then there exists some $g \in G$ such that $C \leq gH_jg^{-1}$ for some j. Write $g = kg_i$ for some i and some $k \in K$. Then $k^{-1}Ck \leq g_iH_jg_i^{-1} \cap K$. □

Lemma 1.1.9. Let G be a group satisfying $b\mathcal{F}$ where $\mathcal{F}$ is a family of Noetherian subgroups, i.e. any subgroup of an element $H \in \mathcal{F}$ is finitely generated. Then G satisfies the ascending chain condition on normal subgroups.

Proof. The group G can be written as $G = \bigcup_{i=1}^n \bigcup_{g \in G} H_i^g$ where $\{H_i \mid 1 \leq i \leq n\}$ is a witness to $b\mathcal{F}$. But then any normal subgroup N of G can be likewise expressed as $N = \bigcup_{i=1}^n \bigcup_{g \in G} (N \cap H_i)^g$.

Let (N_j) be an ascending chain of normal subgroups of G. For any i, the chain $(N_j \cap H_i)_j$ has to stabilize since H_i was Noetherian, i.e. there exists j_i such that $N_j \cap H_i = N_{j+1} \cap H_i$ for all $j \geq j_i$. Then the original chain stabilizes at $j_{\max} = \max_{1 \leq i \leq n} j_i$. □

1.2. The Classifying Space for Virtually Cyclic Subgroups

In [JL06] Juan-Pineda and Leary formulated the following conjecture, which will be the main motivation for this thesis.

Conjecture 1.2.1. A group G admits a finite model for $\underline{\underline{E}}G$ if and only if G is virtually cyclic.

In the same paper Juan-Pineda and Leary verified their conjecture for the class of hyperbolic groups, relying on work of Gromov. In Chapter 3 we give an alternative proof of this fact using conjugacy growth. Later Kochloukova, Martínez-Pérez and Nucinkis verified the conjecture for elementary amenable groups [KMN11] and Groves and Wilson [GW13] gave a simplified proof for the class of solvable groups. As most of the proofs only use the fact that $\underline{\underline{E}}G$ has a finite 0-skeleton, we suggest the following strengthening of the conjecture.

Conjecture 1.2.2. A group G has a model for $\underline{\underline{E}}G$ of finite type if and only if G is virtually cyclic.

The following notion has been introduced in [GW13] by Groves and Wilson.

Definition 1.2.3. We say that a group G has BVC if there are finitely many virtually cyclic subgroups $V_1, \dots, V_n$ of G such that every virtually cyclic subgroup of G is conjugate to a subgroup of some V_i. The set $\{V_1, V_2, \dots, V_n\}$ is called a *witness* to BVC and we shall similarly call the V_i *witnesses* to BVC.

By Lemma 1.1.3 a group G has BVC if and only if it admits a classifying space $\underline{\underline{E}}G$ with finite 0-skeleton. If G has a model for $\underline{\underline{E}}G$ of finite type, then there is a model of finite type for $\underline{E}G$ as well as EG by the transitivity principle Proposition 1.1.5. This follows since there are models of finite type for $\underline{E}V$ and EF for V virtually cyclic and F finite. In particular, it follows that G is finitely presented. Moreover, Theorem 1.1.4 gives further conditions on the Weyl groups $W_G(H)$ for $H \leq G$ finite. In almost all cases with the notable exception of elementary amenable groups these additional conditions are rarely useful nor necessary to settle Conjecture 1.2.1 affirmatively for reasonable classes of groups. Most arguments revolve around the BVC property.

The following is well-known, for a proof see e.g. [JL06, Proposition 4].

Lemma 1.2.4. Let V be a virtually cyclic group. Then V contains a unique maximal normal finite subgroup F such that exactly one of the following holds

(a) the finite case, $V = F$;

(b) the *orientable* case, V/F is infinite cyclic;

(c) the *nonorientable* case, V/F is isomorphic to the infinite dihedral group D_∞.

Sometimes orientable resp. nonorientable virtually cyclic groups are called virtually cyclic groups of type I resp. of type II and we shall denote by $\mathcal{VC}yc_I$ the family of subgroups consisting of the finite as well as the orientable virtually cyclic subgroups. A useful consequence of Lemma 1.2.4 is that torsion-free virtually cyclic groups are cyclic. In particular, for torsion-free groups there is no difference between the $b\mathcal{C}yc$ and BVC property.

Lemma 1.2.5. For any nonorientable virtually cyclic group V there exists a model of finite type for $E_{\mathcal{VC}yc_I}(V)$.

Proof. We will see below in Lemma 1.3.6 that there exists a model of finite type for $E_{\mathcal{C}yc}(D_\infty)$. If V is an arbitrary nonorientable virtually cyclic group, there exists an epimorphism $\pi \colon V \to D_\infty$ with finite kernel. The model of finite type for $E_{\mathcal{C}yc}(D_\infty)$, viewed via π as a V-CW-complex, is a classifying space for the family $\mathcal{VC}yc_I$. $\square$

By an application of the transitivity principle, see Proposition 1.1.5, we can thus record:

Corollary 1.2.6. If G is a group admitting model of finite type for $\underline{\underline{E}}G$, then there is also model of finite type for $E_{\mathcal{VC}yc_I}(G)$.

Definition 1.2.7. Let G be a group. An element $g \in G$ is called *primitive* if g cannot be written as a proper power, i.e. g cannot be written as $g = h^n$ for some $h \in G$ and $n \geq 2$.

Of course, a primitive element is always of infinite order. And it is easy to see that an element $g \in G$ is primitive if and only if the subgroup $\langle g \rangle$ is maximal cyclic. As the following example shows, when counting the number of primitive elements in a group, special care has to be taken if torsion is present.

Example 1.2.8. The group $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ contains infinitely many primitive conjugacy classes. In fact, let $g_i = (-1, 2^i) \in G$. Then g_i is primitive for any $i \geq 1$: Suppose $(-1, 2^i) = (x, y)^k$ for some $k > 1$, then $ky = 2^i$. In particular, k is even and thus x^k cannot equal -1.

It is not hard to see that in a virtually cyclic group any two infinite cyclic subgroups have to intersect non-trivially. The following lemma provides a quantitative variant of this statement.

Lemma 1.2.9. Let V be an infinite virtually cyclic group. Then there exists some non-zero $k \in \mathbb{Z}$ and some infinite order element $v_0 \in V$ such that for any element $v \in V$ of infinite order there exists some $m \in \mathbb{Z}$ such that $v^k = v_0^{km}$.

Proof. Suppose V is nonorientable, and let $\pi\colon V \to \mathbb{Z} \rtimes \mathbb{Z}/2$ be an epimorphism onto the infinite dihedral group with finite kernel. Since the kernel of π is finite and all infinite order elements of $\mathbb{Z} \rtimes \mathbb{Z}/2$ lie in $\mathbb{Z} \rtimes \{0\}$, any infinite order element of V lies in $\pi^{-1}(\mathbb{Z} \rtimes \{0\}) \leq V$. Moreover, note that $\pi^{-1}(\mathbb{Z} \rtimes \{0\})$ is an orientable virtually cyclic subgroup. So we can suppose from the beginning that $V \cong F \rtimes_{\varphi} \mathbb{Z}$ is orientable, where F is some finite group and φ is an automorphism of F. Let $k = |\varphi| \cdot |F|$ where $|\varphi|$ denotes the order of φ. We define $v_0 = (e, 1)$ for e the neutral element of F. Let $v = (x, m) \in V$ be arbitrary, then $v^k = (y, |\varphi| \cdot m)^{|F|}$ for some $y \in F$. And thus $v^k = (e, km) = v_0^{km}$. $\square$

Lemma 1.2.10. Let G be a group and let $H \leq G$ be a finite index subgroup. If G has BVC, then so does H.

Proof. The proof proceeds the same way as the proof of Lemma 1.1.8. $\square$

A virtually cyclic group contains only finitely many conjugacy classes of finite subgroups. This immediately implies:

Lemma 1.2.11. Let G be a group with BVC. Then G has finitely many conjugacy classes of finite subgroups. In particular, the order of finite subgroups in G is bounded.

Lemma 1.2.12. Let $\pi\colon G \to Q$ be a surjective group homomorphism and suppose that Q is torsion-free. If G has BVC, then Q has $b\mathcal{C}yc$.

Proof. If $V_1, V_2, \ldots, V_n$ are virtually cyclic witnesses to BVC for G, then it is easy to see that $\pi(V_1), \pi(V_2), \ldots, \pi(V_n)$ are cyclic witnesses to $b\mathcal{C}yc$ for Q. $\square$

We will see in Chapter 4 that the BVC property does not pass to quotients in general, so the assumption of torsion-freeness in Lemma 1.2.12 is essential.

Lemma 1.2.13. Let G be a torsion-free group. If G has infinitely many conjugacy classes of primitive elements, then G does not have $b\mathcal{C}yc$.

The following lemma is a slight generalization of [GW13, Lemma 2.2], where we have replaced the BVC by the $b\mathcal{VC}yc$ condition. The arguments given by Groves and Wilson carry over and we will repeat them here for the convenience of the reader.

Lemma 1.2.14. Let G be a group with $b\mathcal{VC}yc$. Then the following assertions hold.

(1) The group G satisfies the ascending chain condition for normal subgroups.

(2) If L and M are normal subgroups of G with $M < L$ and L/M a torsion group, then there are only finitely many normal subgroups K of G such that $M \leq K \leq L$.

(3) The group G has no quotient which is an extension of an infinite abelian torsion group by an infinite cyclic group.

(4) Let
$$1 = G_n \leq G_{n-1} \leq \cdots \leq G_1 \leq G_0 = G$$
be a series of normal subgroups of G. Then the number of factors G_i/G_{i-1} that are not torsion groups is bounded by the number of infinite groups in a witness to $b\mathcal{VC}yc$ for G.

Proof. (1) is Lemma 1.1.9. For (2) let $V_1, \ldots, V_n$ be witnesses to $b\mathcal{VC}yc$ for G. Let $W_i = L \cap V_i$ and define $\overline{W_i} = MW_i/M$. As L/M is a torsion group, $\overline{W_i}$ is finite. By the $b\mathcal{VC}yc$ property any element of L is conjugate in G to an element of W_i. Then also every element of L/M is conjugate in G/M to an element of $\overline{W_i}$. If K is a normal subgroup of G such that $M \leq K \leq L$, then K/M can be written as a union of conjugacy classes of elements in the finite set $\bigcup_{i=1}^{n} \overline{W_i}$. Hence there are only finitely many such subgroups K. For (3) note that for T the infinite cyclic group a $\mathbb{Z}T$-module with finitely many submodules is necessarily finite. Combining this fact with (2) yields the claim. For the last claim (4), suppose that G_{n-1} is not a torsion group. Then it contains an infinite subgroup of some V_i and thus the image of V_i in G/G_{n-1} is finite. The claim then follows by induction. □

Theorem 1.2.15. If G is solvable and G has $b\mathcal{VC}yc$, then G is virtually cyclic.

Proof. The corresponding statement for BVC has been proven by Groves and Wilson in [GW13] and carries over in our slightly more general context. Their key result [GW13, Lemma 2.4] deals with torsion-free groups with the BVC property. But for torsion-free groups there is no difference between the BVC and $b\mathcal{VC}yc$ property. All other statements proven in [GW13] also hold for the $b\mathcal{VC}yc$ property, see for example Lemma 1.2.14. □

Since an abelian group with $b\mathcal{VC}yc$ is virtually cyclic we obtain:

Corollary 1.2.16. If G is a group having $b\mathcal{VC}yc$, then the abelianization G^{ab} is finitely generated of rank at most one.

Example 1.2.17. The Thompson groups are a family of three finitely presented groups, $F \leq T \leq V$. Thompson's group F can be defined by the presentation $\langle A, B \mid [AB^{-1}, A^{-1}BA] = [AB^{-1}, A^{-2}BA^2] = 1\rangle$, see [CFP96]. Since $F^{\mathrm{ab}} \cong \mathbb{Z}^2$, it follows that F does not have $b\mathcal{VC}yc$. Since the orders of finite cyclic subgroups in T and V are unbounded, we see that T and V also do not have $b\mathcal{VC}yc$.

Motivated by previous proofs of Conjecture 1.2.2 that mostly only depend on the BVC property, we ask:

Question 1.2.18. Is a finitely presented group with $b\mathcal{VC}yc$ (or with BVC) already virtually cyclic?

For the formulation of the preceding question it is important that we require the group to be finitely presented. There are non virtually cyclic groups that are finitely generated and have $b\mathcal{VC}yc$. For example, Ivanov [Ols91, Theorem 41.2] constructed finitely generated infinite torsion groups that have only finitely many conjugacy classes.

1.3. The Classifying Space for Cyclic Subgroups

An analogous conjecture as Conjecture 1.2.2 can be formulated if one replaces the family of virtually cyclic subgroups by the family of cyclic subgroups. In fact, Lück–Reich–Rognes–Varisco asked in [Lüc+17, Question 4.9] whether a group G that admits a model of finite type for $E_{\mathcal{C}yc}(G)$ is already finite, cyclic or infinite dihedral. Now, note that for important classes of groups the $b\mathcal{VC}yc$ property already implies that the group at hand is virtually cyclic. As a matter of fact, the following chapters are mostly dedicated to this problem. Since a group with $b\mathcal{C}yc$ certainly has the $b\mathcal{VC}yc$ property, in this section we want to address the question which virtually cyclic groups have the $b\mathcal{C}yc$ property. Moreover, we will determine which virtually cyclic groups admit a finite resp. finite-dimensional classifying space for the family of cyclic subgroups. Contents of this section have also previously appeared in [vW17].

Example 1.3.1. Let $D_\infty = \mathbb{Z} \rtimes \mathbb{Z}/2 = \langle t, s \mid s^2 = 1, sts = t^{-1}\rangle$ be the infinite dihedral group. Then $\langle t\rangle$, $\langle s\rangle$ and $\langle ts\rangle$ are witnesses to $b\mathcal{C}yc$ for D_∞ since $tst^{-1} = t^{1-2n}s$. A straightforward calculation also shows that there cannot be fewer witnesses.

Remark 1.3.2. Observe that $b\mathcal{C}yc$ fails to pass to finite index overgroups, a counterexample is provided by $\mathbb{Z} \leq \mathbb{Z} \times \mathbb{Z}/2$.

Note that there is no assumption about absence of torsion in the following (cf. Lemma 1.2.13).

Observation 1.3.3. If G has $b\mathcal{C}yc$, then G has only finitely many primitive conjugacy classes.

Lemma 1.3.4. Let F be a finite group and suppose that $V = F \rtimes_\varphi \mathbb{Z}$ is a group with $b\mathcal{C}yc$. Then $F = 1$.

Proof. Let d be the order of φ. Then $F \times d\mathbb{Z}$ is a subgroup of index d in $F \rtimes_\varphi \mathbb{Z}$. Hence by Lemma 1.1.8, we can assume $V = F \times \mathbb{Z}$.

Now assume that F is nontrivial. Let c be an element of maximal order in F and let p be a prime that divides its order. Then for any $n \geq 1$, $g_n = (c, p^n) \in F \times \mathbb{Z}$ is primitive in $F \times \mathbb{Z}$. If fact, if $(x,k)^m = (x^m, mk) = (c, p^n)$, for some $m > 1$, then p divides m. On the other hand since $x^m = c$, c lies in the subgroup generated by x. But since c has maximal order, we have x and c generate the same cyclic subgroup in F. But since p divides the order of c and m, this cannot happen. When $n \neq m$, g_n is not conjugate to g_m since the second coordinate differs. Thus by Observation 1.3.3, the claim follows. □

Proposition 1.3.5. A virtually cyclic group V has $b\mathcal{C}yc$ if and only if V is finite, infinite cyclic or infinite dihedral.

Proof. By Lemma 1.2.4 and Lemma 1.3.4, the only case left to consider is if V is nonorientable, i.e. there is an exact sequence

$$1 \to F \to V \to D_\infty \to 1$$

with F finite. But then V has a finite index subgroup isomorphic to $F \rtimes \mathbb{Z}$, hence $F = 1$ and the claim follows from Example 1.3.1. □

Lemma 1.3.6. There exists a model of finite type for $E_{\mathcal{C}yc}D_\infty$ and any model for $E_{\mathcal{C}yc}D_\infty$ has to be infinite-dimensional.

Proof. Let $D_\infty = \mathbb{Z} \rtimes \mathbb{Z}/2 = \langle s, t \mid s^2 = 1, sts = t^{-1}\rangle$. We claim that the join $E = \mathbb{Z} * E\mathbb{Z}/2$, given an appropriate action, is a model for $E_{\mathcal{C}yc}D_\infty$. We write $[x, y, q]$ for an element in E, where $x \in \mathbb{Z}$, $y \in E\mathbb{Z}/2$ and $q \in [0, 1]$. Note that $[x, y, 0] = [x, y', 0]$ and $[x, y, 1] = [x', y, 1]$ for all $x, x' \in \mathbb{Z}$ and $y, y' \in E\mathbb{Z}/2$. We then define the action as follows:

$$\begin{aligned} t \cdot [x, y, q] &= [x + 2, y, q] \\ s \cdot [x, y, q] &= [-x, s \cdot y, q] \end{aligned}$$

Then one observes that the stabilizer of $[x, y, q]$ with $0 < q < 1$ is trivial. The stabilizer of $[x, y, 0]$ is equal to $\langle t^x s\rangle$ and the stabilizer of $[x, y, 1]$ equals $\langle t\rangle$. One furthermore checks that for $n \neq 0$

$$E^{\langle t^n\rangle} = E\mathbb{Z}/2 \simeq *\,,$$

and for n arbitrary

$$E^{\langle t^n s\rangle} = \mathbb{Z}^{\langle t^n s\rangle} = \{n\}.$$

Since E itself is contractible as well, it follows that E is a model for $E_{\mathcal{C}yc}(G)$ of finite type. The claim about the infinite-dimensionality of any model for $E_{\mathcal{C}yc}(G)$ follows from Lemma 1.3.9 below by noting that $\langle t\rangle$ is a normal maximal cyclic subgroup of D_∞. Alternatively, observe that E/D_∞ is homotopy equivalent to the suspension of $\mathbb{R}P^\infty$. □

Corollary 1.3.7. Let G be a virtually cyclic group, then it has a model for $E_{\mathcal{C}yc}(G)$ of finite type if and only if it is finite, infinite cyclic or infinite dihedral.

Proof. By Proposition 1.3.5, we only need to prove that there is a model of finite type for $E_{\mathcal{C}yc}(G)$ if G is finite, infinite cyclic or infinite dihedral. If G is a finite group, then the standard bar-construction provides such a model. If G is infinite cyclic, we can take $E_{\mathcal{C}yc}(G)$ to be a point. In case G is infinite dihedral Lemma 1.3.6 provides a model of finite type. □

Observation 1.3.8. Let H be a subgroup of a group G and let X be a model for $E_{\mathcal{C}yc}(G)$, then $\operatorname{res}_H^G X$ is a model for $E_{\mathcal{C}yc}(H)$.

For the following lemma, recall that the classifying space EF of a non-trivial finite group F cannot be finite-dimensional [Bro82, VIII.2.5].

Lemma 1.3.9. Let G be a group and suppose that $H \leq G$ is a maximal cyclic subgroup. Moreover, assume that $[N_G(H) : H]$ is finite but not equal to one. Then any model for $E_{\mathcal{C}yc}(G)$ has to be infinite-dimensional.

Proof. Let X be a model for $E_{\mathcal{C}yc}(G)$. Since H is cyclic, the CW-complex X^H is contractible. Observe that all isotropy groups of X^H are equal to H since H was maximal cyclic. This implies that the Weyl group $N_G(H)/H$ of H acts freely on X^H. Since $N_G(H)/H$ is non-trivial finite, X^H has to be infinite-dimensional. □

Proposition 1.3.10. Let G be a finite group with a finite-dimensional model for $E_{\mathcal{C}yc}(G)$. Then G is already cyclic.

Proof. We prove the claim by induction on the order of G. Then by Observation 1.3.8 we only need to consider finite groups G such that every proper subgroup is cyclic. If G is a p-group, then G is in particular solvable. Otherwise any Sylow p-subgroup is cyclic and thus G is solvable by [Rob, Theorem 10.1.10]. In any case, the proper subgroup $[G,G]$ has to be cyclic. Let H be a maximal cyclic subgroup containing $[G,G]$, then $N_G(H) = G$. By Lemma 1.3.9, it follows that $H = G$ and hence G is cyclic. □

Proposition 1.3.11. Let V be a virtually cyclic group. Then $E_{\mathcal{C}yc}V$ is finite-dimensional if and only if V is cyclic.

Proof. By Proposition 1.3.10 we only need to prove the claim if V is infinite. Suppose V is orientable, i.e. $V \cong F \rtimes_\varphi \mathbb{Z}$ for some finite group F and some $\varphi \in \operatorname{Aut}(F)$ and assume that $E_{\mathcal{C}yc}V$ is finite-dimensional. If d denotes the order of φ then $F \times \mathbb{Z} \cong F \rtimes_\varphi d\mathbb{Z}$ and by Observation 1.3.8 also $F \times \mathbb{Z}$ has a finite-dimensional classifying space. But $\mathbb{Z} \leq F \times \mathbb{Z}$ is a normal maximal cyclic subgroup, thus $F = 1$ by Lemma 1.3.9.

Now, suppose V was nonorientable having a finite-dimensional model for $E_{\mathcal{C}yc}V$. Let F be the maximal normal finite subgroup of $V \cong F \rtimes D_\infty$, then $F \rtimes \mathbb{Z}$ is a subgroup of V of finite index. By the above, it follows that $F = 1$, so V is infinite dihedral. But this is impossible by Lemma 1.3.6. □

Corollary 1.3.12. A virtually cyclic group V has a finite or finite-dimensional model for $E_{\mathcal{C}yc}V$ if and only if V is cyclic.

From Proposition 1.3.11 we immediately obtain the following observation:

Observation 1.3.13. If G is a group having a finite-dimensional model for $E_{\mathcal{C}yc}(G)$, then there is a finite-dimensional model for $\underline{\underline{E}}G$. Conversely, suppose that G is a group having a finite-dimensional model for $\underline{\underline{E}}G$. Then G admits a finite-dimensional model for $E_{\mathcal{C}yc}(G)$ if and only if $\mathcal{C}yc(G) = \mathcal{V}\mathcal{C}yc(G)$.

Obviously the condition $\mathcal{C}yc(G) = \mathcal{VC}yc(G)$ holds whenever the group G is torsion-free. However, this is not necessary, even for virtually free groups. For example, groups of the form $G = *_{i=1}^{n}\mathbb{Z}/n_i\mathbb{Z}$ where $n_i \geq 0$ admit a finite-dimensional model for $E_{\mathcal{C}yc}(G)$ if and only if $n_i \neq 2$ for all i or $G \cong \mathbb{Z}/2$ by the Kurosh subgroup theorem.

Lemma 1.3.14. Let A be an abelian group with $E_{\mathcal{C}yc}(A)$ finite-dimensional. Then A is cyclic, torsion-free of finite rank or locally finite cyclic.

Proof. By Proposition 1.3.10 we can assume in the following that A is infinite. If A is finitely generated, we can write $A \cong \mathbb{Z}^n \times F$ with F finite abelian and $n \geq 1$. In particular, A contains $\mathbb{Z} \times F$, so $F = 1$, i.e. A is torsion-free. More generally, if A contains an element of infinite order x, then any finite set $\{y_1, \ldots, y_n\} \subseteq A$ together with the element x will generate an infinite abelian subgroup, which must be torsion-free by the previous observation. The claim about the rank of A then follows since $\underline{\underline{\mathrm{gd}}}\,(\mathbb{Z}^n) = n + 1$ if $n \geq 2$, see [LW12, Example 5.21]. The only case that remains is A being an infinite torsion group. But since any finite subgroup has to be cyclic, it follows that A is locally finite cyclic. □

We also want to remark that a locally cyclic group A is isomorphic to a subquotient of the group of rational numbers [Kur55, Chapter VIII, Section 30]. In particular, A is countable. By [LW12, Theorem 4.3] it follows that the minimal dimension of a model for $E_{\mathcal{C}yc}(A)$ is at most one. If A is torsion-free abelian of finite rank, then A embeds into the finite-dimensional $\mathbb{Q}$-vector space $A \otimes_{\mathbb{Z}} \mathbb{Q}$. Hence A is countable as well and since any finitely generated subgroup H of A has a classifying space $E_{\mathcal{C}yc}(H)$ of dimension at most $\mathrm{rank}(A) + 1$, [LW12, Theorem 4.3] implies that A has a finite-dimensional model for $E_{\mathcal{C}yc}(A)$. So the converse of Lemma 1.3.14 holds as well.

Proposition 1.3.15. Let G be elementary amenable and suppose that there is a finite-dimensional model for $E_{\mathcal{C}yc}(G)$. Then G is virtually solvable of finite Hirsch length.

Proof. Since $E_{\mathcal{C}yc}(G)$ has a finite-dimensional model, so does $E_{\mathcal{F}cyc}(G)$ by Proposition 1.1.5, where $\mathcal{F}cyc$ denotes the family of finite cyclic subgroups. It follows that the Hirsch length $\mathrm{h}(G)$ of G is finite, since $\mathrm{h}(G) \leq \mathrm{cd}_{\mathbb{Q}}(G) \leq \mathrm{gd}_{\mathcal{F}cyc}(G) < \infty$. The first inequality follows from [Hil91, Lemma 2]. For the second inequality note that $\mathbb{Q}[G/F]$ is a projective $\mathbb{Q}G$-module for F finite [Bro82, I.8 Ex. 4] and thus the cellular chain complex of $E_{\mathcal{F}cyc}(G)$ yields a projective resolution of $\mathbb{Q}$ over $\mathbb{Q}G$. Moreover, note that any locally finite subgroup H of G has to be locally cyclic by Proposition 1.3.11, in particular H is abelian. Combined with the structure theorem of elementary amenable groups of finite Hirsch length [HL92], it follows that G is virtually solvable. □

In contrast to the result of Proposition 1.3.15 we want to mention that any elementary amenable group of finite Hirsch length and cardinality $\aleph_n$ admits a finite-dimensional model for the classifying space of virtually cyclic subgroups [FN13; DP13].

2. Free Products, HNN Extensions and One-Relator Groups

In this chapter we study the $b\mathcal{VC}yc$ property for some standard group-theoretic constructions such as free products and HNN extensions. Using some quite technical arguments we will show that ascending HNN extensions of finitely generated free groups do not have the $b\mathcal{VC}yc$ property. In Chapter 4 we will later see that the question whether an ascending HNN extension has the $b\mathcal{C}yc$ property depends heavily on the base group. As an application of the result on HNN extensions of free groups we will answer Question 1.2.18 affirmatively for the class of one-relator groups using an inductive argument. Most of the results of this chapter have appeared, with slight changes, in [vW].

We begin by recalling some standard results on free products of groups. Let A and B be groups and let $G = A * B$ be the free product of A and B. A sequence of elements $g_1, \ldots, g_n$ of G is called *reduced* if each g_i is non-trivial and is contained in one of the factors, A or B, and consecutive elements g_i, g_{i+1} lie in distinct factors. We allow $n = 0$ for the empty sequence.

Lemma 2.0.1 (Normal form for free products)**.** In a free product $G = A * B$ the following two equivalent statements hold:

(1) Any element of $g \in G$ can be written uniquely as $g = g_1 \ldots g_n$ such that $g_1, \ldots, g_n$ is a reduced sequence.

(2) If $g = g_1 \ldots g_n$ with $n > 0$ and $g_1, \ldots, g_n$ is a reduced sequence, then $g \neq 1$ in G.

Proof. This is given as [LS, Theorem IV.1.2]. □

We call an element $g = g_1 \ldots g_n$ of $G = A * B$ *cyclically reduced* if $g_1, \ldots, g_n$ is a reduced sequence and if g_1 and g_n lie in different factors or $n \leq 1$.

Lemma 2.0.2 (Conjugation in free products)**.** Each element of $G = A * B$ is conjugate to a cyclically reduced element. Suppose $g = g_1 \ldots g_n$ and $h = h_1 \ldots h_m$ are cyclically reduced elements that are conjugate in G. Then $n = m$. If $n > 1$, then the sequences $g_1, \ldots, g_n$ and $h_1, \ldots, h_m$ are cyclic permutations of each other. If $n \leq 1$, then g and h are contained in the same factor and are conjugate in this factor.

Proof. Consult [LS, Theorem IV.1.4]. □

Proposition 2.0.3. Let $G = A * B$ be a free product with A and B nontrivial, then G has $b\mathcal{VC}yc$ if and only if G is virtually cyclic.

Proof. If A and B are finite groups, then $A * B$ is a virtually free group. But note that the free group F_n on n letters has $b\mathcal{VC}yc$ if and only if $n = 1$. So in the following we can assume without loss of generality that A is infinite. Then $A * B$ is not virtually cyclic. Let $a_1, a_2, \ldots$ be an infinite sequence of pairwise different elements in A and let $b \in B$ be a non-trivial element. Then the elements $a_i b$ for $i \geq 1$ are cyclically reduced and form infinitely many conjugacy classes of primitive elements in G. Suppose G had $b\mathcal{VC}yc$, then there would be some i and j with $i \neq j$ such that $\langle a_i b \rangle$ and $\langle a_j b \rangle$ would be contained in the same virtually cyclic subgroup up to conjugation. By Lemma 1.2.9 we would have that $(a_i b)^m$ is conjugate to $(a_j b)^n$ in G for some $m, n \neq 0$. Lemma 2.0.2 then implies that $n = m$ and $(a_i b)^n$ would be a cyclic permutation of $(a_j b)^n$. But since $a_i \neq a_j$, this is impossible. $\square$

Given a group H and an isomorphism $\theta \colon A \to B$ between two subgroups A and B of H, we can define a new group $H*_\theta = H*_{A^t = B}$, called the HNN extension of H along θ, by the presentation $\langle H, t \mid t^{-1}xt = \theta(x), x \in A \rangle$. The letter t is called *stable letter*. If $H = A$ or $H = B$, we call the associated HNN extension *ascending* and if $H = A$ and B is a proper subgroup of H (or vice versa), we call the ascending HNN extension *proper*. In the study of HNN extensions, Britton's Lemma and Collins' Lemma provide important information about normal forms and the conjugation action. We give a quick review of the two lemmas and refer to [LS, IV.2] for proofs.

Definition 2.0.4. A sequence $g_0, t^{\epsilon_1}, g_1, \ldots, t^{\epsilon_n}, g_n$ of elements with $g_i \in H$ and $\epsilon_i \in \{-1, +1\}$ is said to be *reduced* if there is no pinch, where we define a *pinch* to be a consecutive sequence t^{-1}, g_i, t with $g_i \in A$ or t, g_j, t^{-1} with $g_j \in B$.

Lemma 2.0.5 (Britton's Lemma)**.** If the sequence $g_0, t^{\epsilon_1}, g_1, \ldots, t^{\epsilon_n}, g_n$ is reduced and $n \geq 1$, then $g_0 t^{\epsilon_1} g_1 \cdots t^{\epsilon_n} g_n \neq 1$ in $H*_\theta$.

In the following we will not distinguish between a sequence of words as above and the element it defines in the HNN extension $H*_\theta$.

Give any $g \in H*_\theta$, we can write g in a reduced form. Let $w = g_0 t^{\epsilon_1} g_1 \ldots t^{\epsilon_n} g_n \neq 1$ be any reduced word in $H*_\theta$ which represents g. Then we define the *length* of g, written as $|g|$, to be the number n of occurrences of $t^{\pm}$ in w. Moreover, we call an element $w = g_0 t^{\epsilon_1} g_1 \ldots t^{\epsilon_n} g_n \neq 1$ cyclically reduced if all cyclic permutations of the sequence $g_0, t^{\epsilon_1}, g_1, \ldots, t^{\epsilon_n}, g_n$ are reduced. Every element of $H*_\theta$ is conjugate to a cyclically reduced element.

Lemma 2.0.6 (Collins' Lemma)**.** Let $G = \langle H, t \mid t^{-1}xt = \theta(x), x \in A \rangle$ be an HNN extension. Let $u = g_0 t^{\epsilon_1} g_1 \ldots t^{\epsilon_n} g_n$ and v be cyclically reduced elements of G that are conjugate and $n \geq 1$. Then $|u| = |v|$, and u can be obtained from v by taking a suitable cyclic permutation v^* of v, which ends in t^{ϵ_n}, and then conjugating by an element z, where $z \in A$ if $\epsilon_n = -1$, and $z \in B$ if $\epsilon_n = 1$.

Proposition 2.0.7. Let H be a group and let $\theta \colon A \to B$ be an isomorphism between two subgroups of H. If $[H : A], [H : B] \geq 2$, then the corresponding HNN extension $G = H*_\theta = \langle H, t \mid t^{-1}at = \theta(a), a \in A \rangle$ does not have $b\mathcal{VC}yc$.

Proof. We choose $\alpha \in H \setminus A$ and $\beta \in H \setminus B$ and define

$$w_n = t^{-1} \alpha t^{n+1} \beta \in G$$

for $n \geq 1$. Note that the elements w_n are of infinite order and cyclically reduced. By Collins' Lemma, they are not conjugate to each other. If G had $b\mathcal{V}\mathcal{C}yc$, there would exist a virtually cyclic subgroup $V \leq G$ and two natural numbers $n \neq m$ such that w_n and w_m are contained in V up to conjugation. Thus there would exist some $p_n, p_m \in \mathbb{Z}$ such that $w_n^{p_n}$ is conjugate to $w_m^{p_m}$. We claim that this is impossible. In fact, first note that $w_n^{p_n}$ and likewise $w_m^{p_m}$ are cyclically reduced. Since we assumed that $w_n^{p_n}$ is conjugate to $w_m^{p_m}$, their lengths must coincide by Collins' Lemma. Hence we arrive at the equation $|p_n|(n+2) = |p_m|(m+2)$. On the other hand, there is a canonical quotient map $q\colon G \to \langle t \rangle \cong \mathbb{Z}$. We would then obtain $q(w_n^{p_n}) = q(w_m^{p_m})$. This means $p_n n = p_m m$. But the two equations can never hold at the same time when $n, m \geq 1$ unless $n = m$. □

If $G = H*_\theta$ where $H = A$ or $H = B$, i.e. H is an ascending HNN extension, it is not easy to decide whether G has $b\mathcal{V}\mathcal{C}yc$. In fact, we will later see in Chapter 4 that there are torsion-free groups H which do not have $b\mathcal{C}yc$, but such that $G = H \rtimes_\theta \mathbb{Z}$ has $b\mathcal{C}yc$ for some $\theta \in \operatorname{Aut}(H)$. So in order to show that an extension $H \rtimes_\theta \mathbb{Z}$ does not have $b\mathcal{V}\mathcal{C}yc$ we need to impose additional conditions on either H or θ or on both.

Given an automorphism θ of a group H, we say that two elements h, h' in H are θ-conjugate if $h = xh'\theta(x^{-1})$ for some $x \in H$. This is an equivalence relation whose equivalence classes are called θ-twisted conjugacy classes. The number of θ-twisted conjugacy classes is sometimes called the Reidemeister number of θ and denoted by $R(\theta)$. For $\theta = \mathrm{id}_H$ one recovers the usual notion of conjugacy.

Lemma 2.0.8. Let θ be an automorphism of H such that H has infinitely many θ-twisted conjugacy classes, then the semidirect product $G = H \rtimes_\theta \mathbb{Z}$ does not have $b\mathcal{V}\mathcal{C}yc$.

Proof. Note that in $H \rtimes_\theta \mathbb{Z}$, the elements $(h, 1)$ and $(h', 1)$ are primitive and they are in the same conjugacy class if and only if h and h' are in the same θ-twisted conjugacy class in H. In fact, $(h, 1)$ is conjugate to $(h', 1)$ in $H \rtimes_\theta \mathbb{Z}$ if and only if we can find $(x, k) \in G$ such that $(x, k)(h, 1)(x, k)^{-1} = (x\theta^k(h)\theta(x^{-1}), 1) = (h', 1)$. This is equivalent to saying that $\theta^k(h)$ is θ-conjugate to h'. But h and $\theta(h)$ are θ-conjugate in H since $\theta(h) = h^{-1}h\theta(h)$.

Since H has infinitely many θ-twisted conjugacy classes, we have infinitely many primitive elements of the form $(h, 1) \in G$ that are not conjugate to each other. If G had $b\mathcal{V}\mathcal{C}yc$, there would be infinitely many elements $(h_1, 1), (h_2, 1), \ldots$ that are not conjugate to each other, but that lie in the same virtually cyclic subgroup. In particular, the elements h_i are pairwise distinct and the group V generated by $(h_1, 1), (h_2, 1), \ldots$ is virtually cyclic. Consider the canonical quotient map $q\colon H \rtimes_\theta \mathbb{Z} \to \mathbb{Z}$. Note that q is onto when restricted to V and thus the kernel of $q|_V$ must be finite since V is virtually cyclic. However, this contradicts the fact that there are infinitely many pairwise distinct h_i. Thus G does not have $b\mathcal{V}\mathcal{C}yc$. □

A group is said to have property R_∞ if it has infinitely many θ-twisted conjugacy classes for any automorphism θ.

Corollary 2.0.9. Suppose H is a group with the property R_∞. Then any semidirect product $H \rtimes_\theta \mathbb{Z}$ does not have $b\mathcal{V}\mathcal{C}yc$.

The question of which classes of groups have the R_∞ property was first addressed in [FH94]. Many groups with the R_∞ property are now known, for example non-elementary hyperbolic groups, relatively hyperbolic groups and most generalized Baumslag-Solitar groups. For more information about groups with the property R_∞ and further examples, see [FT15].

In the following we will analyze the case of an ascending HNN extension of a free group F of finite rank in detail. We will first deal with the case that $\theta\colon F \to F$ is injective with its image lying in the commutator subgroup of F. Given a group G, we denote the r-th term in the lower central series by $\Gamma_r(G) = [\Gamma_{r-1}(G), G]$ where $\Gamma_1(G) = G$. By [jHal, Corollary 10.3.5] we know that $[\Gamma_r(G), \Gamma_s(G)] \leq \Gamma_{r+s}(G)$.

Lemma 2.0.10. For any free group F of finite rank we have:

(1) $\bigcap_{r\geq 1} \Gamma_r(F) = \{1\}$.

(2) $\Gamma_r(F)/\Gamma_{r+1}(F)$ is a free abelian group for any r.

Proof. The proof can be found in [jHal, Chapter 11]. □

Corollary 2.0.11. Let $\theta\colon F \to F$ be an injective map of the finitely generated free group F with the image of θ lying in the commutator subgroup of F. If $x \in \Gamma_r(F)$, then $\theta(x) \in \Gamma_{2r}(F)$.

Proof. If $x \in \Gamma_1(F) = F$, then by assumption on θ we have $\theta(x) \in [F, F] = \Gamma_2(F)$. Let $r \geq 2$ and suppose that for any $s < r$ the claim holds. If $x \in \Gamma_r(F) = [\Gamma_{r-1}(F), F]$, then by induction we get $\theta(x) \in [\Gamma_{2(r-1)}(F), \Gamma_2(F)] \leq \Gamma_{2r}(F)$. □

Lemma 2.0.12. Let $G = \langle H, t \mid t^{-1}xt = \theta(x), x \in H\rangle$ be an ascending HNN extension of a group H. Then any element of G can be written in the form $t^p h t^{-q}$ with $p, q \geq 0$ and $h \in H$. Moreover, we have $\langle H\rangle^G = \bigcup_{i\geq 0} t^i H t^{-i}$ where $\langle H\rangle^G$ denotes the normal closure of H in G.

Proof. The claim about the form elements of G take follows since for any $h \in H$, $ht = t\theta(h)$ and similarly $t^{-1}h = \theta(h)t^{-1}$ in G. For the second part, notice that certainly $t^i H t^{-i} \leq \langle H\rangle^G$ for any i. Since $G/\langle H\rangle^G \cong \langle t\rangle$, we have that if $g = t^p h t^{-q} \in \langle H\rangle^G$, then $p = q$. Thus $\langle H\rangle^G = \bigcup_{i\geq 0} t^i H t^{-i}$. □

Lemma 2.0.13. Let $G = F*_\theta$ be an ascending HNN extension of a non-abelian free group F of finite rank with $\mathrm{im}(\theta) \leq [F, F]$. Suppose that $x, y \in F$ are non-primitive in G and generate a free subgroup of rank 2. Then xy is primitive in G.

Proof. Suppose x, y and xy are all non-primitive. Let $x = u^m, y = v^n, xy = w^l$ for some $u, v, w \in G$ and $m, n, l \geq 2$. Let q be the canonical quotient map from G to $\langle t\rangle \cong \mathbb{Z}$ mapping F to 0. Then $u, v, w \in \ker q$ as x and y lie F. Note that $\ker(q)$ is the normalizer of F in G. By Lemma 2.0.12, there exist some $p \geq 0$ such that u, v, w lie in the free subgroup $t^p F t^{-p}$. But by [LS62], the equation $u^m v^n = w^l$ has a solution in a free group only if u, v, w generate a free subgroup of rank 1. This contradicts our hypothesis on x and y. □

For future reference we record the following simple lemma.

Lemma 2.0.14. Let $f\colon A \to A$ be an automorphism of a free abelian group A. If $f(ka) = la$ for some $a \neq 0$ and positive integers k, l, then $k = l$.

Proof. We have $A \cong \bigoplus_{i\in I} \mathbb{Z}$ for some index set I. Note that non-trivial element $a \in A$ is primitive if and only if the greatest common divisor of its finitely many non-zero coordinates equals 1. Moreover, any non-trivial $a \in A$ can be written as $a = d \cdot x$ with x primitive and $d \in \mathbb{N}$. Since f is an automorphism, it will preserve primitive elements. Now, suppose that $f(ka) = la$ with $k, l \in \mathbb{N}$ and $a \neq 0$. We write $a = d \cdot x$ as above with x primitive. Then $kf(x) = lx$ and by cancelling common factors we might as well assume that k and l are coprime. Since k divides all coordinates of the prime element x, it has to equal to 1 and the same holds for l since $f(x)$ is primitive. $\square$

Proposition 2.0.15. Let $G = \langle F, t \mid t^{-1}xt = \theta(x), x \in F\rangle$ be an ascending HNN extension of a non-abelian free group F of finite rank, and suppose that the image of θ lies in the commutator subgroup of F. If $x, y \in F \setminus [F, F]$ generate a non-abelian free subgroup in F and x is primitive, then the elements $\{x^k yx^k y^{-1} \mid k \geq 2\}$ form pairwise distinct primitive conjugacy classes. In particular, G does not have *b*$\mathcal{C}$*yc*.

Proof. Note first that $x^k yx^k y^{-1} = x^k \cdot (yxy^{-1})^k$ does not lie in $[F, F]$ and is primitive when $k \geq 2$ by Lemma 2.0.13. Note that every element in G can be written in the form $t^p wt^{-q}$ for some $p \geq 0, q \geq 0$ and $w \in F$ by Lemma 2.0.12. Now if $x^k yx^k y^{-1}$ is conjugate to $x^l yx^l y^{-1}$ for some $k \neq l$, then $x^k yx^k y^{-1} = (t^p wt^{-q})x^l yx^l y^{-1}(t^q w^{-1}t^{-p})$ for some $p, q \geq 0$ and $w \in F$. Hence $\theta^p(x^k yx^k y^{-1}) = w\theta^q(x^l yx^l y^{-1})w^{-1}$.

If $p \neq q$, the equation never holds. In fact, assume without loss of generality that $p > q$. By Lemma 2.0.10 we know that $\theta^q(x) \in \Gamma_r(F) \setminus \Gamma_{r+1}(F)$ for some $r \geq 2$. Then $\theta^p(x) \in \Gamma_{r+1}(F)$ by Corollary 2.0.11 and thus $\theta^p(x^k yx^k y^{-1}) \in \Gamma_{r+1}(F)$. On the other hand, $\theta^q(x^l) \in \Gamma_r(F) \setminus \Gamma_{r+1}(F)$ for any $l > 0$ since $\Gamma_r(F)/\Gamma_{r+1}(F)$ is a free abelian group by Lemma 2.0.10. Now $x^l yx^l y^{-1} = x^{2l} \cdot [x^l, y^{-1}]$ so that $\theta^q(x^l yx^l y^{-1}) = \theta^q(x^{2l})[\theta^q(x^l), \theta^q(y^{-1})]$ and $[\theta^q(x^l), \theta^q(y^{-1})] \in \Gamma_{r+1}(F)$ by Corollary 2.0.11, we have $\theta^q(x^l yx^l y^{-1}) \in \Gamma_r(F)\setminus\Gamma_{r+1}(F)$. So we would obtain that $w\theta^q(x^l yx^l y^{-1})w^{-1} \in \Gamma_r(F) \setminus \Gamma_{r+1}(F)$, whereas $\theta^p(x^k yx^k y^{-1}) \in \Gamma_{r+1}(F)$. Hence the equation cannot hold.

If $p = q$, then the equation again cannot hold unless $k = l$. In fact, let $r \in \mathbb{N}$ such that $\theta^p(x) \in \Gamma_r(F) \setminus \Gamma_{r+1}(F)$, then $\theta^p(x^k yx^k y^{-1})$ lies in $\Gamma_r(F) \setminus \Gamma_{r+1}(F)$ by the same argument as above. By forming the quotient by $\Gamma_{r+1}(F)$ we obtain an equation in the free abelian group $\Gamma_r(F)/\Gamma_{r+1}(F)$. Writing elements in the quotient using brackets, we would have $k\left([\theta^p(x)] + [\theta^p(yxy^{-1})]\right) = l\left([w\theta^p(x)w^{-1}] + [w\theta^p(yxy^{-1})w^{-1}]\right)$. Note that $\Gamma_r(F)/\Gamma_{r+1}(F)$ is a free abelian group by Lemma 2.0.10 and the action of w on $\Gamma_r(F)/\Gamma_{r+1}(F)$ induced by conjugation is an isomorphism. Thus the equation $k\left([\theta^p(x)] + [\theta^p(yxy^{-1})]\right) = l\left([w\theta^p(x)w^{-1}] + [w\theta^p(yxy^{-1})w^{-1}]\right)$ can never hold unless $k = l$ by Lemma 2.0.14. $\square$

Actually we have some supporting evidence that the ascending HNN extensions appearing in Proposition 2.0.15 are actually hyperbolic. Recall that containing a Baumslag-Solitar group is an obstruction for a group to be hyperbolic. For some classes of groups like one-relator groups and ascending HNN extensions of finitely generated free groups it is conjectured that this is the only obstruction. Kapovich [Kap00] shows that this conjecture holds for ascending HNN extensions of finitely generated free groups where the associated injective endomorphism used to form the HNN extension is a so-called immersion [Kap00, Definition 3.1]. However, the endomorphims we consider are not necessarily immersions.

Proposition 2.0.16. Let $G = \langle F, t \mid t^{-1}xt = \theta(x), x \in F\rangle$ be an ascending HNN extension of a non-abelian free group F of finite rank, and suppose that the image of θ lies in the commutator subgroup of F. Then G does not contain any Baumslag-Solitar subgroup.

Proof. Let N be the kernel of the canonical homomorphism $\pi\colon G \to \langle t \rangle \cong \mathbb{Z}$ and note that N is locally free. Suppose G contains a Baumslag-Solitar subgroup generated by a, b which satisfy $ba^m b^{-1} = a^n$ for some non-zero $m, n \in \mathbb{Z}$. By applying the homomorphism π we see that $a \in \ker(\pi) = N$ or $m = n$. Let us consider the first case. By Lemma 2.0.12 we can write $a = t^k x t^{-k}$ and $b = t^p y t^{-q}$ for some $k, p, q \geq 0$ and $x, y \in F$. The equation then reads $yt^\alpha x^m t^{-\alpha} y^{-1} = t^\beta x^n t^{-\beta}$ or equivalently $x^{-n} t^{-\beta} y t^\alpha x^m t^{-\alpha} y^{-1} t^\beta = 1$ where $\alpha = k - q$ and $\beta = k - p$. If $\alpha \geq 0$ and $\beta \geq 0$, we obtain $x^{-n}\theta^\beta(y) t^{\alpha-\beta} x^m t^{-(\alpha-\beta)} \theta^\beta(y)^{-1} = 1$. By Britton's Lemma this equation can only hold if $\alpha = \beta$ or we have a pinch, so $\gamma = \beta - \alpha > 0$. If $\alpha = \beta$, then $p = q$ and so $b \in N$. But as N is locally free, it does not contain a Baumslag-Solitar group. So assume that $\gamma > 0$ in the following. If we let $\omega = \theta^\beta(y)$ we then obtain $\omega\theta^\gamma(x^m)\omega^{-1} = x^n$. However, this is impossible by Lemma 2.0.10 and the fact that the image of θ is contained in $[F, F]$. If $\alpha \geq 0$ and $\beta < 0$, then it is easy to see that the expression is already reduced and thus non-trivial. If $\alpha < 0$ and $\beta < 0$, we observe that the expression $x^{-n} t^{-\beta} y \theta^\alpha(x^m) y^{-1} t^\beta$ is reduced and thus represents a non-trivial element. Similarly, one can exclude the case that $\alpha < 0$ and $\beta > 0$. Lastly, if $\alpha < 0$ and $\beta = 0$, we obtain $y\theta^\alpha(x^m)y^{-1} = x^n$, which is also impossible by Lemma 2.0.10.

Hence we are left to consider the case that $n = m$. Suppose that $g, h \in G$ generate a free abelian group of rank 2. Recall that $G \cong N \rtimes \mathbb{Z}$ so that after taking suitable powers g^i and h^j we can arrange that $g^i h^{-j} \in N$. Hence in the following we can suppose without loss of generality that $g \in N$. We can write $g = t^k x t^{-k}$ and $h = t^p y t^{-q}$ with $k, p, q \geq 0$ and $x, y \in F$. Since g and h commute, we obtain $1 = t^{-\alpha} x^{-1} t^\alpha y t^{-\beta} x t^\beta$ where $\alpha = p - k$ and $\beta = q - k$. If $\alpha \geq 0$ and $\beta \geq 0$, we obtain $y\theta^\beta(x)y^{-1} = \theta^\alpha(x)$ which implies that $\alpha = \beta$ using Lemma 2.0.10. Hence $p = q$ and $h \in N$. But N does not contain a free abelian group of rank 2. If $\alpha > 0$ and $\beta < 0$, then we observe that $\theta^\alpha(x^{-1}) y t^{-\beta} x t^\beta$ does not contain a pinch. Similarly one can exclude the case that $\alpha < 0$ and $\beta > 0$. If $\alpha < 0$ and $\beta < 0$ we rewrite $y = t^{-\alpha} x^{-1} t^\alpha y t^{-\beta} x t^\beta = t^{-\alpha} x^{-1} t^{-\beta} \theta^{-(\alpha+\beta)}(y) t^\alpha x t^\beta$ and the latter expression does not contain any pinch. The remaining cases that $\alpha = 0$ and $\beta < 0$ resp. $\alpha < 0$ and $\beta = 0$ can be excluded in a similar way. □

Theorem 2.0.17. Let G be an HNN extension of a free group of finite rank, then G does not have $b\mathcal{C}yc$.

Proof. By Proposition 2.0.7, we can assume $G = \langle F_n, t \mid t^{-1}xt = \theta(x), x \in F_n \rangle$, where $\theta\colon F_n \to F_n$ is injective and F_n denotes a free group of rank n. For $n = 1$ the group G is solvable but not virtually cyclic. Thus G does not have $b\mathcal{C}yc$ by Theorem 1.2.15. So in the following we assume that $n > 1$.

Note first that we have an induced map $\bar{\theta}\colon F_n/[F_n, F_n] \to F_n/[F_n, F_n] \cong \mathbb{Z}^n$. Since the rank of the abelian group is finite, there exists some $k \geq 1$ such that $\mathrm{rank}(\ker(\bar{\theta}^{k+1})) = \mathrm{rank}(\ker(\bar{\theta}^k))$. But since $\mathbb{Z}^n$ is free abelian, it follows that $\ker(\bar{\theta}^{k+1}) = \ker(\bar{\theta}^k)$, and we will denote this group by K. This implies that $\bar{\theta}^k$ induces an injective endomorphism of $\mathbb{Z}^n/K$. If K is a proper subgroup of $\mathbb{Z}^n$, we consider the induced quotient map $F_n *_{\theta^k} \to (\mathbb{Z}^n/K)*_{\bar{\theta}^k}$. Note that the quotient is a torsion-free metabelian group which is not virtually cyclic. Hence

$F_n *_{\theta^k}$ does not have $b\mathcal{C}yc$ by Theorem 1.2.15 and Lemma 1.1.7. As $F_n *_{\theta^k}$ is a finite index subgroup of $F_n *_\theta$ (see for example [Kap00, 2.2]) we conclude that the latter group does not have $b\mathcal{C}yc$ by Lemma 1.1.8.

If $K = \mathbb{Z}^n$, we are in the situation that the image of θ^k lies in the commutator subgroup of F_n. By Proposition 2.0.15 the group $F_n *_{\theta^k}$ does not have $b\mathcal{C}yc$. Again by Lemma 1.1.8 it follows that $F_n *_\theta$ does not have $b\mathcal{C}yc$. □

We now want to apply the previous results to answer Question 1.2.18 affirmatively for the class of one-relator groups. Recall that a *one-relator group* is a group G which has a presentation with a single relation, so $G = \langle x_1, \ldots, x_n \mid r \rangle$ where r is a word in the free group F on the letters $x_1, \ldots, x_n$. The group G is torsion-free precisely when r, as an element of the free group F, is not a proper power. If $r = s^n$ for some maximal $n \geq 2$ and $s \in F$, then s, considered as an element in G, is of order n. In all cases there exists a finite G-CW model for $\underline{\underline{E}}G$, see for example [Lüc05, 4.12].

A one-relator group with torsion is a hyperbolic group by Newman's Spelling Theorem [New68]. In particular, the one-relator groups containing torsion satisfy Conjecture 1.2.2 by the work of Juan-Pineda and Leary. However, our proof of the following theorem does not depend on this fact.

Theorem 2.0.18. A one-relator group has $b\mathcal{VC}yc$ if and only if it is cyclic.

Proof. Let G be a one-relator group. If the one-relator presentation of G contained three or more generators then G would surject to $\mathbb{Z}^2$, in particular G would not have $b\mathcal{VC}yc$ by Corollary 1.2.16. Thus we can restrict to the case that G has two generators, so

$$G = \langle a, b \mid R(a, b) = 1 \rangle$$

for some word $R(a, b)$ in the free group on the two generators a, b. By [LS, Lemma V.11.8] we can moreover assume that the exponent sum of one of the generators in the single relator equals to zero, say for the generator a. The following rewriting procedure, which we outline for the reader's convenience, is standard. The proofs of the mentioned facts can be found in [LS, IV.5]. We let $b_i = a^i b a^{-i}$ for all $i \in \mathbb{Z}$. Then R can be rewritten as a cyclically reduced word R' in terms of these, so $R' = R'(b_m, \ldots, b_M)$ for some $m \leq M$, such that the elements b_m, b_M occur in R'. If $m = M$, then $R(a, b) = b^m$ for some $m \in \mathbb{Z}$ and thus $G \cong \mathbb{Z}$ or $G \cong \mathbb{Z} * \mathbb{Z}/|m|$ where $|m| \geq 2$. Note that by Proposition 2.0.3 the latter group does not have $b\mathcal{VC}yc$. So in the following we can assume that $m < M$. We let

$$H = \langle b_m, \ldots, b_M \mid R'(b_m, \ldots, b_M) = 1 \rangle.$$

Moreover we define A to be the subgroup of H generated by $b_m, \ldots b_{M-1}$ and we let B to be the subgroup of H generated by $b_{m+1}, \ldots b_M$. Then A and B are free subgroups of the one-relator group H and G is isomorphic to the HNN extension $H *_\theta$ where $\theta \colon A \to B$ is the isomorphism defined by $\theta(b_i) = b_{i+1}$ for $m \leq i < M$.

If $[H : A] \geq 2$ and $[H : B] \geq 2$, then G does not have $b\mathcal{VC}yc$ by Proposition 2.0.7. Otherwise G is an ascending HNN extension, say with $H = A$. Since A was free, G is an ascending HNN extension of a finitely generated free group. The claim now follows from Theorem 2.0.17. □

3. Conjugacy Growth and Finiteness of Classiying Spaces

In this chapter we shall establish a connection between the $b\mathcal{VC}yc$ property and the so-called conjugacy growth function for finitely generated groups under the assumption that cyclic subgroups are undistorted. The basic idea being that a group G with $b\mathcal{VC}yc$ should "look" like a virtually cyclic group up to conjugation and thus should have the same conjugacy growth function as a virtually cyclic group. As applications we will be able to prove Conjecture 1.2.2 on the finiteness of the classifying space for virtually cyclic subgroups for the class of linear groups and CAT(0) cube groups. The proof for the class of linear groups has already been given in [vW17], whereas for CAT(0) groups we provide an alternative proof.

First, let us set up some notation. Let G be a finitely generated group and let S be a finite generating set that is symmetric, i.e. $S = S^{-1}$. Recall that with such a choice of generating set we can define the so-called *word norm* on G by setting $|g|_S = \min\{n \mid g = s_1 s_2 \ldots s_n \text{ where } s_i \in S\}$. The word norm on G induces the *word metric* by setting $d_S(g,h) = |g^{-1}h|$ for $g,h \in G$. Let $B_{G,S}(n)$ denote the ball of radius n around the identity element of G with respect to the word metric d_S. We define the word growth function $\beta_S^G \colon \mathbb{N} \to \mathbb{N}$ of G with respect to S by $\beta_S^G(n) = |B_{G,S}(n)|$, so $\beta_S^G(n)$ measures the number of elements in G whose shortest length expression in terms of the generating set S does not exceed n.

In recent years, also popularized by Guba and Sapir [GS10], a growth function of a similar spirit received increasing attention:

Definition 3.0.1. Let G be a finitely generated group with S a symmetric finite generating set. The *conjugacy growth function* $\gamma_S^G \colon \mathbb{N} \to \mathbb{N}$ of G with respect to S is defined by

$$n \mapsto |\{(g) \mid (g) \cap B_{G,S}(n) \neq \emptyset\}| .$$

Here, (g) denotes the conjugacy class of an element $g \in G$. Of course, $\gamma_S^G(n) \leq \beta_S^G(n)$.

In order to obtain an invariant of the group which does not depend on the specific generating set, we need to impose an equivalence relation. For two functions $f, g \colon \mathbb{N} \to \mathbb{N}$ we write $f \preceq g$ if there exists some $C \in \mathbb{N}$ such that $f(n) \leq g(Cn)$ for all $n \in \mathbb{N}$. And we write $f \sim g$ if $f \preceq g$ and $g \preceq f$.

With this notion of equivalence, the class of the word growth resp. conjugacy growth function does not depend on the generating set. If S and T are finite symmetric generating sets of G, let $K = \max\{|s|_T \mid s \in S\}$. Then $|\omega|_T \leq K \cdot |\omega|_S$ for any $\omega \in G$ and from this it follows that $\gamma_T^G(Kn) \geq \gamma_S^G(n)$, thus $\gamma_S^G \preceq \gamma_T^G$.

In the following we will only talk about the class of the word growth resp. conjugacy growth function and thus we will omit the generating set from the notation.

Examples 3.0.2. (1) The free abelian group $\mathbb{Z}^m$ has word growth $\beta(n) \sim n^m$. Since the conjugation action is trivial, $\gamma(n) \sim \beta(n)$.

(2) A non-abelian finitely generated free group F has exponential word growth $\beta(n) \sim 2^n$. Since in a free group two reduced words are conjugate if and only if they are cyclic permutations of each other, the conjugacy growth is exponential as well since $\gamma(n) \sim 2^n/n \sim 2^n$. More generally, non-elementary hyperbolic groups have exponential conjugacy growth [CK02].

(3) Let us consider the Baumslag-Solitar group $BS(1,2) = \langle a, t \mid t^{-1}at = a^2 \rangle$. Observe that $t^{-n}at^n = a^{2^n}$, which implies that the word length of a^m is $O(\log(|m|))$. Since a^k and a^l are not conjugate if $k \neq l$ and k, l are odd, we see that $BS(1,2)$ has exponential conjugacy growth.

(4) The Heisenberg group $H = \langle x, y, z \mid [x,y] = z, [z,x] = 1 = [y,z] \rangle$ has word growth $\beta(n) \sim n^4$ but conjugacy growth $\gamma(n) \sim n^2 \log(n)$, see for example [GS10].

Geometrically, one can interpret the conjugacy growth function as follows. Given a closed Riemannian manifold M, the set of free homotopy classes of loops in M is in bijective correspondence with the set of conjugacy classes of $\pi_1(M)$ and by the Švarc-Milnor Lemma the conjugacy growth function of $\pi_1(M)$ is then equivalent to the function counting free homotopy classes of loops which have a representative of a given length.

Let us record here the following two basic properties of the conjugacy growth function.

Lemma 3.0.3. Let G be a finitely generated group. Then the following assertions hold:

(1) Suppose $H \leq G$ is a finite index subgroup. Then $\gamma^H \preceq \gamma^G$.

(2) If Q is a quotient of G, then $\gamma^Q \preceq \gamma^G$.

Proof. This is [Bd10, Lemma 3.1]. □

For metric spaces, and in particular for finitely generated groups, there is an equivalence relation called quasi-isometry, that tries to capture the large-scale geometry of the metric space. For finitely generated groups the inclusion of a finite index subgroup into the group is an example of a quasi-isometry. It is known that the word growth β is an invariant under quasi-isometry. However, quasi-isometry invariance of the conjugacy growth γ fails in the most extreme way: Hull and Osin [HO13] show that there exists a finitely generated group G of exponential conjugacy growth that contains a subgroup of index two which contains only two conjugacy classes. In particular, this finite index subgroup has constant conjugacy growth. In Chapter 4 we will build on their work to show that there also exists a finitely generated group without *b$\mathcal{C}$yc* which has a subgroup of index two with property *b$\mathcal{C}$yc*.

The next question we want to address shortly is which functions (up to the mentioned equivalence relation) can occur as the word growth or conjugacy growth function of a finitely generated group. For the following, keep the example of the Heisenberg group in mind. A celebrated theorem of Gromov asserts that a finitely generated group G with polynomially bounded word growth is already virtually nilpotent. And by a theorem of Bass [Bas72] a finitely generated virtually nilpotent group has polynomial word growth $\beta(n) \sim n^{d(G)}$, where the exponent $d(G)$ can be computed via $d(G) = \sum_{k\geq 1} k \cdot \operatorname{rank}(\Gamma_k/\Gamma_{k+1})$. Here Γ_k denotes the the k-th term in the lower central series of G and rank denotes the rank of an abelian group. In particular, from the above considerations it follows that there is no group that has word growth $n^2 \log(n)$ for example. The situation for the conjugacy growth is again very different. Note that the conjugacy growth function is at most exponentially growing as well as non-decreasing. A theorem of Osin and Hull [HO13] asserts that these are the only restrictions, i.e. any exponentially bounded non-decreasing function can be realized as the conjugacy growth function of a finitely generated group.

Guba and Sapir made a couple of conjectures in [GS10] about the behaviour of the conjugacy growth function for certain "reasonable" classes of groups. Some of these have been resolved by now and we want to highlight two of these results:

Theorem 3.0.4 (Breuillard–de Cornulier, [Bd10])**.** If G is a virtually solvable finitely generated group that is not virtually nilpotent, then G has exponential conjugacy growth.

Finitely generated linear groups are known to satisfy the Tits alternative, which says that such a group is either virtually solvable or contains a non-abelian free subgroup. In particular, a non virtually solvable linear group has exponential word growth. But more is true:

Theorem 3.0.5 (Breuillard–de Cornulier–Lubotzky–Meiri, [Bre+13])**.** Let G be a finitely generated linear group that is not virtually solvable. Then G has exponential conjugacy growth.

Before we can prove the main theorem connecting the $b\mathcal{VC}yc$ and conjugacy growth notion, we need to set up some further notation. Let G be a group with a finite symmetric generating set S. For an element $g \in G$, we define its *length up to conjugacy* by

$$|g|_S^c = \min\left\{\left|hgh^{-1}\right|_S \mid h \in G\right\}.$$

By definition, this number only depends on the conjugacy class (g) of g.

Definition 3.0.6. [BH99, III.Γ.3.13] Let G be a finitely generated group with S a symmetric finite generating set of G. The *algebraic translation number* of an element $g \in G$ with respect to S, denoted by $||g||_S$, is defined by the limit

$$||g||_S \coloneqq \lim_{n\to\infty} \frac{|g^n|_S}{n}.$$

An element $g \in G$ is *undistorted* if the translation number $||g||_S$ is positive.

It is easy to see that an element $g \in G$ of a finitely generated group G is undistorted if and only if the cyclic subgroup $\langle g\rangle$ is quasi-isometrically embedded in G.

Theorem 3.0.7. Let G be a finitely generated group with $b\mathcal{VC}yc$. Suppose that the virtually cyclic witnesses are quasi-isometrically embedded. Then the conjugacy growth function of G is at most linear.

Proof. Let S be a finite generating set for G and let $\{V_1, \ldots, V_m\}$ be a witness to $b\mathcal{VC}yc$. First note that there are only finitely many conjugacy classes of elements of finite order in a virtually cyclic subgroup, so in the following it suffices to count the number of infinite order elements. We denote by $o(g)$ the order of an element $g \in G$. Now observe that

$$\begin{aligned}\{(g) \mid o(g) = \infty, |g|_S^c \leq n\} &\subseteq \bigcup_{i=1}^{m} \{(g) \mid o(g) = \infty, |g|_S^c \leq n, \text{ where } g \in V_i\} \\ &\subseteq \bigcup_{i=1}^{m} \{g \in V_i \mid o(g) = \infty, |g|_S^c \leq n\}\ .\end{aligned}$$

Now $|g|_S^c \geq ||g||_S$, hence $\{g \in V_i \mid o(g) = \infty, |g|_S^c \leq n\} \subseteq \{g \in V_i \mid o(g) = \infty, ||g||_S \leq n\}$. Since the subgroup V_i is quasi-isometrically embedded, the cardinality of the latter set is bounded by $C_i n$ for some constant $C_i > 0$: We know from Lemma 1.2.9 that there exists some $g_0 \in V_i$ and $k \in \mathbb{Z}$ (that only depends on V_i) such that for any $g \in V_i$ of infinite order there exists some $m \in \mathbb{Z}$ such that $g^k = g_0^m$. Hence $|k| \cdot ||g||_S = ||g^k||_S = ||g_0^m||_S = |m| \cdot ||g_0||_S$. In particular $|m| \leq \frac{n|k|}{||g_0||_S}$. The last expression makes sense, since $||g_0||_S > 0$, as $\langle g_0 \rangle$ is quasi-isometrically embedded. It then follows that $|\{g \in V_i \mid o(g) = \infty, ||g||_S \leq n\}| \leq 2\frac{n|k|}{||g_0||_S}|F_i|$, where F_i is the unique maximal normal finite subgroup of V_i. □

Conjecture 1.2.1 due to Juan-Pineda and Leary has been verified for hyperbolic groups in their original paper [JL06]. Alternatively, this also follows from Theorem 3.0.7 together with a result due to Coornaert–Knieper [CK02] which states that non-elementary hyperbolic groups have exponential conjugacy growth.

Corollary 3.0.8. A hyperbolic group G has $b\mathcal{VC}yc$ if and only if G is virtually cyclic.

3.1. Linear Groups

The goal of this section is to prove Conjecture 1.2.2 for the class of linear groups by basically using results on the conjugacy growth of these groups. Special care has to be taken if there are distorted elements present, so in general Theorem 3.0.7 is not directly applicable.

Definition 3.1.1. For a field $\mathbb{K}$ and $d \in \mathbb{N}$, a subgroup of the general linear group $\mathrm{GL}_d(\mathbb{K})$ is called a *linear group*.

Let A be a finitely generated domain. It is a theorem of Platonov [Pla68] that $\mathrm{GL}_d(A)$ is virtually residually p-finite for all but finitely many primes p if $\mathrm{char}(A) = 0$. If $\mathrm{char}(A) = p$, then $\mathrm{GL}_d(A)$ is residually p-finite. From this Selberg's Lemma follows easily: A finitely generated linear group over a field of characteristic 0 is virtually torsion-free. Moreover, we have that a finitely generated linear group over an arbitrary field is residually finite.

In [GS10] it was conjectured that a non-virtually solvable finitely generated linear group has exponential conjugacy growth, which was later proven in [Bre+13]. In order to verify Conjecture 1.2.2 for linear groups, we rely on the following stronger result:

Theorem 3.1.2. [Bre+13, Theorem 1.2] For every d, there exists a constant $c(d) > 0$ such that if $\mathbb{K}$ is a field and S is a finite symmetric subset of $\mathrm{GL}_d(\mathbb{K})$ generating a non-virtually solvable subgroup, then

$$\liminf_{n\to\infty} \frac{\log \chi_S(n)}{n} \geq c(d)\,,$$

where $\chi_S(n)$ is the number of elements in $\mathbb{K}[X]$ appearing as characteristic polynomials of elements of $B_{G,S}(n)$.

Definition 3.1.3. Let $\mathbb{K}$ be a field. An *absolute value* on $\mathbb{K}$ is a function

$$|\cdot|\colon \mathbb{K} \to \mathbb{R}_{\geq 0}$$

that satisfies the following conditions:

(1) $|x| = 0$ if and only if $x = 0$.

(2) $|xy| = |x||y|$ for all $x, y \in \mathbb{K}$.

(3) $|x + y| \leq |x| + |y|$ for all $x, y \in \mathbb{K}$.

Lemma 3.1.4. Let G be finitely generated subgroup of $\mathrm{GL}_d(\mathbb{K})$ where $\mathbb{K}$ is some field. Let $g \in G$ be an element such that at least one of its eigenvalues is not a root of unity. Then g is undistorted.

Proof. First of all we can assume without loss of generality that $\mathbb{K}$ is a finitely generated field containing all eigenvalues of the element g since G is finitely generated. Let λ be an eigenvalue of g which is not a root of unity. By [Tit72, Lemma 4.1], up to replacing g by its inverse, there exists an absolute value $|\cdot|$ on a field extension $\mathbb{K}'$ of $\mathbb{K}$ such that $|\lambda| > 1$. Let $||\cdot||$ be a submultiplicative matrix norm on the vector space of $n \times n$ matrices over $\mathbb{K}'$. For example, we can take

$$||A|| = \max_i \Sigma_{j=1}^n |a_{ij}|$$

where $A = (a_{ij})$. Then for two $n \times n$ matrices A, B over $\mathbb{K}'$ we have $||AB|| \leq ||A|| \cdot ||B||$ and $|\mu| \leq ||A||$ for any eigenvalue μ of A.

Now, let $s_1, \ldots, s_m$ be the elements of some finite symmetric generating set S for G and let $s = \max_{1\leq i\leq m} ||s_i||$. If g can be written as a word of length l in the generators S, then $||g|| \leq s^l$. Hence $1 < |\lambda| \leq s^l$, so $l \geq \log_s |\lambda|$. Since g^k has eigenvalue λ^k, we have

$$|g^k|_S \geq \log_s |\lambda|^k\,,$$

thus

$$||g||_S = \lim_{k\to\infty} \frac{|g^k|_S}{k} \geq \log_s |\lambda|\,.$$

Therefore g is undistorted. $\square$

Lemma 3.1.5. Let G be finitely generated subgroup of $\mathrm{GL}_d(\mathbb{K})$ where $\mathbb{K}$ is a field of positive characteristic. Then any element of infinite order in G is undistorted.

Proof. If an element $g \in G$ has at least one eigenvalue which is not a root of unity, we are done by Lemma 3.1.4. So suppose that all eigenvalues of g are roots of unity. We claim that g must have finite order. In fact, some power h of g will only have eigenvalues equal to one, i.e. h is unipotent in $\mathrm{GL}_d(\mathbb{K})$. So $(h-I)^m = 0$ for some m. Choose n with $p^n \geq m$, where p is the characteristic of $\mathbb{K}$. Then

$$0 = (h-I)^{p^n} = h^{p^n} - I,$$

thus h has finite order, and so g has finite order. □

Proposition 3.1.6. Let $G \leq \mathrm{GL}_d(\mathbb{K})$ be a finitely generated group where $\mathbb{K}$ is a field of positive characteristic. Then G has $b\mathcal{VC}yc$ if and only if G is virtually cyclic.

Proof. If G is virtually solvable, then Theorem 1.2.15 implies the result. Otherwise we obtain a contradiction from Theorem 3.0.5 and Theorem 3.0.7 since virtually cyclic subgroups are undistorted by Lemma 3.1.5. □

For linear groups over fields of characteristic zero a slightly more involved argument has to be used since not all virtually cyclic subgroups are undistorted. However, counting the number of characteristic polynomials and using Theorem 3.1.2 suffices to show:

Theorem 3.1.7 ([vW17])**.** A finitely generated linear group has $b\mathcal{VC}yc$ if and only if G is virtually cyclic.

Since the property $b\mathcal{VC}yc$ passes to quotients by Lemma 1.1.7, we can immediately conclude that representations of finitely generated groups having $b\mathcal{VC}yc$ are rather trivial:

Corollary 3.1.8. Let $\varphi\colon G \to L$ be a surjective homomorphism where G is a finitely generated group with $b\mathcal{VC}yc$ and L is linear. Then L is virtually cyclic.

3.2. CAT(0) Groups

In this section, we study the conjugacy growth of CAT(0) groups. For example, we will show that CAT(0) groups containing $\mathbb{Z}^2$ as a subgroup have strictly faster than linear conjugacy growth. Moreover, we will be able to deduce that CAT(0) cube groups have linear conjugacy growth if and only if they are virtually cyclic. As an application we can then verify Conjecture 1.2.2 for the class of CAT(0) cube groups. Xiaolei Wu and I have shown this with different means already in [vW]. However, the basic ideas are quite similar.

Let us first recall the basic definition of CAT(0) spaces and CAT(0) groups. Given a metric space (X,d), we say that X is *geodesic* if any two points $p,q \in X$ can be joined by a geodesic, i.e. there is a map $\gamma\colon [0,l] \to X$ such that $\gamma(0) = p$, $\gamma(1) = q$ and $d(\gamma(t),\gamma(t')) = |t-t'|$ for all $t,t' \in [0,l]$. In particular, $l = d(p,q)$. We call the image of a geodesic connecting p and q a *geodesic segment* and denote it by $[p,q]$ (although there might be several such segments). A *geodesic triangle* Δ is given by three points x, y, z and geodesic segments $[x, y], [y, z], [z, x]$. For any such Δ there is a corresponding *comparison triangle* $\overline{\Delta}$ in Euclidean space, i.e. it is given by three points $\overline{x}, \overline{y}, \overline{z}$ that satisfy $d(x, y) = d(\overline{x}, \overline{y})$, $d(y, z) = d(\overline{y}, \overline{z})$ and $d(z, x) = d(\overline{z}, \overline{x})$. A point $\overline{p} \in [\overline{x}, \overline{y}]$ is called a *comparison point* of $p \in [x, y]$ if $d(x, p) = d(\overline{x}, \overline{p})$ and similarly there are comparison points for the other two geodesic segments. The triangle Δ is said to satisfy the CAT(0) inequality if $d(p, q) \leq d(\overline{p}, \overline{q})$ for all comparison points $\overline{p}, \overline{q}$. We say that X is a *CAT(0) space* if all geodesic triangles in X satisfy the CAT(0) inequality. Without going into details we want to mention that instead of considering general CAT(0) spaces one also often considers CAT(0) cube complexes which are CAT(0) spaces arising from gluing standard cubes. These CAT(0) cube complexes have a more combinatorial flavor and stronger ridigity results are known.

A group G is called a *CAT(0) group* resp. a *CAT(0) cube group* if it acts acts properly and cocompactly via isometries on a CAT(0) space resp. a CAT(0) cube complex. It is known that CAT(0) groups are finitely presented, have only finitely many conjugacy classes of finite subgroups and solvable subgroups are virtually abelian [BH99, III.Γ.1.1]. Ontaneda has shown [Ont05, Proposition A] that a CAT(0) group G admits a finite model for $\underline{E}G$. Moreover, Lück has proven in [Lüc09] that there is a finite-dimensional model for $\underline{\underline{E}}G$.

For studying the conjugacy growth function of groups it is usually important to find a good conjugacy invariant. For CAT(0) groups this invariant will be the translation length:

Definition 3.2.1. [BH99, II.6.1] Let X be a metric space and let g be an isometry of X. The *displacement function* of g is the function $d_g \colon X \to \mathbb{R}_{\geq 0}$ defined by $d_g(x) \coloneqq d(gx, x)$. The *translation length* of g is the number $|g| \coloneqq \inf\{d_g(x) \mid x \in X\}$. The set of points where d_g attains this infimum will be denoted by $\mathrm{Min}(g)$. For a group G acting by isometries on X, we let $\mathrm{Min}(G) \coloneqq \bigcap_{g \in G} \mathrm{Min}(g)$. An isometry g is called *semi-simple* if $\mathrm{Min}(g)$ is non-empty. An action of a group by isometries of X is called *semi-simple* if all of its elements are semi-simple.

It is clear that the translation length is invariant under conjugation, i.e. $|hgh^{-1}| = |g|$ for any $g, h \in G$. Moreover, for g semi-simple, we have that $|g^n| = |n| \cdot |g|$ for any $n \in \mathbb{Z}$. If G is a CAT(0) group, then any element of G is semi-simple [BH99, II.6.10]. Another important ingredient of our proofs will be the following theorem that translates the existence of a free abelian group into geometric data:

Theorem 3.2.2 (Flat Torus Theorem, [BH99, II.7.1])**.** Let A be a free abelian group of rank n acting properly by semi-simple isometries on a CAT(0) space X. Then:

(1) $\mathrm{Min}(A) = \bigcap_{\alpha \in A} \mathrm{Min}(\alpha)$ is non-empty and splits as a product $Y \times \mathbb{E}^n$, here $\mathbb{E}^n$ denotes $\mathbb{R}^n$ equipped with the standard Euclidean metric.

(2) Every element $\alpha \in A$ leaves $\mathrm{Min}(A)$ invariant and respects the product decomposition; α acts as the identity on the first factor Y and as a translation on the second factor $\mathbb{E}^n$.

(3) The quotient of each n-flat $Y \times \mathbb{E}^n$ by the action of A is an n-torus.

The question whether the converse of the Flat Torus Theorem holds, i.e. the question whether the existence of an n-dimensional flat in a CAT(0) space X implies that a group G

acting properly and cocompactly on X contains a free abelian subgroup of rank n, is known as the Flat Closing Conjecture. The Flat Closing Conjecture would imply, for example, that a CAT(0) group is hyperbolic if and only if it does not contain $\mathbb{Z}^2$.

For $x \in \mathbb{R}_{>0}$, denote by $B(x)$ the number of natural numbers which are expressible as the sum of two square integers. Landau and Ramanujan have shown that $B(x)$ is asymptotically proportional to $x/\sqrt{\ln(x)}$, i.e. the limit

$$K = \lim_{x\to\infty} \frac{x}{\sqrt{\ln(x)}}$$

exists and is positive. The number

$$K = \frac{1}{\sqrt{2}} \prod_{p\equiv 3 \pmod 4} \left(\frac{1}{1-1/p^2}\right)^{1/2} \approx 0.764\,,$$

where p denotes a prime number, is also known as the *Landau–Ramanujan constant.* A generalization of this result has been obtained by Paul Bernays in his Ph.D. thesis [Ber12]:

Theorem 3.2.3. Let $f(x,y) = ax^2 + bxy + cy^2 \in \mathbb{Z}[x,y]$ be a primitive (i.e. the coefficients a, b, c have no common non-trivial divisor) positive-definite quadratic form with negative discriminant $D = b^2 - 4ac$. Let $B_f(n)$ be the number of positive integers less than or equal to n which are representable by f. Then $B_f(n)$ grows asympotically proportional to $n/\sqrt{\ln n}$.

Recall that a two-dimensional lattice L is called *arithmetic* if there exists some real number s such that sL is isometric to a $\mathbb{Z}$-submodule of rank two in an imaginary quadratic number field. Otherwise the lattice is called *non-arithmetic.*

Proposition 3.2.4. Let v_1, v_2 be two linearly independent vectors in the plane $\mathbb{R}^2$, and for any $n \in \mathbb{N}$ let $S(n)$ be the number of elements in the set

$$\{||v|| \mid v = xv_1 + yv_2, ||v|| \leq n, x, y \in \mathbb{Z}\}\,.$$

Then $S(n)$ grows asympotically proportional to $n^2/\sqrt{\ln n}$ or n^2.

Proof. This is [MO06, Proposition 1]. If the lattice corresponding to v_1, v_2 is non-arithmetic, we obtain quadratic growth by [Küh96, Corollary, p.166]. Otherwise, possibly after scaling, the associated quadratic form of the lattice is positive definite with negative discriminant and we can apply Theorem 3.2.3 to obtain a growth rate of $n^2/\sqrt{\ln n}$. □

Proposition 3.2.5. Suppose that G is a CAT(0) group which contains a subgroup isomorphic to $\mathbb{Z}^2$. Then the conjugacy growth of G is strictly faster than linear.

Proof. Suppose G is acting properly and cocompactly on the CAT(0) space X and let $H \leq G$ be a free abelian subgroup of rank two. By the Flat Torus Theorem, H acts on a flat plane P inside X via translations. Let x_0 be a point in P, then the translation length of any $h \in H$ can be calculated easily via $d_X(x_0, hx_0)$, again by the Flat Torus Theorem. Now given $n > 0$, let $B^c_H(n)$ be the set of G-conjugacy classes of elements in H with word length up to conjugacy at most n. Since the translation length is an invariant of the conjugacy classes and $|h| = d_X(x_0, hx_0)$ for any $h \in H$, Proposition 3.2.4 together with the Švarc-Milnor lemma [BH99, I.8.19] imply that $|B^c_H(n)|$ grows asympotically at least as fast as $n^2/\sqrt{\ln n}$. □

A semi-simple isometry is called *hyperbolic* if its translation length is strictly positive. Moreover, one calls a hyperbolic isometry *rank one* if no axis of this isometry bounds a flat half-plane.

Lemma 3.2.6. Let G be a group which acts on a CAT(0) cube complex X properly and cocompactly via isometries and suppose that G is not virtually cyclic. Then G contains a rank one isometry or G contains a free abelian subgroup of rank 2.

Proof. This result is essentially due to Caprace and Sageev [CS11], see also [vW, Lemma 4.15]. □

Theorem 3.2.7. A CAT(0) cube group has at most linear conjugacy growth if and only if it is virtually cyclic.

Proof. By Lemma 3.2.6, we only need to deal with the case G contains a rank one isometry or a subgroup isomorphic to $\mathbb{Z}^2$. If G contains a rank-one isometry, then G is acylindrically hyperbolic [Sis16] and thus has exponential conjugacy growth by [HO13, Theorem 1.1]. If G contains $\mathbb{Z}^2$, the result follows from Proposition 3.2.5. □

Corollary 3.2.8. A CAT(0) group containing $\mathbb{Z}^2$ does not have $b\mathcal{V}\mathcal{C}yc$. In particular, a CAT(0) cube group has $b\mathcal{V}\mathcal{C}yc$ if and only if it is virtually cyclic.

Proof. Since infinite order elements in a CAT(0) group are undistorted, Theorem 3.0.7 applies. Then Proposition 3.2.5 respectively Theorem 3.2.7 yield the claim. □

4. Constructions of Monster Groups

In this chapter we want to construct groups that exhibit wild behaviour with respect to the BVC property and its variants $b\mathcal{C}yc$ and $b\mathcal{VC}yc$. Our constructions heavily rely on the machinery of HNN extensions that was introduced in Chapter 2. The output of these constructions will usually be a countable group with the desired exotic properties. To obtain a finitely generated group with the same properties, we will make use of small cancellation theory over relatively hyperbolic groups as developed in [Osi10] and [HO13]. This theory was used by Osin to give the first constructions of finitely generated groups with finitely many conjugacy classes. Most of the contents of this chapter have been published in [vW17].

There are various notions of relative hyperbolicity, most notable the definitions due to Bowditch and Farb [Bow12; Far98] that build on Gromov's idea of relative hyperbolicity. These turn out to be equivalent if one additionally imposes a condition called Bounded Coset Penetration or BCP for short in Farb's definition. We will quickly outline Osin's more general approach via relative Dehn functions in the following, see also [Osi06].

Given a group G and a collection $\{H_\lambda\}_{\lambda\in\Lambda}$ of subgroups of G, we say that G is generated by $X \subseteq G$ relative $\{H_\lambda\}_{\lambda\in\Lambda}$ if G is generated by $\bigcup_{\lambda\in\Lambda} H_\lambda \cup X$. We shall always assume that X is closed under taking inverses. We have a natural quotient map

$$F = (*_{\lambda\in\Lambda} H_\lambda) * F(X) \to G$$

where $F(X)$ is the free group with free basis X. We denote by N the kernel of this quotient map. Moreover, we let $\mathcal{H} = \bigsqcup H_\lambda \setminus \{1\}$ and by $(\mathcal{H} \cup X)^*$ we denote the free monoid generated by $\mathcal{H} \cup X$. We say that G has a *relative presentation* with generators X and relations $\mathcal{R} \subseteq (\mathcal{H} \cup X)^*$ if N is the normal closure of $\mathcal{R}$ in F. The relative presentation is said to be finite if X and $\mathcal{R}$ are finite. Any word $W \in (\mathcal{H} \cup X)^*$ that represents the trivial element in G can be written as $W = \prod_{i=1}^{k} f_i^{-1} R_i f_i$ in F where $f_i \in F$ and $R_i \in \mathcal{R}$. A function $f\colon \mathbb{N} \to \mathbb{N}$ is called a *relative isoperimetric function* if for any $n \in \mathbb{N}$ and any word $W \in (\mathcal{H} \cup X)^*$ of length at most n that represents the trivial element in G there is an expression as above with at most $k \leq f(n)$ relations. The smallest relative isoperimetric function of the given relative presentation is called *Dehn function*.

Definition 4.0.1. A group G is *hyperbolic relative* to a collection $\{H_\lambda\}_{\lambda\in\Lambda}$ of subgroups of G if G is finitely presented with respect to $\{H_\lambda\}_{\lambda\in\Lambda}$ and the relative Dehn function with respect to $\{H_\lambda\}_{\lambda\in\Lambda}$ is linear.

If G is a group that is hyperbolic relative to a family $\{H_\lambda\}_{\lambda\in\Lambda}$ of subgroups, we call an element $g \in G$ *parabolic*, if it is conjugate to an element lying in one of the parabolic subgroups H_λ. Non-parabolic elements of infinite order are called *loxodromic*. For $g \in G$ a loxodromic element, there exists a unique maximal virtually cyclic subgroup $E_G(g)$ that contains g. It is given by

$$E_G(g) = \{h \in G \mid \exists\ m \in \mathbb{N} \setminus \{0\} \text{ such that } h^{-1}g^m h = g^{\pm m}\}.$$

Recall that two elements $a, b \in G$ are called *commensurable* if there exists $k, l \in \mathbb{Z} \setminus \{0\}$ such that a^k is conjugate to b^l. A subgroup S of G is called *suitable* if there exist two loxodromic elements $s_1, s_2 \in S$ that are not commensurable such that $E_G(s_1) \cap E_G(s_2) = 1$.

Theorem 4.0.2 ([HO13, Theorem 6.2])**.** Let G be a group hyperbolic relative to a collection of subgroups $\{H_\lambda\}_{\lambda\in\Lambda}$, S a suitable subgroup and $t_1, \dots, t_m$ arbitrary elements of G. Let $N \in \mathbb{N}$ and X a finite relative generating set of G. Then there exists a group $\overline{G}$ and an epimorphism $q\colon G \to \overline{G}$ such that:

(a) The group $\overline{G}$ is hyperbolic relative to $\{q(H_\lambda)\}_{\lambda\in\Lambda}$.

(b) We have $q(t_i) \in q(S)$ for $1 \leq i \leq m$.

(c) The map q is injective on $B_{G,\mathcal{H}\cup X}(N)$.

(d) $q(S)$ is a suitable subgroup of $\overline{G}$.

(e) If G is torsion-free, then so is $\overline{G}$.

(f) If $g, g' \in B_{G,\mathcal{H}\cup X}(N)$, then g and g' are conjugate if and only if $q(g)$ and $q(g')$ are conjugate.

(g) If $g \in B_{G,\mathcal{H}\cup X}(N)$ is loxodromic, then $E_{\overline{G}}(q(g)) = q(E_G(g))$.

As in previous chapters, $B_{G,\mathcal{H}\cup X}(N)$ denotes the ball of radius N in the Cayley graph $\Gamma(G, \mathcal{H} \cup X)$. Note that the Cayley graph is in general not locally finite. In our applications we usually only use that $\bigcup_{\lambda\in\Lambda} H_\lambda \subseteq B_{G,\mathcal{H}\cup X}(N)$. The group $\overline{G}$ is defined by $\overline{G} = G/N$ where $N = \langle t_1w_1, \dots, t_mw_m\rangle^G$ for some elements $w_1, \dots, w_m \in S$. It is possible to choose $w_1, \dots, w_m \in [S, S]$, which will be important later on if we wish to define homomorphisms from $\overline{G}$ onto abelian groups that are induced from a corresponding homomorphism defined on G.

We will make use of the following two lemmas repeatedly. For the convenience of the reader, we recall their statements:

Lemma 4.0.3 ([Osi06, Theorem 1.4])**.** Let G be a group hyperbolic relative to a collection of subgroups $\{H_\lambda\}_{\lambda\in\Lambda}$. Then for every $\lambda \in \Lambda$ and $g \in G \setminus H_\lambda$ the intersection $H_\lambda \cap H_\lambda^g$ is finite.

In particular, if G is torsion-free and $h, h' \in H_\lambda$ are not conjugate in H_λ, then they are not conjugate in G.

Lemma 4.0.4 ([HO13, Lemma 2.14])**.** Let G be a group and A, B two isomorphic subgroups. Let $g \in G$ be an element that is not conjugate to any element of $A \cup B$. Then in the HNN extension $G*_{A^t=B}$

(1) g is conjugate to some $g' \in G$ in $G*_{A^t=B}$ if and only if g and g' are conjugate in G.

(2) If g is primitive in G, then it is primitive as an element of $G*_{A^t=B}$.

Proof. We will reproduce here the proof of (2), also correcting an inconsequential mistake. Suppose $\omega \in G*_{A^t=B}$ with $\omega^n \in G$. We claim that it follows that $\omega \in G$ or ω is conjugate to an element of $A \cup B$. To prove this we will induct on the t-length of ω. If a reduced word representing ω contains no stable letters, then certainly $\omega \in G$. Since $\omega^n \in G$ it also follows that the t-length of ω is even. Suppose now that the t-length of ω equals two, then we can write $\omega = g_0 t^\epsilon g_1 t^{-\epsilon} g_2$ where $\epsilon \in \{-1, 1\}$ and $g_0, g_1, g_2 \in G$. Then Britton's Lemma implies that $t^{-\epsilon} g_2 g_0 t^\epsilon$ is a pinch or freely trivial, so $t^{-\epsilon} g_2 g_0 t^\epsilon = h \in A \cup B$. Without loss of generality, suppose that $h \in A$, then $g_2 g_0 \in B$. We then obtain $\omega^n = g_0 t^\epsilon (g_1 h)^{n-1} g_1 t^{-\epsilon} g_2$. Since $\omega^n \in G$, by Britton's Lemma it follows that $t^\epsilon (g_1 h)^{n-1} g_1 t^{-\epsilon}$ is trivial or a pinch and thus $t^\epsilon (g_1 h)^{n-1} g_1 t^{-\epsilon} = h'$ for some $h' \in B$. Hence $\omega^n = g_0 h' g_2 = g_0 h' g_2 g_0 g_0^{-1}$ is conjugate to $h' g_2 g_0 \in B$.

For the induction step, write $\omega = g_0 e^{\epsilon_0} \dots t^{-\epsilon_0} g_n$. As before, it follows that $t^{-\epsilon_0} g_n g_0 t^{\epsilon_0} = h$ for some $h \in A \cup B$. Let $u' = t^{-\epsilon_0} g_0^{-1} \omega g_0 t^{\epsilon_0} = g_1 t^{\epsilon_1} \dots g_{n-1} h$ and let u be a cyclically reduced conjugate of u'. Then u is conjugate to ω, so u^n is conjugate to $\omega^n \in G$. As u^n is cyclically reduced it follows that $u^n \in G$. Since u has shorter t-length than ω the induction hypothesis applies. ☐

Lemma 4.0.5. Let G be hyperbolic relative to a subgroup H and suppose that G is torsion-free. Let $h \in H$ be primitive as an element of H. Then h is primitive in G.

Proof. First note that non-trivial powers of loxodromic elements are loxodromic again. In fact, let g be loxodromic and suppose that g^n is parabolic for some $n \neq 0$, i.e. $g^n = \alpha y \alpha^{-1}$, where $y \in H$ and $\alpha \in G$. Then it would follow that $0 = \tau^{\mathrm{rel}}(y) = \tau^{\mathrm{rel}}(g^n) = |n| \tau^{\mathrm{rel}}(g) > 0$ by [Osi06, Lemma 4.24, Theorem 4.25], where $\tau^{\mathrm{rel}}(g)$ denotes the relative translation number of g.

So if $h = g^n$ for some $g \in G$ and $n \geq 1$, then g has to be parabolic, i.e. $g = \alpha x \alpha^{-1}$ for some $x \in H$ and $\alpha \in G$. By Lemma 4.0.3 it follows that $\alpha \in H$, thus $n = 1$, since h was primitive in H. ☐

Lemma 4.0.6. Let G be a group and let $a, b \in G$ be two primitive elements. Then any primitive element $g \in G$, considered as an element of the HNN extension $G*_{a^t=b}$ is still primitive.

Proof. Let $g \in G$ be a primitive element. If g is neither conjugate to an element of $\langle a \rangle$ nor $\langle b \rangle$, then Lemma 4.0.4 implies that g is primitive as an element of the HNN extension. So we can assume without loss of generality that $g = a$. Let $a = \omega^n$ with $n \geq 1$, where ω is of t-length 2, so $\omega = g_0 t^\epsilon g_1 t^{-\epsilon} g_2$ for $g_0, g_1, g_2 \in G$ and $\epsilon \in \{\pm 1\}$. For the equality $a = \omega^n$ to hold, the expression $t^{-\epsilon} g_0 g_2 t^\epsilon$ must be a pinch or trivial, so say $g_2 g_0 = b^m$ for some m. Then $t^{-\epsilon} g_2 g_0 t^\epsilon = a^m$. Expanding the power of ω, we obtain

$$\omega^n = g_0 t^\epsilon g_1 (a^m g_1)^{n-1} t^{-\epsilon} g_2 \,.$$

This implies that $g_1 (a^m g_1)^{n-1} \in \langle a \rangle$, say $g_1 (a^m g_1)^{n-1} = a^k$. Thus

$$a = \omega^n = g_0 b^k g_2 = g_0 b^k g_2 g_0 g_0^{-1} = g_0 b^{k+m} g_0^{-1}$$

But since a is primitive in G, it follows that $k + m \in \{\pm 1\}$. The equation $g_1 (a^m g_1)^{n-1} = a^k$ is equivalent to $(a^m g_1)^n = a^m a^k = a^{m+k} = a^{\pm 1}$, which implies that $n = 1$, again since a is primitive. The induction step works as in the proof of Lemma 4.0.4. ☐

Lemma 4.0.7. Let G be a group and let $a, b \in G$ be arbitrary non-trivial elements. Then any primitive element $g \in G$, considered as an element of the HNN extension $G*_{(a^n)^t=b^m}$ is primitive as long as $|n|, |m| \geq 2$.

Proof. Let $g \in G$ be a primitive element. Then g is neither conjugate to an element of $\langle a^n \rangle$ nor $\langle b^m \rangle$. Thus the claim follows from Lemma 4.0.4. □

The next proposition shows that the converse of Lemma 1.2.10 does not hold, even if we additionally impose finite generation on the group.

Proposition 4.0.8. There exists a finitely generated torsion-free group G with a finite index subgroup H such that H has *b$\mathcal{C}$yc*, but G does not.

Proof. The construction of [HO13, Theorem 7.2] already provides an example. We give the additional arguments here that are necessary to show that the constructed group fails to have *b$\mathcal{C}$yc*. First, in [HO13, Lemma 7.1] a countable torsion-free group C is constructed that contains a subgroup N of index 2 such that N has exactly two conjugacy classes. Moreover, there is a free group $F \leq N$ of rank 2 and an element $a \in C$ such that for any two distinct elements $f_1, f_2 \in F$ the elements af_1 and af_2 are not conjugate. The construction of C proceeds by iteratively forming HNN extensions starting with the free group $A_0 = \langle a, b, c \rangle$ of rank 3 and the epimorphism $\varepsilon_0 \colon A_0 \to \langle a \mid a^2 = 1 \rangle \cong \mathbb{Z}_2$. We let $F = \langle b, c \rangle$. It is then clear that af with $f \in F$ is primitive in A_0. Suppose A_n and $\varepsilon_n \colon A_n \to \mathbb{Z}_2$ have already been constructed. Let $K_n = \ker(\varepsilon_n)$ and enumerate all elements of $K_n \setminus \{1\} = \{k_0, k_1, \ldots\}$ and form the multiple HNN extension

$$A_{n+1} = \langle A_n, (t_i)_{i \in \mathbb{N}} \mid k_i^{t_i} = k_0 \rangle .$$

We can extend ε_n to A_{n+1} by mapping all stable letters t_i to the neutral element of $\mathbb{Z}_2$. Note that $\varepsilon_n(af)$ for $f \in F$ is non-trivial. Hence by Lemma 4.0.4 it follows that the elements af with $f \in F$ are primitive in A_{n+1}. The group C is defined by $\bigcup_{n \geq 0} A_n$ and $N = \bigcup_{n \geq 0} K_n$. It is then clear that the elements af with $f \in F$ are still primitive in C.

In [HO13, Theorem 7.2] small cancellation theory is then used to produce a finitely generated torsion-free group G from C which contains a subgroup H of index 2 with only two conjugacy classes but such that G has exponential conjugacy growth. In particular, we know that H has *b$\mathcal{C}$yc*. We can now simply adapt the proof of Theorem 7.2. of [HO13] and observe that the elements af with $f \in F$ are primitive in the finite stages $G(i)$ of the construction by Lemma 4.0.5 since they lie in the parabolic subgroup C. Since af_1 and af_2 lie in different conjugacy classes for distinct elements $f_1, f_2 \in F$, the group G has infinitely many primitive conjugacy classes. Hence G does not have *b$\mathcal{C}$yc* by Lemma 1.2.13. □

Lemma 4.0.9. Let H be a torsion-free countable group. There exists a 2-generated torsion-free group G that contains H as a subgroup such that

(1) Any $g \in G$ is conjugate to an element of H.

(2) If $h \in H$ is primitive, then it is primitive as an element of G.

(3) If $h, h' \in H$ are not conjugate, then they are not conjugate in G.

Proof. Let
$$G(0) = H * F(x, y)$$
where $F(x, y)$ is the free group on the free generators x and y. Enumerate the elements of $H = \{1 = h_0, h_1, h_2, \ldots\}$ as well as $G(0) = \{1 = g_0, g_1, g_2, \ldots\}$.

Suppose the group $G(i)$ has been constructed such that $G(i)$ is hyperbolic relative to H, $\langle x, y\rangle$ is a suitable subgroup and $h_1, \ldots, h_i$ lie in $\langle x, y\rangle$ and g_j for $1 \leq j \leq i$ is conjugate to an element of H. Construct $G(i+1)$ from $G(i)$ as follows: If g_{i+1} is parabolic, then let $G'(i) = G(i)$, otherwise let $\iota\colon E_{G(i)}(g_{i+1}) \to \langle h_1\rangle$ be an isomorphism and form
$$G'(i) = \langle G_i, t \mid e^t = \iota(e) \text{ for } e \in E_{(G(i)}(g_{i+1})\rangle\,.$$

By [HO13, Corollary 2.16], $G'(i)$ is still hyperbolic relative to H and $\langle x, y\rangle$ is again suitable. Now apply Theorem 4.0.2 to the suitable subgroup $\langle x, y\rangle$, the words $\{h_{i+1}, t\}$ resp. $\{h_{i+1}\}$ to obtain $G(i+1)$. Observe that there is a canonical quotient map $G(i) \to G(i+1)$. Here we do not distinguish between H and its image in $G'(i)$ or $G(i+1)$. Note that $G(i+1)$ is also hyperbolic relative to H and $\langle x, y\rangle$ is again suitable.

Letting G be the direct limit of the $G(i)$, it follows that G will be two-generated and any element of G will be conjugate to an element of H. Moreover, if $h \in H$ is primitive, then it will remain primitive in $G(i)$ by Lemma 4.0.5 for any i, thus it will be primitive in G. By Lemma 4.0.3 non-conjugate elements in H remain non-conjugate in G. $\square$

Proposition 4.0.10. There exists a finitely generated torsion-free group G which has exactly three conjugacy classes $\{(1), (x), (x^2)\}$, where $x \in G$ is a primitive element.

Proof. We first construct a countable group as follows. We let $G_0 = \langle x\rangle \cong \mathbb{Z}$. Of course, the only primitive elements in G_0 are x and x^{-1}. Suppose we have already constructed a chain $G_0 \leq G_1 \leq \ldots \leq G_n$ of countable torsion-free groups such that the element x, viewed as an element of G_n, is primitive. To construct G_{n+1} out of G_n, we first enumerate all primitive elements of G_n by $\{p_1, p_2, \ldots\}$ and enumerate all non-trivial elements that are non-primitive by $\{g_1, g_2, \ldots\}$. Secondly, we form the multiple HNN extension
$$G_{n+1} = \langle G_n, \{s_i\}_{i\in\mathbb{N}}, \{t_i\}_{i\in\mathbb{N}} \mid p_i^{s_i} = x, g_i^{t_i} = x^2\rangle\,.$$

By an inductive application of Lemma 4.0.6 and Lemma 4.0.7 it follows that x remains primitive in G_{n+1}. Finally, we let $G = \bigcup_{n\geq 0} G_n$. By construction, G satisfies our desired properties. Note that since x is primitive, x and x^2 are non-conjugate. To obtain a finitely generated example we can apply Lemma 4.0.9. $\square$

Remark 4.0.11. If we let G be a group as constructed in Proposition 4.0.10 and $x \in G$ a primitive element, then $G \times \mathbb{Z}$ does not have *b$\mathcal{C}$yc*, since it has infinitely many primitive conjugacy classes $\{(x, n) \mid n \in \mathbb{Z}\}$. On the other hand, $G \times \mathbb{Z}$ has *b$\mathcal{C}$yc* if G is a torsion-free group with exactly two conjugacy classes.

As we have noted, if G is a torsion-free group with exactly two conjugacy classes $G \times \mathbb{Z}$ has *b$\mathcal{C}$yc*. However, the situation changes if we allow for a semidirect product:

Proposition 4.0.12. There exists a countable torsion-free group H with exactly two conjugacy classes such that a certain extension $H \rtimes \mathbb{Z}$ does not have *b*$\mathcal{C}$*yc*.

Proof. Let $G_0 = \langle a, b \rangle$ be a free group of rank 2, let $\varepsilon_0 \colon G_0 \to \mathbb{Z}$ be defined by mapping a to 0 and b to 1. Note that for any $m \in \mathbb{Z}$, the element ab^m is primitive and $\varepsilon_0(ab^m) = m$.

Suppose G_n and $\varepsilon_n \colon G_n \to \mathbb{Z}$ have been constructed. To obtain G_{n+1}, enumerate all non-trivial elements of $\ker \varepsilon_n$ by $\{g_1, g_2, \ldots\}$ and form the multiple HNN extension

$$G_{n+1} = \langle G_n, \{t_i\}_{i \in \mathbb{N}} \mid g_i^{t_i} = a \rangle .$$

We can extend ε_n to G_{n+1} to define $\varepsilon_{n+1} \colon G_{n+1} \to \mathbb{Z}$ by arbitrarily assigning a value to the stable letters t_i. Now note that for $m \neq 0$, $ab^m \in G_0 \leq G_n$ is neither conjugate to an element of $\langle g_i \rangle$, nor to an element of $\langle a \rangle$. Thus, by Lemma 4.0.4, the elements ab^m are primitive in G_{n+1} for $m \neq 0$.

Let G be the direct limit of the G_n, and let $\varepsilon \colon G \to \mathbb{Z}$ be induced by the epimorphisms ε_n. Any non-trivial element of $\ker(\varepsilon)$ is then conjugate to a. However, since for $m \neq 0$, the elements ab^m are primitive and obviously in different conjugacy classes as $\varepsilon(ab^m) = m$, it follows that G does not have *b*$\mathcal{C}$*yc*. $\square$

Proposition 4.0.13. For any $m \geq 1$, there exists a finitely generated torsion-free group G that has exactly $n + 1$ conjugacy classes $(1), (x_1), \ldots, (x_m)$ such that x_i^k is conjugate to x_i for any i and any $k \neq 0$.

Proof. Note that any torsion-free group with exactly two conjugacy classes will have the property that x^k is conjugate to x as long as x is non-trivial. So we will demonstrate the claim for $m = 2$, the general case follows from an analogous argument. Let $G_{-1} = \langle a, b \rangle$ be a free group of rank two, and define

$$G_0 = \langle G_{-1}, \{s_i\}_{i \in \mathbb{Z} \setminus \{0\}}, \{t_i\}_{i \in \mathbb{Z} \setminus \{0\}} \mid (a^i)^{s_i} = a, (b^i)^{t_i} = b \rangle .$$

Now observe that the elements a and b are not conjugate in G_0 by repeated application of Lemma 4.0.4. If we form an HNN extension with relation $(a^i)^{s_i} = a$ we apply Lemma 4.0.4 to the element b. For relations of the type $(b^i)^{t_i} = b$ we apply the same lemma to the element a.

We proceed constructing countable torsion-free groups G_n for $n \geq 1$ inductively. First, observe that we can write $G_n \setminus \{1\} = S_0 \sqcup S_a \sqcup S_b$, where S_a resp. S_b are those elements of G_n which have a non-trivial power that is conjugate to a resp. b, and S_0 being defined as the complement of $S_a \cup S_b$. Note that $S_a \cap S_b = \emptyset$: If $g \in S_a \cap S_b$, then $g^k \sim a$ and $g^l \sim b$ for some $k, l \neq 0$. But then $g^{kl} \sim a^l \sim a$, and at the same time $g^{kl} \sim b^k \sim b$. But this is impossible since a and b are not conjugate in G_n by induction. Our construction proceeds in two steps:

Step 1. Enumerate all element of $S_a \cup S_b = \{g_1, g_2, \ldots\}$. We form the multiple HNN extension

$$Q = \langle G_n, \{t_i\}_{i \in \mathbb{N}} \mid g_i^{t_i} = b \text{ if } g_i \in S_b \text{ , otherwise } g_i^{t_i} = a \rangle .$$

In other words Q is the direct limit of a sequence of HNN extensions $Q_0 \leq Q_1 \leq Q_2 \leq \ldots$ where $Q_0 = G_n$ and

$$Q_i = \langle Q_{i-1}, t_i \mid g_i^{t_i} = b \text{ if } g_i \in S_b \text{ , otherwise } g_i^{t_i} = a \rangle \, .$$

Now we prove by induction that a and b are not conjugate in Q_i for any i. Suppose the claim is true for Q_{i-1}. If $g_i \in S_a$ then apply Lemma 4.0.4 to the element b. Note that b is not conjugate to a power of a in Q_{i-1} by induction. Moreover b is not conjugate to g_i^n for any $n \neq 0$ in Q_{i-1}. Otherwise, it would follow that $b \sim b^k \sim g_i^{nk} \sim a^n \sim a$ in Q_{i-1} since there is some $k \neq 0$ such that $g_i^k \sim a$. Interchanging the roles of a and b, we see that the same conclusion holds if $g_i \in S_b$. Hence it follows that a and b are non-conjugate in Q.

Step 2. Enumerate all elements of $S_0 = \{h_1, h_2, \ldots\}$. Again we construct a sequence of HNN extensions $P_0 \leq P_1 \leq \ldots$, starting with $P_0 = Q$. Suppose P_{i-1} has been constructed and a, b are non-conjugate in P_{i-1}. To form P_i, we consider the following cases:

1. If a non-trivial power of h_i is conjugate to a in P_{i-1}, we form the HNN extension

   $$P_i = \langle P_{i-1}, s_i \mid h_i^{s_i} = a \rangle \, .$$

   We can again employ Lemma 4.0.4 to the element b to prove that a and b are non-conjugate in P_i using the same argument as in step 1.

2. If a non-trivial power of h_i is conjugate to b in P_{i-1}, we let

   $$P_i = \langle P_{i-1}, s_i \mid h_i^{s_i} = b \rangle \, .$$

   Again, interchanging the roles of a and b one sees that these two elements remain non-conjugate in P_i.

3. In the remaining case we can choose

   $$P_i = \langle P_{i-1}, s_i \mid h_i^{s_i} = a \rangle \, .$$

   and observe that Lemma 4.0.4 can be applied.

We let $G_{n+1} = \bigcup_{i \geq 0} P_i$. Note that a and b are non-conjugate in G_{n+1} and all elements of $G_n \setminus \{1\}$ are either conjugate to a or b in G_{n+1}.

Finally, we define $G = \bigcup_{n \geq 0} G_n$. Again, Lemma 4.0.9 yields a finitely generated example. □

We see in particular that for a group G as constructed in the previous proposition, the group $G \times \mathbb{Z}$ has $b\mathcal{C}yc$.

Example 4.0.14. Letting G be an infinite 2-generated group of exponent p with exactly p conjugacy classes (for example, as constructed in [Ols91, Theorem 41.2]), then the group $G \times \mathbb{Z}$ does not have $b\mathcal{C}yc$. This can be seen by considering the elements (x, p^n) for $n \in \mathbb{N}$ where $x \in G$ is non-trivial.

It is easy to see that a torsion-free group with infinitely many commensurability classes cannot have $b\mathcal{C}yc$. The following shows that a converse to Lemma 1.2.13 does not hold.

Proposition 4.0.15. There exists a finitely generated torsion-free group G without primitive elements that does not have $b\mathcal{C}yc$.

Proof. We first prove that there exists a torsion-free countable group without primitive elements and infinitely many commensurability classes. We start by an inductive procedure, letting $G_0 = F_2$ be the free group on two generators. In fact, any countable torsion-free group with infinitely many commensurability classes of elements would work as well. Suppose G_n has been constructed, enumerate all non-trivial elements $G_n \setminus \{1\} = \{g_1, g_2, \ldots\}$ and define G_{n+1} as the following multiple HNN extension:

$$G_{n+1} = \langle G_n, \{t_i\}_{i\in\mathbb{N}} \mid g_i^{t_i} = g_i^2 \rangle$$

Suppose $x, y \in G_n \setminus \{1\}$ are not commensurable. For any $i \in \mathbb{N}$ and for any $k, l \in \mathbb{Z} \setminus \{0\}$ it follows that x^k is not conjugate to an element of $\langle g_i \rangle$ or y^l is not conjugate to an element of $\langle g_i \rangle$. By Lemma 4.0.4 it follows that x and y are not commensurable in G_{n+1}. Letting G be the direct limit of the G_n, we have that there are infinitely many commensurability classes in G and any non-trivial element of G can be written as a proper power of a conjugate of itself. To obtain a finitely generated example, apply Lemma 4.0.9. □

Proposition 4.0.16. There exists a finitely generated torsion-free group G without $b\mathcal{C}yc$ and exactly two commensurability classes.

Proof. Let $G_0 = \langle a, b \rangle$ be a free group of rank two. Suppose G_n has been constructed, then enumerate all elements $\{g_1, g_2, \ldots\}$ of $G_n \setminus \{1\}$ that are not primitive. We form the multiple HNN extension

$$G_{n+1} = \langle G_n, \{t_i\}_{i\in\mathbb{N}} \mid g_i^{t_i} = b^2 \rangle .$$

By Lemma 4.0.7 any primitive element of G_n stays primitive in G_{n+1}. Similarly, also non-conjugate primitive elements $g, h \in G_n$ will stay non-conjugate in G_{n+1} by Lemma 4.0.4. If we let G be the direct limit of the G_n, then G contains infinitely many primitive conjugacy classes, thus G fails to have $b\mathcal{C}yc$. However, given any non-trivial element $g \in G$, by construction g^2 will be conjugate to b^2. Thus there are precisely two commensurability classes. Finally, to obtain a finitely generated group with the same properties, apply Lemma 4.0.9. □

Lemma 4.0.17. Let G be a group such that centralizers of all non-trivial elements are infinite cyclic. Let $a, b \in G$ and suppose that $a^n = b^m$ for some $m, n \neq 0$. If a is primitive, then $b \in \langle a \rangle$.

Proof. Note that $C_G(a^n) = \langle x \rangle$ for some $x \in G$ and $a \in C_G(a^n)$ and $b \in C_G(a^n)$, thus $a = x^k$ for some k and $b = x^l$ for some l. Since a is primitive it follows that $k = \pm 1$. Hence $b \in \langle a \rangle$. □

In a hyperbolic group the centralizers of infinite order elements are virtually cyclic [BH99, III.Γ.3.10]. In particular if G is torsion-free hyperbolic and g is a primitive element, then $C_G(\langle g \rangle) = \langle g \rangle$. Then $N_G(\langle g \rangle)$ is virtually cyclic, thus infinite cyclic, since G is torsion-free. So $N_G(\langle g \rangle) = \langle x \rangle$. As $g \in N_G(\langle g \rangle) = \langle x \rangle$ and g is primitive, we have $N_G(\langle g \rangle) = \langle g \rangle$ as well.

Lemma 4.0.18. Let G be a torsion-free hyperbolic group and let a, b be two primitive elements such that a is not conjugate to $b^{\pm 1}$. Then the HNN extension $G*_{a^t=b^k}$ is hyperbolic for any nonzero interger k.

Proof. By [KM98, Corollary 1], we only need to show that the HNN extension $G*_{a^t=b^k}$ is separated. Recall that a subgroup U of G is called conjugate separated if the set $\{u \in U \mid u^x \in U\}$ is finite for all $x \in G \setminus U$. And an HNN extension $G*_\theta$ for an isomorphism $\theta\colon U \to V$ is called separated if either U or V is conjugate separated, and the set $U \cap V^g$ is finite for all $g \in G$. Now $\langle a\rangle$ is conjugate separated since $C_G(\langle a\rangle) = N_G(\langle a\rangle) = \langle a\rangle$. And if $\langle a\rangle \cap \langle g^{-1}b^k g\rangle$ was non-empty, then $a^n = (g^{-1}bg)^{km}$ for some $m, n \neq 0$. By Lemma 4.0.17 it follows that b is conjugate to $a^{\pm 1}$ which contradicts our assumptions. □

Proposition 4.0.19. There exists a countable torsion-free group G and an epimorphism $\varepsilon\colon G \to \mathbb{Z}$ such that G has $b\mathcal{C}yc$ but $\ker(\varepsilon)$ does not.

Proof. Let $G_0 = \langle a, c, d\rangle$, and $\varepsilon_0\colon G_0 \to \mathbb{Z}$ be defined by mapping a to 1 and the other free generators to 0. Moreover, choose a bijection $\phi_0\colon \mathbb{N}_0 \to G_0 \setminus \{1\}$.

For each $n > 0$ we construct a countable torsion-free group G_n, an epimorphism $\varepsilon_n\colon G_n \to \mathbb{Z}$ and choose a bijection $\phi_n\colon \mathbb{N}_0 \to G_n \setminus \{1\}$ such that

(a) G_n is either an HNN extension of G_{n-1} through the stable letter t_n or equals G_{n-1}. Moreover, G_n is a hyperbolic group.

(b) $\varepsilon_n|_{G_{n-1}} = \varepsilon_{n-1}$.

(c) Any primitive element $x \in \ker(\varepsilon_{n-1})$ is primitive as an element of G_n.

(d) If two primitive elements $x, y \in \ker(\varepsilon_0)$ are conjugate in G_n, then the t_{n-1}-length of ω is at most one.

Furthermore we choose the bijection $\phi\colon \mathbb{N}_0 \to \mathbb{N}_0 \times \mathbb{N}_0$ which enumerates the elements of $\mathbb{N}_0 \times \mathbb{N}_0$ diagonally, i.e. $\{(0,0), (1,0), (0,1), (0,2), (1,1), \ldots\}$.

Now, suppose G_n has been constructed. Let $(i, j) = \phi(n)$ and let $g_n = \phi_i(j) \in G_n$. In G_n, if g_n is not primitive, or if it is conjugate to an element of $\langle a\rangle$ or $\langle d\rangle$, then set $G_{n+1} = G_n$, $\varepsilon_{n+1} = \varepsilon_n$ and $\phi_{n+1} = \phi_n$. Otherwise we construct G_{n+1} as an HNN extension depending on the value of $\varepsilon_n(g)$ as follows:

(i) If $\varepsilon_n(g_n) \neq 0$, we set
$$G_{n+1} = \langle G_n, t_n \mid g_n^{t_n} = a^{\varepsilon_n(g_n)}\rangle\,.$$

(ii) If $g_n \in \ker(\varepsilon_n)$, we define
$$G_{n+1} = \langle G_n, t_n \mid g_n^{t_n} = d\rangle\,.$$

Note that in both cases Lemma 4.0.18 applies and thus G_n is hyperbolic.

If g_n is conjugate in G_n to an element of $\langle c, d\rangle$, say $g_n = \alpha_n^{-1} x_n \alpha_n$ for some $x_n \in \langle c, d\rangle$, we define $\varepsilon_{n+1}\colon G_{n+1} \to \mathbb{Z}$ by $t_n \mapsto |\varepsilon_n(\alpha_n)| + 4\varepsilon(t_{n-1}) + 1$, otherwise we let $t_n \mapsto \varepsilon_n(t_{n-1}) + 1$.

Here, we interpret $\varepsilon(t_{-1}) = 1$. Note that α_n and x_n are not unique here, but we fix our choices for each such g_n.

Furthermore we choose a bijection $\phi_{n+1} \colon \mathbb{N}_0 \to G_{n+1} \setminus \{1\}$.

Proof of (c). Let $x \in \ker(\varepsilon_n)$ be primitive. The claim in case (i) follows directly from Lemma 4.0.4 since x is not conjugate to any element in $\langle g_n \rangle \cup \langle a \rangle$. In case (ii) we can apply Lemma 4.0.6 since since g_n is primitive in G_n by assumption and $d \in \ker(\varepsilon_0)$ is primitive in G_n by induction.

Proof of (d). Let $x, y \in \ker(\varepsilon_0) \leq G_{n+1}$ be primitive and let $\omega \in G_{n+1}$ be a reduced word such that $\omega^{-1} x \omega = y$. If ω contains no t_n or t_n^{-1}, then we are certainly done, thus we can moreover assume that we are in case (ii). Suppose the t_n-length of ω is at least two, then we can write $\omega = \omega_1 t_n^{\pm 1} \omega_2 t_n^{\pm 1} \omega_3$ as a reduced expression, where $\omega_2 \in G_n$ and $\omega_1, \omega_3 \in G_{n+1}$.

If $\omega = \omega_1 t_n \omega_2 t_n \omega_3$ we know that $t_n^{-1} \omega_1^{-1} x \omega_1 t_n$ has to be a pinch, so $\omega_1^{-1} x \omega_1 \in \langle g_n \rangle$, i.e. $\omega_1^{-1} x \omega_1 = g_n^k$. Since x is primitive as an element of G_{n+1}, it follows that $k = \pm 1$. But we also know that $t_n^{-1} \omega_2^{-1} d^k \omega_2 t_n$ has to be a pinch, thus $\omega_2^{-1} d^k \omega_2 = g_n^m$ where $m = \pm 1$. Since $\omega_2 \in G_n$, this is impossible by our choice of g_n. Similarly the case that $\omega = \omega_1 t_n^{-1} \omega_2 t_n^{-1} \omega_3$ is impossible.

If ω contains two adjacent stable letters whose exponents are different, we first consider the case that $\omega = \omega_1 t_n \omega_2 t_n^{-1} \omega_3$. Then $t_n^{-1} \omega_1^{-1} x \omega_1 t_n$ has to be a pinch, thus $\omega_1^{-1} x \omega_1 = g_n^k$ with $k = \pm 1$, so that $t_n^{-1} g_n^k t_n = d^k$. Now we also know that $t_n \omega_2^{-1} d^k \omega_2 t_n^{-1}$ has to be a pinch, thus $\omega_2^{-1} d^k \omega_2 \in \langle d \rangle$, so $\omega_2 \in \langle d \rangle$ since G_n is hyperbolic. But then ω was not a reduced word to begin with. Thus we have shown that the reduced element ω has t_n-length at most one. If $\omega = \omega_1 t_n^{-1} \omega_2 t_n \omega_3$ then an analogous argument applies since $\langle g_n \rangle$ is self-normalizing as well since g_n is primitive in case (ii).

We now define G as the direct limit of the G_n. Note that the ε_n induce an epimorphism $\varepsilon \colon G \to \mathbb{Z}$.

G has $b\mathcal{C}yc$**.** Let $g \in G$ be a non-trivial element. We claim that it is conjugate to an element in $\langle a \rangle \cup \langle d \rangle$. We can find n such that $g \in G_n$. Since G_n is hyperbolic we can find a primitive element h in G_n such that g is some power of h. If h is conjugate to an element of $\langle a \rangle \cup \langle d \rangle$ or if h is conjugate to g_{n+1} in G_{n+1} we are done. Otherwise, h remains primitive in G_{n+1} by Lemma 4.0.4. On the other hand, our enumeration function ϕ and the construction guarantees that in the end any primivite element will be conjugate to an element in $\langle a \rangle \cup \langle d \rangle$.

$\ker(\varepsilon)$ **does not have** $b\mathcal{C}yc$**.** We first prove that if x, y are two primitive elements in $\langle c, d \rangle \leq \ker(\varepsilon_0)$ and there is some $\omega \in G_{n+1}$ such that $\omega^{-1} x \omega = y$, then $|\varepsilon(\omega)| \leq 2\varepsilon(t_n)$, where we interpret $\varepsilon(t_{-1}) = 1$ as above. Let $n = -1$, and note that the conjugating element ω lies in $\langle c, d \rangle$ since G_0 is free. In particular, $\varepsilon(\omega) = 0 \leq 2\varepsilon(t_{-1})$. Now suppose $n \geq 0$ and let $\omega \in G_{n+1}$ such that $\omega^{-1} x \omega = y$. By (d) it follows that the t_n-length of ω is at most one. If the t_n-length equals zero, we are done by induction since $\varepsilon(t_{n-1}) < \varepsilon(t_n)$. If the t_n-length is non-zero we can assume without loss of generality that $\omega = \omega_1 t_n \omega_2$ where ω_1 and ω_2 are elements in G_n. Since $\omega^{-1} x \omega = y$, it follows that $\omega_1^{-1} x \omega_1 \in \langle g_n \rangle$ and similarly $\omega_2^{-1} d^{\pm 1} \omega_2 = y$. Here, g_n is the element in the kernel of ε_n that was used to construct G_{n+1} from G_n via an HNN extension.

Suppose $\omega_1^{-1} x \omega_1 = g_n^{\pm 1}$. Then we also know that $g_n = \alpha_n^{-1} x_n \alpha_n$, thus by induction we know that $|\varepsilon(\omega_1 \alpha_n^{-1})| \leq 2\varepsilon(t_{n-1})$ since $x^{\omega_1 \alpha_n^{-1}} = x_n^{\pm 1}$, so $|\varepsilon(\omega_1)| \leq |\varepsilon(\alpha_n)| + 2\varepsilon(t_{n-1})$. Moreover, by induction we also conclude that $|\varepsilon(\omega_2)| \leq 2\varepsilon(t_{n-1})$. Altogether we obtain

$$\begin{aligned} |\varepsilon(\omega)| &\leq |\varepsilon(\omega_1)| + \varepsilon(t_n) + |\varepsilon(\omega_2)| \\ &\leq 2\varepsilon(t_n)\,. \end{aligned}$$

We are now ready to show that $\ker(\varepsilon)$ contains infinitely many primitive conjugacy classes. Let x, y be two primitive elements in subgroup $\langle c, d\rangle \leq \ker(\varepsilon_0)$ such that x is not conjugate to y in $\ker(\varepsilon_0)$. Suppose x and y are conjugate via some $\omega \in \ker(\varepsilon)$, i.e. $\omega^{-1} x \omega = y$. There is some $n \in \mathbb{N}$ such that $x, y, \omega \in G_{n+1}$. As in the proof above we can assume without loss of generality that $\omega = \omega_1 t_n \omega_2$ with $\omega_1, \omega_2 \in G_n$ and $\omega_1^{-1} x \omega_1 = g_n^{\pm 1}$, $\omega_2 d^{\pm 1} \omega_2 = y$ such that $|\varepsilon(\omega_2)| \leq 2\varepsilon(t_{n-1})$ and $|\varepsilon(\omega_1)| \leq |\varepsilon(\alpha_n)| + 2\varepsilon(t_{n-1})$. But since we chose $\varepsilon(t_n) > |\varepsilon_n(\alpha_n)| + 4\varepsilon(t_{n-1})$, we see that ω cannot lie in the kernel of ε.

□

Theorem 4.0.20. There exists a finitely generated torsion-free group $G = H \rtimes \mathbb{Z}$ such that G has *b$\mathcal{C}$yc* but H does not.

Proof. Let C be a torsion-free countable group having *b$\mathcal{C}$yc* and admitting an epimorphism $\varepsilon\colon C \to \mathbb{Z}$ such that $\ker(\varepsilon)$ contains infinitely many conjugacy classes that are primitive in C, see Proposition 4.0.19. Let

$$G(0) = C * F(x, y)\,.$$

We extend ε to $\alpha_0\colon G(0) \to \mathbb{Z}$ by mapping x and y to $1 \in \mathbb{Z}$. Moreover, we enumerate the elements of $C = \{c_0 = 1, c_1, c_2, \ldots\}$ and those of $G(0) = \{g_0 = 1, g_1, g_2, \ldots\}$. Essentially the same argument as in the proof of [HO13, Theorem 7.2] applies. There is a sequence of groups $G(i)$ and epimorphisms $\alpha_i\colon G(i) \to \mathbb{Z}$ such that $G(i+1)$ is a quotient of $G(i)$ and α_i descends to an epimorphism $\alpha_{i+1}\colon G(i+1) \to \mathbb{Z}$. Under the quotient maps the group C embeds into $G(i)$ such that $G(i)$ is hyperbolic relative to C. Moreover, in $G(i)$ the following holds: (a) the elements $c_1, \ldots, c_i$ are contained in $\langle x, y\rangle$ and (b) the elements $g_1, \ldots, g_i$ are conjugate to elements of C. If we define G as the direct limit of the $G(i)$, we obtain an induced epimorphism $\alpha\colon G \to \mathbb{Z}$. By (a) G is 2-generated and by (b) G has *b$\mathcal{C}$yc* since C has *b$\mathcal{C}$yc*. Since $G(i)$ is hyperbolic relative to C, if elements $c, c' \in C$ are conjugate in $G(i)$, i.e. $wcw^{-1} = c'$ for some $w \in G(i)$, then $w \in C$ by Lemma 4.0.3. Thus Lemma 4.0.5 together with the previous observation imply that $\ker(\alpha)$ contains infinitely many primitive conjugacy classes. □

Proposition 4.0.21. There exists a countable torsion-free group G and an epimorphism $\varepsilon\colon G \to \mathbb{Z}$ such that both G and $\ker(\varepsilon)$ have *b$\mathcal{C}$yc*, and $\ker(\varepsilon)$ contains a non-abelian free subgroup.

Proof. We will first inductively construct a specific sequence $G_0 \leq G_1 \leq \ldots$ of groups, together with epimorphisms $\varepsilon_n\colon G_n \to \mathbb{Z}$ such that $\varepsilon_{n+1}|_{G_n} = \varepsilon_n$ as follows: We let $G_0 = \langle a, b, c\rangle$ be a non-abelian free group and let $\varepsilon_0\colon G_0 \to \mathbb{Z}$ be defined by mapping a to 1 and b, c to 0. Now, suppose G_n has been constructed such that $G_{n-1} \leq G_n$, together with an epimorphism $\varepsilon_n \colon G_n \to \mathbb{Z}$. We enumerate all elements of $G_n = \{1 = g_0, g_1, g_2, \ldots\}$ and define G_{n+1} as the following multiple HNN extension

$$G_{n+1} = \langle G_n, \{t_i\}_{i \in \mathbb{N}} \mid g_i^{t_i} = a^{\varepsilon_n(g_i)} \text{ if } \varepsilon_n(g_i) \neq 0 \text{ and } g_i^{t_i} = b \text{ otherwise } \rangle \,.$$

We can then extend ε_n to G_{n+1} to define ε_{n+1}, by mapping the stable letters t_i to $0 \in \mathbb{Z}$. Finally, we let G be the direct limit of the G_n. Observe that G has $b\mathcal{C}yc$ with witnesses $\langle a \rangle$ and $\langle b \rangle$ and that there is an induced epimorphism $\varepsilon \colon G \to \mathbb{Z}$ such that $\langle b, c \rangle \leq \ker(\varepsilon)$. Moreover, since the stable letters of the HNN extensions are contained in $\ker(\varepsilon)$, also $\ker(\varepsilon)$ has $b\mathcal{C}yc$ with only one cyclic group $\langle b \rangle$ as the witness. □

Using arguments as in the proof of [HO13, Theorem 7.2] one can construct a group as in the previous proposition that is additionally finitely generated.

We have shown in Theorem 3.0.7 that a finitely generated group with $b\mathcal{VC}yc$ whose virtually cyclic subgroups are quasi-isometrically embedded has at most linear conjugacy growth. The following proposition shows that one cannot omit the assumption on the cyclic subgroups being undistorted.

Proposition 4.0.22. There exists a torsion-free finitely generated group G of exponential conjugacy growth that has $b\mathcal{C}yc$.

Proof. As a first step, we will prove that there exists a torsion-free countable group G that contains an infinite cyclic subgroup $\langle a \rangle$ such that G has $b\mathcal{C}yc$ and the elements a^{2k+1} are pairwise non-conjugate. Moreover, there is an element $t \in G$, such that $a^t = a^2$. In the end, the latter property will ensure that the word length of an element a^m is $O(\log(|m|))$. We will construct G as direct limit of countable groups $G_0 \leq G_1 \leq \ldots$ as follows: We let $G_0 = \langle a, t \mid a^t = a^2 \rangle$ be the Baumslag-Solitar group $BS(1, 2)$. Note that this group has exponential conjugacy growth, as the elements a^{2k+1} are pairwise non-conjugate, see [GS10, Example 2.3]. To construct G_{n+1} from G_n inductively, we first enumerate all elements in $G_n \setminus (\bigcup_{g \in G} \langle a^g \rangle) = \{g_1, g_2, \ldots\}$ and then form the multiple HNN extension

$$G_{n+1} = \langle G_n, \{s_i\}_{i \in \mathbb{N}} \mid g_i^{s_i} = t \rangle \,.$$

It follows inductively from Lemma 4.0.4 that the elements a^{2k+1} are pairwise non-conjugate viewed as elements of G_{n+1}. The direct limit $G = \bigcup_{n \geq 0} G_n$ then satisfies the previously required properties as any element in $G \setminus (\bigcup_{g \in G} \langle a^g \rangle)$ will be conjugate to the element $t \in G_0$.

In the second step we want to construct a group with the same properties but which is additionally finitely generated. In the following we will write C instead of G for the previously constructed countable group. We let

$$G(0) = C * F(x, y)$$

and enumerate the elements of $C = \{c_0 = 1, c_1, c_2, \ldots\}$ resp. $G(0) = \{g_0 = 1, g_1, g_2, \ldots\}$. Note that $G(0)$ is hyperbolic relative to C and x, y generate a suitable subgroup of $G(0)$. In the following we will not distinguish notationally between elements of $G(0)$ and their representatives in quotients of $G(0)$. We will inductively construct quotient groups $G(i)$ of $G(0)$ such that

(a) the subgroup C embeds under the quotient map into $G(i)$. Again, we will not distinguish between C and its image in $G(i)$.

(b) $G(i)$ is torsion-free and hyperbolic relative to C. Moreover, x and y generate a suitable subgroup of $G(i)$.

(c) The elements c_j for $1 \leq j \leq i$, considered as elements in $G(i)$, lie in the subgroup generated by x and y.

(d) In $G(i)$, for $1 \leq j \leq i$, the elements g_j are conjugate to elements in C.

(e) The elements a^{2k+1} are pairwise non-conjugate in $G(i)$.

To construct $G(i+1)$ from $G(i)$, we proceed as follows: If g_{i+1} is parabolic, we set $G'(i) = G(i)$, otherwise we choose an isomorphism $\iota\colon E_{G(i)}(g_{i+1}) \to \langle t \rangle$ and form the HNN extension

$$G'(i) = \langle G(i), s \mid e^s = \iota(e), e \in E_{G(i)}(g_{i+1}) \rangle \,.$$

Note that $\langle x, y \rangle$ is still a suitable subgroup of $G'(i)$ [HO13, Corollary 2.16].

In the next step, we apply Theorem 4.0.2 to $G'(i)$ and the elements $\{s, c_{i+1}\}$ resp. $\{c_{i+1}\}$ in the case that g_{i+1} is parabolic, to obtain a quotient $G(i+1)$ of $G'(i)$. Since s will lie in the subgroup $\langle x, y \rangle$, we obtain a quotient map $G(i) \to G(i+1)$. By construction, (d) holds for $G(i+1)$. The properties (a)-(c) follow directly from Theorem 4.0.2. The last statement (e) is a consequence of Lemma 4.0.3 and the fact that $G(i+1)$ is torsion-free.

Finally, let G be defined as the direct limit of the $G(i)$. By (c) it follows that G is 2-generated, property (d) implies that G has $b\mathcal{C}yc$ since the same was already true for C. Moreover, by (e), the elements $a^{2k+1} \in C$ are pairwise non-conjugate in G as well. Thus G has exponential conjugacy growth. $\square$

Proposition 4.0.23. Let Q be a countable group with n conjugacy classes. Then there exists a torsion-free countable group G with $n+1$ conjugacy classes such that Q is isomorphic to a quotient of G.

Proof. Let $\{q_0 = 1, q_1, \ldots, q_{n-1}\} \subseteq Q$ be representatives of conjugacy classes of elements in Q. Since Q is countable, there is a countable free group G_0 and an epimorphism $\varepsilon_0\colon G_0 \to Q$. We can moreover assume without loss of generality that $\ker(\varepsilon_0)$ is non-trivial. Choose preimages $g_1, \ldots, g_{n-1}$ of $q_1, \ldots, q_{n-1}$ under ε_0 and choose some non-trivial element $g_0 \in \ker(\varepsilon_0)$.

We now inductively define countable torsion-free groups G_m together with epimorphisms $\varepsilon_m\colon G_m \to Q$ such that $G_{m-1} \leq G_m$ and $\varepsilon_m|_{G_{m-1}} = \varepsilon_{m-1}$. Suppose G_m and ε_m have already been constructed. Enumerate all non-trivial elements $\{h_1, h_2, \ldots\}$ of G_m and form the multiple HNN extension

$$G_{m+1} = \langle G_m, \{t_i\}_{i\in\mathbb{N}} \mid \text{ relations explained below } \rangle \,.$$

For any $i \geq 1$ we know that $\varepsilon_n(h_i)$ is conjugate to q_{j_i} for some j_i. If $q_{j_i} = 1$, then we impose the relation $h_i^{t_i} = g_0$. Otherwise there is some $\alpha_i \in G_n$ such that $\varepsilon_m(\alpha_i^{-1} h_i \alpha_i) = q_{j_i}$. We then impose the relation $(\alpha_i^{-1} h_i \alpha_i)^{t_i} = g_i$. With these choices we can extend ε_m to $\varepsilon_{m+1}\colon G_{m+1} \to Q$ by mapping all stable letters t_i to the trivial element in Q.

Finally, we let G be the direct limit of the groups G_m. By construction, representatives of the conjugacy classes of G are $\{1, g_0, g_1, \ldots, g_{n-1}\}$. $\square$

Note that the above construction is optimal in the sense that if Q has n conjugacy classes and contains torsion then any torsion-free group G that surjects onto Q must have at least $n+1$ conjugacy classes.

Example 4.0.24. Let $G = \bigoplus_{n=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$. An application of [Osi10, Theorem 1.1] yields an embedding of G into a finitely generated group with only three conjugacy classes. In particular, this latter group has $b\mathcal{C}yc$ and $b\mathcal{VC}yc$. But it cannot have BVC by Lemma 1.2.11, since the orders of finite subgroups in G are not bounded.

The previous example combined with Proposition 4.0.23 now shows:

Corollary 4.0.25. There exists a group G with BVC such that a quotient of G fails to have BVC.

This corollary should serve as motivation why we study the $b\mathcal{VC}yc$ instead of the BVC property.

5. Finite Groups and Residually Finite Groups

We have seen in Chapter 2 and Chapter 3 that ascending HNN extensions of finitely generated free groups and linear groups satisfy Conjecture 1.2.2. Recall that a group is residually finite if the intersection of all its finite index subgroups is trivial. It is well-known that finitely generated linear groups are residually finite and even virtually residually p-finite. In [BS05] Borisov and Sapir show that ascending HNN extensions of finitely generated free groups are residually finite. Actually, they even prove that ascending HNN extensions of finitely generated linear groups are residually finite. In [BS09] they improve upon this result by showing that ascending HNN extensions of finitely generated free groups are virtually residually p-finite for every sufficiently large prime p. Note that non-ascending HNN extensions of free groups need not be residually finite. A prominent example is given by the Baumslag-Solitar group $\mathrm{BS}(2,3) = \langle a, t \mid t^{-1}a^2t = a^3\rangle$ which is not even Hopfian. Mal'cev [Mal83] proved that any split extension of a finitely generated residually finite group by a residually finite group is again residually finite. In particular, ascending non-proper HNN extensions, i.e. semidirect products with $\mathbb{Z}$, of finitely generated residually finite groups are residually finite. It has been proven by Sapir and Wise that ascending HNN extensions of residually finite groups need not be residually finite [SW02]. Given our previous results on the BVC property and its variants, we formulate the following conjecture.

Conjecture 5.0.1. A residually finite group with BVC or $b\mathcal{C}yc$ is virtually cyclic.

One goal of this chapter is to give supporting evidence for this conjecture. By the following lemma we might as well assume from the beginning that the group appearing in Conjecture 5.0.1 is torsion-free, so that there is no difference between the BVC and $b\mathcal{C}yc$ property.

Lemma 5.0.2. Let G be a residually finite group with BVC or $b\mathcal{C}yc$. Then there is a torsion-free finite index subgroup in G that has $b\mathcal{C}yc$.

Proof. If G has BVC or $b\mathcal{C}yc$, there are only finitely many conjugacy classes of finite order elements by Lemma 1.2.11, say $(g_1), \ldots, (g_n)$ with $g_i \in G$ of finite order. For each i choose some finite index normal subgroup $N_i \trianglelefteq G$ such that $g_i \notin N_i$, so $(g_i) \cap N_i = \emptyset$. Let $N = \bigcap_{i=1}^n N_i \trianglelefteq G$. Note that N is of finite index in G and N is torsion-free by construction. Since N is of finite index in G, it has $b\mathcal{C}yc$ by Lemma 1.1.8 resp. Lemma 1.2.10. □

Definition 5.0.3. Let G be a group and H a subgroup of G. We call H *conjugate-dense* in G if $G = \bigcup_{g\in G} H^g$.

By a simple counting argument it follows that a group G does not admit a proper finite index conjugate-dense subgroup. In particular, a finite group has no proper conjugate-dense subgroup. We can thus record:

Proposition 5.0.4. Let G be a residually finite group with $1\mathcal{C}yc$. Then G is cyclic.

Proof. As G has $1\mathcal{C}yc$, any finite quotient of G will have a cyclic conjugate-dense subgroup and thus will be cyclic. As G is residually finite, it thus embeds into a direct product of cyclic subgroups. Hence G is abelian, from which the claim follows easily. □

We want to remark that there are groups G which are not virtually cyclic but which have $1\mathcal{C}yc$ nevertheless. For example, there is even a finitely generated group with exactly two conjugacy classes by the work of Osin [Osi10]. So even in this very special case of having a single witness we need to impose additional properties on the group in order to deduce that it is virtually cyclic.

Proposition 5.0.5. Let $G = \prod_{i \in I} F_i$ with F_i finite. If G has $b\mathcal{C}yc$, then G is finite.

Proof. Since G has $b\mathcal{C}yc$, there are only finitely many conjugacy classes of finite order elements. In particular, there exists some $M > 0$ such that $\exp(F_i) \leq M$ for all $i \in I$. Here, exp denotes the exponent of a finite group, i.e. the least common multiple of all element orders in the group. The uniform bound on the exponents implies that G is torsion. As G has $b\mathcal{C}yc$, it follows that G has only finitely many conjugacy classes. Since G is residually finite, by [KMT14, Theorem 2.3] it follows that G is finite. □

One might also consider a weaker variant of Conjecture 5.0.1 where one demands that the group in question is even residually p-finite. Here we want to provide an argument giving some supporting evidence why such a conjecture might hold.

Lemma 5.0.6. A finite p-group cannot be the union of p proper subgroups.

Proof. Suppose $G = \bigcup_{i=1}^{p} H_i$ for H_i some proper subgroups of G. If $|G| = p^n$, then $|H_i| \leq p^{n-1}$ and thus

$$p^n = |G| \leq 1 + \sum_{i=1}^{p} |H_i \setminus \{1\}| \leq 1 + p(p^{n-1} - 1)\,,$$

which is impossible. □

Lemma 5.0.7. Let G be a finite p-group with at most n conjugacy classes of maximal cyclic subgroups with $n < p$. Then G is cyclic.

Proof. We prove the claim by induction on s, where $|G| = p^s$. If $s = 1$, the claim is obviously true. So let G be a finite p-group with at most n conjugacy classes of maximal cyclic subgroups, and $|G| > p$. Since a p-group has non-trivial center, $G/Z(G)$ has order strictly smaller than G and $G/Z(G)$ also has at most n conjugacy classes of maximal cyclic subgroups. Thus $G/Z(G)$ is cyclic by induction. This implies that G itself was abelian. By Lemma 5.0.6 the claim follows. □

Theorem 5.0.8. Let G be a residually p-finite group for infinitely many primes p. If G has $b\mathcal{C}yc$, then G is virtually cyclic.

Proof. We know that G has $n\mathcal{C}yc$ for some $n \in \mathbb{N}$. Choose some prime $p > n$ such that G is residually p-finite. Lemma 5.0.7 implies that all finite p-quotients are cyclic. Thus G is residually cyclic. In particular, G is abelian and the claim follows. □

Note that the property of being residually p-finite for infinitely many primes p seems to be quite restrictive. Groups satisfying this property are for example free groups and finitely generated torsion-free nilpotent groups [Iwa43; Gru57]. Also certain free products with amalgamation of free groups or finitely-generated torsion-free nilpotent groups satisfy this property, see e.g. [KM93, Theorem 4.4]. Also observe that Theorem 5.0.8 is not enough to prove Conjecture 5.0.1 for the class of finitely generated linear groups over a field of characteristic 0. Although such linear groups are virtually residually p-finite for infinitely many primes p, the indices of the corresponding subgroups usually grow with the size of the prime and thus also the bound on the number of cyclic witnesses grows. A proof along these lines might still be possible if one can bound the indices of the subgroups well enough. However, we were not able to do so.

In unpublished work we also investigated the number of maximal cyclic subgroups as well as the number of conjugacy classes of cyclic subgroups in finite p-groups for odd primes p. We were able to establish lower bounds on these quantities that increase with the order of the group. The ultimate aim was to answer the following question.

Question 5.0.9. Does the number of conjugacy classes of maximal cyclic subgroups of a finite p-group for $p > 2$ grow with the order of the group?

Despite quite some effort we were neither able to prove this property nor provide examples of arbitrarily large p-groups that only have a bounded number of conjugacy classes of maximal cyclic subgroups. For $p = 2$, the generalized quaternion groups provide such an infinite family as we shall see below (Lemma 5.2.19).

Instead of asking whether a residually finite group G with BVC is virtually cyclic, one could weaken the conclusion and ask whether the group is just finitely generated. For an arbitrary residually finite group this does not seem to simplify the situation. However, we can answer the question if we demand that the group G is locally extended residually finite or LERF, sometimes also called subgroup-separable. Recall that this means that for any finitely generated subgroup H of G and any $g \in G \setminus H$ there exists an epimorphism $\pi\colon G \to F$ onto a finite group F such that $\pi(g) \notin \pi(H)$.

Lemma 5.0.10. Let G be a LERF group with BVC. Then G is finitely generated.

Proof. Let $V_1, \dots, V_n \leq G$ be the virtually cyclic witnesses and let $H = \langle V_1, \dots, V_n \rangle \leq G$. Observe that H is finitely generated as virtually cyclic groups are finitely generated. Moreover, the subgroup H is conjugate-dense in G. If $\pi\colon G \to F$ is an epimorphism onto a finite group F, then $\pi(H)$ is a conjugate-dense subgroup of F, hence $\pi(H) = F$. Now G being LERF implies that $H = G$. □

Definition 5.0.11. For a group G we let $\sigma(G)$ be the smallest integer such that G is the union of $\sigma(G)$ many cyclic subgroups. If there is no such integer we let $\sigma(G) = \infty$. Similarly, we define $\gamma(G)$ resp. $\delta(G)$ to be the minimal number of cyclic subgroups such that G is the union of G-conjugates resp. $\mathrm{Aut}(G)$-conjugates of these cyclic subgroups and $\sigma(G) = \infty$ resp. $\delta(G) = \infty$ if there is no such number.

If G is finite, then $\sigma(G)$ equals the number of maximal cyclic subgroups of G and $\gamma(G)$ equals the number of conjugacy classes of maximal cyclic subgroups.

Lemma 5.0.12. Suppose $G = H_1 \times H_2 \times \ldots \times H_n$ where the H_i are non-trivial torsion-free groups. Then $\gamma(G) \geq 2^n - 1$. If $G = \prod_{i\in I} H_i$ with H_i non-trivial torsion-free and $|I| = \infty$, then $\gamma(G) = \infty$.

Proof. Let $\pi_i \colon H \to H_i$ denote the canonical projections. Pick elements $h_i \in H_i \setminus \{1\}$ and for each non-empty subset $S \subseteq \{1, \ldots n\}$ define the element h_S by $\pi_i(h_S) = h_i$ if $i \in S$ and $\pi_i(h_S) = 1$ otherwise. Then let $C_S = \langle h_S \rangle$. If $C_S^g \leq K$ for some cyclic subgroup K and $g \in G$, then the support of a generator k of K, i.e. the set of those integers i such that $\pi_i(k) \neq 1$, equals S since G is torsion-free. This implies that $\gamma(G) \geq 2^n - 1$. The last claim follows analogously. □

Note that the bound given in Lemma 5.0.12 is optimal. For example, let H be a torsion-free group with exactly two conjugacy classes. Then $\gamma(H \times H) = 3$ with the corresponding maximal cyclic subgroups generated by $(h, 1), (1, h), (h, h)$, where h is a non-trivial element of H. This example generalizes to multiple factors.

Finite groups with two conjugacy classes of maximal cyclic subgroups are abundant. For example, the finite dihedral groups whose order is not divisible by 4 belong to this class and we shall see many more examples below. The bigger part of this chapter is devoted to proving the following theorem.

Theorem 5.0.13. A finite group G with at most two conjugacy classes of maximal cyclic subgroups is solvable of derived length at most 4.

The fact that such groups are solvable will follow from a result we prove in Appendix A about the distribution of element orders in finite simple groups, where we rely on the classification of the finite simple groups. To obtain a bound on the derived length we will need to carefully analyze the structure of these groups, sometimes coming close to a classification result. We were heavily inspired by the work of Costantini and Jabara. In [CJ09] they study finite groups whose cyclic subgroups of the same order are conjugate. They call these groups csc-groups and they prove:

Theorem 5.0.14 ([CJ09, Corollary 2.9])**.** A solvable csc-group has derived length at most 4.

At the end of this chapter we actually show that $G/Z(G)$ is a csc-group for a finite group G with $\gamma(G) = 2$. Hence, assuming the groups are solvable, Theorem 5.0.13 can be seen as a corollary to Theorem 5.0.14. However, we see that $G/Z(G)$ is a csc-group only after a detailed structural analysis that sometimes parallels the arguments used to derive Theorem 5.0.14. Using Theorem 5.0.13 it is now easy to verify Conjecture 5.0.1 if we have at most two virtually cyclic witnesses.

Theorem 5.0.15. Let G be a residually finite group with $2\mathcal{C}yc$. Then G is virtually cyclic.

Proof. For any $g \in G$ there is an epimorphism $\varphi_g \colon G \to F_g$ where F_g is a finite group and $\varphi_g(g) \neq 1$. Now, by Theorem 5.0.13 we know that F_g is solvable of derived length at most 4. Moreover, G embeds into $\prod_{g \in G} F_g$. Since the derived length of the F_g is bounded, the product $\prod_{g \in G} F_g$ is itself solvable. Thus G is solvable as well and by Theorem 1.2.15 it follows that G is virtually cyclic. □

For a solvable group G, let us denote by $\mathrm{dl}(G)$ the derived length of G. Theorem 5.0.13 also motivates the following question.

Question 5.0.16. Does there exist a function $f \colon \mathbb{N} \to \mathbb{N}$ such that for any finite solvable group G one has $\mathrm{dl}(G) \leq f(\gamma(G))$?

An affirmative answer to the previous question would imply that residually solvable groups, in particular residually p-finite groups, would satisfy Conjecture 5.0.1 by the proof of Theorem 5.0.15. Note that there cannot be an analogous upper bound such as formulated in Question 5.0.16 for the nilpotency class of a nilpotent group. Recall that the maximal nilpotency class of a p-group of order p^n is equal to $n-1$. Now consider the 2-groups of maximal nilpotency class, these are the quaternion, dihedral and semidihedral groups. But these happen to have only three conjugacy classes of maximal cyclic subgroups, independent of their order.

5.1. Group Coverings and Maximal Cyclic Subgroups

Before we study the finite groups G with two conjugacy classes of maximal cyclic subgroups, we want to a highlight some related problems and afterwards make some easy observations about maximal cyclic subgroups. Note that a group G with $\gamma(G) = 2$ can be written as the union $G = \bigcup_{g \in G} C^g \cup D^g$ with C and D maximal cyclic subgroups of G. On the other hand, it is an easy exercise to show that no group can be written as the union of two proper subgroups. If a group G admits an epimorphism onto the Klein four-group $K_4 = C_2 \times C_2$, then pulling back the three non-trivial cyclic subgroups of K_4 shows that G is the union of three proper subgroups. Conversely, Scorza's theorem [Zap91] tells us that if $G = H_1 \cup H_2 \cup H_3$, where the H_i are proper subgroups of G, then each subgroup H_i has index two in G and $N \coloneqq H_1 \cap H_2 = H_1 \cap H_3 = H_2 \cap H_3$ is a normal subgroup such that $G/N \cong K_4$.

Given a group G and a collection $\mathcal{H}$ of proper subgroups of G, we say that $\mathcal{H}$ is a *cover* of G if $\bigcup_{H \in \mathcal{H}} H = G$. A cover of minimal possible size is called *minimal cover* and a cover is called *irredundant* if no proper subcollection is also a cover. A nice survey on group coverings can be found in [Bha09]. For example, generalizing Scorza's theorem, Cohn [Coh94] has classified the groups which admit a minimal cover of size $4, 5$ or 6. By Tomkinson [Tom97] there does not exist a group that has a minimal cover with 7 elements. There are also interesting results if one restricts the class of groups that one allows in a cover:

Theorem 5.1.1 (Baer, [Rob, Theorem 4.16])**.** A group is central-by-finite if and only if it admits a finite covering consisting of abelian subgroups.

Let us now concentrate on coverings by cyclic subgroups and start with a couple of easy examples.

Examples 5.1.2. (1) The quaternion group Q_8 has the Klein four group as a quotient and thus can be covered by three proper subgroups. In fact, we have $\sigma(Q_8) = 3$ with each maximal cyclic subgroup of order 4.

(2) For any $n \geq 0$ we have $\sigma(C_{4n+2} \times C_2) = 3$. The generators of the maximal cyclic subgroups are given by $(1,0), (1,1), (2,1)$. All of these elements have order $4n+2$, hence the corresponding cyclic subgroups are indeed maximal.

For two natural numbers n, m we denote by (n, m) the greatest common divisor of n and m and by $[n, m]$ the least common multiple of n and m.

Lemma 5.1.3. Let H be a finite group and let $n \geq 2$ be some natural number such that $(n, |H|) = 1$. Then $G = C_n \times H$ has $\sigma(G) = \sigma(H)$.

Proof. Let $C_n = \langle t \rangle$ and let $h \in H$ be a generator of a maximal cyclic subgroup in H. Since n and $\mathrm{ord}(h)$ are coprime there exists some $\alpha \in \mathbb{N}$ such that $\alpha n \equiv 1 \mod \mathrm{ord}(h)$. Let k, m be some natural numbers and let $l = (m-k)\alpha n + k$. Note that $l \equiv m \mod \mathrm{ord}(h)$. Hence

$$(th)^l = t^l h^l = t^k h^m$$

It follows that G can be covered by $\sigma(H)$-many cyclic subgroups. □

From Lemma 5.1.3 it follows in particular, that there are arbitrarily large non-solvable groups with a bounded number of maximal cyclic subgroups.

Observation 5.1.4. If $\pi\colon G \to Q$ is an epimorphism of finite groups, then for any maximal cyclic K of Q there exists some maximal cyclic $D \leq G$ such that $\pi(D) = K$.

Proof. Let $K \leq Q$ be a maximal cyclic subgroup. Of course, there is some cyclic subgroup $C \leq G$ such that $\pi(C) = K$. Let $C \leq D$ with D maximal cyclic. Then $\pi(C) \leq \pi(D)$ and since $\pi(D)$ is cyclic and $\pi(C) = K$ was maximal cyclic, it follows that $\pi(C) = \pi(D)$. □

Remark 5.1.5. Of course, even if $\pi\colon G \to Q$ is an epimorphism, the image of a maximal cyclic subgroup of G under π need not be maximal cyclic. For example, consider the projection $C_2 \times C_2 \to C_2$ onto one factor.

Lemma 5.1.6. Let G be a finite group and let $\pi\colon G \to Q$ be a surjective group homomorphism. If $\gamma(G) = \gamma(Q)$, then the image of any maximal cyclic subgroup of G under π is maximal cyclic in Q.

Proof. Let $C_1, \ldots, C_n$ and $V_1, \ldots, V_n$ be representatives of conjugacy classes of maximal cyclic subgroups of G resp. Q. Note that for any V_i there is some maximal cyclic subgroup $D_i \leq G$ such that $\pi(D_i) = V_i$. Now D_i is conjugate to one of the C_j. As $\gamma(G) = \gamma(Q)$ it follows that there exists a bijection $\sigma \in S_n$ such that $\pi(C_k) = V_{\sigma(k)}$ for all $k \in \{1, \ldots, n\}$ and the claim follows. □

Definition 5.1.7. For a finite group G we let $\mathcal{M}(G)$ be the set of maximal cyclic subgroups of G. We define

$$\Psi(G) \coloneqq \bigcap_{M \in \mathcal{M}(G)} M \,,$$

and call it the *maximal cyclic residual*.

It is easy to see that the subgroup $\Psi(G)$ is a characteristic subgroup of G.

Lemma 5.1.8. Let G be a finite group. The subgroup $\Psi(G)$ satisfies the following properties:

(1) $\Psi(G) \leq Z(G)$.

(2) $\Psi\left(G/\Psi(G)\right) = 1$.

(3) $\sigma(G) = \sigma\left(G/\Psi(G)\right)$ and $\gamma(G) = \gamma\left(G/\Psi(G)\right)$.

Proof. For (1) let $x \in \Psi(G)$ and $y \in G$. Then $\langle y \rangle \leq C$ for some maximal cyclic subgroup C of G. Since $x \in \Psi(G)$, it follows that $x \in C$. Hence x and y commute.

To prove (2) let $\pi\colon G \to G/\Psi(G)$ denote the quotient homomorphism and let $K \leq G/\Psi(G)$ be a maximal cyclic subgroup. Then there is some maximal cyclic subgroup $C \leq G$ such that $\pi(C) = K$. Thus $\pi^{-1}(K) = C\Psi(G)$. Since $\Psi(G) \leq C$, it follows that $\pi^{-1}(K) = C$, i.e. preimages of maximal cyclic subgroups are again maximal cyclic. Also, if $D \leq G$ is a maximal cyclic subgroup, then $\pi(D) \leq L$ for some maximal cyclic subgroup $L \leq G/\Psi(G)$, hence $D \leq \pi^{-1}(L)$ and by our previous consideration we have $D = \pi^{-1}(L)$. With these observations it follows that

$$\pi^{-1}\left(\bigcap_{L \in \mathcal{M}(G/\Psi(G))} L\right) = \Psi(G)$$

and thus $\Psi(G/\Psi(G)) = 1$. Also (3) follows from the observations in the proof of (2). $\square$

Lemma 5.1.9. Let G be a finite group and let $C_1, C_2, \ldots, C_n$ be representatives of the conjugacy classes of the maximal cyclic subgroups of G. Then $\Psi(G) = C_1 \cap C_2 \cap \ldots \cap C_n$.

Proof. Let $H = \langle C_1, C_2, \ldots, C_n \rangle$. Then H is a conjugate-dense subgroup of G, thus $H = G$. Let $N = C_1 \cap C_2 \cap \ldots C_n$. Since G is generated by $C_1, C_2, \ldots, C_n$ and the C_i are cyclic, it follows that N is central, in particular normal. Thus $\Psi(G) = \bigcap_{g \in G} N^g = N$ as claimed. $\square$

Lemma 5.1.10. Let G be a finite group and N a subgroup of G. Then $\gamma(N) \leq [G : N] \cdot \gamma(G)$.

Proof. This follows from the proof of Lemma 1.1.8. $\square$

Lemma 5.1.11. Let G be a finite non-cyclic subgroup and suppose that C is a maximal cyclic normal subgroup. Then $\gamma(G/C) < \gamma(G)$.

Proof. This is straightforward. $\square$

Corollary 5.1.12. If G is a finite group with $\gamma(G) = 2$ such that one of the maximal cyclic subgroups is normal, then G is metacyclic.

5.2. Finite Groups with Few Cyclic Subgroups up to Conjugation

As we will be investigating finite groups G with $\gamma(G) = 2$ in detail in this section, let us make the following definition.

Definition 5.2.1. For any $n \geq 1$ we let $\Gamma_{\leq n}$ resp. Γ_n be the class of finite groups G such that $\gamma(G) \leq n$ resp. $\gamma(G) = n$. We denote by $\Gamma^I_{\leq n}$ resp. Γ^I_n the subclass of $\Gamma_{\leq n}$ resp. Γ_n which consists of those groups in which any two distinct maximal cyclic subgroups intersect trivially.

Moreover, we introduce the following notation: If S is a subset of a group G, we let

$$[S]^G := \bigcup_{g \in G} S^g \,.$$

As mentioned in the introduction of this chapter, our goal is to prove that any group $G \in \Gamma_{\leq 2}$ is solvable of derived length at most 4. The following is an easy, but very important observation:

Lemma 5.2.2. Let G be a finite group and $H, K \leq G$ be two subgroups whose conjugates cover G, i.e.

$$G = [H]^G \cup [K]^G \,.$$

Then $N_G(K) = K$ or $N_G(H) = H$. In particular, if $G \in \Gamma_2$, then at least one maximal cyclic subgroup is self-normalizing.

Proof. First of all we can assume without loss of generality that both H and K are proper subgroups of G. Also note that we only need to take conjugates of H (resp. K) by elements representing the cosets of $N_G(H)$ (resp. $N_G(K)$). Thus

$$|G| \leq [G : N_G(H)] \cdot |H| + [G : N_G(K)] \cdot |K| \,.$$

Dividing by the order of G we obtain

$$1 \leq \frac{1}{[N_G(H) : H]} + \frac{1}{[N_G(K) : K]} \,.$$

Hence it follows that H or K is self-normalizing or $[N_G(H) : H] = 2 = [N_G(K) : K]$. We assume the latter case and consider the equation $G = \bigcup_{g \in G} H^g \cup K^g$ again, this time we avoid overcounting the identity element to arrive at the following inequality:

$$|G| \leq 1 + [G : N_G(H)] \cdot (|H| - 1) + [G : N_G(K)] \cdot (|K| - 1) \,.$$

Hence

$$\begin{aligned} 1 &\leq \frac{1}{|G|} + \frac{1}{2}\frac{|H| - 1}{|H|} + \frac{1}{2}\frac{|K| - 1}{|K|} \\ &= \frac{1}{|G|} + 1 - \frac{1}{2}\left(\frac{[G : H]}{|G|} + \frac{[G : K]}{|G|}\right) \,. \end{aligned}$$

With this it would follow that $2 \geq [G : K] + [G : H]$. Since H and K are proper subgroups, we arrive at a contradiction. $\square$

Also note that there need not be a self-normalizing maximal cyclic subgroups as soon as $\gamma(G) > 2$, an example being the Klein four-group $C_2 \times C_2$.

Since a finite group G is nilpotent if and only if all proper subgroups $H \leq G$ are properly contained in their normalizer $N_G(H)$, we can record:

Corollary 5.2.3. There is no finite nilpotent group G with $\gamma(G) = 2$.

Proposition 5.2.4. There is no nilpotent group G with $\gamma(G) = 2$.

Proof. By Theorem 1.2.15 such a group is necessarily virtually cyclic and by Corollary 5.2.3 we can assume that G is infinite. Note that the infinite dihedral group D_∞ is not nilpotent. Since the quotient of a nilpotent group is nilpotent, it follows that a nilpotent infinite virtually cyclic group has to be orientable. By Proposition 1.3.5 we know that an orientable virtually cyclic group V that is non-cyclic cannot have $b\mathcal{C}yc$. $\square$

The proof of Proposition 5.2.4, together with Example 1.3.1, also shows:

Lemma 5.2.5. A virtually cyclic group V with $\gamma(V) \leq 2$ has to be infinite cyclic or finite.

Definition 5.2.6. In a finite group G a nilpotent subgroup H with $N_G(H) = H$ is called a *Carter subgroup.*

It was proven by Carter [Car61] that any solvable group contains a Carter subgroup and any two Carter subgroups are conjugate. A finite non-solvable group need not contain a Carter subgroup, for example A_5 does not contain a Carter subgroup. However, it was shown much later by Vdovin [Vdo08] that any two Carter subgroups of a not necessarily solvable finite group are conjugate. The proof of this result is deep and relies on the classification of finite simple groups. Even though groups $G \in \Gamma_2$ will turn out to be solvable, we will rather rely on the result of Vdovin for the moment.

Definition 5.2.7. A subgroup $H \leq G$ is called *abnormal* if $g \in \langle H, H^g \rangle$ for all $g \in G$.

The following was already shown by Carter for solvable groups and the same proof combined with a result of Vdovin gives this more general result.

Proposition 5.2.8. Let G be a finite group and let $H \leq G$ be a Carter subgroup. Then H is abnormal in G.

Proof. Let $g \in G$ and let $K = \langle H, g^{-1}Hg \rangle$. Now H and $g^{-1}Hg$ are nilpotent self-normalizing subgroups of K. By [Vdo08] there exists some $k \in K$ such that $k^{-1}Hk = g^{-1}Hg$, thus $gk^{-1} \in N_G(H) = H \leq K$. Hence $g \in K$ as desired. $\square$

Lemma 5.2.9. Let $G \in \Gamma_2$ and let C and D be representatives of the conjugacy classes of maximal cyclic subgroups of G. Then $[D : C \cap D]$ divides $[G : C]$ and similarly $[C : C \cap D]$ divides $[G : D]$. In particular, it follows that ${}^{|C|\cdot|D|}/_{|C \cap D|}$ divides the order of G.

Proof. Let $I = C \cap D$. Note that D acts on the set X of right cosets Cg of C in G via right multiplication. The stabilizer of Cg is then given by $D \cap C^g = C \cap D = I$. The claim now follows from decomposing the set X into orbits and the orbit-stabilizer theorem. Each orbit has cardinality $|D/I|$. □

Lemma 5.2.10. Let $G \in \Gamma_2$, then exactly one conjugacy class of a maximal cyclic subgroup is self-normalizing.

Proof. By Lemma 5.2.2 we know that at least one maximal cyclic subgroup is self-normalizing, say C. Let D be a maximal cyclic subgroup whose conjugacy class is distinct from the class of C. If D was self-normalizing as well, the subgroups C and D would be conjugate by [Vdo08], which would imply that G is cyclic. □

Throughout this chapter we will adapt the convention that, if not explicitly stated otherwise, a subgroup C of a group $G \in \Gamma_2$ is a self-normalizing maximal cyclic subgroup, which is unique up to conjugation by Lemma 5.2.10. With $D \leq G$ we designate a maximal cyclic subgroup which is not self-normalizing. In the same vein we shall usually write c resp. d for a generator of C resp. D.

Note that C being self-normalizing also implies that C is maximal nilpotent, i.e. if $C \leq H \leq G$ with H nilpotent, then $C = H$.

Lemma 5.2.11. Let $G \in \Gamma_2$ and suppose that N is a normal subgroup of G such that G/N is cyclic. Then $G = NC$. In particular, it follows that G/N is cyclic if and only if $G = NC$.

Proof. The homomorphic image of a Carter subgroup is again a Carter subgroup by [Vdo08]. Hence $CN/N \leq G/N$ is maximal cyclic, so that $CN/N = G/N$. □

Since the abelianization of a group $G \in \Gamma_2$ is certainly cyclic we obtain similarly $G^{\mathrm{ab}} = C[G,G]/[G,G] \cong C/(C \cap [G,G])$. We also want to mention that $G' = [G,G]$ is a proper subgroup of G, which follows from a result on the existence of self-normalizing cyclic subgroups in finite simple groups, see Theorem 5.2.69.

Observe that the intersection $C \cap D$ where C, D are representatives of the maximal cyclic subgroups of a group $G \in \Gamma_2$ equals the intersection of all maximal cyclic subgroups $\Psi(G)$ by Lemma 5.1.9.

Lemma 5.2.12. A group $G \in \Gamma_2$ is generated by the cyclic subgroups C and D.

Proof. Let $H = \langle C \cup D \rangle$. Then H is a conjugate-dense subgroup of G, so $G = H$. □

Lemma 5.2.13. If $G \in \Gamma_2$, then $[G,G] = [C,D]$.

Proof. Let $N = [C,D]$, we prove that N is normal using that G is generated by c and d. Namely, we prove that $\gamma^{-1}[c^n, d^k]\gamma \in N$ when $\gamma = c$ or $\gamma = d$. One observes that

$$[c^n \cdot c, d^k] = [c^n, d^k]^c \cdot [c, d^k]$$

and likewise

$$[c^n, d^k \cdot d] = [c^n, d] \cdot [c^n, d^k]^d$$

Thus N is normal. Moreover G/N is abelian, thus $[G,G] \leq N$. Since $N \leq [G,G]$, the claim follows. □

Remark 5.2.14. For $G \in \Gamma_2$ we certainly have $G = \langle C \rangle^G \cup \langle D \rangle^G$, thus at least one of the subgroups $\langle C \rangle^G$ or $\langle D \rangle^G$ equals G. Hence G is normally generated by a single element. Such a group is called a group of weight one. It has been shown in [Kut76] that a finite group has weight one if and only if its abelianization is cyclic. Note that any simple group is of weight one. Of course, if G is infinite with property $2\mathcal{C}yc$, then G has weight one as well. It is therefore the quotient of a knot group by [Gon75].

Sometimes the following lemma is useful in establishing lower bounds on γ. Here, φ denotes the Euler totient function.

Lemma 5.2.15. Let G be a finite group and $d \in \mathbb{N}$. Then the number of conjugacy classes of elements in G of order d is at most $\varphi(d) \cdot \gamma(G)$.

5.2.1. Cyclic Subgroups up to Automorphism

If G is a finite group with $\gamma(G) \leq n$ and $N \trianglelefteq G$, then N can be covered by at most n cyclic subgroups up to conjugation in G, hence $\delta(N) \leq n$. Because of this fact it will turn out to be useful to know the number of maximal cyclic subgroups up to automorphism for certain families of groups like generalized quaternion groups. Let us first consider dihedral groups. Let D_{2n} be the dihedral group of order $2n$ and recall that it has the following presentation:

$$D_{2n} = \langle r, s \mid r^n = s^2 = (sr)^2 = 1 \rangle = C_n \rtimes C_2 \,.$$

Note that the center of D_{2n} is trivial if $n > 2$ is odd and $Z(D_{2n}) = \langle r^{n/2} \rangle \cong C_2$ for $n > 2$ even.

Lemma 5.2.16. For $n \geq 2$ we have that $\gamma(D_{2n}) = 2$ if n is odd and $\gamma(D_{2n}) = 3$ if n is even. Moreover, any two distinct maximal cyclic subgroups intersect trivially, so $D_{2n} \in \Gamma_2^I$ for $n > 2$ odd.

Proof. Observe that $rsr^{-1} = r^2 s$, thus $r^m s r^{-m} = r^{2m} s$. Since for n odd, $2 \in (\mathbb{Z}/n\mathbb{Z})^\times$, it follows that any element $r^k s$ is conjugate to s in D_{2n}. Hence for n odd D_{2n} has exactly two conjugacy classes of maximal cyclic subgroups, given by $\langle r \rangle$ and $\langle s \rangle$. If n is even, one has $\langle r \rangle$, $\langle s \rangle$ and $\langle rs \rangle$ as representatives of conjugacy classes of maximal cyclic subgroups. As s and rs are not conjugate if n is even, we have $\gamma(D_{2n}) = 3$. The claim about the intersection of maximal cyclic subgroups follows from this description immediately since $\langle r \rangle$ is a normal subgroup. □

By a deep result of Shult [Shu69a] we know that a p-group G with p odd and $\delta(G) = 1$ is elementary abelian. A p-group G with $\delta(G) = 2$ can be non-abelian:

Example 5.2.17. For p an odd prime the Heisenberg group $H_p = \langle x, y, z \mid x^p = y^p = z^p = 1, [x, z] = 1 = [y, z], [x, y] = z\rangle$ has $\delta(H_p) = 2$. Representatives of the $\mathrm{Aut}(H_p)$-conjugacy classes of maximal cyclic subgroups are given by $Z(H_p) = \langle z\rangle$ and $\langle x\rangle$.

Lemma 5.2.18. The dihedral group $D_{2n} = \langle r, s \mid r^n = s^2 = (sr)^2 = 1\rangle = C_n \rtimes C_2$ has $\delta(D_{2n}) = 2$ for $n \geq 3$. Moreover, $\delta(D_2) = \delta(D_4) = 1$.

Proof. Suppose $n \geq 3$. In the proof of Lemma 5.2.16 we have seen that $\langle r\rangle, \langle s\rangle$ and $\langle rs\rangle$ are representatives of not necessarily distinct conjugacy classes of maximal cyclic subgroups. There is a homomorphism $\psi\colon D_{2n} \to D_{2n}$ defined by $r \mapsto r$ and $s \mapsto rs$. As $\psi^n = \mathrm{id}$ the map ψ is an isomorphism. Hence $\delta(D_{2n}) \leq 2$. Also note that for $n \geq 3$, $\langle r\rangle$ is the unique cyclic subgroup of order n in D_{2n}, hence $\langle r\rangle$ is characteristic, and n is the maximal element order in D_{2n}. This implies that $\delta(D_{2n}) \geq 2$ as s does not lie in $\langle r\rangle$. The claims for $n < 3$ are immediate as D_2 is of order 2 and $D_4 \cong C_2 \times C_2$. □

Recall the presentation of the generalized quaternion groups $Q_{2^{n+1}} = \langle a, b \mid a^{2^n} = 1, b^2 = a^{2^{n-1}}, b^{-1}ab = a^{-1}\rangle$. Any element in $Q_{2^{n+1}}$ can be uniquely represented in the form a^ib^j where $0 \leq i < 2^n$ and $j \in \{0, 1\}$. The center of $Q_{2^{n+1}}$ is cyclic of order 2, generated by b^2.

Lemma 5.2.19. The quaternion groups $Q_{2^{n+1}}$ have $\gamma(Q_{2^{n+1}}) = 3$ for all $n \geq 2$.

Proof. Observe that $a^{-1}(a^nb)a = a^{n-2}b$. This implies that any element a^ib is conjugate to the element b or ab, depending on the parity of i. Hence the conjugates of $\langle a\rangle, \langle b\rangle$ and $\langle ab\rangle$ cover the quaternion group, so $\gamma(Q_{2^{n+1}}) \leq 3$. Using the normal form of elements and the fact that $b^{-1}(a^nb)b = a^{-n}b$ and $a^{-1}(a^nb)a = a^{n-2}b$ one sees that none of the three cyclic subgroups $\langle a\rangle, \langle b\rangle$ and $\langle ab\rangle$ is redundant. Hence $\gamma(Q_{2^{n+1}}) = 3$. □

Lemma 5.2.20. We have $\delta(Q_8) = 1$ with a maximal cyclic subgroup of order 4 and for $n > 2$ we have $\delta(Q_{2^{n+1}}) = 2$ with representatives of maximal cyclic subgroups of order 4 and 2^n.

Proof. The proof of Lemma 5.2.19 shows that conjugates of $\langle a\rangle$, $\langle b\rangle$ and $\langle ab\rangle$ cover $Q_{2^{n+1}}$. One checks that $(ab)^2 = b^2$, which implies that $\psi\colon Q_{2^{n+1}} \to Q_{2^{n+1}}$, defined on generators by $a \mapsto a$, $b \mapsto ab$, is a homomorphism. As ψ is surjective, it is an isomorphism. Thus $\delta(Q_{2^{n+1}}) \leq 2$. If $n = 2$, the map given on generators by $a \mapsto b^{-1}$, $b \mapsto a^{-1}$ is an isomorphism that conjugates $\langle a\rangle$ to $\langle b\rangle$. Hence $\delta(Q_8) = 1$. If $n > 2$, then we have $\delta(Q_{2^{n+1}}) \geq 2$ as well by Lemma 5.2.18 since $Q_{2^{n+1}}/Z(Q_{2^{n+1}}) \cong D_{2^n}$. □

5.2.2. The class Γ_2^I

Before we investigate the class Γ_2, we consider groups in the smaller class Γ_2^I, in which distinct maximal cyclic subgroups intersect trivially. It turns out that for proving the solvability of the groups in Γ_2^I we will not need to rely on the classification of finite simple groups. Let us first give a couple of examples of groups in the class Γ_2^I.

Examples 5.2.21. (1) The symmetric group S_3 has two conjugacy classes of maximal cyclic subgroups of order 2 resp. 3, hence $S_3 \in \Gamma_2^I$.

(2) The (up to isomorphism) unique non-abelian group of order 21, i.e. the metacyclic group $G = C_7 \rtimes C_3 = \langle c, d \mid d^7 = 1, c^3 = 1, c^{-1}dc = d^2 \rangle$ lies in Γ_2^I.

(3) Lemma 5.2.16 shows that the dihedral groups $D_{2n} \in \Gamma_2^I$ for $n > 2$ odd.

(4) The alternating group A_4 is contained in Γ_2^I. The group A_4 has two conjugacy classes of maximal cyclic subgroups, generated by the elements $(1,2)(3,4)$ and $(1,2,3)$. Note that, although the class of $(1,2,3)$ splits in A_4, the subgroup generates all conjugacy classes with the same cycle type. Also observe that distinct maximal cyclic subgroups intersect trivially. The group A_4 is not metacyclic and has Fitting subgroup $F(A_4) \cong C_2 \times C_2$ and $A_4/F(A_4) \cong C_3$. So in general, a group $G \in \Gamma_2^I$ does not split as $G \cong D \rtimes C$.

Let $G \in \Gamma_2^I$ and write $G = [C]^G \cup [D]^G$. Then it follows that

$$|G| - 1 = [G : N_G(C)] \cdot (|C| - 1) + [G : N_G(D)] \cdot (|D| - 1)$$

Since $N_G(C) = C$, we obtain the following important equation:

$$[G : C] = 1 + [G : N_G(D)] \cdot (|D| - 1)$$

Moreover, by Lemma 5.2.9 we know that $|C| \cdot |D|$ divides $|G|$.

Observation 5.2.22. For $G \in \Gamma_2^I$ we have $|G| = \left|[D]^G\right| \cdot |C|$.

Proof. Using that $\left|[D]^G\right| = [G : N_G(D)] \cdot (|D| - 1) + 1$ and $[G : C] = 1 + [G : N_G(D)] \cdot (|D| - 1)$ the claim follows. ☐

We will later see that actually $C_G(D) = [D]^G$ and $G = C_G(D) \rtimes C$. The next result could have also been deduced from the fact that Carter subgroups are unique up to conjugation, see Lemma 5.2.10. In this special case, a simpler argument suffices.

Lemma 5.2.23. For a group $G \in \Gamma_2^I$, there is exactly one conjugacy class of a maximal cyclic subgroup that is self-normalizing.

Proof. There is at least one by Lemma 5.2.2. Suppose that $C = N_G(C)$ and $D = N_G(D)$. Then by the above equation $|G| - 1 = [G : C] \cdot (|C| - 1) + [G : D] \cdot (|D| - 1)$, which can be rewritten as

$$|C| \cdot |D| = |G| \cdot (|D| + |C| - |C| \cdot |D|)$$

Hence $|G|$ divides $|C| \cdot |D|$. By Lemma 5.2.9 it follows that $|G| = |C| \cdot |D|$. This implies that $1 = |D| + |C| - |C| \cdot |D|$ or in other words $(|C| - 1) \cdot (1 - |D|) = 0$, which yields a contradiction. ☐

Lemma 5.2.24. Let G be a finite group such that distinct maximal cyclic subgroups of G intersect trivially. Then any abelian subgroup of G is cyclic or elementary abelian.

Proof. First note that if $K, K' \leq G$ are two cyclic subgroups of the same order then $K = K'$ or $K \cap K' = 1$. Now let $A \leq G$ be abelian and decompose A using the invariant factor decomposition

$$A \cong C_{k_1} \oplus C_{k_2} \oplus \ldots \oplus C_{k_n},$$

where $k_i | k_{i+1}$. Now the claim follows from the fact that a group $C_k \oplus C_{km}$ where $k, m > 1$ cannot be contained in G, since the elements $(1,1)$ and $(0,1)$ have both order km but $\langle (1,1) \rangle \cap \langle (0,1) \rangle \neq 1$. $\square$

Lemma 5.2.25. For a group $G \in \Gamma_2^I$ we have $|G| = |C| \cdot |D|$ if and only if $G = CD$ if and only if D is a normal subgroup of G.

Proof. We already know that $G = CD$ if and only if $|G| = |C| \cdot |D|$. The remaining claim then follows from the fact that

$$[G : C] = 1 + [G : N_G(D)] \cdot (|D| - 1) .$$

$\square$

Observation 5.2.26. If $G \in \Gamma_2^I$ contains a non-trivial normal cyclic subgroup, then D is a normal subgroup.

Proof. Let $K \leq G$ be a non-trivial normal cyclic subgroup. Suppose $K \leq C^g$ for some $g \in G$. Then $K \leq C^g$ for all $g \in G$. This yields a contradiction since $[G : N_G(C)] = [G : C] > 1$ and different maximal cyclic subgroups intersect trivially. Hence $K \leq D^g$ for some $g \in G$, and then also for all $g \in G$, since K is normal. Hence $D^g \cap D \neq 1$, so $D^g = D$ for all $g \in G$. In other words, D is a normal subgroup of G. $\square$

Lemma 5.2.27. A group $G \in \Gamma_2^I$ has trivial center.

Proof. Suppose that $Z(G) \neq 1$. Note that $Z(G)$ is cyclic since $\gamma(G) = 2$. If $Z(G) \leq C$, then the condition on trivial intersections of maximal cyclic subgroups would imply that C is a normal subgroup. Thus $Z(G) \leq D$ and D is a normal subgroup of G by Observation 5.2.26. But $Z(G) \leq C_G(C) = C$. Since $C \cap D = 1$, we arrive at a contradiction. $\square$

Lemma 5.2.28. For $G \in \Gamma_2^I$ and $C' \leq C$ non-trivial or $D' \leq D$ non-trivial, we have $N_G(C') = N_G(C) = C$ and $N_G(D') = N_G(D)$.

Proof. Let $g \in N_G(C')$, then $1 \neq C' = g^{-1}C'g \leq C \cap g^{-1}Cg$, thus $C = g^{-1}Cg$, i.e. $g \in N_G(C) = C$. With the same argument the claim for D' follows. $\square$

Lemma 5.2.29. Let $G \in \Gamma_2^I$ and let $D' \leq D$ be a non-trivial subgroup. Then $C_G(D') \cap C^g = 1$ for all $g \in G$.

Proof. Let $x \in C_G(D')$ be a non-trivial element and let $D' = \langle d' \rangle$. So $x^{-1}d'x = d'$, equivalently $d'^{-1}xd' = x$, i.e. $d' \in C_G(x)$. Suppose x is conjugate to an element of C, so $x = g^{-1}c^m g$ for some $c^m \neq 1$ and $g \in G$. Then $d' \in C_G(x) = g^{-1}C_G(c^m)g = g^{-1}Cg$ by Lemma 5.2.28. Thus it would follow that $D' \cap g^{-1}Cg \neq 1$, which is a contradiction. $\square$

As $C_G(D) \cap C^g = 1$ for all $g \in G$, it follows that $C_G(D)$ acts freely on the set of right cosets of C in G. In particular, it follows that $|C_G(D)|$ divides $[G : C]$. Moreover, the fact that $C_G(D) \cap C^g = 1$ implies that

$$D \leq C_G(D) \leq [D]^G .$$

Below in Theorem 5.2.47 we will actually see that $C_G(D) = [D]^G$.

Lemma 5.2.30. If $G \in \Gamma_2^I$ and $D \trianglelefteq G$, then $C_G(D) = D$.

Proof. The claim follows since $D \leq C_G(D) \leq [D]^G = D$. □

Observation 5.2.31. Let $G \in \Gamma_2^I$ and let $D' \leq D$ be a non-trivial subgroup. Then $C_G(D) \trianglelefteq C_G(D')$.

Proof. Let $x \in C_G(D)$ and $g \in C_G(D')$. Since $C_G(D') \leq N_G(D') = N_G(D)$ by Lemma 5.2.28, we know that $gdg^{-1} = d^n$ for some $n \in \mathbb{N}$. Thus

$$\begin{aligned}(g^{-1}x^{-1}g)d(g^{-1}xg) &= g^{-1}(x^{-1}d^n x)g \\ &= g^{-1}d^n g \\ &= d\end{aligned}$$

Thus $g^{-1}xg \in C_G(D)$ and $C_G(D)$ is a normal subgroup of $C_G(D')$. □

Lemma 5.2.32. Let $G \in \Gamma_2^I$ with $|G| = |C| \cdot |D|$. Then $C_G(D) = D \trianglelefteq G$.

Proof. By Lemma 5.2.25 we know that that $D \trianglelefteq G$ is a normal subgroup and $G = CD$. Suppose $c^k d^n \in C_G(D)$, then $c^k dc^{-k} = d$, so $d^{-1}c^k d = c^k$. If $c^k \neq 1$, then $d^{-1}Cd \cap C \neq 1$, thus $d^{-1}Cd = C$. But this is impossible. Hence $C_G(D) = D$. □

Lemma 5.2.33. Let $G \in \Gamma_2^I$ and suppose that $g^n \in C$ for some $n \in \mathbb{Z}$ such that $g^n \neq 1$. Then $g \in C$.

Proof. Note that $g^n \in C^g \cap C$, hence $g \in N_G(C) = C$. □

Lemma 5.2.34. Let $G \in \Gamma_2^I$ and let $H \leq G$ be a nilpotent subgroup. Suppose that $H \cap C^g \neq 1$ for some $g \in G$. Then H is cyclic.

Proof. Let $C' = H \cap C^g \leq C^g$. Then

$$N_H(C') = H \cap N_G(C') = H \cap N_G(C^g) = H \cap C^g = C'$$

by Lemma 5.2.28. Thus C' is self-normalizing in H, hence $C' = H$. □

Proposition 5.2.35. Let $G \in \Gamma_2^I$ and let $H \leq [C]^G$ be a subgroup. Then H is cyclic.

Proof. We prove the claim by induction on the order of H. We can thus assume that all proper subgroups of H are cyclic. Then H is solvable. Namely, either H is a p-group for some prime p or all Sylow subgroups of H are proper. In the latter case H is solvable by [Rob, Theorem 10.1.10] since all Sylow subgroups of H are cyclic by assumption. As H is solvable, H' is a proper subgroup of H and thus cyclic. If H' is trivial then H is cyclic by Lemma 5.2.34. Otherwise there is some $g \in G$ such that $H' \leq C^g$ and

$$H = N_H(H') = N_G(H') \cap H = C^g \cap H \leq C^g\,,$$

since $N_G(H') = N_G(C^g) = C^g$. □

Observation 5.2.36. Let $G \in \Gamma_2^I$ and $H \leq G$ be a subgroup such that $H \cap C^g \neq 1$ for some $g \in G$. Then $N_H(H \cap C^g) = H \cap C^g$.

Proof. Without loss of generality we can assume that $g = 1$. We let $C' = H \cap C$. Note that $C' = H \cap C = H \cap N_G(C') = N_H(C')$ by Lemma 5.2.28. □

Lemma 5.2.37. Let $G \in \Gamma_2^I$ and let $H \leq G$ be nilpotent. Then $H \subseteq [D]^G$ or H is cyclic.

Proof. Suppose that H is non-trivial and not contained in $[D]^G$, hence $H \cap C^g \neq 1$ for some $g \in G$. Now $H \cap C^g$ is a non-trivial self-normalizing subgroup of H by Observation 5.2.36. Since H is nilpotent, $H = H \cap C^g$ and thus H is cyclic. □

Corollary 5.2.38. Let $G \in \Gamma_2^I$, then any Sylow subgroup of G is either contained in $[D]^G$ or in $[C]^G$.

Corollary 5.2.39. For $G \in \Gamma_2^I$ we have $(|C|, |D|) = 1$.

Proof. Suppose p is a prime dividing $|C|$ as well as $|D|$. Consider the Sylow p-subgroup P of G. Since there is $C' \leq C$ of order p, C' is subconjugate to P. Similarly the subgroup $D' \leq D$ of order p is subconjugate to P. However this contradicts Corollary 5.2.38. □

We can strengthen Corollary 5.2.39 to:

Corollary 5.2.40. For $G \in \Gamma_2^I$ we have $(|C|, |C_G(D)|) = 1$. Moreover, $(|C|, [G : C]) = 1$.

Proof. Suppose p is a common prime divisor of $|C|$ and $|C_G(D)|$. Then there is an element $x \in C_G(D)$ of order p. Since $C_G(D) \subseteq [D]^G$ by Lemma 5.2.29 it follows that p divides $|D|$. But this contradicts Corollary 5.2.39. If p is a common prime divisor of $[G : C]$ and $|C|$, then the Sylow p-subgroup $P \leq G$ has to be conjugate to a subgroup of C by Lemma 5.2.37, which yields a contradiction. □

Remark 5.2.41. Note that Corollary 5.2.40 cannot be strengthened to $(|C|, |N_G(D)|) = 1$. For example, in $G = S_3$, we have $|C| = 2$ and $D \trianglelefteq G$, thus $(|C|, |N_G(D)|) = (2, 6) = 2$.

Lemma 5.2.42. Let $G \in \Gamma_2^I$ and let $N \trianglelefteq G$ be a normal subgroup lying in $[D]^G$. Then

$$|N| = 1 + [G : N_G(D)] \cdot (|D \cap N| - 1)$$

Proof. We know that $N = [D \cap N]^G$ since N is normal in G. Since all cyclic subgroups $(D \cap N)^g \leq N$ have the same order, they either intersect trivially or are equal. Hence $|N| = 1 + [G : N_G(D \cap N)] \cdot (|D \cap N| - 1)$. Since $N_G(D \cap N) = N_G(D)$ the claim follows. □

The following is a special case of Theorem 5.2.47 that we will prove below. It only relies on Burnside's normal p-complement theorem instead of Thompson's theorem on the nilpotency of Frobenius kernels.

Lemma 5.2.43. Let $G \in \Gamma_2^I$ and suppose $|C| = p^n$ for some prime p. Then $[D]^G$ is a subgroup.

Proof. We know that C is a Sylow p-subgroup of G since $(|C|, |D|) = 1$. Since $N_G(C) = C$, it follows by Burnside's normal p-complement theorem that there is a normal subgroup N of index p^n. Moreover, $N \leq [D]^G$ as $|N|$ is coprime to p. By Lemma 5.2.42 we have $|N| = 1 + [G : N_G(D)](|D \cap N| - 1)$. At the same time $|N| = [G : C] = 1 + [G : N_G(D)](|D| - 1)$. So $|D| = |D \cap N|$, thus $D \leq N$ and the claim follows. $\square$

Lemma 5.2.44. Let $G \in \Gamma_2^I$ and suppose that $N = [D]^G$ is a subgroup. Then $[G, G] \leq N$, or in other words $[G, G] \cap C^g = 1$ for all $g \in G$.

Proof. We have that $[d^n, c^m] = d^{-n}(c^{-m} d^n c^m) \in N$. Together with the fact that $[G, G] = [C, D]$, the claim follows. $\square$

Let us recall the following important notion:

Definition 5.2.45. A finite group G is called *Frobenius* if there exists a non-trivial proper subgroup H that is malnormal, i.e. $H^g \cap H = 1$ for all $g \in G \setminus H$. The subgroup H is called *Frobenius complement*.

Given a Frobenius group G with Frobenius complement H, one defines the *Frobenius kernel* $K = \left(G \setminus [H]^G\right) \cup \{1\}$. Using character theory Frobenius has shown that K is actually a subgroup [Fro01] and there is still no proof known that does not rely on character theory. One has $|K| \equiv 1 \mod |H|$ and Frobenius groups split as semidirect products $G = K \rtimes H$. It is a theorem proven by Thompson in his Ph.D. thesis that Frobenius kernels are nilpotent [Isa08, Theorem 6.24]. Moreover, the Frobenius kernel equals the Fitting subgroup $F(G)$ of G and any two Frobenius complements are conjugate by the Schur-Zassenhaus theorem. Sometimes we shall make use of the following result:

Lemma 5.2.46 ([Isa08, Theorem 6.4])**.** Let K be a normal subgroup of a finite group G and suppose that H is a complement for K in G. Then the following are equivalent:

(1) $H \cap H^g = 1$ for all $g \in G \setminus H$.

(2) $C_G(h) \leq H$ for all non-trivial $h \in H$.

(3) $C_G(k) \leq K$ for all non-trivial $k \in K$.

We are now ready to formulate the main theorem of this section:

Theorem 5.2.47. Let $G \in \Gamma_2^I$. Then G is a Frobenius group with Frobenius kernel $F(G) = G' = C_G(D) = [D]^G$ and Frobenius complement $C \cong G^{\mathrm{ab}}$ and exactly one of the following holds:

(1) The cyclic subgroup D is normal, so that G is metacyclic and splits as $G = D \rtimes C$. Moreover, all Sylow subgroups of G are cyclic.

(2) The subgroup $C_G(D)$ is a non-cyclic elementary abelian p-group for some prime p. Moreover, $C_G(D)$ is, being normal, the Sylow p-subgroup of G.

In particular, the derived length of G equals 2.

Proof. We know that $C \cap C^g = 1$ for all $g \in G \setminus C$, so G is a Frobenius group with Frobenius complement C. Let K be the Frobenius kernel, then $K = [D]^G$. The derived subgroup of G is then given by $G' = K[C, C] = K$. By [Isa08, Theorem 6.24] K is a nilpotent group, in particular the center $Z(K)$ is non-trivial. If $Z(K)$ is cyclic, then $Z(K)$ is a non-trivial normal cyclic subgroup of G. Thus D is normal by Observation 5.2.26 and since G is Frobenius with Frobenius kernel D we have $C_G(D) \leq D$, hence $D = C_G(D)$. By Corollary 5.2.38 all Sylow subgroups of G are cyclic.

So suppose in the following that $Z(K)$ is non-cyclic. Then $\langle D, Z(K)\rangle$ is a non-cyclic abelian subgroup of G. By Lemma 5.2.24 it follows that D is of order p where p is some prime. Thus $C_G(D) \subseteq [D]^G$ is a p-group. Since $|G| = [G : C_G(D)] \cdot |C_G(D)| = [G : C] \cdot |C|$ and $(|C_G(D)|, |C|) = 1$, it follows that p divides $[G : C]$. Suppose for the moment that p divides $[G : C_G(D)]$ as well. But

$$[G : C] \cdot [N_G(D) : C_G(D)] = [N_G(D) : C_G(D)] + [G : C_G(D)] \cdot (|D| - 1)$$

implies that p would divide $[N_G(D) : C_G(D]$ as well. Now, $N_G(D)/C_G(D) \hookrightarrow \mathrm{Aut}(|D|)$ and the latter group has order $p - 1$, which yields a contradiction. Hence $([G : C_G(D)], p) = 1$, so $C_G(D)$ is the Sylow p-subgroup of G.

Let $q \neq p$ be another prime and suppose that q divides $[G : C_G(D)]$ as well as $[G : C]$, let $[G : C_G(D)] = q^\alpha \cdot n$ and $[G : C] = q^\beta \cdot m$ where $(q, n) = 1 = (q, m)$ and $\alpha, \beta \geq 1$. Since D is of order p and $(|C|, |D|) = 1$, we have $|C| = q^\gamma k$ for some $\gamma \geq 1$ and $k \in \mathbb{N}$ such that $(q, k) = 1$. Then $|G| = [G : C] \cdot |C| = q^{\beta+\gamma} mk = [G : C_G(D)] \cdot |C_G(D)| = q^\alpha n \cdot |C_G(D)|$. Since $(|C_G(D)|, q) = 1$, it follows that $\alpha = \beta + \gamma$. Let Q be the Sylow q-subgroup, which is of order q^α. Since D is of order p, we have $Q \cap D^g = 1$ for all $g \in G$. Hence $Q \subseteq [C]^G$ and by Proposition 5.2.35 it follows that Q is cyclic. But then $|Q|$ divides $|C|$ which yields a contradiction. Thus we have shown that $([G : C_G(D)], [G : C]) = 1$. Since $(|C_G(D)|, |C|) = 1$ as well, it follows that $[G : C_G(D)] = |C|$ and $[G : C] = |C_G(D)|$. Recall that $C_G(D) \subseteq [D]^G$ and the latter subset contains $1 + [G : N_G(D)](|D| - 1) = [G : C] = |C_G(D)|$ elements. Hence $C_G(D) = [D]^G$ and thus $C_G(D)$ is a normal subgroup, so $C_G(D) = C_G(D)^g = C_G(D^g)$. In particular, $C_G(D)$ is an abelian subgroup of G. □

Corollary 5.2.48. Let $G \in \Gamma_2^I$ and suppose that $C_G(D) = D$. Then D is normal.

Even if $D < C_G(D)$ is a proper subgroup, it is in general not the case that $C_G(D) = N_G(D)$. There is a group $G \in \Gamma_2^I$ of order 72 with $C_G(D) = F(G) \cong C_3 \times C_3$ and $|C| = 8$ such that $[N_G(D) : C_G(D)] = 2$.

Corollary 5.2.49. Let $G \in \Gamma_2^I$. Then $C_G(D') = C_G(D)$ for any non-trivial subgroup $D' \leq D$.

Proof. We always have $C_G(D) \leq C_G(D')$. As $C_G(D)$ is the Frobenius kernel of G, and D' is non-trivial, the reverse inclusion holds as well by Lemma 5.2.46. □

Lemma 5.2.50. Let $G \in \Gamma_2^I$. Then the number of conjugacy classes $k(G)$ is given by

$$k(G) = \frac{[G : C] - 1}{|C|} + |C|\,.$$

Proof. By Corollary 5.2.49 we know that $C_G(D') = C_G(D)$ for all non-trivial subgroups $D' \leq D$. Moreover, we have $|G| = |C_G(D)| \cdot |C|$ by Theorem 5.2.47. We consider the class equation for G and denote by k the number of conjugacy classes in G that intersect D. Then

$$\begin{aligned}|G| &= 1 + k \cdot [G : C_G(D)] + (|C| - 1) \cdot [G : C_G(C)] \\ &= 1 + k \cdot [G : C_G(D)] - [G : C] + |G|\end{aligned}$$

Now $k(G) = 1 + k + (|C| - 1)$ and the claim follows since $[G : C_G(D)] = |C|$. □

Corollary 5.2.51. Let $G \in \Gamma_2^I$ and suppose that D is a normal subgroup of G. Then $|C|$ divides $|D| - 1$ and the number $k(G)$ of conjugacy classes is given by $k(G) = {}^{(|D|-1)}/_{|C|} + |C|$.

Proposition 5.2.52. Let $G \in \Gamma_2^I$ and suppose that G^{ab} is of order two. Then G is a dihedral group.

Proof. By Theorem 5.2.47 we know that C is of order two. By Lemma 5.1.10 it follows that $\gamma(C_G(D)) \leq 2 \cdot \gamma(G) = 4$. First let us assume that $C_G(D)$ is non-cyclic, thus $C_G(D)$ is an elementary p-abelian group C_p^n for some prime p and some $n \geq 2$. Since $\gamma(C_p^n) = p^{n-1} + p^{n-2} + \ldots + p + 1$, it follows that $p \in \{2, 3\}$ and $n = 2$. As $(|C|, |D|) = 2$, we must have $p = 3$. Let $\varphi \in \mathrm{Aut}(C_3 \times C_3)$ be an automorphism of order two and let $x \in C_3 \times C_3$ be a non-trivial element. Either $x = \varphi(x)$ or $\langle x\varphi(x^2)\rangle$ is a non-trivial subgroup. Note that $\varphi(x\varphi(x^2)) = \varphi(x)x^2 = (x\varphi(x^2))^2$. Thus in both cases there exists a non-trivial cyclic subgroup that is invariant under φ. But then $(C_3 \times C_3) \rtimes_\varphi C_2$ would contain a non-trivial normal cyclic subgroup which contradicts Observation 5.2.26. Hence we conclude that $C_G(D) = D$ with D of odd order. Let $|D| = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ and recall that there is a unique element of order two in the automorphism group of $C_{p_i^{k_i}}$ given by $z \mapsto z^{-1}$ as long as p_i is odd. Since the automorphism group of D is the direct product of the automorphism groups of $C_{p_i^{k_i}}$ and $Z(G) = 1$, it follows that C acts on $D = \langle d \rangle$ via $d \mapsto d^{-1}$. Hence G is a dihedral group. □

Lemma 5.2.53. Let $G \in \Gamma_2^I$ and suppose that D is even. Then D is of order two and $F(G) = N_G(D) = C_G(D)$ is an elementary abelian 2-group.

Proof. Suppose that D is a normal subgroup and let $D' \leq D$ be of order two. We have $N_G(D') = C_G(D')$ as D' is of order two. It would follow that $G = N_G(D) = N_G(D') = C_G(D') = D$ by Corollary 5.2.49. Thus the claim follows from Theorem 5.2.47. □

Lemma 5.2.54. If $G \in \Gamma_2^I$, then $\langle D \rangle^G$ is a proper subgroup and G is normally generated by C.

Proof. Note that $D \leq C_G(D) \trianglelefteq G$ and $C_G(D)$ is a proper subgroup of G. Now $C_G(D) = [D]^G$, in particular $\langle D \rangle^G = C_G(D)$. Since $G = \langle C \rangle^G \cup \langle D \rangle^G$ is the union of two subgroups, it follows that $G = \langle C \rangle^G$. □

5.2.2.1. Classification

In this section we want to improve upon Theorem 5.2.47 and obtain a classification of the groups $G \in \Gamma_2^I$ in the sense that we will list the groups that appear, though not necessarily determining if some of them are isomorphic. We begin by analyzing the metacyclic groups $G \in \Gamma_2^I$ in detail.

Lemma 5.2.55. Let p be an odd prime and let K be a cyclic group of order p^n for some $n \geq 1$. Let $\varphi \in \mathrm{Aut}(K)$ be a non-trivial automorphism whose order is coprime to p. Then $\mathrm{Fix}(\varphi) = \{y \in K \mid \varphi(y) = y\} = \{1\}$, i.e. φ acts fixed point freely on K.

Proof. Let $K = \langle x \rangle$. We know that $|\mathrm{Aut}(K)| = p^{n-1}(p-1)$, so the order of φ divides $p-1$. We can write $\varphi(x) = x^m$ for some m that satisfies

$$\begin{aligned}(m, p) &= 1\\ p^n &\mid \left(m^{p-1} - 1\right)\end{aligned}$$

Now, let $y \in \mathrm{Fix}(\varphi)$, say $y = x^k$. Then $x^k = \varphi(x^k) = x^{km}$, so p^n divides $k(m-1)$. If p^n divides k, then $y = 1$. So we can assume that p divides $m - 1$. We now write

$$\begin{aligned}m^{p-1} - 1 &= ((m-1)+1)^{p-1} - 1\\ &= \sum_{i=0}^{p-1} \binom{p-1}{i} (m-1)^i - 1\\ &= (m-1) \sum_{i=1}^{p-1} \binom{p-1}{i} (m-1)^{i-1}\end{aligned}$$

Note that

$$\sum_{i=1}^{p-1} \binom{p-1}{i} (m-1)^{i-1} = p - 1 + \binom{p-1}{2}(m-1) + \ldots + \binom{p-1}{p-1}(m-1)^{p-2}$$

Since p divides $m-1$ and $p \geq 3$ it follows that p cannot divide $\sum_{i=1}^{p-1} \binom{p-1}{i}(m-1)^{i-1}$. Since p^n divides $m^{p-1} - 1$, it follows that p^n has to divide $m - 1$. Thus $\varphi(x) = x^m = x$, so φ is the identity. □

Lemma 5.2.56. Suppose $G \in \Gamma_2^I$ with $F(G) = D$ cyclic of order p^n for some odd prime p. Then the order of C divides $p - 1$. Conversely, for any odd prime power p^n and divisor d of $p - 1$ there exists precisely one group $G \in \Gamma_2^I$ up to isomorphism such that $F(G)$ is cyclic of order p^n and the order of the maximal cyclic subgroup C equals d.

Proof. First note that the natural homomorphism $C \to \mathrm{Aut}(D)$ is injective since $C_G(D) = D$. As p is odd, the group $\mathrm{Aut}(D)$ is cyclic and thus the uniqueness statement follows. Since C has order coprime to $|D| = p^n$ it follows that $|C|$ divides $p - 1$ as $C \leq \mathrm{Aut}(D)$ and the latter group is of order $p^{n-1}(p-1)$.

Now let us prove the existence statement. Let D be a cyclic group of order p^n and choose the subgroup $C \leq \mathrm{Aut}(D)$ of order d and define $G = D \rtimes C$. For $a \in C$ we denote by φ_a the corresponding automorphism of D. We will show that $G \in \Gamma_2^I$ with corresponding maximal cyclic subgroups C and D. Let $(x, a) \in G$. If $a = 1$, then the element is contained in D. So suppose $a \neq 1$. We can compute for any $y \in D$

$$(y, 1)^{-1}(x, a)(y, 1) = (y^{-1} x \varphi_a(y), a)\,.$$

Let us define the set $S = \{y\varphi_a(y)^{-1} \mid y \in D\} \subseteq D$ and the map $f\colon D \to S$, $y \mapsto y\varphi_a(y)^{-1}$. If $f(y) = f(z)$ then $z^{-1}y \in \mathrm{Fix}(\varphi_a)$. By Lemma 5.2.55 the latter subgroup is trivial. Hence f is injective, thus also surjective since $S \subseteq D$. In particular, for $x \in D$ there exists some $y \in D$ such that $x = y\varphi_a(y)^{-1}$. Thus (x, a) is conjugate to $(1, a) \in C$. The claim about maximal cyclic subgroups intersecting trivially follows easily since C is self-normalizing, D is normal and $(|C|, |D|) = 1$. □

Theorem 5.2.57. Let $G = D \rtimes C \in \Gamma_2^I$ be metacyclic and let $\pi(|D|) = \{p_1, \dots, p_r\}$. Then $|C|$ divides $(p_1 - 1, p_2 - 1, \dots, p_r - 1)$. Conversely, for any two given two numbers n, m with $\pi(n) = \{p_1, \dots, p_r\}$ and m a divisor of $(p_1 - 1, p_2 - 1, \dots, p_r - 1)$, there exists at least one group $D \rtimes C \in \Gamma_2^I$ with $|D| = n$ and $|C| = m$.

Proof. Let P_i be the Sylow p_i-subgroup of G. As $(|C|, |D|) = 1$ and D is normal in G, $P_i \le D$. Actually, $F(G) = D = P_1P_2 \dots P_r$. As P_i is a characteristic subgroup of G we can form $G_i = P_iC$. Now, observe that C is a Carter subgroup of G_i and as $G = DC$ one sees that $G_i \in \Gamma_2^I$. Then Lemma 5.2.56 applies and so $|C|$ divides $p_i - 1$ for all $1 \le i \le r$. Using the construction in the proof of Lemma 5.2.56 the second claim follows as well. □

Example 5.2.58. There are two non-isomorphic groups in Γ_2^I of the form $C_{65} \rtimes C_4$. First, note that $65 = 5 \cdot 13$, $(\mathbb{Z}/5\mathbb{Z})^\times$ is of order 4 with generators $\{2, 3\}$. The group $(\mathbb{Z}/13\mathbb{Z})^\times$ is generated by 2 and the cyclic subgroup of $(\mathbb{Z}/13\mathbb{Z})^\times$ of order 4 has the generators $\{5, 8\}$. Let us define

$$G_{n,m} = \langle \alpha, \beta, c \mid \alpha^5 = \beta^{13} = c^4 = 1, [\alpha, \beta] = 1, \alpha^c = \alpha^n, \beta^c = \beta^m \rangle$$

Then $K = G_{2,5} \cong G_{3,8}$ and $L = G_{2,8} \cong G_{3,5}$ lie in Γ_2^I by the proof of Theorem 5.2.57. However, one can show that K and L are not isomorphic.

We will now determine the structure of the groups $G \in \Gamma_2^I$ where $F(G)$ is a non-cyclic elementary abelian p-group. First, let us construct some prototypical examples. Note that, if not mentioned otherwise, the group of units of a field is acting in the natural way on the field by multiplication.

Lemma 5.2.59. For any $n \ge 1$ the group $G = \mathbb{F}_{p^n} \rtimes \mathbb{F}_{p^n}^\times$ lies in Γ_2^I. Moreover, $N_G(D) = \mathbb{F}_{p^n} \rtimes \mathbb{F}_p^\times$ where $D = \langle (1, 1) \rangle$.

Proof. Note that the group multiplication is given by $(x, a) \cdot (y, b) = (x + ay, ab)$ and so $(y, b)^{-1} = (-b^{-1}y, b^{-1})$ where $(x, a), (y, b) \in G = \mathbb{F}_{p^n} \rtimes \mathbb{F}_{p^n}^\times$. We let $D = \langle (1, 1) \rangle$ and we let $C = \langle (0, t) \rangle$ where t is a generator of $\mathbb{F}_{p^n}^\times$.

Let $(x, a) \in G$. If $a = 1$ and $x \ne 0$, then $(0, x^{-1})(x, 1)(0, x^{-1})^{-1} = (1, 1)$, so $(x, 1)$ lies in D up to conjugation. If $a \ne 1$, then note that for any $y \in \mathbb{F}_{p^n}$ we have

$$(y, 1)(x, a)(y, 1)^{-1} = (x + y - ay, a) = (x + y(1 - a), a)$$

So we can choose $y = -x(1 - a)^{-1}$ in order to conjugate (x, a) to $(0, a)$.

We now are left to show that C is malnormal, i.e. $C^g \cap C = 1$ unless $g \in C$. We compute

$$(y, b) \cdot (0, a) \cdot (y, b)^{-1} = (y \cdot (1 - a), a)$$

If $(y \cdot (1-a), a) \in C$, then $y = 0$ so that $(y, b) = (0, b) \in C$ or $a = 1$. As D is of order p it follows that $G \in \Gamma_2^I$.

The last claim about the normalizer of D follows from a straightforward computation. $\square$

Observation 5.2.60. Let $C \le \mathbb{F}_{p^n}^\times$, then C, considered as a subgroup of $\mathbb{F}_{p^n} \rtimes C$ is malnormal by Lemma 5.2.59.

Lemma 5.2.61. Let $n \ge 2$ and let $C \le \mathbb{F}_{p^n}^\times$ be of order ${}^{p^n-1}/{}_{p-1}$. Then $(C \cdot x) \cap \mathbb{F}_p \neq \emptyset$ for all $x \in \mathbb{F}_{p^n}$ if and only if $(n, p-1) = 1$. If $(n, p-1) = 1$, then $C \cdot x$ intersects $\mathbb{F}_p$ in precisely one point.

Proof. Note that C acts without fixed points on $\mathbb{F}_{p^n}^\times$ with exactly $(p-1)$ orbits. Consider the orbits $C \cdot 1, \ldots, C \cdot (p-1)$. If the orbits are not pairwise distinct, there will exist another orbit that will not intersect $\mathbb{F}_p$. Observe that the orbits are pairwise distinct if and only if $C \cap \mathbb{F}_p^\times = 1$. Since $\mathbb{F}_{p^n}^\times$ is cyclic, this happens precisely if $(|C|, |\mathbb{F}_p^\times|) = 1$. As $({}^{p^n-1}/{}_{p-1}, p-1) = (n, p-1)$ by Lemma A.0.8, the claim follows. $\square$

Lemma 5.2.62. Let $n \ge 2$ and let $C \le \mathbb{F}_{p^n}^\times$ be of order ${}^{p^n-1}/{}_{p-1}$. If $G = \mathbb{F}_{p^n} \rtimes C \in \Gamma_2$ then $(n, p-1) = 1$. Conversely, if $(n, p-1) = 1$, then $G \in \Gamma_2^I$.

Proof. For the convenience of the reader we recall that conjugation in G is given by

$$(y, b) \cdot (x, a) \cdot (y, b)^{-1} = (b \cdot x + y - a \cdot y, a)\,.$$

First, let us assume that $G \in \Gamma_2$. By Observation 5.2.60 the subgroup C is malnormal and hence a self-normalizing maximal cyclic subgroup. Since $|G|$ is divisible by p, but $(|C|, p) = 1$, the subgroup D has order divisible by p. It follows that any element $(x, 1)$ with $x \in \mathbb{F}_{p^n}$ lies in D up to conjugation. Now,

$$(y, b) \cdot (x, 1) \cdot (y, b)^{-1} = (b \cdot x, 1)$$

and by Lemma 5.2.61 we can conclude that $(n, p-1) = 1$.

For the converse, let us assume that $(n, p-1) = 1$. Let $D = \langle (1, 1) \rangle \le \mathbb{F}_{p^n}$. If $(x, a) \in G$ with $a \neq 1$, then choosing $y = -x(1-a)^{-1}$ yields

$$(y, 1) \cdot (x, a) \cdot (y, 1)^{-1} = (0, a) \in C\,.$$

Also observe that

$$(0, b) \cdot (x, 1) \cdot (0, b)^{-1} = (b \cdot x, 1)\,.$$

By Lemma 5.2.61 we know that for any $x \in \mathbb{F}_{p^n}$ there exists some $b \in C$ such that $b \cdot x \in \mathbb{F}_p$. Moreover, by Observation 5.2.60 it follows that distinct maximal cyclic subgroups intersect trivially, so $G \in \Gamma_2^I$. $\square$

Let p be a prime and let $q = p^m$ for some $m \ge 1$. The Cayley-Hamilton theorem implies that the maximum element order of $\mathrm{GL}_n(q)$ is bounded by $q^n - 1$. In fact, view the finite field $\mathbb{F}_{q^n}$ as an n-dimensional $\mathbb{F}_q$-vector space and for a *primitive element* $\alpha \in \mathbb{F}_{q^n}^\times$, i.e. a generator of the cyclic group $\mathbb{F}_{q^n}^\times$, consider the $\mathbb{F}_q$-linear invertible map $\mathbb{F}_{q^n} \to \mathbb{F}_{q^n}, x \mapsto \alpha \cdot x$.

Of course, the latter map has order $|\mathbb{F}_{q^n}^\times| = q^n - 1$. Any element in $\mathrm{GL}_n(q)$ of this maximal order $q^n - 1$ is called a *Singer cycle*. The corresponding cyclic subgroup that is generated by a Singer cycle is called a *Singer cyclic subgroup*. It is a standard fact that any two Singer cyclic subgroups of $\mathrm{GL}_n(q)$ are conjugate [Hup67, II.7].

Proposition 5.2.63. Let $G \in \Gamma_2^I$ with $F(G)$ an elementary abelian p-group of order p^n with $n \geq 2$. Then $p^n - 1/p-1$ divides $|C|$ and $|C|$ divides $p^n - 1$.

Proof. By the discussion preceding this proposition, the maximum element order of $\mathrm{GL}_n(p)$ is equal to $p^n - 1$. Now, we have $p^n = 1 + [C : N_C(D)](p - 1)$, so

$$[C : N_C(D)] = \frac{p^n - 1}{p - 1}\,.$$

In particular, we have $|C| \geq p^n - 1/p-1$. We also know that $|C|$ is coprime to p. We now claim that these facts together already imply that C is contained in a Singer cyclic subgroup. Let $c \in C$ be a generator and we view C as a subgroup of $\mathrm{GL}_n(p)$. As the order of c is coprime to p, the corresponding matrix has distinct eigenvalues in the algebraic closure and thus is diagonalizable. Putting c into the primary rational canonical form, the matrix is a block sum of companion matrices associated to irreducible polynomials. Suppose for the moment that the primary rational canonical form of c contains more than one block. Each block of size m, being the companion matrix of an irreducible matrix, acts as the power of a Singer cycle, and thus its order divides $p^m - 1$. It follows that the order of c, being the least common multiple of the orders of the blocks, is strictly smaller than $p^n - 1/p-1$, yielding a contradiction. Hence the primary rational canonical form of c contains a single block and thus C is contained in a Singer cyclic subgroup. Hence $|C|$ divides $p^n - 1$ as claimed.

□

5.2.3. The class Γ_2

Let us now consider the more general class Γ_2 which contains the finite groups with exactly two conjugacy classes of maximal cyclic subgroups. Recall that csc-groups are finite groups whose cyclic subgroups of the same order are conjugate. It turns out that some of the ideas used in the analysis of csc-groups are also applicable here [CJ09], although our arguments tend to be much more involved.

Remark 5.2.64. Let $G \in \Gamma_2$. Since $G = [C]^G \cup [D]^G$ it is impossible that both $[D]^G$ and $[C]^G$ are subgroups of G. We have seen in the previous section that for groups $G \in \Gamma_2^I$ the set $[D]^G$ forms a subgroup. In contrast, for groups in Γ_2, it can happen that both, $[C]^G$ and $[D]^G$ are not subgroups. For example, there is a group $G \in \Gamma_2$ of order 168 with $F(G) \cong (C_2)^3$ and complement of the form $C_7 \rtimes C_3$. The subgroup C is of order 6 and D is of order 7 and neither $[C]^G$ nor $[D]^G$ are subgroups of G. For example, one can show that $[D]^G$ contains 7^2 elements, but the Sylow 7-subgroup of G is cyclic of order 7.

Remark 5.2.65. We also want to mention that not every group $G \in \Gamma_2$ is a csc-group. There is a group G of order 896 which contains two conjugacy classes of involutions. It has $|C| = 14$, $|D| = 4$, $Z(G) \cong C_2$ but $C \cap D = 1$. Moreover, the Fitting subgroup $F(G)$

equals the Sylow 2-subgroup P of G and $Z(G) = Z(P)$ such that $P/Z(P)$ is a Suzuki 2-group of order 64 (we shall recall the definition and properties of Suzuki 2-groups below in Definition 5.2.110).

In the following, φ denotes the Euler totient function.

Lemma 5.2.66. Let $G \in \Gamma_2$ and suppose $\Psi(G) = C \cap D = 1$. Then

$$|G| = 1 + \sum_{1 \neq C' \leq C} [G : N_G(C')] \cdot \varphi(|C'|) + \sum_{1 \neq D' \leq D} [G : N_G(D')] \cdot \varphi(|D'|)$$

Proof. This is a consequence of the fact that $G = [C]^G \cup [D]^G$ and $[C]^G \cap [D]^G = 1$ by Lemma 5.1.9. □

Now, suppose that $G \in \Gamma_2$ and $Z(G) = 1$. Then the class equation yields

$$|G| = 1 + \sum_{1 \neq C' \leq C} [G : C_G(C')] \cdot \varphi(|C'|) + \sum_{d_i} [G : C_G(d_i)]$$

where the latter sum ranges over representatives d_i of non-trivial conjugacy classes that intersect D. Combining this equation with the one from Lemma 5.2.66 we obtain:

$$\sum_{1 \neq D' \leq D} [G : N_G(D')] \cdot \varphi(|D'|) = \sum_{d_i} [G : C_G(d_i)]$$

Also note that in a group $G \in \Gamma_2$ the number of maximal cyclic subgroups is $|\mathcal{M}(G)| = [G : N_G(C)] + [G : N_G(D)]$. As C is self-normalizing, we certainly have $|\mathcal{M}| \geq [G : C] + 1$. This bound is sharp, as can be seen by considering $G = S_3$.

Lemma 5.2.67. Let $G \in \Gamma_2$ with $C \cap D = 1$. If D is a normal subgroup, then $G \in \Gamma_2^I$.

Proof. Since D is normal, it follows that $|G| = |C| \cdot |D|$ since G/D is cyclic and has order $|C|$ since $C \cap D = 1$. We know that $G = [C]^G \cup D$. Thus

$$|G| \leq 1 + [G : N_G(C)] \cdot (|C| - 1) + (|D| - 1) = |D| \cdot |C|$$

Thus we have actually an equality and thus $C^g \cap C = 1$ if $C^g \neq C$. □

Lemma 5.2.68. Suppose $G \in \Gamma_2$. Then $G = \langle C, D \rangle = \langle C, C^d \rangle = \langle C^{(c^d)}, C^d \rangle$.

Proof. The first claim was already proven in Lemma 5.2.12. Let $d \in D$ be a generator. Now, observe that $C \leq G$ is abnormal, hence $d \in \langle C, C^d \rangle$. Since C and D generate G, it follows that $\langle C, C^d \rangle = G$. For the last claim, let $H = \langle C^{c^d}, C^d \rangle$. Note that $C^{c^d} = C^{d \cdot d^{-2}cd} = (C^d)^{d^{-2}cd}$. Since C^d is abnormal, it follows that $d^{-2}cd \in H$. Also $d^{-1}cd \in H$, then $d^{-1} \in H$ as $d^{-2}cd = d^{-1}d^{-1}cd$. Thus $c \in H$ as well. The claim follows. □

5.2.3.1. Solvability of Groups in Γ_2

We shall prove now that any group $G \in \Gamma_2$ is solvable. We do so by relying on a result proven in Appendix A which ultimately considers the distribution of element orders in finite simple groups. First, we want to highlight a result by Zhang, which he also obtained using the classification of finite simple groups:

Theorem 5.2.69 ([Zha89])**.** There are no self-normalizing cyclic subgroups in non-abelian finite simple groups.

In particular, this implies that there is no finite simple group G with $\gamma(G) = 2$ by Lemma 5.2.2. The following example shows that having a cyclic self-normalizing subgroup is not enough to deduce solvability:

Example 5.2.70. The smallest non-solvable group that contains a cyclic self-normalizing subgroup is the special semilinear group $\Sigma\mathrm{L}_2(8) = \mathrm{SL}_2(8) \rtimes C_3$. It has order 1512 and $\gamma(\Sigma\mathrm{L}_2(8)) = 4$.

In [Bra81] Brandl introduces the problem of covering a finite group G by $\mathrm{Aut}(G)$-conjugates of a proper subgroup, i.e. for which groups G and proper subgroups U is

$$G = \bigcup_{\varphi \in \mathrm{Aut}(G)} \varphi(U)\,?$$

For example, Brandl shows that a finite solvable group that is covered up to automorphism by a nilpotent subgroup is already nilpotent. He also asks whether a finite group G containing a solvable subgroup that covers G up to automorphism is already solvable and provides a reduction theorem to finite simple groups [Bra81, Theorem 6]. The question has since been answered affirmatively by Saxl [Sax88]. We shall use ideas from the reduction theorem of Brandl to prove:

Theorem 5.2.71. Any group $G \in \Gamma_2$ is solvable.

Proof. We prove the claim by induction on the order of G. Let $N \trianglelefteq G$ be a minimal normal subgroup of G. By induction G/N is solvable. Since N is minimal normal, hence characteristically simple, there exists some simple group S such that N is isomorphic to the direct product of n factors of S for some $n \in \mathbb{N}$. Suppose that S is non-abelian. Since N is normal in G, it is covered by two cyclic subgroups up to automorphism, say

$$N = \bigcup_{\varphi \in \mathrm{Aut}(N)} \varphi(C) \cup \varphi(D)$$

where $C, D \leq N$ are cyclic. Let $g \in S$, then there exists some $\varphi \in \mathrm{Aut}(N)$ such that $\varphi((g, \ldots, g)) \in C$ or $\varphi((g, \ldots, g)) \in D$. We know that $\mathrm{Aut}(N) \cong \mathrm{Aut}(S) \wr S_n$ as S is non-abelian simple, so there are automorphisms $\varphi_i \in \mathrm{Aut}(S)$ such that $\varphi((g, \ldots, g)) = (\varphi_1(g), \ldots, \varphi_n(g))$. Let $\pi_i \colon N \to S$ denote the i-th canonical projection. It follows that $\varphi_i(g) \in \pi_i(C)$ or $\varphi_i(g) \in \pi_i(D)$ for all i. In particular S is covered by two cyclic subgroups up to automorphism. By Corollary A.0.3, this is only possible if S is cyclic of order p, which yields a contradiction. Thus G is solvable. $\square$

As a consequence of the solvability of groups in Γ_2 we can record:

Lemma 5.2.72. Suppose $G \in \Gamma_2$ and $F(G)$ is cyclic, then G is metacyclic.

Proof. Note that G acts on $F(G)$ by conjugation and the kernel of this action equals $C_G(F(G)) = F(G)$ since G is solvable. Thus $G/F(G)$ is isomorphic to a subgroup of $\mathrm{Aut}(F(G))$. But the latter is abelian, thus $G/F(G)$ is cyclic. □

5.2.3.2. The Center and Conjugacy Classes

Lemma 5.2.73. Let G be a finite group and let $A \leq G$ be an abelian Carter subgroup. Then $C_G(B) = N_G(B)$ for all $B \leq A$.

Proof. Let $g \in N_G(B)$. Note that $A \leq C_G(B)$ and also $A^g \leq C_G(B^g) = C_G(B)$. Hence $\langle A, A^g\rangle \leq C_G(B)$. Now A and A^g are Carter subgroups of $\langle A, A^g\rangle$, hence by [Vdo08] there exists some $h \in \langle A, A^g\rangle$ such that $A^h = A^g$. This implies that $hg^{-1} \in N_G(A) = A$. Since $h \in C_G(B)$ and $hg^{-1} \in C_G(B)$, also $g \in C_G(B)$. □

Lemma 5.2.74. Let G be a finite group with abelian Carter subgroup A. Then $Z(G) = A_G$.

Proof. Observe that A is maximal nilpotent. If $g \in Z(G)$, then $\langle g, A\rangle$ is abelian, thus $g \in A$. So $Z(G) \leq A$ and since $Z(G)$ is normal in G, it follows that $Z(G) \leq A_G$. By Lemma 5.2.73 we have $G = N_G(A_G) = C_G(A_G)$, so $A_G \leq Z(G)$. □

Lemma 5.2.75. Suppose $G \in \Gamma_2$. For any $g \in G$ we have $C_G(D) \cap C^g \leq Z(G)$. Moreover, $C \cap D \leq Z(G) = C_G = C \cap C^d$.

Proof. By Lemma 5.2.68 we know $G = \langle C, D\rangle = \langle C^g, D\rangle = \langle C, C^d\rangle$, thus $C_G(D) \cap C^g \leq Z(G)$, $C \cap D \leq Z(G)$ and $C \cap C^d \leq Z(G)$. By Lemma 5.2.74 we have $Z(G) = C_G$. Since $Z(G) = C_G \leq C \cap C^d$ the equality follows. □

Corollary 5.2.76. If $G \in \Gamma_2$ and $Z(G) = 1$, then $C_G(D) \subseteq [D]^G$.

Observation 5.2.77. If $G \in \Gamma_2$, then $G/Z(G) \in \Gamma_2$ as well. Suppose $\gamma(G/Z(G)) \leq 1$, then $G/Z(G)$ would be cyclic, thus G abelian. However, this contradicts the fact that $\gamma(G) = 2$. So $\gamma(G/Z(G)) = 2$.

Lemma 5.2.78. If $G \in \Gamma_2$, then $Z(G/Z(G)) = 1$.

Proof. Let $\overline{G} = G/Z(G)$ and $\overline{C} = CZ(G)/Z(G)$. Then $Z(\overline{G}) = \bigcap_{\overline{g}\in\overline{G}} \overline{C}^g$. The preimage of $Z(\overline{G})$ in G is then equal to $\bigcap_{g\in G}(Z(G)C)^g = \bigcap_{g\in G} C^g = Z(G)$, by Lemma 5.2.75. □

Of course, the previous lemma shows once more that any group in Γ_2 is not nilpotent.

Lemma 5.2.79. Let $G \in \Gamma_2$. Then $|Z(G)|$ divides $(|C|, |D|)$.

Proof. Of course, we can assume that $Z(G) \neq 1$. Let $c \in C$ and $d \in D$ be generators. Let $c^k \in Z(G)$ be a generator of $Z(G)$. Note $c^k \cdot d \in C^g$ or $c^k \cdot d \in D^{g'}$. The first case can never happen: if $c^k d = g^{-1}c^m g$ for some $m \in \mathbb{N}$, then $c^k gdg^{-1} = gc^k dg^{-1} = c^m$ since $c^k \in Z(G)$. Thus $gdg^{-1} \in C$, which would imply that G has only a single conjugacy class of maximal cyclic subgroups. Hence it follows that $c^k d \in D^{g'}$. Note that $\operatorname{ord}(c^k d) = \left[\operatorname{ord}(c^k), \operatorname{ord}(d)\right]$ as c^k and d commute. In particular, $|Z(G)| = \operatorname{ord}(c^k)$ divides the order of $c^k d$. But then $|Z(G)|$ divides the order of D. Since $Z(G) \leq C$, the claim follows. □

Lemma 5.2.80. Let $G \in \Gamma_2$ and suppose that the orders of representatives of the two conjugacy classes of maximal cyclic subgroups of $G/Z(G)$ are coprime. Then $(|C|, |D|) = |Z(G)|$.

Proof. Let K, L be representatives of conjugacy classes of maximal cyclic subgroups in $G/Z(G)$. By hypothesis, $(|K|, |L|) = 1$. Let $\pi \colon G \to G/Z(G)$ be the canonical projection. Then, without loss of generality, $\pi(C) = K$ and $\pi(D) = L$. Note that $C \cap Z(G) = Z(G)$, so $|C| = |Z(G)| \cdot |K|$ and $|D| = |Z(G) \cap D| \cdot |L|$. It follows that $(|C|, |D|) \leq |Z(G)|$. Combining this with Lemma 5.2.79 yields the claim. □

Lemma 5.2.81. Let $G \in \Gamma_2$ and suppose that $(|C|, |D|) = 1$. Then any non-cyclic quotient Q of G has two conjugacy classes of maximal cyclic subgroups with coprime orders and $Z(Q) = 1$.

Proof. This is a consequence of Lemma 5.1.6 and Lemma 5.2.79. □

Lemma 5.2.82. Let $G \in \Gamma_2$ and suppose $(|C|, |D|) = 1$. Then $C_G(C') \subseteq [C]^G$ for any non-trivial subgroup $C' \leq C$.

Proof. Suppose $C_G(C') \cap D^g \neq 1$ for some $g \in G$, without loss of generality we can assume that $g = 1$. So there is some non-trivial subgroup $D' \leq D$ such that $D' \leq C_G(C')$. Let $C' = \langle x \rangle$ and $D' = \langle y \rangle$. Since x and y commute, the order of xy is equal to $[|C'|, |D'|] = |C'| \cdot |D'|$, since $|C|$ and $|D|$ were assumed to be coprime. But $xy \in C^g$ or $xy \in D^g$ for some $g \in G$. In particular the order of xy divides the order of C resp. D, which yields a contradiction. □

Observation 5.2.83. Let $G \in \Gamma_2$ with $Z(G) = 1$. Then having $C_G(C') \subseteq [C]^G$ for all $1 \neq C' \leq C$ is equivalent to the statement that $|C|$ and $|D|$ are coprime. Suppose there is a prime p dividing $|C|$ as well as $|D|$. Let $P \leq G$ be a Sylow p-subgroup. Note that P has to intersect $[C]^G$ as well as $[D]^G$ non-trivially as $[C]^G \cap [D]^G \leq Z(G) = 1$ and the orders of C and D are divisible by p. Since $Z(P) \neq 1$, it follows that there exists a non-trivial subgroup $C' \leq C$ with $C_G(C') \cap D^g \neq 1$ for some $g \in G$. The converse of the statement is provided by Lemma 5.2.82.

Remark 5.2.84. We know that $C \cap D \leq Z(G)$ by Lemma 5.2.75. But in general $C \cap D$ is a proper subgroup of $Z(G)$, as we have already seen in Remark 5.2.65. The same example also shows that a group G with $C \cap D = 1$ need not have $(|C|, |D|) = 1$. However, we shall prove at the end of this chapter that $(|C|, |D|) = |Z(G)|$ (cf. Proposition 5.2.149).

Proposition 5.2.85. Let G be a finite group and let C and D be two cyclic subgroups of G such that

$$G = Z(G) \cup [C]^G \cup [D]^G .$$

If $G/Z(G) \in \Gamma_2$, then $G \in \Gamma_2$.

Proof. We can assume without loss of generality that C and D are maximal cyclic such that C maps under $\pi\colon G \to G/Z(G) = \overline{G}$ onto a self-normalizing cyclic subgroup of $\overline{G}$. It then follows that $N_G(C) = Z(G)C = C_G(C)$. Let $H = Z(G)C$ and let $g \in N_G(H)$, then $\overline{g} \in N_{\overline{G}}(\overline{C}) = \overline{C}$. Hence $g \in Z(G)C$. It follows that $N_G(H) = H = C_G(H)$. Hence H is an abelian self-normalizing subgroup, in particular it is a Carter subgroup of G. By Lemma 5.2.74 we have $H_G = Z(G)$. We know that in $\overline{G} = G/Z(G)$, $Z(\overline{G}) = \overline{C}_{\overline{G}}$. Then $\pi^{-1}(\overline{C}_{\overline{G}}) = (Z(G)C)_G = H_G = Z(G)$. It follows that $Z(\overline{G}) = 1$. In particular, it follows that $\overline{C} \cap \overline{D} = 1$.

Now, let $c \in C$ be a generator of C and let $z \in Z(G)$ be arbitrary. Consider the element zc. If $zc \in Z(G)$, then it would follow that $c \in Z(G)$, but then $G/Z(G)$ would be cyclic. If $zc \in [D]^G$, say $zc = g^{-1}d^n g$ for some $d \in D$, $n \in \mathbb{N}$ and $g \in G$, we would have $\overline{c} = \overline{g}^{-1}\overline{d}^n\overline{g}$. However, we have seen that $\overline{C} \cap \overline{D} = 1$, so that this would imply that $\overline{c} = 1$. Again, this is impossible as $G/Z(G)$ is non-cyclic. Hence $zc = g^{-1}c^n g$ for some $n \in \mathbb{N}$ and $g \in G$. Then $g \in N_G(H) = H = Z(G)C$, so that $zc = c^n$, and thus $z \in C$. □

Observation 5.2.86. Suppose G is a finite group and $G = Z(G) \cup [C]^G$ for some cyclic group C. Then $G/Z(G)$ has $CZ(G)/Z(G)$ as a conjugate-dense subgroup. Thus $G/Z(G)$ is cyclic, which implies that G is abelian.

Lemma 5.2.87. If $G \in \Gamma_2$, then the number of conjugacy classes $k(G)$ satisfies the following inequality:

$$1 + |C| \leq k(G) \leq |C| + |D| - 1$$

Proof. Let $x, y \in C \setminus \{1\}$ and suppose $g \in G$ with $g^{-1}xg = y$. In particular, x and y have the same order, and thus $\langle x\rangle = \langle y\rangle \leq C$. Hence $g \in N_G(\langle x\rangle) = C_G(\langle x\rangle)$ by Lemma 5.2.73, which implies that $x = y$. A generator of D together with the elements of C then provide at least $1 + |C|$ conjugacy classes. The upper bound follows easily. □

The bound given in Lemma 5.2.87 is sharp as one observes for the group A_4. It has a cyclic self-normalizing subgroup C of order 3 and $|D| = 2$. Moreover, $k(A_4) = 4$.

5.2.3.3. Direct Products

One might wonder whether direct products of groups in Γ_2 provide further examples of groups with two conjugacy classes of maximal cyclic subgroups. But this happens only in trivial cases:

Proposition 5.2.88. A finite group $G = G_1 \times G_2$ lies in Γ_2 if and only if $G_1, G_2 \in \Gamma_{\leq 2}$ and precisely one of the factors is cyclic and $(|G_1|, |G_2|) = 1$.

Proof. Suppose that neither G_1 nor G_2 is cyclic, i.e. $\gamma(G_1) = \gamma(G_2) = \gamma(G) = 2$. Let $\pi_i\colon G \to G_i$ denote the canonical projections. By Lemma 5.1.6 we know that representatives of the conjugacy classes of maximal cyclic subgroups are of the form $C = \langle c\rangle = \langle (c_1, c_2)\rangle$ and $D = \langle d\rangle = \langle (d_1, d_2)\rangle$, where c_i resp. d_i are generators of the corresponding maximal cyclic subgroups in G_i. We now consider the element (c_1, d_2). Suppose it is conjugate to an element of C, then $(g_1, g_2)^{-1}(c_1, d_2)(g_1, g_2) = (g_1^{-1}c_1g_1, g_2^{-1}d_2g_2) = (c_1^k, c_2^m)$ for some

$k, m \in \mathbb{Z}$. It would follow that $g_2^{-1} d_2 g_2 \in \langle c_2 \rangle$, hence G_2 would have $\gamma(G_2) = 1$. If the element (c_1, d_2) was conjugate to an element of D, it would likewise follow that $\gamma(G_1) = 1$. Hence at least one of G_1 and G_2 has to be cyclic. If both are cyclic, then $G_1 \times G_2$ is abelian and hence it lies in Γ_2 if and only if it is cyclic. And this happens precisely when $|G_1|$ and $|G_2|$ are coprime.

So from now on we assume that G_1 is cyclic and $\gamma(G_2) = 2$. So $G_1 = C_1 = \langle c_1 \rangle$ and we have to choose $c = \langle (c_1, c_2) \rangle$. Note that $N_G(C) = \langle (c_1, 1), (1, c_2) \rangle \cong C_1 \times C_2$ which has to be cyclic, thus C_1 and C_2 have to have coprime orders. Moreover, we have $D = \langle d \rangle$ with the generator of the form $d = (x, d_2)$. Since (c_1, d_2) cannot be conjugate to C (for otherwise $\gamma(G_2) = 1$), we must have that $g^{-1}(c_1, d_2)g = (x, d_2)^k = (x^k, d_2^k)$ for some $g = (g_1, g_2) \in G$ and $k \in \mathbb{Z}$. Since $g_1^{-1} c_1 g_1 = x^k$, i.e. $C_1^{g_1} \leq \langle x \rangle$, it follows that $C_1^{g_1} = \langle x \rangle$. Hence we can choose without loss of generality $x = c_1$, so $d = (c_1, d_2)$.

Now consider the element $(1, d_2)$. An analogous argument as before shows that this element has to lie in a conjugate of D, say $g^{-1}(1, d_2)g = (c_1, d_2)^n = (c_1^n, d_2^n)$. It follows that $|C_1|$ divides n and n is coprime to $|D_2|$. Thus $|C_1|$ and $|D_2|$ are coprime. Since $|C_1|$ and $|C_2|$ are coprime as well, it follows that $|G_1| = |C_1|$ and $|G_2|$ are coprime.

Conversely, let us suppose that $G_1 = \langle c_1 \rangle$ is cyclic, $G_2 \in \Gamma_2$ and $|G_1|$ and $|G_2|$ are coprime. We choose $c = (c_1, c_2)$ and $d = (c_1, d_2)$. Suppose $g = (g_1, g_2) \in G$ with $g_1 = c_1^k$ is an arbitrary element. If $g_2 = \gamma^{-1} c_2^m \gamma$, then $g = (1, \gamma)^{-1}(c_1^k, c_2^m)(1, \gamma)$. But $(c_1^k, c_2^m) \in \langle c \rangle \cong C_1 \times C_2$, since $|C_1|$ and $|C_2|$ are coprime. Similarly, if $g_2 = \gamma^{-1} d_2^m \gamma$, it follows that g is conjugate to (c_1^k, d_2^m). And the latter element lies in $\langle d \rangle \cong C_1 \times D_2$, again since $|C_1|$ and $|D_2|$ are coprime. □

Let $G \in \Gamma_2$. If the orders of $Z(G)$ and $G/Z(G)$ are coprime, then by Schur-Zassenhaus $G \cong Z(G) \times G/Z(G)$. Hence by Proposition 5.2.88 it follows that $G \cong Z(G) \times G/Z(G)$ if and only if the orders of $Z(G)$ and $G/Z(G)$ are coprime.

5.2.3.4. Metacyclic Groups

We have already seen that groups in the class Γ_2^I are not necessarily metacyclic. Nevertheless, understanding the structure of the metacyclic groups lying in Γ_2 will be important later on.

Example 5.2.89. Suppose $G = DC \in \Gamma_2$ with $D \trianglelefteq G$ and $Z(G) = 1$. So $G = D \rtimes_\varphi C$ for some automorphism φ. Note that $dc = d^{-n} c d^n$ for some n. Suppose that $|C| = 2$. Then $1 = (dc)^2 = dcdc = d\varphi(d)$, so $\varphi(d) = d^{-1}$. If $D' \leq D$ is of order 2, then φ fixes D'. Thus $D' \leq C_G(C) = C$, which contradicts the fact that $C \cap D \leq Z(G) = 1$. Hence D is odd, and G is a dihedral group.

Proposition 5.2.90. Let $G \in \Gamma_2$ be metacyclic with $\Psi(G) = C \cap D = 1$. Then $G \in \Gamma_2^I$, and in particular $|D| \equiv 1 \mod |C|$, so $|C|$ and $|D|$ are coprime. Also D is a normal subgroup of G and $G = D \rtimes C$.

Proof. Let $N \leq G$ be a normal cyclic subgroup such that G/N is cyclic. Then $G/N = CN/N$, so $G = CN$. If $N \leq C$, then G would be cyclic. Hence $N \leq D$, and so $N \cap C \leq D \cap C = 1$. Note that $|C| \cdot |D|$ divides $|G| = |C| \cdot |N|$. This implies $|D| = |N|$, so $N = D$. We have $G = D \cup [C]^G$, and thus $|G| = |D| + |[C]^G \setminus \{1\}|$. Note that $|[C]^G \setminus \{1\}| \leq [G : N_G(C)] \cdot (|C|-1) = [G : C] \cdot (|C|-1) = |G| - |D|$. It follows that $|G| \leq |D| + |G| - |D| = |G|$. Hence $|[C]^G \setminus \{1\}| = [G : N_G(C)] \cdot (|C|-1)$, which is only possible if distinct conjugates of C intersect trivially. Together with the fact that D is a normal subgroup, it follows that $G \in \Gamma_2^I$. Since G is a Frobenius group with Frobenius complement C and Frobenius kernel D, we have that $|D| \equiv 1 \mod |C|$. ☐

Lemma 5.2.80 together with the previous proposition implies:

Corollary 5.2.91. For $G \in \Gamma_2$ and G metacyclic, it follows that $|Z(G)| = (|C|, |D|)$.

Corollary 5.2.92. Suppose $G \in \Gamma_2$ is metacyclic and $Z(G) = 1$, then all Sylow subgroups of G are cyclic.

Proof. This is Theorem 5.2.47. ☐

We can read off C resp. D from any decomposition of a metacyclic group:

Corollary 5.2.93. Let $G \in \Gamma_2$ with $Z(G) = 1$ and such that $G = B \rtimes A$ with A and B cyclic. Then $B = D$ and $A = C^g$ for some $g \in G$.

Proof. By Proposition 5.2.90 we know that $G \in \Gamma_2^I$. Since B is cyclic and normal, it follows that $B \leq D$. Moreover, $A \leq C^g$ for some $g \in G$. Otherwise $A \leq D$ and thus G would be cyclic. Note that $|G| = |D| \cdot |C| = |B| \cdot |A|$. The claim follows. ☐

Remark 5.2.94. The recognition property proven in Corollary 5.2.93 fails if we allow $Z(G) \neq 1$. There are metacyclic groups $G \in \Gamma_2$ with normal cyclic $K \trianglelefteq G$ such that G/K is cyclic and such that K is a proper subgroup of D. For example, the group $G = C_3 \rtimes C_4$ has $|D| = 6$ and $|C| = 4$.

Recall that for a finite p-group G one defines for any $i \geq 1$ the following subgroups:

$$\Omega_i(G) = \langle \{g \in G \mid g^{p^i} = 1\} \rangle$$

Furthermore, we abbreviate $\Omega(G) = \Omega_1(G)$.

Proposition 5.2.95. Let $G \in \Gamma_2$ and suppose that $G/Z(G)$ is metacyclic. Then G is metacyclic as well. In fact, all Sylow subgroups of G are cyclic. Moreover, D is a normal subgroup and $Z(G) = C \cap D$.

Proof. We have $G = (Z(G)D)C$ where $N = Z(G)D \trianglelefteq G$. Moreover, by considering the quotient $G/Z(G)$ we obtain that $C_G(D) = Z(G)D$. Observe that $N \cap C = Z(G)$ since N is abelian. Let $P \leq G$ be a Sylow p-subgroup of G. Note that $PZ(G)/Z(G)$ is cyclic as it is a Sylow p-subgroup of $G/Z(G)$. If $PZ(G)/Z(G)$ is contained in $Z(G)C/Z(G) = C/Z(G)$ (up to conjugation), then P is cyclic. Otherwise $PZ(G)/Z(G) \leq DZ(G)/Z(G)$, so $P \leq Z(G)D = N$. In particular, it follows that P is abelian and since P is the Sylow p-subgroup of N, hence characteristic in N, it follows that $P \trianglelefteq G$. If $(p, |Z(G)|) = 1$, then P is actually contained in a conjugate of D, so it is cyclic. So we can assume that p divides $|Z(G)|$. Suppose that P is non-cyclic. Then also $\Omega(P)$ is non-cyclic. Since p divides

$|Z(G)|$ it follows that $\Omega(P)$ intersects C. Since $\Omega(P)$ is non-cyclic, it also intersects D. Let $Z = \Omega(P) \cap C \leq N \cap C = Z(G)$ and $T = \Omega(P) \cap D$. Then

$$\Omega(P) = [Z]^G \cup [T]^G = Z \cup [T]^G .$$

It follows that $p^n = |\Omega(P)| = p + [G : N_G(T)](p-1)$ for some $n \geq 2$. So $[G : N_G(T)]$ is divisible by p. However, $P \leq N_G(T)$, which yields a contradiction. Hence we have shown that any Sylow subgroup of G is cyclic. In particular, any abelian subgroup is cyclic. Thus $Z(G)D = D$, i.e. $Z(G) \leq D$ and D is a normal subgroup. □

A group is called *characteristically metacyclic* if it contains a characteristic cyclic subgroup such that the corresponding quotient is cyclic.

Corollary 5.2.96. A metacyclic group $G \in \Gamma_2$ is characteristically metacyclic.

Proof. Since D is normal subgroup of G and the orders of C and D are distinct, D is a characteristic subgroup of G. □

A finite group G whose Sylow subgroups are cyclic is split metacyclic. So we get:

Corollary 5.2.97. Any metacylic group $G \in \Gamma_2$ splits, so $G = KL$ with K and L cyclic, $K \trianglelefteq G$ and $K \cap L = 1$. Moreover, we have $K \leq D$ and $L \leq C$ (up to conjugation).

Remark 5.2.98. Even though by Corollary 5.2.97 any metacyclic group $G \in \Gamma_2$ splits, it is not necessarily the case that there exists a complement to $D \trianglelefteq G$. Again, the group $G = C_3 \rtimes C_4$ provides an example. It has $|D| = 6$ and $|C| = 4$, but there is no complement to D.

Lemma 5.2.99. Let $G \in \Gamma_2$ and suppose that $N \trianglelefteq G$ is a cyclic subgroup such that G/N is metacyclic. Then G is metacyclic as well.

Proof. Note that $DN/N \leq G/N$ is normal by Proposition 5.2.95. Thus $DN \trianglelefteq G$. If $N \leq D$, then $DN = D \trianglelefteq G$. In particular, G is metacyclic. If $N \leq C$, then $N \leq Z(G)$ since N is normal and the normal core of C equals the center of G. In particular, we know that $G/Z(G)$ is metacyclic being a quotient of G/N. Then G is metacyclic by Proposition 5.2.95. □

Lemma 5.2.100. Let $G \in \Gamma_2$ be metacyclic. Then the number of conjugacy classes that intersect $C \setminus Z(G)$ equals $|C| - |Z(G)|$ and the number of conjugacy classes that intersect $D \setminus Z(G)$ equals

$$|Z(G)| \cdot \frac{|\overline{D}| - 1}{|\overline{C}|} ,$$

where $|\overline{D}| = {}^{|D|}/_{|Z(G)|}$ and $|\overline{C}| = {}^{|C|}/_{|Z(G)|}$. The total number of conjugacy classes in G is given by

$$k(G) = |C| + |Z(G)| \cdot \frac{|\overline{D}| - 1}{|\overline{C}|} = |Z(G)| \cdot \left(|\overline{C}| + \frac{|\overline{D}| - 1}{|\overline{C}|} \right)$$

Proof. We know that $\overline{G} = G/Z(G)$ is a Frobenius group. If $x \in C \setminus Z(G)$, then $C_G(x) = C$ since in the quotient $C_{\overline{G}}(\overline{x}) = \overline{C}$ and $Z(G) = C \cap D$. Similarly, if $y \in D \setminus Z(G)$, then

$C_G(y) = D$. If $x, x' \in C \setminus Z(G)$ and $g^{-1}xg = y$ for some $g \in G$, then $\overline{g}^{-1}\overline{xg} = \overline{y}$ and it follows that $\overline{g} \in N_{\overline{G}}(\langle \overline{x} \rangle) = C_{\overline{G}}(\langle \overline{x} \rangle) = \overline{C}$. Thus $g \in C$, so that $x = y$. Hence there are $|C| - |Z(G)|$ conjugacy classes in G that intersect $C \setminus Z(G)$. Let μ denote the number of conjugacy classes in G that intersect $D \setminus Z(G)$. Then the class equation yields

$$|G| = |Z(G)| + (|C| - |Z(G)|) \cdot [G : C_G(C)] + \mu[G : C_G(D)] .$$

Note that $C_G(C) = C$ and $C_G(D) = D$. We then obtain

$$\mu = |Z(G)| \cdot \frac{[G : C] - 1}{[G : D]} .$$

The claim then follows as $|G| = |Z(G)| \cdot |G/Z(G)| = |Z(G)| \cdot |\overline{C}| \cdot |\overline{D}|$. □

Lemma 5.2.101. Let $G \in \Gamma_2$ be metacyclic with $|D| = p^n$ for some prime p. Then $Z(G) = 1$, so $G \in \Gamma_2^I$.

Proof. First observe that D is the Sylow p-subgroup of G since $|G| = {}^{|C| \cdot |D|}/_{|Z(G)|} = |\overline{C}| \cdot |D|$ where $\overline{D}$ denotes the image of D in $G/Z(G)$. And $|\overline{C}|$ is coprime to $|\overline{D}|$ and thus also coprime to $|D|$ as $|D| = p^n$. Let C'_p denote the subgroup of C whose order is coprime to p. Then C'_p is a complement of D and so $G = DC'_p$. Note that $p \neq 2$ since otherwise $C'_p = 1$ since it has to divide $p - 1$. Note that $Z(G) \leq D$ and since $F(G) = D$, $C'_p \leq \mathrm{Aut}(D)$. By Lemma 5.2.55 C'_p acts fixed point freely on D, which shows that $Z(G) = 1$. □

Lemma 5.2.102. Let G be a finite metacyclic group. Then G contains a non-trivial characteristic cyclic subgroup unless $G \cong C_n \times C_n$ for some $n \in \mathbb{N}$.

Proof. By [Ber08, Theorem A.9.1] a metacyclic group G containing no characteristic subgroup of prime order is isomorphic to a group of the form $C_n \times C_n \times Q_8$ where Q_8 is of odd index in G or it isomorphic to $C_n \times C_n$. In the first case Q_8 is a characteristic Sylow 2-subgroup of G, hence $Z(Q_8)$ would furnish a non-trivial characteristic cyclic subgroup of G. Thus only the latter case remains. □

Lemma 5.2.103. Let $G \in \Gamma_2$ and suppose that $N \leq G$ is a metacyclic subgroup of index 2. Then G is metacyclic.

Proof. Suppose that G is a minimal counterexample. If K was a non-trivial characteristic subgroup of N, then N/K is certainly metacyclic and $N/K \leq G/K \in \Gamma_2$ is of index two. Since G is minimal, it would follow that G/K is metacyclic. But then Lemma 5.2.99 would imply that G is actually metacyclic. Thus we can assume that N does not contain any non-trivial characteristic cyclic subgroups. By Lemma 5.2.102 it then follows that $N \cong C_n \times C_n$ for some $n \geq 2$. By factoring out all Sylow subgroups of N but one we can moreover assume that $n = p$ is a prime number. Note that $N \leq F(G)$ and $F(G)$ is of index two in G since G cannot be nilpotent by Corollary 5.2.3. Thus $N = F(G)$ and so by Lemma 5.2.115 we know that $Z(G) = 1$, hence $N \cap C = 1$. As $G = NC$, it follows that $|C| = 2$. Also $N \subseteq [D]^G$, thus $N = [D \cap N]^C$. Hence

$$p + 1 = \frac{p^2 - 1}{p - 1} = [C : N_C(D \cap N)] .$$

However, this is impossible as C is of order two. □

5.2.3.5. Frobenius Groups

By Theorem 5.2.47 we know that any group $G \in \Gamma_2^I$ is a Frobenius group. We shall now answer the question how Frobenius groups in Γ_2 look like.

Proposition 5.2.104. Let $G \in \Gamma_2$ be a Frobenius group with Frobenius kernel N. Then $G = N \rtimes C$ with C maximal cyclic. Moreover, $N = [D]^G$ and so $|C|$ and $|D|$ are coprime.

Proof. We denote by H a Frobenius complement of G. In particular, H is self-normalizing and $G = N \rtimes H$. Moreover, $|N| \equiv 1 \mod |H|$ and $N = \left(G \setminus [H]^G\right) \cup \{1\}$. Hence $G \setminus N = [H]^G \setminus \{1\}$. Let $C = \langle c \rangle$ be a self-normalizing maximal cyclic subgroup of G. Suppose $C \leq N$. By Thompson's theorem N is nilpotent. But since C is maximal nilpotent it follows that $C = N$. However, N is normal and C is abnormal, which would imply that $G = C$. So we can assume that $C \leq H$, at least up to conjugation. If $D = \langle d \rangle$ was contained in H up to conjugation as well, then a conjugate of an element of $n \in N$ would lie in H. However, since N is normal, this would contradict the fact that $H \cap N = 1$. Hence $D \leq N$.

Let $h \in H$ be an arbitrary non-trivial element. There is some $g \in G$ such that $g^{-1}hg = d^n$ or $g^{-1}hg = c^n$ for some $n \in \mathbb{N}$. In the first case $h \in N$ since $D \leq N$ and $N \trianglelefteq G$. Thus only the latter case can occur. But then $H^g \cap H \neq 1$, which implies that $g \in H$. It follows that $C \leq H$ is a conjugate-dense subgroup of H, hence $C = H$.

Note that $|G| = |N| \cdot |C|$ and $D \leq N$, so $[D]^G \leq N$. Since $G \setminus \{1\} = [D]^G \setminus \{1\} \cup [C]^G \setminus \{1\}$ and $C \cap D \leq Z(G) = 1$, it follows that

$$\begin{aligned} |G| - 1 &= (\left|[D]^G\right| - 1) + [G : N_G(C)] \cdot (|C| - 1) \\ &= \left|[D]^G\right| - 1 + [G : C] \cdot (|C| - 1) \\ &= \left|[D]^G\right| - 1 + |G| - |N| \end{aligned}$$

Hence we have additionally $\left|[D]^G\right| = |N|$ and hence $[D]^G = N$. The last claim follows now since $|N|$ and $|H|$ are coprime. ☐

Remark 5.2.105. There are Frobenius groups $G \in \Gamma_2$ that do not lie in Γ_2^I. For example, there is a unique Frobenius group G of order 84 and this group lies in Γ_2. However, $F(G) \cong C_{14} \times C_2$, so by Theorem 5.2.47 the group does not lie in Γ_2^I since $F(G)$ is not a p-group for a prime p.

Proposition 5.2.106. Let $G \in \Gamma_2$ with $Z(G) = 1$ and suppose that $|C| = p^n$ for some prime p. Then G is a Frobenius group.

Proof. First note that $C = P$ is a Sylow p-subgroup since C is maximal nilpotent. So if p divided $|D|$, then $D \cap C^g \neq 1$, but $Z(G) = 1$. Hence $(|C|, |D|) = 1$. Also, since P is cyclic and $N_G(P) = N_G(C) = C$, it follows that there is a normal p-complement N, so $G = NC$, with $N \trianglelefteq G$ and $N \cap C = 1$. Hence $N \subseteq [D]^G$.

We claim that $D \leq N$. Let $d \in D$ be a generator of D, then $d = gc^k$ for some $g \in N$ and $k \in \mathbb{N}$. Then $d^{p^n} = (gc^k)^{p^n} = \tilde{g}c^{kp^n} = \tilde{g}$ for some $\tilde{g} \in N$ since N is normal in G. Thus

$d^{p^n} \in N$. Since p does not divide the order of D, it follows that $d \in N$. Since $N \subseteq [D]^G$, and $D \leq N$, we have $N = [D]^G$.

So $|G| = \left|[D]^G\right| \cdot |C|$. But also $G \setminus \{1\} = ([C]^G \setminus \{1\}) \dot\cup ([D]^G \setminus \{1\}$, from which it follows that $|G| = |[C]^G| + |[D]^G| - 1$. Putting these two equations together, we obtain that $|[C]^G \setminus \{1\}| = |[D]^G| \cdot (|C| - 1)$. But note that $|[C]^G \setminus \{1\}| \leq [G : N_G(C)] \cdot (|C| - 1) = [G : C] \cdot (|C| - 1) = |[D]^G| \cdot (|C| - 1)$ with equality if and only if distinct conjugates of C intersect trivially. Hence C is a Frobenius complement. $\square$

5.2.3.6. Normal p-Subgroups and Cyclic Quotients

Lemma 5.2.107. Let $G \in \Gamma_2$ with $Z(G) = 1$ and let N be a minimal normal subgroup such that $G = NC$. Then $G \in \Gamma_2^I$, and in particular, G is a Frobenius group.

Proof. Since G is solvable, N is an elementary abelian p-group for some prime p. Note that $N \cap C$ is a normal subgroup of N since N is abelian, also $N \cap C$ is a normal subgroup of C. Thus $N \cap C$ is a normal subgroup of $G = NC$. Since N is minimal normal, $N \cap C = 1$ or $N \cap C = N$. In the latter case $N \leq C$, but this would mean that the normal core of C, which is equal to the center of G, is non-trivial. Hence $N \cap C = 1$, so that $N \subseteq [D]^G$. If K and L are maximal cyclic subgroups of N, there exists $g, h \in G$ such that $g^{-1}Kg \leq D$ and $h^{-1}Lh \leq D$. Since K and L are of the same order, it follows that $g^{-1}Kg = h^{-1}Lh$. But $G = NC$ with N abelian, thus there exists some $c^n \in C$ such that $K = c^{-n}Lc^n$. Hence any two non-trivial cyclic subgroups of N are conjugate via an element of C.

Now let $C' \leq C$ be some subgroup and suppose that $N \cap C_G(C') \neq 1$. Since $C \leq C_G(C')$ it follows by the previous observation that $N \leq C_G(C')$. Hence $G = C_G(C')$. It follows that $C' = 1$.

Let $C' \leq C$ be non-trivial, then $N \cap C_G(C') = 1$. If $gc^k \in C_G(C')$, where $g \in N$, then $g \in C_G(C')$, hence $g = 1$. Thus $C_G(C') = C$. It follows that G is a Frobenius group with Frobenius complement C and Frobenius kernel N. Note that $G = [D]^G \cup [C]^G$ with $[D]^G \cap [C]^G = 1$ and $|[C]^G| = [G : N_G(C)] \cdot (|C|-1)+1 = [G : C](|C|-1)+1 = |G|-[G : C]+1$. Hence

$$\begin{aligned} |G| &= 1 + |[D]^G \setminus \{1\}| + |[C]^G \setminus \{1\}| \\ &= |[D]^G \setminus \{1\}| + |G| - |N| + 1\,. \end{aligned}$$

So $|N| = |[D]^G \setminus \{1\}| + 1 = |[D]^G|$. Since $N \subseteq [D]^G$, it follows that $N = [D]^G$ and so D is of prime order p. Hence $G \in \Gamma_2^I$. $\square$

Lemma 5.2.108. Let $G = (C_{p^k})^n$ be a homocyclic p-group and let $c_i(G)$ be the number of cyclic subgroups of order p^i. Then for $1 \leq i \leq k$ we have

$$c_i(G) = p^{(i-1)(n-1)} \cdot \frac{p^n - 1}{p - 1}\,.$$

Proof. For a finite group, the number of cyclic subgroups of a certain order m is given by the number of elements of order m divided by $\varphi(m)$. In particular, for a finite abelian

p-group G we have

$$c_i(G) = \frac{|\Omega_i(G) \setminus \Omega_{i-1}(G)|}{p^{i-1}(p-1)}.$$

If $G = (C_{p^k})^n$, then $|\Omega_i(G)| = |(C_{p^i})^n| = p^{in}$ and the claim follows. $\square$

Lemma 5.2.109. Let $G \in \Gamma_2$ with $Z(G) = 1$ and suppose that $P \trianglelefteq G$ is an abelian p-group. If G/P is cyclic, then $G \in \Gamma_2^I$ and P is the Sylow p-subgroup. In particular, P is cyclic or elementary abelian.

Proof. First note that $G = PC$ and $P \cap C$ is a normal subgroup of P since P is abelian. Hence $P \cap C$ is a normal subgroup of G. Since $Z(G)$ is the normal core of C and $P \cap C \leq C$, it follows that $P \cap C = 1$. Hence $P \subseteq [D]^G$. Since P is a normal subgroup of G it follows that $\mathrm{Aut}(P)$ acts transitively on the set of cyclic subgroups of P of the same order. By [HBa, Theorem VIII.5.8(b)] we know that P has to be homocyclic. If P is cyclic, then Proposition 5.2.90 applies. So in the following assume that P is non-cyclic.

Let $\exp(P) = p^k$ for some $k \geq 1$. We prove the claim by induction on k. If $\exp(P) = p$, then Lemma 5.2.107 shows the claim. In particular, $|C|$ and $|D|$ are coprime. Suppose $k \geq 2$. Then $\Omega(P) \leq P$ is a characteristic subgroup of P and $\exp(P/\Omega(P)) = p^{k-1}$. Let $\pi\colon G \to G/\Omega(P)$ denote the canonical quotient map. If $G/\Omega(P)$ is cyclic, then $G = \Omega(P)C$ and since $\exp(\Omega(P)) = p$ we are done. Otherwise $G/\Omega(P) \in \Gamma_2$ and $\pi(G) = \pi(P)\pi(C)$. Since $C \cap \Omega(P) \leq C \cap P = 1$, we know that $|C| = |\pi(C)|$. By induction it follows that $|\pi(C)|$ is coprime to p. Hence P is a Sylow p-subgroup of G. If $k \geq 2$, then the number of cyclic subgroups of order p^2 in P is divisible by p by Lemma 5.2.108. Note that C permutes the cyclic subgroups of the same order in P transitively. So if $k \geq 2$, then p would divide $|C|$, a contradiction. $\square$

If we drop the assumption that P is abelian in Lemma 5.2.109, we will need to take into account a certain class of 2-groups that we shall recall here:

Definition 5.2.110 ([HBa, Definition VIII.7.1])**.** A *Suzuki 2-group* G is a non-abelian 2-group which has more than one involution and such that there exists a solvable group of automorphisms of G that permutes the involutions of G transitively.

Suzuki 2-groups have first been classified by Higman in [Hig63]. Let us collect some properties of Suzuki 2-groups, see [HBa, Theorem VIII.7.9]. Let G be a Suzuki 2-group. Then the following assertions hold:

(1) G has nilpotency class 2, exponent 4 and $G' = \Phi(G) = Z(G) = \Omega(Z(G)) = \Omega(G)$ and $|G| = |Z(G)|^2$ or $|G| = |Z(G)|^3$.

(2) The center $Z(G)$ is non-cyclic. If it were cyclic, then $|Z(G)| = 2$ so $|G| = 4$ or $|G| = 8$. But $|G| = 4$ impossible, since G is non-abelian. The non-abelian groups of order 8 are the quaternion group, which contains a unique involution, and the dihedral group D_8 which has $\Omega(D_8) = D_8$.

(3) By [Bry81, Theorem 2] the automorphism group of a Suzuki 2-group is solvable.

Higman identified four different types of Suzuki 2-groups and denoted these by the letters A, B, C, D. The Suzuki 2-groups G with $|G| = |Z(G)|^2$ are of type A, those with $|G| =$

$|Z(G)|^3$ belong to one of the types B, C and D. It will later turn out that only Suzuki 2-groups of type A can appear as the Sylow 2-subgroups of groups in the class Γ_2. Let n be an integer and let $q = 2^n$. Then n is not a power of 2 if and only if there exists a non-trivial automorphism θ of $\mathbb{F}_q$ of odd order. For such an integer n and automorphism θ of odd order Higman defined a Suzuki 2-group $A(n, \theta)$. Higman showed that $A(n, \theta) \cong A(n, \theta')$ if and only if $\theta^{\pm 1} = \theta'$ and any Suzuki 2-group G with $|G| = |Z(G)|^2$ is isomorphic to a group $A(n, \theta)$ for some n and θ.

Note that there are no Suzuki 2-groups of order less than 64 and there are exactly two isomorphism classes of Suzuki 2-groups of order 64. Exactly one of these is of type A.

Lemma 5.2.111. Let $G \in \Gamma_2$ with $Z(G) = 1$ and suppose P is a normal Sylow p-subgroup, such that G/P is cyclic. Then $P = [D]^G$. Moreover, it follows that P is cyclic, elementary abelian or $p = 2$ and P is a Suzuki 2-group. If P is cyclic or elementary abelian, then $G \in \Gamma_2^I$.

Proof. We first claim that if $G = PC \in \Gamma_2$ such that $Z(G) = 1$ and P is a normal Sylow p-subgroup, then $(|C|, |D|) = 1$. We use induction on the nilpotency length of P. If P is abelian, then Lemma 5.2.109 applies. Otherwise $Z(P)$ is a proper subgroup of P and we let $\pi\colon G \to G/Z(P)$ denote the canonical quotient map. Of course, $\pi(G) = \pi(P)\pi(C)$ and $\pi(P)$ is again a normal Sylow p-subgroup of $G/Z(P)$. If $\pi(G)$ is cyclic, then $G = Z(P)C$ and Lemma 5.2.109 applies. So in the following suppose that $G/Z(P)$ is non-cyclic. Also note that $Z(P) \cap C \leq Z(G) = 1$, which implies that $|\pi(C)| = |C|$. By induction it follows that p does not divide $|C|$. Hence $P \cap C = 1$, so $P \subseteq [D]^G$. As $DZ(P)/Z(P)$ is a p-group by induction, it follows that D is a p-group, so that $P = [D]^G$. If P is abelian, then Lemma 5.2.109 directly applies. Otherwise $p = 2$ by a result of Shult [Shu69a; Shu69b]. If P contains a single involution, then this involution is a central element of G as $P \trianglelefteq G$. However this contradicts the fact that $Z(G) = 1$. If P contains more than one involution, then P is a Suzuki 2-group. ☐

5.2.3.7. A Bound on the p-Length

For a finite group G and p a prime, we denote by $O_p(G)$ the largest normal p-subgroup of G. Similarly, $O_{p'}(G)$ denotes the largest normal subgroup of G whose order is coprime to p. The *upper $p'p$ series* is given by alternatingly applying $O_{p'}$ and O_p.

$$1 = P_0 \trianglelefteq N_0 \trianglelefteq P_1 \trianglelefteq N_1 \trianglelefteq \ldots P_n \trianglelefteq N_n \trianglelefteq \ldots$$

Here, $N_i/P_i = O_{p'}(G/P_i)$ and $P_{i+1}/N_i = O_p(G/N_i)$. For the first terms one usually writes $N_0 = O_{p'}(G)$, $P_1 = O_{p'p}(G)$, $N_1 = O_{p'pp'}(G)$, etc. Given a finite solvable group G the length of the upper $p'p$ series is called the *p-length* of G, denoted by $l_p(G)$.

Given the finite field $\mathbb{F}_{p^n}$ we can consider the following transformation group, called the *semilinear group*:

$$\Gamma(p^n) = \{x \mapsto a \cdot \varphi(x) \mid a \in (\mathbb{F}_{p^n})^\times, \varphi \in \mathrm{Aut}(\mathbb{F}_{p^n})\}$$

The group $\Gamma(p^n)$ contains the subgroup of linear transformations $\Gamma_0(p^n) = \{x \mapsto a \cdot \varphi(x) \mid a \in (\mathbb{F}_{p^n})^\times\} \cong \mathbb{F}_{p^n}^\times$ as a normal subgroup. Thus $\Gamma(p^n)$ is metacyclic. Furthermore, we define the *semilinear affine group* as follows:

$$\mathrm{A}\Gamma(p^n) = \{x \mapsto a \cdot \varphi(x) + b \mid a \in (\mathbb{F}_{p^n})^\times, b \in \mathbb{F}_{p^n}, \varphi \in \mathrm{Aut}(\mathbb{F}_{p^n})\}$$

It is not hard to see that $\mathrm{A}\Gamma(p^n)$ is a solvable 2-transitive group.

Theorem 5.2.112 (Huppert's theorem, [HBb, Theorem XII.7.3])**.** Any 2-transitive solvable permutation group of degree p^n is similar to a subgroup of the semilinear affine group $\mathrm{A}\Gamma(p^n)$, except possibly if $p^n \in \{3^2, 5^2, 7^2, 11^2, 23^2, 3^4\}$.

We shall now analyze the exceptional cases appearing in Huppert's theorem:

Lemma 5.2.113. There is no group $G \in \Gamma_2$ such that $F(G)$ is elementary abelian of order $p^n \in \{3^2, 5^2, 7^2, 11^2, 23^2, 3^4\}$ having a non-cyclic complement in G and such that all cyclic subgroups of order p in $F(G)$ are conjugate.

Proof. Let $M \leq G$ be a complement of $F(G)$ in G. As G is solvable, it follows that $C_G(F(G)) = F(G)$. Hence we can consider M as a subgroup of $\mathrm{Aut}(F(G)) \cong \mathrm{GL}_n(p)$. In particular, there are only finitely many groups which satisfy our hypotheses. As all cyclic subgroup of order $F(G)$ are conjugate, M acts irreducibly on $F(G)$, and of course $M \in \Gamma_2$. One can check, for example using GAP (see Appendix B), that there are no such groups with $\gamma(G) = 2$. For example, if $p^n = 3^2$, then M is necessarily isomorphic to $\mathrm{SL}_2(3)$ and the corresponding group G has $\gamma(G) = 4$. $\square$

Theorem 5.2.114. Any group $G \in \Gamma_{\leq 2}$ has p-length at most 1 for any prime p.

Proof. Let G be a counter-example of minimal order. Then any proper quotient of G lies in $\Gamma_{\leq 2}$ and thus has p-length at most 1. By [Rob12, 9.3.8] it follows that $G = NH$ for $O_{p'p}(G) = F(G) = N$ an elementary abelian p-group of order p^n which is the unique minimal normal subgroup of G and H a complement of N, which is also a maximal subgroup. Moreover, we know that $C_G(N) = N$. Suppose $Z(G) \neq 1$. Then $N \leq Z(G) \leq C$, which would imply that $N = C_G(N) = N_G(N) = G$. Thus $Z(G) = 1$.

Suppose that N intersects C as well as D non-trivially. Then any element of order p in H will be conjugate to N, so it will lie in N as N is a normal subgroup. But $H \cap N = 1$, thus H is a p'-subgroup. However, this would imply that G has p-length equal to 1.

Hence we can assume that $N \subseteq [C]^G$ or $N \subseteq [D]^G$. In particular, all subgroups of order p in N are conjugate. We can view H as a subgroup of $\mathrm{GL}_n(p)$ acting naturally on the $\mathbb{F}_p$-vector space $F(G)$. Let $\hat{H} = H \cdot Z(\mathrm{GL}_n(p))$ and consider $\hat{G} = F(G)\hat{H}$. Then $\hat{H}$ is a maximal subgroup of $\hat{G}$ and $\hat{G}$ is a solvable 2-transitive primitive permutation group. By Theorem 5.2.112 and Lemma 5.2.113 it follows that $\hat{H}$ and thus also H is metacyclic. We get that $G = NH = NDC$ where $K = ND \trianglelefteq G$ is a normal subgroup.

Suppose $N \subseteq [C]^G$, let $Z = N \cap C$ and so $N = [Z]^G = [Z]^D$ as N is abelian and $G = NDC$. By Lemma 5.2.73 $N_D(Z) = C_D(Z)$ and certainly $C_D(Z) = C_D(Z^d)$ for all $d \in D$. Since $N = [Z]^D$ we obtain that $C_D(Z) = C_D(N)$ and $C_D(N) = C_G(N) \cap D = N \cap D = 1$. The last equality follows from the fact that $Z(G) = 1$. Hence $N_D(Z) = 1$ and so we obtain ${}^{p^n-1}/_{p-1} = [D : N_D(Z)] = |D|$. But then $|D|$ would be coprime to p and this would imply that all cyclic subgroups of order p would be conjugate, so the p-length of G would be 1.

If $N \subseteq [D]^G$, then $N \cap D \leq Z(K)$ and it follows that $N \leq Z(K)$ since K is normal and $N = [N \cap D]^G$. As K is abelian and $C_G(N) = N$ it follows that $D \leq N$, i.e. $K = N$. But then G/N is cyclic. However, Lemma 5.2.109 would then imply that N is the Sylow p-subgroup, again showing that G has p-length equal to 1. □

5.2.3.8. The Fitting Subgroup

Lemma 5.2.115. Let $G \in \Gamma_2$ with $F(G) = P$ an abelian Sylow p-subgroup. Then $Z(G) = 1$.

Proof. As P is abelian, $\Omega(P) = \{g \in P \mid g^p = 1\}$ is an elementary abelian p-group. Suppose $Z(G) \neq 1$. Since $Z(G)$ is cyclic, $Z = C \cap \Omega(P) = Z(G) \cap \Omega(P) \neq 1$. Let $T = D \cap \Omega(P)$. Then $\Omega(P) = Z \cup [T]^G$. Let $|\Omega(P)| = p^n$. Suppose for the moment that $T \neq 1$ and $Z \cap T = 1$. Then $n \geq 2$ and

$$\frac{p^n - 1}{p - 1} = 1 + [G : N_G(T)] \,.$$

Since $P \leq C_G(T) \leq N_G(T)$ we arrive at a contradiction since the equation implies that $[G : N_G(T)]$ is divisible by p. If $T = 1$ or $Z = T$, then $\Omega(P) = Z$ is cyclic. Thus also P is cyclic. Since $F(G)$ is cyclic, G is metacyclic by Lemma 5.2.72. But then Lemma 5.2.101 implies that $Z(G) = 1$ in this case as well. □

Similarly we obtain:

Lemma 5.2.116. Let $G \in \Gamma_2$ and $F(G) = P$ be the Sylow p-subgroup of G. Then $Z(G) = 1$ or $Z(P)$ is cyclic.

Proof. Note that $Z(G) \leq F(G)$, hence $Z(G) \leq Z(P)$. Let $N = \Omega(Z(P))$. Suppose $Z(G) \neq 1$. Then $Z = N \cap Z(G) \neq 1$. If N was non-cyclic, then $T = N \cap D \neq 1$ and $N = Z \cup [T]^G$. If N is of rank $n \geq 2$, then ${}^{p^n-1}/_{p-1} = 1 + [G : N_G(T)]$. So it would follow that $[G : N_G(T)]$ is divisible by p, which is impossible as $P \leq N_G(T)$. Thus N must be cyclic and so also $Z(P)$ is cyclic. □

Lemma 5.2.117. Let $G \in \Gamma_2$ and suppose that $F(G) = P$ is an elementary abelian Sylow p-subgroup. Then $F(G)$ is minimal normal.

Proof. If P only intersects C (or only intersects D) then the claim follows easily. So suppose that P intersects C as well as D, so $Z = P \cap C \neq 1$ and $T = P \cap D \neq 1$. Let $H \leq P$ be a non-trivial normal subgroup of G that is contained in H. If H intersects C and D, then again $H = P$. So assume that it either intersects C or D, say D. Then $H = [H \cap D]^G$. Note that $H \cap D = P \cap D = T$. We also know that the number of non-trivial cyclic subgroups in P equals $[G : N_G(Z)] + [G : N_G(T)]$. Let $|P| = p^n$ and $|H| = p^m$ for $n \geq 2$ and $1 \leq m < n$. Then

$$\frac{p^n - 1}{p - 1} = [G : N_G(Z)] + [G : N_G(T)] = [G : N_G(Z)] + \frac{p^m - 1}{p - 1}$$

From this it follows that $[G : N_G(Z)]$ is divisible by p. However, since P is abelian we know that $P \leq C_G(Z) \leq N_G(Z)$. Since P is the Sylow p-subgroup of G we know that $[G : N_G(Z)]$ is coprime to p, a contradiction. □

Lemma 5.2.118. Let $G \in \Gamma_2$ such that $F(G)$ is the Sylow p-subgroup of G with $|F(G)| = p^n \in \{2^6, 3^4, 3^6, 7^2, 7^4, 13^2, 17^2, 19^2, 23^2, 29^2, 31^2, 47^2\} \cup \{3^4, 5^4, 7^4, 11^4, 23^4, 3^8\}$. Then $G/F(G)$ is cyclic.

Proof. Let M be a complement of $P = F(G)$ in G, so $G = PM$. Then as in the proof of Lemma 5.2.113 one sees that the complement M is isomorphic to a subgroup of $\mathrm{GL}_n(p)$ and so there are only finitely many groups G that we need to consider. To further restrict the groups to consider, we see that by Lemma 5.2.115 we have $Z(G) = 1$ and the complement M has to be an irreducible solvable subgroup of $\mathrm{GL}_n(p)$ by Lemma 5.2.117 which has order coprime to p. For example, if $p^n = 7^2$, then up to isomorphism the possible non-cyclic complements are $S_3, C_3 \rtimes C_4$ and $\mathrm{SL}_2(3)$, none of which yield a group G with $\gamma(G) = 2$. The other cases can similarly be dealt with, for example using GAP, see also Appendix B. $\square$

Theorem 5.2.119. Let $G \in \Gamma_2$ and suppose that $F(G) = P$ an elementary abelian Sylow p-subgroup. Then $G/F(G)$ is metacyclic.

Proof. First note that by Lemma 5.2.115 we know that $Z(G) = 1$. By Lemma 5.2.117 $F(G)$ is minimal normal and thus $\Phi(G) = 1$ as $\Phi(G)$ is a proper subgroup of $F(G)$. Hence there exists some maximal subgroup M such that $F(G)$ is not contained in M. Then $G = F(G)M$. Note that $F(G) \cap M \trianglelefteq F(G)$ as $F(G)$ is abelian. Thus $F(G) \cap M$ is a normal subgroup of G contained in $F(G)$. By the minimality of $F(G)$ and since M does not contain $F(G)$, it follows that $F(G) \cap M = 1$, so M is a complement. Moreover, as $C_G(F(G)) = F(G)$, we can think of M as embedded in $\mathrm{Aut}(F(G)) \cong \mathrm{GL}_n(p)$ where n is such that $|F(G)| = p^n$. Let $\hat{M} = M \cdot Z(\mathrm{GL}_n(p))$ and consider $\hat{G} = F(G)\hat{M}$. Then $\hat{M}$ is a maximal subgroup of $\hat{G}$ and $\hat{G}$ is a solvable primitive permutation group of rank 3. In [Fou69, Theorem 1.1] these were classifed and we have three cases to consider:

(1) G is a subgroup of the affine semilinear group, and thus M is metacyclic.

(2) The group G belongs to a finite set of exceptional groups where

$$p^n \in \{2^6, 3^4, 3^6, 7^2, 7^4, 13^2, 17^2, 19^2, 23^2, 29^2, 31^2, 47^2\}\,.$$

These were handled in Lemma 5.2.118.

(3) In the last case G is imprimitive and G acts on the socle $V = V_1 \oplus V_2$, where V_1 and V_2 are minimal imprimitivity subspaces. Then $\hat{M}$ contains an index 2 subgroup that acts transitivley on the non-zero elements of V_1 and hence is determined by Theorem 5.2.112. As $\dim V_1 = \dim V_2$, the degrees of the exceptional cases in Huppert's theorem are squared, so $p^n \in \{3^4, 5^4, 7^4, 11^4, 23^4, 3^8\}$. By Lemma 5.2.118 the complement M has to be cyclic.

In the non-exceptional case of Huppert's theorem we have that $\hat{M}|_{V_1}$ is metacyclic and of index two in $\hat{M}$. Note that $Z(\hat{M}) = Z(M) \cdot Z$ where $Z = Z(\mathrm{GL}_n(p))$. Thus $\hat{M}/Z(\hat{M}) \cong M/Z(M)$ and the latter group lies in $\Gamma_{\leq 2}$ as M is a quotient of G. The image of the group $\hat{M}|_{V_1}$ under the canonical map $\hat{M}|_{V_1} \hookrightarrow \hat{M} \to \hat{M}/Z(\hat{M})$ is then of index 1 or 2. As the image of a metacyclic group is metacyclic and $\hat{M}/Z(\hat{M}) \in \Gamma_{\leq 2}$ it follows by Lemma 5.2.103 that $\hat{M}/Z(\hat{M})$ is metacyclic. Thus $M/Z(M)$ is metacyclic. Since $M \in \Gamma_{\leq 2}$, it follows by Proposition 5.2.95 that M itself is metacyclic.

□

Lemma 5.2.120. Let $G \in \Gamma_2$ with $F(G)$ an elementary abelian Sylow p-subgroup. Suppose that $G/F(G)$ is metacyclic, but not cyclic. Then $F(G) \subseteq [C]^G$ and D is a self-normalizing subgroup of $F(G)D$. Moreover, if $|F(G)| = p^n$, then $|D| = {}^{p^n-1}/_{p-1}$ and $N_D(Z) = C_D(Z) = 1$, where $Z = F(G) \cap C$. So D acts fixed point freely on $F(G)$ and $(n, p-1) = 1$.

Proof. First note that by Lemma 5.2.115 we have that $Z(G) = 1$. We know that $DF(G)/F(G)$ is normal in $G/F(G)$ by Proposition 5.2.95, so $N = F(G)D \trianglelefteq G$. Suppose that $F(G) = P$ intersects C as well as D. First observe that $P \cap D \leq Z(N)$, so $[P \cap D]^G \subseteq Z(N)$ since $Z(N)$ is normal in G. In particular, we have $H = \langle [P \cap D]^G \rangle \leq Z(N) \cap P$, and H is a normal subgroup of G. We also know that $G = NC$. Note that $Z(N) \cap C \leq Z(G) = 1$, hence $Z(N) \subseteq [D]^G$. Since $H \leq Z(N) \subseteq [D]^G$, it follows that $H = [D \cap P]^G$. Thus H is a proper non-trivial normal subgroup contained in P. But this contradicts the fact that P is minimal normal by Lemma 5.2.117. Hence we know that $P \subseteq [D]^G$ or $P \subseteq [C]^G$. Suppose $P \subseteq [D]^G$, then $P \leq Z(N)$ so that N is abelian. Note that $C_G(F(G)) = F(G)$, hence $D \leq F(G) = P$. In particular, it would follow that $G/F(G) = G/P$ is cyclic, which we excluded in our hypotheses. Hence $P \subseteq [C]^G$.

Let $Z = P \cap C$. Then $P = [Z]^G = [Z]^D$ since $G = F(G)DC$ and $F(G)$ is abelian. It follows that ${}^{p^n-1}/_{p-1} = [D : N_D(Z)] = [D : C_D(Z)]$ since $N_G(Z) = C_G(Z)$. Now observe that $C_D(Z) = C_D(Z^x)$ for any $x \in D$. Thus $C_D(Z) = C_D(P) = D \cap C_G(P) = D \cap P = 1$. Using that $C_D(Z) = 1$ it also follows that $C_G(Z) = C_G(F(G) \cap C) = F(G)C$. Moreover, we know that we can view $D \leq \operatorname{Aut}(P)$ and since the order of D equals ${}^{p^n-1}/_{p-1}$ it acts as a Singer cyclic subgroup. Then by Observation 5.2.60 it follows that D is a self-normalizing subgroup of PD. As $PD \trianglelefteq G$ any G-conjugate of D lies in PD. Since D is a Carter subgroup, it then follows that for each $g \in G$ there exists some $g' \in PD$ such that $D^g = D^{g'}$. This implies that $N = PD \in \Gamma_2^I$. Then by Lemma 5.2.62 it follows that $(n, p-1) = 1$. □

Let $D \leq \mathbb{F}_{p^n}^\times$ be the cyclic subgroup of order ${}^{p^n-1}/_{p-1}$. We define $\tilde{\Gamma}(p^n) = \{x \mapsto a \cdot \varphi(x) \mid a \in D, \varphi \in \operatorname{Aut}(\mathbb{F}_{p^n})\} \leq \Gamma(p^n)$ and call it the *reduced semilinear* group. Let us record the following curious fact:

Lemma 5.2.121. Suppose $(p-1, n) = 1$. Then the reduced semilinear group $\tilde{\Gamma}(p^n)$ is isomorphic to $\Gamma(p^n)/Z(\Gamma(p^n))$.

Proof. Let $G = \Gamma(p^n)$ and $H = \tilde{\Gamma}(p^n)$. Observe that $Z(G) = \mathbb{F}_p^\times$ and the composition $H \to G \to G/Z(G)$ of the natural inclusion and projection is a homomorphism with kernel $H \cap Z(G) = D \cap F_p^\times = 1$ since $(p-1, n) = 1$. As the groups H and $G/Z(G)$ have the same order, the claim follows. □

I learned a proof of the following from Jyrki Lahtonen.

Lemma 5.2.122. Let $\mathbb{F}_{p^n}$ be the finite field of order p^n and suppose τ is a generator of the (cyclic) Galois group of the field extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ Let $V = \{y - \tau(y) \mid y \in \mathbb{F}_{p^n}\}$. Then for any $x \in \mathbb{F}_{p^n}$ the set $(V + x) \cap \mathbb{F}_p$ is non-empty if and only if $(p, n) = 1$. Moreover, if $(p, n) = 1$, then $|(V + x) \cap \mathbb{F}_p| = 1$.

Proof. Note that V is a vector space over $\mathbb{F}_p$ of dimension $n-1$ as the canonical linear map $\mathbb{F}_{p^n} \to V, y \mapsto y - \tau(y)$ has kernel $\mathbb{F}_p$.

Consider the trace map $\mathrm{tr}\colon \mathbb{F}_{p^n} \to \mathbb{F}_p, x \mapsto x + x^p + \ldots + x^{p^{n-1}}$. Note that $V \subseteq \ker(\mathrm{tr})$ since $\mathrm{tr}(x^p) = \mathrm{tr}(x)$. Moreover $\ker(\mathrm{tr})$ contains at most p^{n-1} elements as it is given by a polynomial of degree p^{n-1}. Thus $V = \ker(\mathrm{tr})$. Also note that if $x \in \mathbb{F}_p$, then $\mathrm{tr}(x) = nx$. So if p divides n, then $\mathrm{tr}(x) = 0$ for all $x \in \mathbb{F}_p$, thus $\mathbb{F}_p \subseteq V$. If $(p, n) = 1$, then $\mathbb{F}_p \cap V = 0$, so $\mathbb{F}_{p^n} = V \oplus \mathbb{F}_p$ as $\dim(V) = n - 1$.

If p divides n, we can pick $x \in \mathbb{F}_{p^n} \setminus V$, which will then satisfy $(V + x) \cap \mathbb{F}_p \subseteq (V + x) \cap V = \emptyset$. If $(p, n) = 1$, the decomposition $\mathbb{F}_{p^n} = V \oplus \mathbb{F}_p$ implies that any coset of V intersects $\mathbb{F}_p$ in a single element. □

Proposition 5.2.123. Let p and n be prime numbers such that $(p - 1, n) = 1$. Then the reduced semilinear group $G = \tilde{\Gamma}(p^n)$ lies in Γ_2^I.

Proof. Let D be the subgroup of $\mathbb{F}_{p^n}^\times$ of order $p^n-1/p-1$ and $C = C_n$. We will show that these subgroups are representatives of the conjugacy classes of the maximal cyclic subgroups. The group law is given by $(a, \alpha) \cdot (b, \beta) = (a \cdot \alpha(b), \alpha \circ \beta)$. Here we view C_n as the group of automorphisms of the field $\mathbb{F}_{p^n}$. Note that $(a, \alpha)^{-1} = (\alpha^{-1}(a^{-1}), \alpha^{-1})$. Let $(b, \beta) \in G$ be an arbitrary element. If $\beta = \mathrm{id}$, then the element is contained in D. So suppose $\beta \neq \mathrm{id}$. In general, conjugation is given by the following formula

$$(a, \alpha)(b, \beta)(a, \alpha)^{-1} = (a\alpha(b)\beta(a^{-1}), \beta)$$

Let $\tau(a) = a^p$ be the Frobenius automorphism which is the generator of C_n. Then $\beta = \tau^k$ for some k. If $(n, k) \neq 1$, then n would divide k has n is prime. This would imply that $\beta = \mathrm{id}$, so $\beta(a) = a^{p^k}$. As we assumed that β is non-trivial, it follows that $(n, k) = 1$. By Lemma A.0.9 it then follows that $\left(p^k - 1, p^n-1/p-1\right) = (p - 1, n) = 1$. Thus for any $b \in D$ there exists some $a \in D$ such that $b = a^{p^k - 1} = \beta(a)a^{-1}$. By the formula above

$$(a, \mathrm{id}) \cdot (b, \beta) \cdot (a, \mathrm{id})^{-1} = (ba\beta(a)^{-1}, \beta) = (1, \beta) \in C_n$$

Thus $G \in \Gamma_2$. As the maximal cyclic subgroups D and C_n intersect trivially, it also follows that $Z(G) = 1$, thus $G \in \Gamma_2^I$ as G is metacyclic. □

Lemma 5.2.124. Let $G = \mathbb{F}_{p^n} \rtimes H$ with $H = \tilde{\Gamma}(p^n)$ reduced semilinear. Assume that n is a prime different from p and that $(n, p - 1) = 1$. Then $G \in \Gamma_2$.

Proof. We write $P = \mathbb{F}_{p^n}$. Multiplication of elements in the group G is given as follows

$$(x, a, \alpha) \cdot (y, b, \beta) = (x + a \cdot \alpha(y), a \cdot \alpha(b), \alpha \circ \beta)$$

We let $D \leq H$ be the cyclic subgroup of order $p^n-1/p-1$ that is contained in $\mathbb{F}_{p^n}^\times$. And we set $C = \langle (1, 1, \tau) \rangle$ with τ the Frobenius automorphism. Observe that $(1, 1, \tau)^k = (k, 1, \tau^k)$. As $(p, n) = 1$ it follows that C has order pn.

By Proposition 5.2.123 H and by Lemma 5.2.62 PD both lie in Γ_2. We are thus left to show that any element $(x, 1, \alpha)$ with $\alpha \neq \mathrm{id}$ is conjugate to an element of C. Observe that

$$(y, b, \mathrm{id}) \cdot (x, 1, \alpha) \cdot (y, b, \mathrm{id})^{-1} = (b \cdot x + y - b\alpha(b^{-1})\alpha(y), b\alpha(b^{-1}), \alpha)$$

We can now choose $b = 1$. Then we are left to show that $x + y - \alpha(y) \in \mathbb{F}_p$ for some $y \in \mathbb{F}_{p^n}$. But this is the case by Lemma 5.2.122 since n is prime and thus α is a generator of C_n. □

Lemma 5.2.125. Let $H \leq \mathbb{F}_{p^n}^\times \rtimes C_n = G$ where $D \leq \mathbb{F}_{p^n}^\times$ of order ${p^n-1}/{p-1}$ is contained in H. Suppose that $(n, p-1) = 1$ and $D \trianglelefteq H$ is maximal cyclic. Then $H \leq D \rtimes C_n = \tilde{\Gamma}(p^n)$.

Proof. First note that $Z(G) = \mathbb{F}_p^\times$. Since $D \leq \mathbb{F}_{p^n}^\times$ we know that $D(H \cap Z(G)) \leq \mathbb{F}_{p^n}^\times$. Note that $D \cap (H \cap Z(G)) = 1$ as $D \cap Z(G) = 1$ because $(|D|, |Z(G)|) = 1$. As D is maximal cyclic and contained in the cyclic subgroup $D(H \cap Z(G))$ it follows that $H \cap Z(G) = 1$. Now let $h = (z \cdot x, \alpha) \in H \leq G$ where $z \in Z(G)$ and $x \in D$. Recall that multiplication of group elements is given by $(a, \alpha) \cdot (b, \beta) = (a \cdot \alpha(b), \alpha \circ \beta)$ in $\mathbb{F}_{p^n}^\times \rtimes C_n$. Then $h^n = (z^n \cdot x \cdot \alpha(x) \cdot \ldots \alpha^{n-1}(x), \alpha^n) = (z^n \cdot x \cdot \alpha(x) \cdot \ldots \alpha^{n-1}(x), \mathrm{id})$ since $\alpha(z) = z$ because $z \in \mathbb{F}_p^\times$. Let $x' = x \cdot \alpha(x) \cdot \ldots \alpha^{n-1}(x) \in D$ and let $m = |D| = {p^n-1}/{p-1}$. Then $(z^n \cdot x', \mathrm{id})^m = (z^{nm}, \mathrm{id}) = h^{nm} \in H$. As $H \cap Z(G) = 1$ it follows that $z^{nm} = 1$. Now observe that $(p-1, nm) = 1$ since $(p-1, n) = 1 = (p-1, m)$, so $z = 1$. The claim follows. □

We now establish a converse of Lemma 5.2.124.

Proposition 5.2.126. Let $G \in \Gamma_2$ with $F(G) = P$ an elementary abelian Sylow p-subgroup such that $G/F(G) \in \Gamma_2$. Then G is isomorphic to the group described in Lemma 5.2.124. In particular, the rank n of P is a prime number different from p, $|C| = p \cdot n$ and $|D| = {p^n-1}/{p-1}$ and $(n, p-1) = 1$.

Proof. By Lemma 5.2.120 and another application of Theorem 5.2.112 it follows that G is isomorphic to a subgroup of $\mathbb{F}_{p^n} \rtimes (\mathbb{F}_{p^n}^\times \rtimes C_n)$. By H we denote the complement of $F(G) = P$, which then lies in $\mathbb{F}_{p^n}^\times \rtimes C_n$. First let us suppose that $Z(H) \neq 1$. Then the maximal cyclic C is generated by an element (x, a, α) where $a \in Z(H) \setminus \{1\}$ and without loss of generality we can assume that $x \in \mathbb{F}_p$. We then obtain

$$(x, a, \alpha)^k = \left(x \cdot (1 + a + a^2 + \ldots + a^{k-1}), a^k, \alpha^k\right) = \left(x \cdot \frac{a^k - 1}{a - 1}, a^k, \alpha^k\right).$$

But then it would follow that $C \cap P = 1$ since if $a^k = 1$, then also the first component of $(x, a, \alpha)^k$ would be trivial. However $C \cap P$ is non-trivial, hence $Z(H) = 1$. By Lemma 5.2.125 H is of the form $L \rtimes C_k$ with $L \leq \mathbb{F}_{p^n}^\times$ of order ${p^n-1}/{p-1}$ and k a divisor of n. Suppose $C_k = \langle \sigma \rangle$ is a proper subgroup of the Galois group C_n. Then $\mathrm{Fix}(C_k) = \mathbb{F}_{p^m} \subsetneq \mathbb{F}_{p^n}$ where $m = {n}/{k}$. But then $Z(H)$ would contain $L \cap \mathbb{F}_{p^m}^\times$ which is cyclic of order $({p^n-1}/{p-1}, p^m - 1) = {p^m-1}/{p-1} \cdot ({n}/{m}, p-1)$ by Lemma A.0.9. So if $m > 1$, then the center $Z(H)$ would be non-trivial. We conclude that $H = L \rtimes C_n$. We can thus assume that the generator of C is of the form $(x, 1, \tau)$ with τ a generator of the Galois group.

We know that $H \in \Gamma_2$ is metacyclic with $Z(H) = 1$. Thus H is a Frobenius group by Proposition 5.2.90 with Frobenius complement $\overline{C} = \langle (1, \tau) \rangle$. In particular, $C_H(\overline{C}') = \overline{C}$ for any non-trivial subgroup $\overline{C}' \leq \overline{C}$. If n is not prime, there exists some proper non-trivial subgroup $\overline{C'} = \langle 1, \sigma \rangle$ of $\overline{C}$ and as above we see that $\mathrm{Fix}(\langle \sigma \rangle)$ intersects non-trivially with the subgroup of $\mathbb{F}_{p^n}^\times$ of order ${p^n-1}/{p-1}$. Let a be a non-trivial element of this intersection, then $(a, 1)(1, \sigma)(a, 1)^{-1} = (a\sigma(a)^{-1}, \sigma) = (1, \sigma)$ and $(a, 1)$ is not contained in $\overline{C}$. It follows that n is a prime number.

If $(n, p) \neq 1$, then $n = p$ as they are both primes. But then $(x, 1, \tau)^p = (p \cdot x, 1, \mathrm{id}) = (0, 1, \mathrm{id})$, so C would have order p, which yields a contradiction. □

Remark 5.2.127. The orders of the maximal cyclic subgroups C and D are coprime in the group described in Proposition 5.2.126. Namely, let $q = p-1$ and write $p^n - 1 = ((p-1)+1)^n - 1 = \sum_{k=1}^{n} \binom{n}{k} q^k$. As n is a prime number, the binomial coefficients $\binom{n}{k}$ are divisible by n if $1 \leq k < n$. Hence we obtain

$$\frac{p^n - 1}{p-1} \equiv q^{n-1} \mod n\,.$$

But we also know that $(n, p-1) = (n, q) = 1$. Thus we see that $(|C|, |D|) = (np, {}^{p^n-1}/_{p-1}) = (n, {}^{p^n-1}/_{p-1}) = 1$.

Proposition 5.2.128. Let $G \in \Gamma_2$ and let $F(G) = P$ be the Sylow p-subgroup. Assume that $G/F(G) \in \Gamma_2$. Then $P \subseteq [C]^G$ and $Z(G) = 1$. Moreover, P is elementary abelian or $p = 2$ and P is a Suzuki 2-group.

Proof. We will additionally prove that D is a self-normalizing subgroup of PD and that $|D|$ is coprime to p. We prove the claims by induction on the order of G.

If $\Phi(P) = 1$, then the claims follow from Lemma 5.2.120. So suppose $\Phi(P) \neq 1$, then we have $Z(P) \cap \Phi(P) \neq 1$ and we can choose $N \trianglelefteq G$ a minimal normal subgroup contained in $Z(P) \cap \Phi(P)$. We let $Z = N \cap C$ and $T = N \cap D$.

Suppose first that $Z(G) \neq 1$. Then $Z(P)$ is cyclic by Lemma 5.2.116. We first claim that $N \leq C$. If $Z(P) \leq C$ there is nothing to show, so suppose $Z(P) \leq D$, hence $N = T$ is a normal subgroup of G. Thus we obtain a monomorphism $C/C_C(T) \hookrightarrow \mathrm{Aut}(T)$ where the latter group is of order $p-1$. Note that by Proposition 5.2.126 $|C|$ and $p-1$ are coprime. Hence C centralizes T. Thus $N = T \leq Z(G) \leq C$ also in this case. Suppose $x \in P$ is an arbitrary element conjugate to an element of D. Then in G/N we have xN conjugate to an element of DN/N. But by induction $Z(G/N) = 1$ and PN/N is a contained in the union of conjugates of CN/N. Since CN/N and DN/N intersect trivially we obtain that $x \in N \leq C$. Hence $P \subseteq [C]^G$. Note that P cannot be abelian by Lemma 5.2.115. By [Shu69a] we then have $p = 2$ and $P \cong Q_8$ or P is a Suzuki 2-group. The first case is impossible since we would obtain a group $G/\Phi(P) \in \Gamma_2$ with Fitting subgroup $P/\Phi(P) \cong C_2 \times C_2$ whose quotient by $P/\Phi(P)$ is non-cyclic. Actually, one sees by direct inspection that there is a unique group $H \in \Gamma_2$ up to isomorphism with $F(H) \cong C_2 \times C_2$, namely A_4. Also P being a Suzuki 2-group is impossible, since a Suzuki 2-group has non-cyclic center.

So for the rest of the proof we can assume that $Z(G) = 1$. We also know that $G/F(G)$ is metacyclic by Theorem 5.2.119. Let $K = PD \trianglelefteq G$. Since P is normal in G, also $Z(P)$ is normal in G. Suppose that $T \neq 1$. We know that $T \leq N \leq Z(P)$ and $T \leq D$, hence $T \leq Z(PD) = Z(K)$. Thus $\langle [T]^G \rangle \leq Z(K)$ Since $Z(G) = 1$, we have $Z(K) \cap C = 1$, i.e. $Z(K) \subseteq [D]^G$. This implies that $[T]^G = \langle [T]^G \rangle$. Since N is minimal normal, it follows that $N = [T]^G$.

We write $\pi\colon K \to K/N$. We can write $D = D_p \cdot D_{p'}$ where $|D_p| = p$ and $D_{p'}$ is of order coprime to p. By the inductive hypothesis, DN/N is a self-normalizing subgroup of $PD/N = K/N$. Hence, for any $g \in G$ there exists some $k \in K$ such that $\pi(D^g) = \pi(D^k)$. Observe that $\pi(D_{p'}) = D_{p'}N/N \cong D_{p'}$ is of order $|D_{p'}|$. In particular, $\pi(D_{p'}^g) \leq \pi(D^k)$ and $\pi(D_{p'}^k) \leq \pi(D^k)$ are both cyclic subgroups of the same order. Hence $\pi(D_{p'}^g) = \pi(D_{p'}^k)$. Let

$d_{p'}$ be a generator of $D_{p'}$, hence $g^{-1}d_{p'}g = k^{-1}d_{p'}^{\alpha}k \cdot z$ for some α and $z \in N$. Taking a p-power we obtain that $g^{-1}d_{p'}^{p}g = k^{-1}d_{p'}^{\alpha p}k$. And since $d_{p'}^{p}$ is also a generator of $D_{p'}$, it follows that $g^{-1}D_{p'}g = k^{-1}D_{p'}k$. Thus $K = N \cup [C]^K \cup [D]^K$. Then by Proposition 5.2.85 we can conclude that $K \in \Gamma_2$. In particular, $Z(K)$ is cyclic, so $N = T$ is cyclic. As above we then obtain that C centralizes T, so $T \leq Z(G)$. A contradiction, as we already established that $Z(G)$ is trivial. Thus it follows that $T = N \cap D = 1$ and so $|D| = |DN/N|$ is coprime to p by induction. Hence we obtain $P \subseteq [C]^G$. If P is abelian, then by the proof of Lemma 5.2.109 we obtain that P is elementary abelian since $P = [P \cap C]^G = [P \cap C]^D$ and $|D|$ is coprime to p. By Lemma 5.2.120 we have that D is a self-normalizing subgroup of PD. If P is non-abelian, then $p = 2$. As before, $P \cong Q_8$ is impossible. So P is a Suzuki 2-group. By Remark 5.2.127 $C\Phi(P)/\Phi(P)$ and $D\Phi(P)/\Phi(P) \cong D$ have coprime orders and thus also $|C|$ and $|D|$ are coprime as $(|D|, p) = 1$. By Lemma 5.2.82 it then follows that $C_G(C') \leq [C]^G$ for any non-trivial $C' \leq P$. Hence $C_K(C') \leq [C]^G \cap K = [C \cap K]^G$. Now, $(C \cap K)P/P \leq K/P \cong D$ is trivial as $|C|$ and $|D|$ are coprime, so $C \cap K \leq P$. Thus $C_K(C') \leq P$ and thus $K = PD$ is a Frobenius group with Frobenius complement D. In particular, D is a self-normalizing subgroup of K. ☐

5.2.3.9. Sylow Subgroups and Derived Length

For determining the structure of the Sylow subgroups of groups in Γ_2 it has previously been helpful to appeal to a result of Shult [Shu69a] as well as Higman [Hig63]. For example, recall the arguments used in the proof of Lemma 5.2.111. However, a complication arises in the general case, since we cannot expect that cyclic p-subgroups of the same order are conjugate:

Remark 5.2.129. For $G \in \Gamma_2$, if $C \cap D = 1$ and $P \trianglelefteq G$ is a normal Sylow p-subgroup. It does not necessarily follow that $P \subseteq [C]^G$ or $P \subseteq [D]^G$. Again the group G of order 896 that was already mentioned in Remark 5.2.65 is an example. It contains a normal Sylow 2-subgroup of order 2^7. We have $|[C]^G| = 770$ and $|[D]^G| = 127$ and there is a single 2-element in $[C]^G$, namely an element of order 2.

Lemma 5.2.130. If $G \in \Gamma_2$ and $F(G) = P$ is the Sylow p-subgroup and $G/F(G)$ is cyclic and $Z(G) \neq 1$, then $Z(G) = Z(P)$. If $Z(G) \leq D$, then $G \cong \mathrm{SL}_2(3)$.

Proof. By Proposition 5.2.128 we already know that $Z(G) \leq Z(P)$ and $Z(P)$ is cyclic. If $Z(P) \leq C$, we are done. If $Z(P) \leq D$, we know that $Z(G) = C \cap D$. We denote by $\overline{G} = G/Z(G)$. We know that $\overline{P} \subseteq [\overline{D}]^{\overline{G}}$. Let $x \in P$. If $\overline{x} = 1$, then $x \in Z(G) \leq D$. Otherwise $\overline{x} \in \overline{D}^{\overline{g}}$, so $x = g^{-1}d^m g \cdot z$ for some $z \in Z(G)$. As $Z(G) \leq D$ it follows that $x \in D^g$. Hence $P \subseteq [D]^G$ and as in the proof of Lemma 5.2.111 it follows that P is abelian, a Suzuki 2-group or the quaternion group Q_8. The group P cannot be abelian, otherwise $Z(G) = 1$ by Lemma 5.2.115. Also P is not a Suzuki 2-group since these have non-cyclic center, so the only group remaining is the quaternion group $Q_8 \cong P$. Let $H \leq G$ be a complement of P, so $G = PH$ with $H \cap P = 1$. As $F(G) = P$ is self-centralizing, it follows that $H \leq \mathrm{Aut}(Q_8) \cong S_4$. A quick computation, e.g. via GAP, reveals that there is a unique group (even if we allow non-cyclic complements H) up to isomorphism in Γ_2 with these properties, namely $\mathrm{SL}_2(3)$. For $G = \mathrm{SL}_2(3)$ we know that $C \cap D = Z(G)$ is of order 2 and thus $Z(P) = Z(G)$ also in this case. □

Lemma 5.2.131. Suppose $G \in \Gamma_2$ and $F(G) = P$ is a non-cyclic Sylow p-subgroup where $p \neq 2$ and $G/F(G)$ is cyclic. Then $G \in \Gamma_2^I$, so in particular P is elementary abelian and $P = [D]^G$.

Proof. We prove the claim by induction on the order of G. If $\Phi(P) = 1$, we are done. If $Z(G) = 1$ we are also done by Lemma 5.2.111. So assume that $Z(G) \neq 1$ and $\Phi(P) \neq 1$. By Lemma 5.2.116 it follows that $Z(P)$ is cyclic and of course also $Z(P) \cap \Phi(P) \neq 1$. Choose a minimal normal subgroup $N \leq Z(P) \cap \Phi(P)$ of G.

If P/N is cyclic, then P is abelian since $N \leq Z(P)$. By Lemma 5.2.115 it follows that $Z(G) = 1$ and hence P is elementary abelian by Lemma 5.2.109. So we can assume that P/N is non-cyclic. By induction it then follows that P/N is elementary abelian and covered by conjugates of DN/N. Suppose $N \cap D \neq 1$, then $N \leq D$ and this implies that $P \subseteq [D]^G$. As in the proof of Lemma 5.2.111 the claim follows in this case. So we can assume that $N \cap D = 1$. Then the p-subgroups of D and C are of order p, so P has exponent p, thus $|Z(P)| = p$. Hence $N = Z(P)$. Let $T = P \cap D$, then $P = Z(P) \cup [T]^G$. Note also that $N \leq Z(P) \cap \Phi(P)$, hence $Z(P) \leq \Phi(P)$. Since P/N is elementary abelian it follows that $\Phi(P) \leq N$. Thus $Z(P) = \Phi(P)$ and hence P is an extraspecial p-group of exponent p. Note that we can write $G = PC_{p'}$ with $C_{p'} \leq C$ of order coprime to p and $C_{p'} \leq \mathrm{Aut}(P)$ since $F(G) = P$. Let $\varphi \in C_{p'}$ be a generator of $C_{p'}$. As φ acts trivially on $Z(P)$ and as it acts irreducibly on $P/\Phi(P)$ we get from [Win72, Corollary 2] that the order of φ divides $p^n + 1$ where $|P| = p^{2n+1}$. Note that $|P/\Phi(P)| = p^{2n}$ and by Proposition 5.2.63 it follows that $p^{2n}-1/p-1$ divides $|C_{p'}|$. Since $|C_{p'}|$ also divides $p^n + 1$, we obtain that $n = 1$, so $|C_{p'}| = p + 1$. But then $G/Z(P)$ would be a group of the form $(C_p \times C_p) \rtimes C_{p+1} \in \Gamma_2^I$. But this is impossible by Lemma 5.2.62 since $(2, p-1) \neq 1$ as p is odd.

□

Lemma 5.2.132. Let $G \in \Gamma_2$ with $F(G) = P$ a Suzuki 2-group as the Sylow 2-subgroup. Also suppose that $G/F(G)$ is cyclic. Then the subgroup $H = Z(P)C$ lies in Γ_2^I and $P \cong A(n, \theta)$ for some θ and $n \in \mathbb{N}$.

Proof. We know that $Z(G) = 1$ by Lemma 5.2.130 since Suzuki 2-groups have non-cyclic center. Moreover, by Lemma 5.2.111 we have $G = PC$ with $P \cap C = 1$ and $P = [D]^G$. By Lemma 5.2.82 we know that $C_G(y) \subseteq [C]^G$ for any non-trivial element $y \in C$. Since $|C|$ and p are coprime it follows that $C_G(x) \leq P$ for any $x \in P \setminus \{1\}$. Thus $H = Z(P)C$ is a Frobenius group with Frobenius complement C by Lemma 5.2.46. In particular, C is a self-normalizing subgroup of H. For any $g \in G$ the group C^g is a Carter subgroup of H, hence there is some $h \in H$ such that $C^g = C^h$. Let $T = D \cap Z(P)$. Note that $Z(P) = [T]^G = [T]^C$ as $G = PC$. Let $x \in H$ be an arbitrary element, then if x, considered as an element of $G = PC \cong P \rtimes C$, has a non-trivial C-component, then it has to lie in a conjugate of C. And by the previous observation, any G-conjugate of C is an H-conjugate. If $x \in Z(P)$, then $x \in T^g$ for some $g \in C \leq H$. It follows that H lies in Γ_2 as well. As T is of order p and C is malnormal, it follows that $H \in \Gamma_2^I$. By Proposition 5.2.63 we have

$|C| = |Z(P)| - 1$. Note that also $G/Z(P) \in \Gamma_2^I$ and thus $|C| = |P/Z(P)| - 1$ by the same lemma. Hence $|Z(P)| = |P/Z(P)|$ and this implies that $P \cong A(n, \theta)$. $\square$

Lemma 5.2.133. Suppose $G \in \Gamma_2$ and $F(G) = P$ is the Sylow 2-subgroup of G, $P/Z(P) \cong A(n, \theta)$ is a Suzuki 2-group, $G/F(G)$ is cyclic and $Z(G) \neq 1$. Then $Z(G) = Z(P)$ is of order 2 and P is of exponent 4, $\Omega(P)$ is elementary abelian of rank $n+1$ and $P/\Omega(P)$ is elementary abelian of rank n. Moreover, $C \cap D = 1$ and the largest powers of 2 that divide $|C|$ resp. $|D|$ are 2 resp. 4. In particular, all cyclic subgroups of G of order 4 are conjugate.

Proof. By Lemma 5.2.130 we know that $Z(G) = Z(P)$. Write $\overline{G} = G/Z(G)$. Then $|D| = |Z(G) \cap D| \cdot |\overline{D}|$ and $|\overline{D}| = p^2$ by Lemma 5.2.111 where $p = 2$. So D is a p-group, hence $D \leq P$. Suppose for the moment that $C \cap D = Z(G) \cap D \neq 1$. In particular there would exist a cyclic subgroup of order p in $C \cap D$. This implies that any two cyclic subgroups of order $p = 2$ are conjugate in G. However, as $Z(P)$ is non-trivial, this implies that P contains a unique involution since $Z(P)$ is a normal subgroup of G. This would imply that P is cyclic or a generalized quaternion group, a contradiction. Hence it follows that $C \cap D = Z(G) \cap D = 1$, so $|D| = |\overline{D}| = p^2$. Also note that $|C| = |C \cap Z(G)| \cdot |\overline{C}| = |Z(G)| \cdot |\overline{C}|$ where $|\overline{C}|$ is coprime to p. By Lemma 5.2.80 we know that $|Z(G)| = (|C|, |D|)$ since in $G/Z(G)$ the order of $\overline{C}$ and $\overline{D}$ are coprime. Thus $|Z(G)|$ either equals 2 or 4. Observe that $P = Z(P) \cup [D]^G$. Suppose $Z(G) = Z(P)$ is of order 4, then the number of cyclic subgroups of order 4 in P equals $1 + [G : N_G(D)]$. As P is neither cyclic nor of maximal class, the number of cyclic subgroups of order 4 is even by [Ber08, Theorem 1.17 (b)]. Thus $[G : N_G(D)]$ is odd and so $P \leq N_G(D)$, in other words $D \trianglelefteq P$. As the exponent of $P/Z(P) \cong A(n, \theta)$ equals 4, this would imply that all cyclic subgroups and hence all subgroups of $A(n, \theta)$ are normal. But this is impossible.

Hence $Z(P)$ is of order 2. Let $D' \leq D$ be the subgroup of order 2, we then claim that $\Omega(P) = Z(P) \cup [D']^G$. First note that $\overline{P} = [\overline{D}]^{\overline{G}}$ and so $\Omega(\overline{P}) = [\overline{D}']^{\overline{G}}$ since $\overline{P}$ is a Suzuki 2-group and $D \cap Z(P) = 1$. Let $x, y \in Z(P) \cup [D']^G$ be two elements of order 2, and suppose $x \cdot y$ is of order 4. Then $\langle x \cdot y \rangle = D^g$ for some $g \in G$. But then $\overline{x} \cdot \overline{y}$ would be of order 4 as $D \cap Z(G) = 1$, which contradicts the fact that $\Omega(\overline{P})$ is elementary abelian. Hence $\Omega(P) = Z(P) \cup [D']^G$. As $\Omega(\overline{P}) = [\overline{D}']^{\overline{G}}$ it follows that $P/\Omega(P)$ is elementary abelian of order p^n and thus $|\Omega(P)| = p^{n+1}$. $\square$

Theorem 5.2.134. Let $G \in \Gamma_2$ and let P be a Sylow p-subgroup of G. Then P is cyclic or elementary abelian or $p = 2$ and the Sylow p-subgroup is isomorphic to Q_8, a Suzuki 2-group or $Z(P) \cong C_2$ with $P/Z(P)$ a Suzuki 2-group.

Proof. Let $P \leq G$ be a Sylow p-subgroup. By Theorem 5.2.114 we can assume that P is normal, possibly after factoring out $O_{p'}(G)$. Moreover, we can factor out successively Sylow q-subgroups of $F(G)$ for $q \neq p$. After finitely many steps we can thus assume that $G \in \Gamma_{\leq 2}$ such that $F(G) = P$. If G is cyclic, we are done, so assume $G \in \Gamma_2$. We have to consider two cases:

(1) $G/F(G)$ is cyclic. By Lemma 5.2.131 we can assume that $p = 2$. If $Z(G) = 1$ then Lemma 5.2.111 yields the result. So suppose that $Z(G) \neq 1$. Note that $Z(G/Z(G)) = 1$ by Lemma 5.2.78 and $F(G/Z(G)) = F(G)/Z(G)$. By Lemma 5.2.130 we know that $Z(G) = Z(P)$. Again by Lemma 5.2.111 we need to consider the following cases:

a) $P/Z(G)$ is cyclic. Then P is abelian. By Lemma 5.2.115 this would imply that $Z(G) = 1$, a contradiction.

b) $P/Z(G)$ is elementary abelian. Let $\overline{G} = G/Z(G)$ and $\overline{D} = DZ(G)/Z(G)$ etc., then it follows that $|D| = |\overline{D}| \cdot |D \cap Z(G)|$ is a power of p, so $D \leq P$. Moreover, we observe that $P = Z(G) \cup [D]^G$. Suppose first that $Z(P) \cap D = Z(G) \cap D = C \cap D = 1$. Then $|D| = |\overline{D}| = p$. Let $z \in Z(G)$ and $d \in D$ be generators of the respective groups. If $zd = g^{-1}c^n g$ for some $g \in G$, $n \in \mathbb{N}$ and $c \in C$, then $\overline{d} = \overline{g}^{-1}\overline{c}^n\overline{g}$ in $\overline{G}$. But $\overline{C} \cap \overline{D} = 1$, thus it would follow that $\overline{d} = 1$, i.e. $d \in Z(G)$, which yields a contradiction. Thus $zd = g^{-1}d^n g$ for some $n \in \mathbb{N}$. Hence $\operatorname{ord}(zd) = \operatorname{ord}(d) = p$, on the other hand $\operatorname{ord}(zd) = [\operatorname{ord}(z), \operatorname{ord}(d)] = [\operatorname{ord}(z), p] = \operatorname{ord} z$. So $\operatorname{ord}(z) = p$ as well, and thus P is abelian since $p = 2$ and all non-trivial elements of P have order 2. As above, this is impossible. So we conclude that $Z(P) \cap D \neq 1$, hence the subgroup of $Z(P)$ order two also lies in all conjugates of D. Thus P is a 2-group containing a unique involution as $P = Z(G) \cup [D]^G$. It follows that P is cyclic or a generalized quaternion group. Now P cannot be cyclic by Lemma 5.2.115 and by Lemma 5.2.19 it follows that $P \cong Q_8$ since $\delta(P) \leq 2$.

c) $P/Z(G)$ is isomorphic to a Suzuki 2-group. Then Lemma 5.2.133 yields that $Z(G) = Z(P)$ is order two.

(2) $G/F(G) \in \Gamma_2$. By Proposition 5.2.128 it follows that $Z(G) = 1$ and P is either elementary abelian or a Suzuki 2-group.

□

The proof of Theorem 5.2.134 also shows:

Corollary 5.2.135. Let $G \in \Gamma_2$ and let $P \leq G$ be a Sylow p-subgroup. If P is elementary abelian or a Suzuki 2-group, then all cyclic p-subgroups are conjugate in G. If $p = 2$, then at least all cyclic subgroups of order 4 are conjugate.

In the following we will prove that certain Suzuki 2-groups actually appear as Sylow 2-subgroups of groups in Γ_2. First, we will prove a couple of easy lemmas.

Lemma 5.2.136. Let $q = 2^n$ and $\alpha \in \mathbb{F}_q^\times$. Let θ be an automorphism of $\mathbb{F}_q$ of odd order and let $V_\alpha = \{\gamma\alpha^\theta + \alpha\gamma^\theta \mid \gamma \in \mathbb{F}_q\}$. Then $\alpha^{\theta+1} \notin V_\alpha$.

Proof. As noted in [Hig63] the map $\psi\colon \mathbb{F}_q \to \mathbb{F}_q, \lambda \mapsto \lambda^{1+\theta}$ is bijective as θ is of odd order. Suppose that $\psi(\alpha) = \alpha^{\theta+1} \in V_\alpha$, so $\psi(\alpha) = \gamma\alpha^\theta + \alpha\gamma^\theta$ for some $\gamma \in \mathbb{F}_q$. Observe that $\psi(\alpha+\gamma) = (\alpha+\gamma)\cdot(\alpha^\theta+\gamma^\theta) = \psi(\alpha)+\psi(\gamma)+\gamma\alpha^\theta+\alpha\gamma^\theta = \psi(\alpha)+\psi(\gamma)+\psi(\alpha) = \psi(\gamma)$. Since ψ is injective, it follows that $\alpha + \gamma = \gamma$, so $\alpha = 0$, which is a contradiction. □

Lemma 5.2.137. Let $\theta \in \operatorname{Aut}(\mathbb{F}_q)$ where $q = 2^n$ and $n \geq 2$. For $\alpha \in \mathbb{F}_q^\times$ the set $V_\alpha = \{\gamma\alpha^\theta + \alpha\gamma^\theta \mid \gamma \in \mathbb{F}_q\}$ is a vector space over $\mathbb{F}_2$. Then V_α is of dimension $n-1$ if and only if θ generates the Galois group of $\mathbb{F}_q/\mathbb{F}_2$. Otherwise the dimension of V_α is strictly smaller than $n-1$.

Proof. Let $\varphi\colon \mathbb{F}_q \to V_\alpha$ be the linear map $\gamma \mapsto \gamma\alpha^\theta + \alpha\gamma^\theta$. Suppose $\gamma\alpha^\theta + \alpha\gamma^\theta = 0$ for some $\gamma \neq 0$. Then $\theta(\alpha\gamma^{-1}) = \alpha\gamma^{-1}$. If θ is a generator of the Galois group it follows that $\alpha\gamma^{-1} \in \mathbb{F}_2$, so $\alpha = \gamma$. Thus $\ker(\varphi) = \{0, \alpha\} \cong \mathbb{F}_2$. □

Putting the previous two lemmas together we obtain:

Lemma 5.2.138. Let $q = 2^n$ and $n \geq 2$ and suppose $\theta \in \mathrm{Aut}(\mathbb{F}_q)$ is a generator of the Galois group and of odd order. Then $\mathbb{F}_q = V_\alpha \cup (\alpha^{\theta+1} + V_\alpha)$ and $V_\alpha \cap (\alpha^{\theta+1} + V_\alpha) = \emptyset$ for each $\alpha \in \mathbb{F}_q^\times$.

The Suzuki 2-group $A(n, \theta)$ admits a cyclic group $\mathbb{F}_q^\times$ of automorphisms that permutes the involutions transitively as described in [Hig63]. In the following proposition the semidirect product is understood with this particular action.

Proposition 5.2.139. Let $q = 2^n$ with $n \geq 2$ and let $\theta \in \mathrm{Aut}(\mathbb{F}_q)$ be a generator of odd order. Then $G = A(n, \theta) \rtimes \mathbb{F}_q^\times \in \Gamma_2$.

Proof. We know from [Hig63] that $P = A(n, \theta)$ is given as a set by $\mathbb{F}_q \times \mathbb{F}_q$ and elements $(\zeta, \alpha), (\eta, \gamma) \in \mathbb{F}_q \times \mathbb{F}_q$ are multiplied as follows:

$$(\zeta, \alpha) \cdot (\eta, \gamma) = (\zeta + \eta + \alpha \cdot \gamma^\theta, \alpha + \gamma)$$

Then

$$(\eta, \gamma)^{-1} = (\gamma^{\theta+1} + \eta, \gamma)$$

And so conjugation is given by

$$(\eta, \gamma) \cdot (\zeta, \alpha) \cdot (\eta, \gamma)^{-1} = (\zeta + \gamma\alpha^\theta + \alpha\gamma^\theta, \alpha)$$

Moreover, an element $\lambda \in \mathbb{F}_q^\times$ acts on an element in P via $(\zeta, \alpha) \mapsto (\lambda^{1+\theta}\zeta, \lambda\alpha)$. Then the group multiplication in $P \rtimes C$ is given by the following formula:

$$(\zeta, \alpha, \lambda) \cdot (\eta, \gamma, \mu) = (\zeta + \lambda^{\theta+1}\eta + \alpha(\lambda\gamma)^\theta, \alpha + \lambda\gamma, \lambda\mu)$$

We choose the cyclic subgroup D to be generated by $(0, 1)$. Then

$$D = \{(0,0), (0,1), (1,0), (1,1)\},$$

where the elements in D of order 4 are $(0, 1)$ and $(1, 1)$. Suppose $(\zeta, \alpha) \in A(n, \theta)$. Note that this element is conjugate to

$$(\lambda^{1+\theta}(\zeta + \gamma\alpha^\theta + \alpha\gamma^\theta), \lambda\alpha),$$

where $\gamma \in \mathbb{F}_q$ and $\lambda \in \mathbb{F}_q^\times$. If $\alpha = 0$, then we see that $(\zeta, 0)$ is conjugate to $(1, 0)$ since $\lambda \mapsto \lambda^{1+\theta}$ is invertible. If $\alpha \in \mathbb{F}_q^\times$, then we can choose $\lambda = \alpha^{-1}$ and by Lemma 5.2.138 there exists some $\gamma \in \mathbb{F}_q$ such that $\zeta = \gamma\alpha^\theta + \alpha\gamma^\theta$ or $\zeta = \alpha^{1+\theta} + \gamma\alpha^\theta + \alpha\gamma^\theta$, corresponding to whether (ζ, α) is conjugate to $(0, 1)$ or $(1, 1)$. So we have shown that $A(n, \theta) \subseteq [D]^G$. Now, suppose that $(\zeta, \alpha, \lambda) \in G$ is given where $\lambda \neq 1$. We compute

$$\begin{aligned}(\zeta, \alpha, \lambda)^{(\eta,\gamma,1)} = ((1 + \lambda^{\theta+1})\eta + \zeta + \gamma\alpha^\theta + (\gamma + \alpha)(\lambda\gamma)^\theta + (\lambda\gamma)^{\theta+1}, \\ (1 + \lambda)\gamma + \alpha, \\ \lambda)\end{aligned}$$

Now observe that $1 + \lambda \neq 0$ and $1 + \lambda^{\theta+1} \neq 0$ and thus we can find γ and η such that $(\zeta, \alpha, \lambda)^{(\eta,\gamma,1)} = (0, 0, \lambda)$. Thus $G \in \Gamma_2$. □

Our next goal will be to show that non-cyclic Sylow subgroups of groups in Γ_2 are already normal.

Observation 5.2.140. Let $G \in \Gamma_2$ and assume that $|C|$ is odd and $|D| = 2$. Then the Sylow 2-subgroup is normal. Namely, let $t \in G$ be an involution. Suppose $t \notin O_2(G)$. Then by [Isa08, Theorem 2.13, p. 55] there exists an element $g \in G$ of odd prime order such that $tgt^{-1} = g^{-1}$. Since g is of odd order it has to be conjugate to an element $c^m \in C$. In particular, it follows that $N_G(\langle g \rangle) = C_G(\langle g \rangle)$. Hence $t \in C_G(\langle g \rangle)$, thus $g = g^{-1}$ which contradicts the fact that g is not an involution. Thus any involution is contained in $O_2(G)$. Since there is no element of order 2^n with $n \geq 2$ in G, it follows that the Sylow 2-subgroup equals $O_2(G)$.

Using ideas from [Sez14, Theorem 4.4] and [CJ09, Corollary 2.8] we are now ready to show:

Theorem 5.2.141. Suppose $G \in \Gamma_2$. Then any non-cyclic Sylow subgroup of G is normal.

Proof. Let p be a prime and denote by P the Sylow p-subgroup of G. We prove the claim by induction on the order of G and distinguish two cases:

(1) Suppose $O_p(G) \neq 1$. If $P/O_p(G)$ is non-cyclic, then by induction $P/O_p(G)$ is a normal subgroup of $G/O_p(G)$, hence P is a normal subgroup of G. So we can assume in the following that $P/O_p(G)$ is cyclic. Suppose P is elementary abelian, then by Corollary 5.2.135 all cyclic subgroups of order p would be conjugate. However, there exist elements of order p in $P \setminus O_p(G)$ that cannot be conjugate to non-trivial elements of $O_p(G)$. Hence we can assume that $p = 2$. If $P \cong Q_8$, then $O_p(G)$ has to one of three normal cyclic subgroups of order 4 in Q_8. But then $P \setminus O_p(G)$ contains 4 elements, each of order 4. As the cyclic subgroups of order 4 are conjugate by Corollary 5.2.135, this again yields a contradiction. Suppose P is a Suzuki 2-group. Note that P^{ab} is elementary abelian, so $P' \leq O_p(G)$ and $P/O_p(G)$ is cyclic of order 2. Then $P = O_p(G) \cup xO_p(G)$. If x was of order two, then $x \in \Omega(P) = P' \leq O_p(G)$, so x is of order 4. If all elements of $O_p(G)$ were of order at most two, then $O_p(G) \leq \Omega(P) = P'$, again yielding a contradiction since P^{ab} is non-cyclic. As all cyclic subgroups of order 4 are conjugate, this yields a contradiction. Finally, suppose that P is such that $Z(P)$ is of order 2 and $P/Z(P)$ is a Suzuki 2-group. If $O_p(G)$ contains a cyclic subgroup of order 4 then all cyclic subgroups of order 4 are contained in $O_p(G)$. As P is the union of $Z(P)$ and all cyclic subgroups of order 4 it follows that $P = Z(P) \cup O_p(G)$. As P is non-abelian it follows that $P = O_p(G)$. If $O_p(G)$ only contains elements of order 2, then $O_p(G) \leq \Omega(P)$. By Lemma 5.2.133 we know that $P/\Omega(P)$ is non-cyclic, contradicting our initial assumption that $P/O_p(G)$ is cyclic.

(2) Suppose $O_p(G) = 1$, and let us abbreviate $F = F(G)$, then $(p, |F|) = 1$. Let $N \trianglelefteq G$ be a minimal normal subgroup, so $N \leq F$. Then PN/N is a normal subgroup of G/N by induction, so $PN/N \leq F(G/N)$. As $F/N \leq F(G/N)$, it follows that $[F, P] \leq N$. If $M \trianglelefteq G$ was another minimal normal subgroup of G, then by the same argument $[F, P] \leq M$. But as N and M are distinct, it follows that $[F, P] \leq N \cap M = 1$. This would imply that $P \leq C_G(F) \leq F$, a contradiction. Hence we can assume that G has a unique minimal normal subgroup. In particular, $|F|$ is divisible by a single prime q. Let Q be the Sylow q-subgroup of G. Then $F \leq Q$. If Q was cyclic, G would be metacyclic by Lemma 5.2.72 and thus all Sylow subgroups would be cyclic as well by Proposition 5.2.95. Hence Q is non-cyclic and then $O_q(G) \neq 1$ and by the result of

(1) we obtain that Q is normal, thus $F(G) = Q$. Moreover, by taking the quotient by $\Phi(Q)$ we can assume that Q is elementary abelian. By Theorem 5.2.119 it follows that $G/F(G)$ is metacyclic with only cyclic Sylow subgroups. This contradicts the fact that $PF/F \cong P$ is non-cyclic.

□

Proposition 5.2.142. Let $G \in \Gamma_2$ and suppose $(|C|, |D|) = 1$. Let $P \leq G$ be a cyclic Sylow p-subgroup of G such that the normal core of P is non-trivial. Then P is a normal subgroup of G.

Proof. First observe that $Z(G) = 1$ by Lemma 5.2.79. Suppose $P \leq C$ up to conjugation, then C contains a non-trivial normal subgroup, which would contradict the fact that $Z(G) = 1$. Hence we can assume that $P \leq D$ and so p divides $|D|$. We now prove the claim by induction on the order of G.

Suppose $N \trianglelefteq G$ is a minimal normal subgroup of G whose order is q^n where q is a prime not equal to p. Let $\pi\colon G \to G/N$ denote the quotient map. Note that $P_G \cap N = 1$ since their orders are coprime. Thus $\pi(P_G) = P_G N/N \cong P_G$ is non-trivial and of course $\pi(P)$ is a Sylow p-subgroup of G/N. By induction $\pi(P)$ is a normal subgroup, hence $H = PN \trianglelefteq G$. Note that $P_G N \cong P_G \times N$. In particular, there exists an element h of order pq in H. The order of h has to divide $|C|$ or $|D|$. Since $|C|$ and $|D|$ are coprime and p divides $|D|$, it follows that also q divides $|D|$. It follows that $N \subseteq [D]^G$ so that $N = [N \cap D]^G$. Since N is abelian, it follows that $N \cap D \leq Z(H)$. Now H is normal in G and since $Z(H)$ is characteristic in H, it follows that $Z(H)$ is normal in G, hence we obtain for all $g \in G$:

$$(N \cap D)^g \leq Z(H)^g = Z(H)\,.$$

This implies $N \leq Z(H)$ and thus H is abelian. Then $P \trianglelefteq N$ is characteristic in N as it is the unique Sylow p-subgroup of H. Hence P is a normal subgroup of G which we wanted to show.

So now we can now assume that all minimal normal subgroups are p-groups and since P is cyclic there is a unique one. It follows that the Fitting subgroup $F(G)$ is a p-group, hence $F(G) \leq P$. So $F(G)$ is cyclic, which implies by Lemma 5.2.72 that G is metacyclic. By Proposition 5.2.90 it follows that D is a normal subgroup of G. In particular, P is a normal subgroup. □

Remark 5.2.143. If $G \in \Gamma_2$ and the normal core of D is non-trivial, then D is not necessarily normal. There is a group $G \in \Gamma_2$ of the form $(C_{14} \times C_2) \rtimes C_3$ which has $|D| = 14$ but $|D_G| = 7$.

Theorem 5.2.144. The derived length of any $G \in \Gamma_2$ is bounded by 4.

Proof. We prove the claim by induction on the order of G. If N, M are two distinct minimal normal subgroups, then the canonical homomorphism $G \to G/N \times G/M$ is injective as $N \cap M = 1$. Hence we can assume that there is a unique minimal normal subgroup N, which is a p-group for some prime p. Then $F(G)$ is a p-group as well. Let $P \leq G$ be a Sylow p-subgroup, so $N \leq F(G) \leq P$. If P is cyclic, then $F(G)$ is cyclic and so G is metacyclic by Lemma 5.2.72. Otherwise P is normal by Theorem 5.2.141, so $P = F(G)$.

Note that the derived length of P is at most 3 by Theorem 5.2.134, so if G/P is cyclic, we are done. If G/P is non-cyclic, then by Proposition 5.2.128 it follows that P is elementary abelian or a Suzuki 2-group. In particular, the derived length of P is at most 2. Hence G has derived length at most 4 since G/P is metacyclic.

□

Observe that the bound on the derived length in Theorem 5.2.144 is sharp by the following example.

Example 5.2.145. There is a group $G \in \Gamma_2$ of order 1344 which splits as $P \rtimes (C_7 \rtimes C_3)$ with $F(G) = P$ the Suzuki 2-group of order 64 with $|Z(P)| = 8$. The group G has derived length equal to 4.

5.2.3.10. Additional Structural Properties

Lemma 5.2.146. Let $G \in \Gamma_2$ with $Z(G) = 1$ and $G/F(G)$ metacyclic. Suppose $F(G) = PK$ with P an elementary abelian Sylow p-subgroup of G and K a cyclic subgroup. Then $K = 1$ or $G/F(G)$ is cyclic.

Proof. Suppose C and D both intersect $F(G)$ non-trivially. By Corollary 5.2.135 all cyclic subgroups of P are conjugate, hence $P \subseteq [C]^G$ or $P \subseteq [D]^G$. Suppose for the moment that $P \subseteq [C]^G$. For any $x \in P \setminus \{1\}$ the subgroup $\langle x \rangle K$ is cyclic since $|K|$ is coprime to p. If $\langle x \rangle K \leq D^g$ for some $g \in G$, then $\langle x \rangle \leq C^h \cap D^g \leq Z(G)$ for some $h \in G$. But this contradicts our assumption on G. Thus we have $F(G) = PK \subseteq [C]^G$. A similar argument shows that $F(G) \subseteq [D]^G$ if $P \subseteq [D]^G$.

By assumption $G/F(G)$ is metacyclic, thus $N = F(G)D$ is a normal subgroup of G. If $F \subseteq [D]^G$, then it would follow that $F \leq Z(N)$ and so N is abelian. Hence $D \leq C_G(F(G)) = F(G)$ and thus $G/F(G)$ is cyclic. If $F(G) \subseteq [C]^G$, then $K \leq C$. But as K is a normal subgroup of G, we have $K \leq Z(G) = 1$. □

Lemma 5.2.147. Let $G \in \Gamma_2$ with $F(G) = PQ$ with P, Q two non-cyclic elementary abelian Sylow subgroups corresponding to distinct primes. Then $Z(G) = 1$.

Proof. The proof is similar to the proof of Lemma 5.2.115. □

Lemma 5.2.148. Let $G \in \Gamma_2$ with $F(G) = PQ$ with P, Q two distinct non-cyclic elementary abelian Sylow subgroups. Suppose $G/F(G)$ is metacyclic but not cyclic. Then $F(G) \subseteq [C]^G$.

Proof. From the previous lemma we know that $Z(G) = 1$. By Corollary 5.2.135 we know that P resp. Q is contained in $[C]^G$ or $[D]^G$. Using $Z(G) = 1$, it follows that $F(G) \subseteq [C]^G$ or $F(G) \subseteq [D]^G$. Assume the latter. We know that $N = F(G)D$ is a normal subgroup of G since $G/F(G)$ is metacyclic. Then $F(G) \leq Z(N)$, and so $N \leq C_G(F(G)) = F(G)$. But this would imply that $G/F(G)$ is cyclic. Hence we obtain $F(G) \subseteq [C]^G$. □

Proposition 5.2.149. For $G \in \Gamma_2$ we have $|Z(G)| = (|C|, |D|)$.

Proof. By Lemma 5.2.80 it suffices to show the claim for groups $G \in \Gamma_2$ with $Z(G) = 1$. Moreover, one direction has been proven in Lemma 5.2.79. For the other, suppose that p is a common prime divisor of $|C|$ and $|D|$. Let $P \leq G$ be the Sylow p-subgroup. Denote by C_p resp. D_p the cyclic subgroups of order p in C resp. D. If P is cyclic, then there is some $g, g' \in G$ such that $C_p^g \leq P$ and $D_p^{g'} \leq P$. But then $C_p^g = D_p^{g'}$ and thus $Z(G) \neq 1$. If P is elementary abelian or a Suzuki 2-group, then by Corollary 5.2.135 C_p and D_p are conjugate and the claim follows as well. In the remaining cases by Theorem 5.2.134 we have that P is non-cyclic with $Z(P)$ of order 2. As P is normal in G by Theorem 5.2.141, $Z(P) \leq Z(G)$, a contradiction. The claim follows. □

Corollary 5.2.150. For a group $G \in \Gamma_2$, the quotient $G/Z(G)$ is a csc-group.

Theorem 5.2.151. A group $G \in \Gamma_2$ contains at most one non-cyclic Sylow subgroup.

Proof. Suppose G contains more one non-cyclic Sylow subgroup. By Theorem 5.2.141 we know that non-cyclic Sylow subgroups of G are normal. By passing to a suitable quotient of G we can thus assume that G contains exactly two distinct non-cyclic Sylow subgroups. Denote by P a non-cyclic Sylow p-subgroup and by Q a non-cyclic Sylow q-subgroup of G for primes $p \neq q$. We can moreover pass to successive quotients of G in order to ensure that $F(G) = PQ$. By modding out $\Phi(F(G))$ we can assume that P and Q are elementary abelian. As all Sylow subgroups of $G/F(G)$ are cyclic, it follows that $G/F(G)$ is metacyclic. By Lemma 5.2.147 we have $Z(G) = 1$ and Proposition 5.2.149 implies that $(|C|, |D|) = 1$. Recall that this implies that any non-cyclic quotient of G has trivial center as well by Lemma 5.2.81. Let us distinguish now two cases:

(1) If $G/F(G)$ is cyclic, we have $G = F(G)C$. As $F(G) = PQ$ is abelian, we have $F(G) \cap C \leq Z(G) = 1$. Thus $F(G) \subseteq [D]^G$. Since $|C|$ and $|D|$ have coprime orders, $C_G(C') \leq C$ for all non-trivial subgroups $C' \leq C$. Hence G is a Frobenius group with Frobenius complement C by Lemma 5.2.46. The same argument applies to the quotient groups G/P and G/Q which therefore lie in the class Γ_2^I. We know that D is cyclic of order pq and hence $F(G) = [D]^G = [D]^C$. Let $|P| = p^n$ and $|Q| = q^m$ where $n, m \geq 2$. The number of cyclic subgroups of order pq in $F(G)$ is given by

$$\left(\frac{p^n - 1}{p - 1}\right) \cdot \left(\frac{q^m - 1}{q - 1}\right) = [C : N_C(D)]$$

As G/P and G/Q lie in Γ_2^I, by Proposition 5.2.63 it then follows that $|C|$ divides $p^n - 1$ as well as $q^m - 1$. Since by the above observation $(p^n-1/p-1) \cdot (q^m-1/q-1)$ divides $|C|$ it follows that $q^m-1/q-1$ divides $p - 1$ and $p^n-1/p-1$ divides $q - 1$. Since we assumed $n, m \geq 2$, it follows in particular that $q + 1 \leq q^m-1/q-1 \leq p - 1$ and $p + 1 \leq p^n-1/p-1 \leq q - 1$. Thus $q + 3 \leq p + 1 \leq q - 1$, a contradiction.

(2) If $G/F(G)$ is non-cyclic, then by Lemma 5.2.148 $F(G) \subseteq [C]^G$. By Proposition 5.2.95 the subgroup $N = F(G)D$ is normal in G. As in (1) we obtain that $C_N(D') \leq D$ for any non-trivial subgroup $D' \leq D$. Thus N is a Frobenius group with Frobenius complement D. In particular, D is a Carter subgroup of N. As $G = NC$ we have $[C]^G \cap N = [C \cap N]^N$. These two facts together imply that $G \in \Gamma_2$. Also note that the two conjugacy classes of maximal cyclic subgroups of N with representatives $C \cap N$ and D have coprime orders. Hence (1) applies and we again arrive at a contradiction.

□

Let us recall the following standard definition:

Definition 5.2.152. A finite group G is called 2-*Frobenius* if there exist normal subgroups $H, K \trianglelefteq G$ such that $1 \leq H \leq K \leq G$ and K is a Frobenius group with Frobenius kernel H and G/H is a Frobenius group with Frobenius kernel K/H.

In proofs in Section 5.2.3.8, see e.g. Lemma 5.2.120, we have already seen that some groups in Γ_2 are 2-Frobenius. We can now record the following important theorem:

Theorem 5.2.153. Let $G \in \Gamma_2$ with $Z(G) = 1$. Then exactly one of the following holds:

(1) $G/F(G)$ is cyclic. Then G is a Frobenius group and $F(G) = [D]^G$. Either G is metacyclic or G contains a unique non-cyclic Sylow p-subgroup $P \trianglelefteq G$ and a cyclic normal subgroup K whose order is coprime to p such that $F(G) = PK$. Moreover, $PC \in \Gamma_2$ and $KC \in \Gamma_2$ if K is non-trivial.

(2) $G/F(G)$ is metacyclic but not cyclic. Then G is a 2-Frobenius group with $F(G) \subseteq [C]^G$. Furthermore, $F(G) = P$ is a non-cyclic Sylow p-subgroup of G and $G/\Phi(F(G))$ has the form described in Proposition 5.2.126. Let n be the rank of $P/\Phi(P)$. Then n is a prime different from p with $(n, p-1) = 1$, $|D| = {}^{p^n-1}/_{p-1}$ and

$$|C| = \begin{cases} p \cdot n, & \text{if } P \text{ elementary abelian} \\ p^2 \cdot n, & \text{if } P \text{ a Suzuki 2-group} \end{cases}$$

Proof. The claims follow easily from the previous results. □

For a finite group G denote by $\pi(G)$ the set of element orders in G that are prime numbers. Then the *prime graph*, sometimes also called *Gruenberg-Kegel graph*, of G has as a vertex set $\pi(G)$ and there is an edge between distinct elements p, q if and only if there exists an element of order pq in G. Now, the Gruenberg-Kegel theorem [Wil81] asserts that a solvable finite group G whose prime graph has at least two connected components is either a Frobenius or a 2-Frobenius group. Observe that a finite group $G \in \Gamma_2$ with $Z(G) = 1$ has $(|C|, |D|) = 1$ by Proposition 5.2.149. This implies that the prime graph of G has at least two components and so the result of Theorem 5.2.153 should be seen as an instance of the Gruenberg-Kegel theorem.

6. Finiteness of the Classifying Space $\underline{\underline{B}}G$

Given a group G and a family of subgroups $\mathcal{F}$ of G we now want to study the finiteness properties of the classifying space $B_{\mathcal{F}}(G) = E_{\mathcal{F}}(G)/G$. Again we shall use the convention that $\underline{B}G = B_{\mathcal{F}in}(G)$ and $\underline{\underline{B}}G = B_{\mathcal{VC}yc}(G)$. As the G-homotopy type of $E_{\mathcal{F}}(G)$ is uniquely determined, so is the homotopy type of $B_{\mathcal{F}}(G)$. However, if $B_{\mathcal{F}}(G) \to X$ is some homotopy equivalence to another CW-complex X, there need not be a G-homotopy equivalence of G-CW complexes whose quotient realizes the given map. The situation is different for the trivial family $\mathcal{F} = \mathcal{T}r$, since EG is the universal cover of BG. Thus finiteness conditions of the G-CW complex EG are equivalent to finiteness conditions of the CW-complex BG. For example, BG has a finite model if and only if EG has a finite model. We shall see below that a corresponding statement fails for finite-dimensionality if we take the family of finite or the family of virtually cyclic subgroups. The following question goes back to [JL06, Remark 17] and motivated our study:

Question 6.0.1. Suppose $\underline{\underline{B}}G$ is homotopy equivalent to a finite CW-complex. Is $\underline{\underline{B}}G$ necessarily contractible?

In contrast to Question 6.0.1, in the case of the family of finite subgroups, Leary and Nucinkis showed [LN01] that every connected CW-complex is homotopy equivalent to $\underline{B}G$ for some group G. By [LN01, Proposition 3] we know that $\pi_1(B_{\mathcal{F}}(G)) \cong G/N$ where N is the smallest normal subgroup of G containing all subgroups of $\mathcal{F}$. In particular, it follows that $\underline{\underline{B}}G$ is simply-connected for any group G. Then Question 6.0.1 is equivalent to the question whether $\underline{\underline{B}}G$ is contractible if all homology groups $H_*(\underline{\underline{B}}G;\mathbb{Z})$ are finitely generated. Question 6.0.1 appears to be more difficult than Conjecture 1.2.2 in the sense that our proofs for certain classes of groups depend on the validity of Conjecture 1.2.2.

In the following let us discuss the question whether $\underline{\underline{B}}G$ being homotopy-equivalent to a finite-dimensional complex implies the existence of a finite-dimensional model for $\underline{\underline{E}}G$. It is consistent with Zermelo-Fraenkel set theory with axiom of choice (ZFC) that for G locally finite of cardinality $\aleph_n$ the minimal dimension of $\underline{E}G$ is equal to $n+1$ [LW12, Example 5.32]. A lower bound for the dimension of $\underline{E}G$ is provided by the rational cohomological dimension, namely we have $\mathrm{cd}_{\mathbb{Q}}(G) \leq \underline{\mathrm{gd}}\,(G)$. And it is consistent with ZFC that $\mathrm{cd}_{\mathbb{Q}}(G) = n+1$. Note that for G locally finite $\mathcal{VC}yc(G) = \mathcal{F}in(G)$ and $\underline{\underline{B}}G = \underline{B}G$ is contractible as we shall see below. In particular, it is consistent with ZFC that the gap between the minimal dimension of a model for $\underline{B}G$ and the minimal dimension of a model for $\underline{E}G$ is arbitrarily large. Actually, it is then also consistent with ZFC that there exists a locally finite group of cardinality $\aleph_\omega$ which does not admit a finite-dimensional model for $\underline{\underline{E}}G = \underline{E}G$. Summarizing, we have seen that if $\underline{\underline{B}}G$ is homotopy-equivalent to a finite CW-complex, it is in general impossible to conclude that $\underline{\underline{E}}G$ is finite-dimensional.

Lemma 6.0.2. Let V be a virtually cyclic group. Then $\underline{\underline{B}}V$ is contractible if and only if V is finite or nonorientable. If V is orientable, then $\underline{\underline{B}}V = S^1$. In particular, $H_n(\underline{\underline{B}}V; \mathbb{Z}) = 0$ for $n \geq 2$ in all cases.

Proof. For $V = \mathbb{Z}$, we have of course $\underline{\underline{B}}V = BV = K(V, 1) = S^1$. For $V = D_\infty = \mathbb{Z}/2 * \mathbb{Z}/2$ the infinite dihedral group, we get that $\pi_1(\underline{\underline{B}}D_\infty) = 1$ since D_∞ is generated by elements of finite order. But more is true: we have $\mathbb{R}$ as a model for $\underline{\underline{E}}D_\infty$, and moreover $\mathbb{R}/D_\infty \cong [0, 1/2]$ (see also Examples 1.0.4).

More generally, if V is an orientable virtually cyclic group, there exists an epimorphism $\pi\colon V \to \mathbb{Z}$ with finite kernel. Then $\mathbb{R}$ serves as a model for $\underline{\underline{E}}V$ by pulling back the standard $\mathbb{Z}$-action on $\mathbb{R}$ via π. Thus $\underline{\underline{B}}V = S^1$. Similarly, if V is nonorientable, then $\underline{\underline{B}}V$ is contractible. $\square$

6.1. Locally $\mathcal{F}$ Groups

For G a group and $\mathcal{F}$ a family of finitely generated subgroups of G we want to give an easy argument here to show that $B_{\mathcal{F}}G$ is contractible for G locally $\mathcal{F}$, i.e. a group such that all its finitely generated subgroups lie in the family $\mathcal{F}$. In [JL06, p. 10] Juan-Pineda and Leary note that $\underline{\underline{B}}G$ is contractible for G locally virtually cyclic and provide a proof in the case that G is countable by constructing an explicit model.

Ramras [Ram18] has a given a nice account on functorial models for $E_{\mathcal{F}}(G)$ resp. $B_{\mathcal{F}}(G)$. We shall use in the following that $B_{\mathcal{F}}(G)$ can be viewed as the geometric realization of the nerve of the orbit category $\mathbf{Or}_{\mathcal{F}}(G)$. Recall that the category $\mathbf{Or}_{\mathcal{F}}(G)$ has as objects transitive G-sets G/H with $H \in \mathcal{F}$ and as morphisms G-maps. One observes that

$$\operatorname{Hom}(G/H, G/K) \cong \{g \in G \mid gHg^{-1} \leq K\}/\sim$$

where $g \sim gk$ for all $k \in K$.

Also recall that a category $\mathcal{C}$ is *filtered* if the following two conditions are met:

(1) For any two objects X, Y in $\mathcal{C}$ there exists an object Z in $\mathcal{C}$ and morphisms $X \to Z$ and $Y \to Z$.

(2) For two morphisms $f, g\colon X \to Y$ there exists an object Z in $\mathcal{C}$ and a morphism $h\colon Y \to Z$ such that $hf = hg$.

By a classical result, the nerve of a filtered category is contractible, see e.g. [Qui10, Corollary 2, p. 93].

Proposition 6.1.1. Let G be a group and let $\mathcal{F}$ be a family of finitely generated subgroups of G. If G is locally $\mathcal{F}$, then $B_{\mathcal{F}}G$ is contractible.

Proof. We verify that the orbit category $\mathbf{Or}_{\mathcal{F}}(G)$ is filtered.

(1) For two transitive G-sets G/H, G/H', we note that $\langle H, H'\rangle$ is again in $\mathcal{F}$ since H, H' are finitely generated and G is locally $\mathcal{F}$. Then certainly there are G-maps $G/H \to G/\langle H, H'\rangle$ and $G/H' \to G/\langle H, H'\rangle$.

(2) Let two G-maps $\alpha, \beta\colon G/H \to G/K$ be given. These are represented by elements $a \in G$ and $b \in G$, i.e. $\alpha(H) = aK$ and $\beta(H) = bK$. We consider the finitely generated subgroup $L = \langle a, b, K\rangle \in \mathcal{F}$. Then we let $\pi\colon G/K \to G/L$ be the canonical map. It follows that $\pi\alpha = \pi\beta$.

□

In particular, Proposition 6.1.1 implies that $\underline{\underline{B}}G$ is contractible for all locally virtually cyclic groups G. One might ask whether there are groups G that are not locally virtually cyclic but which nevertheless have a contractible classifying space $\underline{\underline{B}}G$. These certainly exist by [JL06, Example 4]. However, we cannot find such new examples by only considering filtered categories as the following result shows.

Proposition 6.1.2. Let G be a group and let $\mathcal{F}$ be a family of finitely generated subgroups containing all cyclic subgroups. The category $\mathbf{Or}_{\mathcal{F}}(G)$ is filtered if and only if G is locally $\mathcal{F}$.

Proof. The proof of Proposition 6.1.1 showed that a locally $\mathcal{F}$ group has a filtered orbit category. So let us suppose that $\mathbf{Or}_{\mathcal{F}}(G)$ is a filtered category. Let $a \in G$ be non-trivial element and let $K \in \mathcal{F}$. Consider the two G-maps $\pi\colon G/1 \to G/K, 1 \mapsto K$ and $\alpha\colon G/1 \to G/K, 1 \mapsto aK$. By the second property of filtered categories, there exists some $V \in \mathcal{F}$ and a G-map $\lambda\colon G/K \to G/V$ such that $\lambda \circ \pi = \lambda \circ \alpha$. Let $x \in G$ so that $\lambda(K) = xV$. Since λ is a G-map, we have $K \leq xVx^{-1}$. Moreover, $xV = (\lambda \circ \pi)(1) = (\lambda \circ \alpha)(1) = \lambda(aK) = axV$ implies that $a \in xVx^{-1}$. Thus a and K both lie in the same subgroup $xVx^{-1} \in \mathcal{F}$. Now, if $H \leq G$ is a finitely generated subgroup, then by an inductive argument we obtain that $H \in \mathcal{F}$. The assumption that $\mathcal{F}$ contains all cyclic subgroups is needed in the beginning of the induction. □

6.2. Lück-Weiermann Construction

Suppose we have a group G and two families of subgroups $\mathcal{F} \subseteq \mathcal{G}$ of G. We want to recall a construction due to Lück and Weiermann [LW12] that allows us to obtain a model for $E_{\mathcal{G}}(G)$ from a model for $E_{\mathcal{F}}(G)$ using a pushout. The spaces that are being attached are classifying spaces for certain generalized normalizer subgroups. We will be interested in the case that $\mathcal{F} = \mathcal{F}in$ and $\mathcal{G} = \mathcal{VC}yc$. As mentioned before, for large classes of groups there exist finite models for the classifying space of proper actions. Our strategy in answering Question 6.0.1 can then be outlined as follows: For certain classes of groups we shall obtain $\underline{\underline{E}}G$ from $\underline{E}G$ by attaching infinitely many classifying spaces. In a second step we compute the homology of $\underline{\underline{E}}G$, at least partially, in the hope that the attached classifying spaces generate enough classes in the homology of $\underline{\underline{E}}G$.

To perform the construction we will assume that the set $\mathcal{G} \setminus \mathcal{F}$ of subgroups of G is equipped with an equivalence relation $\sim$ that satisfies the following additional properties, which we will refer to as (P):

$$\begin{aligned}&(1)\ \text{If } H, K \in \mathcal{G} \setminus \mathcal{F} \text{ with } H \leq K, \text{ then } H \sim K.\\&(2)\ \text{If } H, K \in \mathcal{G} \setminus \mathcal{F} \text{ and } g \in G, \text{ then } H \sim K \Leftrightarrow gHg^{-1} \sim gKg^{-1}.\end{aligned} \tag{P}$$

Notation 6.2.1. We let $[\mathcal{G} \setminus \mathcal{F}]$ denote the set of equivalence classes under the equivalence relation $\sim$ and we denote by $[H] \in [\mathcal{G} \setminus \mathcal{F}]$ the equivalence class of an element $H \in \mathcal{G} \setminus \mathcal{F}$.

By property (2) of (P) the G-action by conjugation on the set $\mathcal{G} \setminus \mathcal{F}$ induces a G-action on $[\mathcal{G} \setminus \mathcal{F}]$. We then define the subgroup

$$N_G[H] = \{g \in G \mid [g^{-1}Hg] = [H]\},$$

which is equal to the isotropy group of $[H]$ under the G-action we just explained.

Moreover, we define a family of subgroups of $N_G[H]$ by

$$\mathcal{G}[H] = \{K \leq N_G[H] \mid K \in \mathcal{G} \setminus \mathcal{F}, [K] = [H]\} \cup (\mathcal{F} \cap N_G[H]).$$

Note that $\mathcal{G}[H] \subseteq \mathcal{G}$.

Definition 6.2.2 (Equivalence relation on $\mathcal{VC}yc \setminus \mathcal{F}in$)**.** In the case that $\mathcal{F} = \mathcal{F}in$ and $\mathcal{G} = \mathcal{VC}yc$ we choose the equivalence relation defined by

$$V \sim W \Leftrightarrow |V \cap W| = \infty,$$

where $V, W \in \mathcal{VC}yc \setminus \mathcal{F}in$.

Theorem 6.2.3 ([LW12, Theorem 2.3])**.** Let $\mathcal{F} \subseteq \mathcal{G}$ and $\sim$ as above an equivalence relation on $\mathcal{G} \setminus \mathcal{F}$ satisfying (P). Let I be a complete system of representatives $[H]$ of the G-orbits in $[\mathcal{G} \setminus \mathcal{F}]$ under the G-action induced by conjugation. Choose arbitrary $N_G[H]$-CW-models for $E_{\mathcal{F} \cap N_G[H]}(N_G[H])$ and $E_{\mathcal{G}[H]}(N_G[H])$, and an arbitrary G-CW-model for $E_{\mathcal{F}}(G)$. Define a G-CW-complex X by the following cellular G-pushout

$$\begin{tikzcd}
\coprod_{[H] \in I} G \times_{N_G[H]} E_{\mathcal{F} \cap N_G[H]}(N_G[H]) \arrow[r, "i"] \arrow[d, "\coprod_{[H] \in I} \mathrm{id}_G \times_{N_G[H]} f_{[H]}"] & E_{\mathcal{F}}(G) \arrow[d] \\
\coprod_{[H] \in I} G \times_{N_G[H]} E_{\mathcal{G}[H]}(N_G[H]) \arrow[r] & X
\end{tikzcd}$$

such that $f_{[H]}$ is a cellular $N_G[H]$-map for every $[H] \in I$ and i is an inclusion of G-CW-complexes, or such that every map $f_{[H]}$ is an inclusion of $N_G[H]$-CW-complexes for every $[H] \in I$ and i is a cellular G-map. Then X is a model for $E_{\mathcal{G}}(G)$.

Notation 6.2.4. Let $\mathcal{F} \subseteq \mathcal{G}$ be two families of subgroups of G. We say that G satisfies $(\mathrm{M}_{\mathcal{F} \subseteq \mathcal{G}})$ if every subgroup $H \in \mathcal{G} \setminus \mathcal{F}$ is contained in a unique subgroup $H_{\max}$ which is maximal in $\mathcal{G} \setminus \mathcal{F}$, i.e. if $K \in \mathcal{G} \setminus \mathcal{F}$ with $H_{\max} \leq K$, then $K = H_{\max}$.

We say that a group G satisfies $(\mathrm{NM}_{\mathcal{F} \subseteq \mathcal{G}})$ if G satisfies $(\mathrm{M}_{\mathcal{F} \subseteq \mathcal{G}})$ and every maximal subgroup $H_{\max} \in \mathcal{G} \setminus \mathcal{F}$ is a self-normalizing subgroup, i.e. $N_G H_{\max} = H_{\max}$.

Corollary 6.2.5. Let G be a group satisfying $(\mathrm{M}_{\mathcal{F}in\subseteq\mathcal{VC}yc})$. Let $\mathcal{M}$ be a complete system of representatives of the conjugacy classes of maximal infinite virtually cyclic subgroups $V \leq G$. Then $\underline{\underline{E}}G$ can be obtained by the following cellular G-pushout:

$$\begin{tikzcd}
\coprod_{V\in\mathcal{M}} G\times_{N_GV} \underline{E}N_GV \arrow[r, "i"] \arrow[d, "\coprod_{F\in\mathcal{M}} \mathrm{id}_G\times f_V"] & \underline{E}G \arrow[d] \\
\coprod_{V\in\mathcal{M}} G\times_{N_GV} EW_GV \arrow[r] & \underline{\underline{E}}G
\end{tikzcd}$$

Here, EW_GV is viewed as an N_GV-CW-complex via the projection map $N_GV \twoheadrightarrow W_GV = N_GV/V$, the maps starting from the left upper corner are cellular and one of them is an inclusion of G-CW-complexes.

Corollary 6.2.6. Let G be a group satisfying $(\mathrm{NM}_{\mathcal{F}in\subseteq\mathcal{VC}yc})$ and let $\mathcal{M}$ be a complete system of representatives of the conjugacy classes of maximal infinite virtually cyclic subgroups. Then $\underline{\underline{E}}G$ can be obtained via the following cellular G-pushout:

$$\begin{tikzcd}
\coprod_{V\in\mathcal{M}} G\times_V \underline{E}V \arrow[r, "i"] \arrow[d, "\coprod_{V\in\mathcal{M}} p"] & \underline{E}G \arrow[d] \\
\coprod_{V\in\mathcal{M}} G/V \arrow[r] & \underline{\underline{E}}G
\end{tikzcd}$$

Here, i is an inclusion of G-CW-complexes and p is the obvious projection.

Lemma 6.2.7. Let G be a group and let I be a complete set of representatives of conjugacy classes of elements in $[\mathcal{VC}yc\setminus\mathcal{F}in]$ as in the statement of Theorem 6.2.3. If G has $b\mathcal{VC}yc$, then I is finite.

Proof. Let $V_1,\dots,V_n$ be witnesses to $b\mathcal{VC}yc$ for G. We claim that $|I|\leq n$. For each V_i that is infinite, choose some infinite cyclic subgroup $H_i \leq V_i$. If $V \leq G$ is some infinite virtually cyclic subgroup, choose some infinite cyclic subgroup $H \leq V$. By the $b\mathcal{VC}yc$ property there exists some $g\in G$ such that $H^g \leq V_j$ for some j. But then $H^g\cap H_j$ is an infinite group, hence $V^g\sim H_j$. □

In the light of Lemma 6.2.7 one has to be cautious that the converse does not hold. First of all, observe that representatives of $[\mathcal{VC}yc\setminus\mathcal{F}in]$ might as well taken to be infinite cyclic. Then having finitely many conjugacy classes of elements in $[\mathcal{VC}yc\setminus\mathcal{F}in]$ is equivalent to the statement that there are only finitely many commensurability classes of infinite order elements in the group. Note that by Proposition 4.0.16 there exists a torsion-free group with only two commensurability classes that fails to have $b\mathcal{C}yc$.

Definition 6.2.8. For a group G we denote by $\mathrm{Tor}(G)$ the subgroup of G which is generated by all elements of finite order.

As noted in the introduction of this chapter, we have $\pi_1(\underline{B}G) \cong G/\operatorname{Tor}(G)$.

Remark 6.2.9. Note that $\operatorname{Tor}(G)$ is a characteristic subgroup of G. In general, the subgroup $\operatorname{Tor}(G)$ contains elements of infinite order and the quotient $G/\operatorname{Tor}(G)$ is not torsion-free. As an example, consider $G = \mathbb{Z} *_{\mathbb{Z}} D_\infty = \langle g, a, b \mid g^2 = ab, a^2 = 1 = b^2 \rangle$. There is an epimorphism $\pi\colon G \to \mathbb{Z}/2$ by killing a and b. In an amalgamated product, an element of finite order is conjugate to an element lying in one of the factor groups. Hence $\operatorname{Tor}(G) \leq \ker(\pi)$, and thus $g \notin \operatorname{Tor}(G)$ defines an element of order 2 in $G/\operatorname{Tor}(G)$.

Suppose $\alpha\colon G \to Q$ is a group homomorphism. It induces a map $\underline{B}\alpha\colon \underline{B}G \to \underline{B}Q$ and $\pi_1(\underline{B}\alpha)$ can then be identified with the natural map

$$G/\operatorname{Tor}(G) \to Q/\operatorname{Tor}(Q)$$

which is induced by α. Thus $H_1(\underline{B}\alpha)\colon H_1(\underline{B}G) \to H_1(\underline{B}Q)$ can be identified with the abelianization of the above map:

$$H_1(\underline{B}\alpha)\colon (G/\operatorname{Tor}(G))^{\mathrm{ab}} \to (Q/\operatorname{Tor}(Q))^{\mathrm{ab}}$$

Also observe that $(G/\operatorname{Tor}(G))^{\mathrm{ab}} \cong G^{\mathrm{ab}}/\operatorname{Tor}(G^{\mathrm{ab}})$. For an abelian group A, we write $A_f = A/\operatorname{Tor}(A)$ for the torsion-free part.

Lemma 6.2.10. *Let G be a group satisfying $(\mathrm{M}_{\mathcal{F}in\subseteq\mathcal{VC}yc})$, then there is an exact sequence*

$$\begin{aligned} \ldots \to \bigoplus_{V\in\mathcal{M}} H_2(\underline{B}N_GV) \to H_2(\underline{B}G) \oplus \bigoplus_{V\in\mathcal{M}} H_2(BW_GV) \to H_2(\underline{\underline{B}}G) \to \\ \to \bigoplus_{V\in\mathcal{M}} (N_GV)^{\mathrm{ab}}_f \to G^{\mathrm{ab}}_f \oplus \bigoplus_{V\in\mathcal{M}} (W_GV)^{\mathrm{ab}} \to \ldots \end{aligned}$$

Proof. The long exact sequence arises as the Mayer-Vietoris sequence for the pushout obtained from Corollary 6.2.5. □

Lemma 6.2.11. *Let G be a group satisfying $(\mathrm{NM}_{\mathcal{F}in\subset\mathcal{VC}yc})$ and let $\mathcal{M}$ be a complete system of representatives of the conjugacy classes of maximal infinite virtually cyclic subgroups. Then there is an exact sequence*

$$0 \to H_2(\underline{B}G) \to H_2(\underline{\underline{B}}G) \to \bigoplus_{V\in\mathcal{M}} V^{\mathrm{ab}}_f \to G^{\mathrm{ab}}_f \to 0\,.$$

Here, $H_2(\underline{B}G) \to H_2(\underline{\underline{B}}G)$ is induced by the canonical map $\underline{B}G \to \underline{\underline{B}}G$ and the inclusions $V \to G$ for $V \in \mathcal{M}$ induce the other map. For $n > 2$, the canonical map $H_n(\underline{B}G) \to H_n(\underline{\underline{B}}G)$ is an isomorphism. Moreover, note that

$$\bigoplus_{V\in\mathcal{M}} V^{\mathrm{ab}}_f \cong \bigoplus_{V\in\mathcal{M}^o} \mathbb{Z}\,,$$

where $\mathcal{M}^o$ denotes the subset of $\mathcal{M}$ consisting only of orientable infinite virtually cyclic subgroups.

Proof. By taking the G-quotient of the pushout of Corollary 6.2.6 we obtain the following long exact sequence

$$\ldots \to \bigoplus_{V\in\mathcal{M}} H_2(\underline{B}V) \to H_2(\underline{B}G) \to H_2(\underline{\underline{B}}G) \to \bigoplus_{V\in\mathcal{M}} H_1(\underline{B}V) \to H_1(\underline{B}G) \to 0$$

The sequence is exact at the right, since $\underline{\underline{B}}G$ is simply-connected, so $H_1(\underline{\underline{B}}G) = 0$. By Lemma 6.0.2, $H_n(\underline{B}V) = 0$ for all virtually cyclic groups V for $n \geq 2$. ☐

By [LW12, Example 3.6] a hyperbolic group satisfies the condition ($\mathrm{NM}_{\mathcal{F}in\subseteq\mathcal{VC}yc}$). Moreover, by [JL06, Theorem 13] there are infinitely many conjugacy classes of orientable maximal infinite virtually cyclic subgroups. Hence we obtain:

Corollary 6.2.12. Let G be a non-elementary hyperbolic group. Then $H_2(\underline{\underline{B}}G)$ contains a free abelian group of infinite rank.

This was already shown by Juan-Pineda and Leary [JL06, Corollary 16], albeit with a slightly different proof.

6.2.1. Abelian and Poly-$\mathbb{Z}$-Groups

Juan-Pineda and Leary computed in [JL06, Example 3] that $H_2(\underline{\underline{B}}\mathbb{Z}^2)$ and $H_3(\underline{\underline{B}}\mathbb{Z}^2)$ are free abelian of infinite rank using an explicit model that we reviewed in Proposition 1.0.5. Let us consider more generally $G = \mathbb{Z}^n$ for $n \geq 2$. Using Corollary 6.2.5 and the fact that $N_G V = G = \mathbb{Z}^n$, $W_G V = G/V \cong \mathbb{Z}^{n-1}$ for V maximal infinite cyclic, we obtain the following long exact sequence

$$0 \to H_{n+1}(\underline{\underline{B}}G) \to \bigoplus_{V\in\mathcal{M}} H_n(BG) \to H_n(BG) \oplus \bigoplus_{V\in\mathcal{M}} H_n(B\mathbb{Z}^{n-1}) \to \ldots,$$

where $\mathcal{M}$ denotes the set of maximal infinite cyclic subgroups of G. Note that $\mathcal{M}$ is infinite and since $H_n(B\mathbb{Z}^{n-1}) = 0$ and $H_n(B\mathbb{Z}^n) \cong \mathbb{Z}$, it follows that $H_{n+1}(\underline{\underline{B}}G)$ is a free abelian group of infinite rank. This also implies that $\underline{\underline{\mathrm{gd}}}\,(\mathbb{Z}^n) \geq n+1$. In fact, by [LW12, Example 5.21] we have $\underline{\underline{\mathrm{gd}}}\,(\mathbb{Z}^n) = n+1$. For G finitely generated abelian we have $G \cong \mathbb{Z}^n \oplus T$ with T finite abelian. It follows that $H_{n+1}(\underline{\underline{B}}G)$ contains a free abelian subgroup of infinite rank as a direct summand whenever G is not virtually cyclic.

Lemma 6.2.13. Let $G = \mathbb{Z}^n$ with $n \geq 2$. Then $H_2(\underline{\underline{B}}G)$ is a free abelian group of infinite rank.

Proof. Of course, G is torsion-free and satisfies $\mathrm{M}_{\mathcal{F}in\subseteq\mathcal{VC}yc}$. By Corollary 6.2.5 we can obtain $\underline{\underline{E}}G$ by the following pushout of G-CW-complexes:

$$\begin{tikzcd}
\coprod_{V\in\mathcal{M}} G \times_{N_G V} EN_G V \arrow[r, "i"] \arrow[d, "\coprod_{V\in\mathcal{M}} \mathrm{id}_G \times_{N_G V} f_V"] & EG \arrow[d] \\
\coprod_{V\in\mathcal{M}} G \times_{N_G V} EW_G V \arrow[r] & \underline{\underline{E}}G
\end{tikzcd}$$

Taking the quotient by G and using that $N_G V = G$ and $W_G V = G/V$, we get:

$$\begin{tikzcd}
\coprod_{V\in\mathcal{M}} BG \arrow[r, "i/G"] \arrow[d, "\coprod_{V\in\mathcal{M}} g_V"] & BG \arrow[d] \\
\coprod_{V\in\mathcal{M}} B(G/V) \arrow[r] & \underline{\underline{B}}G
\end{tikzcd}$$

The corresponding Mayer-Vietoris sequence yields

$$\ldots \to H_2(\underline{\underline{B}}G) \to \bigoplus_{V\in\mathcal{M}} H_1(BG) \to H_1(BG) \oplus \bigoplus_{V\in\mathcal{M}} H_1(B(G/V)) \to H_1(\underline{\underline{B}}G) = 0$$

We let

$$\theta_G \colon \bigoplus_{V\in\mathcal{M}} G \to G \oplus \bigoplus_{V\in\mathcal{M}} G/V$$

be the map that is induced by the sum of the identity id_G and the projections $G \to G/V$ on each summand. Then the long exact sequence yields that $H_2(\underline{\underline{B}}G)$ surjects onto $\ker(\theta_G)$. One computes that $\ker(\theta_G) = \{(g_V)_{V\in\mathcal{M}} \in \bigoplus_{V\in\mathcal{M}} V \mid \sum_{V\in\mathcal{M}} g_V = 0\}$. As $\mathcal{M}$ is infinite, it follows that $\ker(\theta_G)$ is of infinite rank. Since it is free abelian, $H_2(\underline{\underline{B}}G)$ contains a free abelian group of infinite rank. Since the kernel of the map $H_2(\underline{\underline{B}}G) \to \bigoplus_{V\in\mathcal{M}} H_1(BG)$ appearing in the Mayer-Vietoris sequence is free abelian as well, it follows that $H_2(\underline{\underline{B}}G)$ is free abelian of infinite rank. $\square$

Let us generalize the previous result to not necessarily finitely generated abelian groups:

Proposition 6.2.14. Let G be an abelian group that is not locally virtually cyclic. Then $H_2(\underline{\underline{B}}G)$ is not finitely generated.

Proof. First note that an abelian group is locally virtually cyclic if and only if it does not contain a copy of $\mathbb{Z}^2$ as a subgroup. In particular, it follows that the complete set I of representatives of elements in $[\mathcal{VC}yc \setminus \mathcal{F}in]$ is infinite. Since G is abelian we have $N_G[V] = G$ for any virtually cyclic V. By Theorem 6.2.3 there exists a G-pushout

$$\begin{tikzcd}
\coprod_{V\in I} G \times_G \underline{E}G \arrow[r, "i"] \arrow[d, "\coprod_{V\in I} \mathrm{id}_G \times_G f_{[V]}"] & \underline{E}G \arrow[d] \\
\coprod_{V\in I} G \times E_{\mathcal{VC}yc[V]}G \arrow[r] & \underline{\underline{E}}G
\end{tikzcd}$$

Here, $\mathcal{VC}yc[V] = \{K \leq G \mid K \in \mathcal{VC}yc(G) \text{ and } |K \cap V| = \infty\} \cup \mathcal{F}in$. After taking the quotient by G we obtain the following part of the Mayer-Vietoris sequence:

$$\ldots \to H_2(\underline{\underline{B}}G) \to \bigoplus_{V\in I} H_1(\underline{B}G) \to H_1(\underline{B}G) \oplus \bigoplus_{V\in I} H_1(B_{\mathcal{VC}yc[V]}G) \to H_1(\underline{\underline{B}}G) = 0$$

As before, let $G_f = G/\operatorname{Tor}(G)$ denote the torsion-free quotient of G. Now the last non-trivial map in the long exact sequence can be identified with

$$\theta\colon \bigoplus_{V\in I} G_f \to G_f \oplus \bigoplus_{V\in I} G_f/N_V$$

where $N_V = \langle K \mid K \text{ cyclic and } |K\cap V| = \infty\rangle \leq G_f$ and given by the sum of id_G and the canonical projections. Then $\ker(\theta) = \{(g_V)_{V\in I} \in \bigoplus_{V\in I} N_V \mid \sum_{V\in I} g_V = 0\}$ which is not finitely generated. Then $H_2(\underline{\underline{B}}G)$, which surjects onto $\ker(\theta)$ cannot be finitely generated. ☐

We see in particular that an abelian group G has a contractible classifying space $\underline{\underline{B}}G$ if and only if it is locally virtually cyclic. It is also worthwhile to note that a torsion-free locally cyclic group is isomorphic to a subgroup of the rational numbers $\mathbb{Q}$, see e.g [Kur55, Chapter VIII, Section 30].

We call a group G *poly-$\mathbb{Z}$* if there exists a chain of subgroups $1 = G_0 \leq G_1 \leq G_2 \leq \ldots \leq G_n = G$ such that $G_i \trianglelefteq G_{i+1}$ and G_{i+1}/G_i is infinite cyclic for all $i = 0, 1, \ldots, n-1$. Note that poly-$\mathbb{Z}$ groups do not necessarily satisfy the condition $\mathrm{M}_{\mathcal{F}in\subseteq\mathcal{VC}yc}$. An example is already provided by the non-trivial extension $\mathbb{Z} \rtimes \mathbb{Z}$, see [LW12, Example 3.7]. For a poly-$\mathbb{Z}$ group G we know that the cohomological dimension $\mathrm{cd}(G)$ is given by $\mathrm{cd}(G) = \max\{i \mid H_i(G;\mathbb{Z}/2) \neq 0\}$, see e.g. [Lüc05, Example 5.26].

Proposition 6.2.15. Let G be a poly-$\mathbb{Z}$ group that is not infinite cyclic. Then there is some n such that $H_n(\underline{\underline{B}}G;\mathbb{Z}/2)$ is not finitely generated.

Proof. By [Lüc05, Example 5.26] we know that there exists a finite model for $\underline{E}H$ for any virtually poly-$\mathbb{Z}$ group H. In [LW12, Theorem 5.13] a model of minimal dimension for $\underline{\underline{E}}G$ is being constructed. In the course of this proof one obtains the following pushout, where the index set I runs over certain infinite cyclic subgroups of G:

$$\begin{tikzcd}
\coprod_{C\in I} G\times_{N_GC} \underline{E}N_GC \arrow[r, "i"] \arrow[d, "\coprod_{C\in I} \mathrm{id}_G \times_{N_GC} f_C"] & \underline{E}G \arrow[d] \\
\coprod_{C\in I} G\times_{N_GC} \underline{E}W_GC \arrow[r] & \underline{\underline{E}}G
\end{tikzcd}$$

Here, i is an inclusion of G-CW complexes and f_C is a cellular N_GC-map for every $C \in I$. Observe that I has to be infinite. Otherwise, we would obtain a classifying space $\underline{\underline{E}}G$ of finite type since N_GC and W_GC are virtually poly-$\mathbb{Z}$. But this is impossible by Theorem 1.2.15 since G is solvable but not virtually cyclic. By taking the quotient by G one obtains the following pushout:

$$\begin{tikzcd}
\coprod_{C\in I} \underline{B}N_GC \arrow[r] \arrow[d] & \underline{B}G \arrow[d] \\
\coprod_{C\in I} \underline{B}W_GC \arrow[r] & \underline{\underline{B}}G
\end{tikzcd}$$

Of course, as G is torsion-free, we have $\underline{B}G = BG$ and $\underline{B}N_GC = BN_GC$. From the pushout, we obtain the following Mayer-Vietoris sequence, suppressing the coefficient group $\mathbb{Z}/2$ in the notation:

$$\ldots \to H_{k+1}(\underline{\underline{B}}G) \to H_k\left(\coprod_{C\in I} BN_GC\right) \to H_k(BG) \oplus H_k\left(\coprod_{C\in I} \underline{B}W_GC\right) \to \ldots$$

We also observe that $\mathrm{gd}(G) = \mathrm{vcd}(G) = \mathrm{cd}(G)$, $\mathrm{gd}(N_GC) = \mathrm{cd}(N_GC)$ and $\underline{\mathrm{gd}}\,(W_GC) = \mathrm{cd}(N_GC) - 1$, the proof of which can be found in the proof of [LW12, Theorem 5.13] as well. In particular, we see that the homology groups of all spaces appearing in the pushout, will vanish in large enough degrees. Now, let k be the largest integer such that there are infinitely many $C \in I$ with $\mathrm{gd}(N_GC) = k$ and with only finitely many $C \in I$ with $\mathrm{gd}(N_GC) = k+1$. Then there are only finitely many $C \in I$ with $\mathrm{gd}(\underline{B}W_GC) \leq k$. Observe that $H_k(N_GC;\mathbb{Z}/2) \neq 0$ for infinitely many C. As $H_k(BG)$ is finite, the above exact sequence shows that $H_{k+1}(\underline{\underline{B}}G)$ cannot be finitely generated. $\square$

As a corollary we obtain an affirmative answer to Question 6.0.1 for the class of poly-$\mathbb{Z}$-groups.

7. The Farrell-Jones Conjecture for Infinite Products and Minimal Families

The Farrell-Jones conjecture for algebraic K-theory predicts that the so-called assembly map

$$\mathcal{H}_n^G(\underline{\underline{E}}G, \mathbf{K}) \to \mathcal{H}_n^G(\{\mathrm{pt}\}, \mathbf{K}) \cong K_n(RG)$$

induced by the projection $\underline{\underline{E}}G \to \{\mathrm{pt}\}$ is an isomorphism for all groups G and all commutative rings R. Here, $\mathcal{H}_*^G$ is an equivariant homology theory such that $\mathcal{H}_n^G(\{\mathrm{pt}\}, \mathbf{K}) \cong K_n(RG)$ where $\mathbf{K}$ is a spectrum associated to the algebraic K-theory of R and RG is the group ring. The Farrell-Jones conjecture enjoys multiple useful inheritance properties. For example, if G satisfies the conjecture, then any subgroup of G satisfies it as well. One also knows that if groups G_1 and G_2 satisfy the conjecture, then so does the direct product $G_1 \times G_2$. It is an interesting and open problem whether the Farrell-Jones conjecture also has an inheritance property for infinite products of groups. This property would be quite strong. For example, the Farrell-Jones conjecture is trivially true for finite groups, since $\underline{\underline{E}}G = \{\mathrm{pt}\}$ for G finite, and thus it would hold for arbitrary products of finite groups. As the conjecture has the subgroup inheritance property, it would follow that the conjecture holds for all residually finite groups.

In the formulation of the Farrell-Jones conjecture one could also replace the family of virtually cyclic subgroups by another family $\mathcal{F}$ of subgroups of G and study the induced map

$$\mathcal{H}_n^G(E_{\mathcal{F}}G, \mathbf{K}) \to \mathcal{H}_n^G(\{\mathrm{pt}\}, \mathbf{K}).$$

This more general assembly map is obviously an isomorphism if $\mathcal{F} = \mathcal{A}ll$, the family of all subgroups of G, since then $E_{\mathcal{F}}G = \{\mathrm{pt}\}$. This motivates the question, popularized by Wolfgang Lück, whether for any group G there exists a smallest family $\mathcal{F}$ with respect to which the Farrell-Jones conjecture in this more general sense holds.

We will address the relation between the inheritance property for infinite products and the existence of minimal families in the context of the so-called fibered isomorphism conjectures. The fibered isomorphism conjecture is a framework for conjectures like the Farrell-Jones conjecture that has a certain inheritance property already built in. It will turn out that the two mentioned properties, suitably formulated, are actually equivalent in this context.

7.1. The Fibered Isomorphism Conjecture

In the following we want to recall the so-called fibered isomorphism conjecture, FIC for short, for an equivariant homology theory $\mathcal{H}_*^?$. A convenient definition is given in [BLR08], which we shall adapt. We say that G satisfies the fibered isomorphism conjecture for $\mathcal{H}_*^?$ relative to the family $\mathcal{F}$ of subgroups of G if for any group homomorphism $\varphi\colon K \to G$ the induced map

$$\mathcal{H}_*^K(E_{\varphi^*\mathcal{F}}K) \to \mathcal{H}_*^K(\{\mathrm{pt}\})$$

is an isomorphism. Here, $\varphi^*\mathcal{F} = \{H \leq K \mid \varphi(H) \in \mathcal{F}\}$ is a family of subgroups of K.

The fibered isomorphism conjecture automatically enjoys useful inheritance properties, like stability under taking subgroups and the transitivity principle, see [BLR08, Lemma 1.5, Theorem 1.4].

7.2. Equivalence of the Product and Intersection Property

We now formulate the properties whose equivalence we establish below.

(P): For any set of groups and associated families of subgroups $(G_i, \mathcal{F}_i)_{i\in I}$ such that each $(G_i, \mathcal{F}_i)$ satisfies the FIC, the group $\prod_{i\in I} G_i$ satisfies the FIC relative to the family $\prod_{i\in I} \mathcal{F}_i \coloneqq \{H \leq \prod_{i\in I} H_i \mid H_i \in \mathcal{F}_i\}$.

(I): For any group G and families of subgroups $(\mathcal{F}_i)_{i\in I}$ of G such that $(G, \mathcal{F}_i)$ satisfies the FIC for any $i \in I$, the group G satisfies the FIC relative to the family $\bigcap_{i\in I} \mathcal{F}_i$.

Note that in the context of the Farrell-Jones conjecture a proof of property **(P)** would not immediately imply that the Farrell-Jones conjecture holds for infinite products of finite groups, since the product family would coincide with the family of all subgroups. However, if **(P)** holds for the Farrell-Jones conjecture and $(G_i)_{i\in I}$ is a family of torsion-free groups, then also $\prod_{i\in I} G_i$ would satisfies the Farrell-Jones conjecture (with respect to the family of virtually cyclic groups). This follows from the fact that the Farrell-Jones conjecture holds for abelian groups and the transitivity principle [BLR08, Theorem 1.4].

Theorem 7.2.1. The product property **(P)** and the intersection property **(I)** are equivalent.

Proof. **(P)** $\Rightarrow$ **(I)**: Let G be a group and let $(\mathcal{F}_i)_{i\in I}$ be families of subgroups of G such that $(G, \mathcal{F}_i)$ satisfies the FIC for any $i \in I$. By **(P)** we know that $(\prod_{i\in I} G, \prod_{i\in I} \mathcal{F}_i)$ satisfies the FIC. Let $\Delta\colon G \to \prod_{i\in I} G$ denote the diagonal map. By the fibered property, we then know that G satisfies the FIC relative to the family $\Delta^*(\prod_{i\in I} \mathcal{F}_i)$. Now observe that $\Delta^*(\prod_{i\in I} \mathcal{F}_i) = \bigcap_{i\in I} \mathcal{F}_i$ by the following calculation:

$$\begin{aligned} H \in \Delta^*\left(\prod_{i\in I} \mathcal{F}_i\right) &\Leftrightarrow \Delta(H) \in \prod_{i\in I} \mathcal{F}_i \\ &\Leftrightarrow \prod_{i\in I} H = \Delta(H) \leq \prod_{i\in I} H_i \text{ for some } H_i \in \mathcal{F}_i \\ &\Leftrightarrow H \leq H_i \text{ for all } i \in I \text{ and some } H_i \in \mathcal{F}_i \\ &\Leftrightarrow H \in \bigcap_{i\in I} \mathcal{F}_i \end{aligned}$$

(I) $\Rightarrow$ **(P)**: Let $(G_i, \mathcal{F}_i)_{i\in I}$ be a family of groups and associated families of subgroups. Suppose that each $(G_i, \mathcal{F}_i)$ satisfies the FIC. Now consider the canonical projection maps

$p_j\colon \prod_{i\in I} G_i \to G_j$. Using fiberedness we conclude that $\prod_{i\in I} G_i$ satisfies the FIC relative to the family $p_j^*(\mathcal{F}_j)$. Using property **(I)**, it follows that $\prod_{i\in I} G_i$ satisfies the FIC relative to $\bigcap_{i\in I} p_i^*(\mathcal{F}_i)$. We have $\bigcap_{i\in I} p_i^*(\mathcal{F}_i) = \prod_{i\in I} \mathcal{F}_i$ by the following:

$$\begin{aligned}
H \in \prod_{i\in I} \mathcal{F}_i &\Leftrightarrow H \leq \prod_{i\in I} H_i \text{ for some } H_i \in \mathcal{F}_i \\
&\Leftrightarrow p_i(H) \leq H_i \in \mathcal{F}_i \text{ for all } i \in I \\
&\Leftrightarrow p_i(H) \in \mathcal{F}_i \text{ for all } i \in I \\
&\Leftrightarrow H \in p_i^*(\mathcal{F}_i) \text{ for all } i \in I \\
&\Leftrightarrow H \in \bigcap_{i\in I} p_i^*(\mathcal{F}_i)
\end{aligned}$$

□

A. Spectra of Finite Simple Groups

In this appendix we shall provide the arguments that are necessary to show that finite groups with at most two conjugacy classes of maximal cyclic subgroups are solvable, see also Section 5.2.3.1. The arguments involve a careful analysis of the element orders in finite simple groups.

Definition A.0.1. For a finite group G we define the *spectrum* $\omega(G)$ to be the set of element orders in G and we let $\mu(G)$ be the subset of $\omega(G)$ consisting of the maximal elements of $\omega(G)$ with respect to the divisibility relation. We call $\mu(G)$ the *reduced spectrum* of G.

Obviously the spectrum $\omega(G)$ is determined by the reduced spectrum $\mu(G)$. It is an interesting question for which groups the spectrum and the order of the group determine the isomorphism class of the group. For example, In [VGM09] it was proven that a finite simple group G and a finite group H such that $|G| = |H|$ and $\omega(G) = \omega(H)$ are already isomorphic. The spectra of finite simple groups have been investigated thoroughly, for example in [KS09] the maximum element orders of finite groups of Lie type over a field of characteristic $p \neq 2$ have been determined. We shall prove using the classification of the finite simple groups:

Theorem A.0.2. A non-cyclic finite simple group G has $|\mu(G)| \geq 3$.

From this we can immediately deduce:

Corollary A.0.3. A finite simple group G is covered by two cyclic subgroups up to automorphism if and only if G is cyclic of prime order.

Recall that Bertrand's postulate asserts that for any $n > 1$ there exists a prime p with $n < p < 2n$. Using a strengthened version of this postulate we can now estimate the size of the reduced spectrum of alternating groups.

n	$\mu(A_n)$	$\delta(A_n)$
4	2, 3	2
5	2, 3, 5	3
6	3, 4, 5	3
7	4, 5, 6, 7	5
8	4, 6, 7, 15	6
9	7, 9, 10, 12, 15	7

Table A.1.: Spectra and number of automorphic cyclic subgroups for alternating groups

Proposition A.0.4. We have $\mu(A_n) \geq 3$ for all $n \geq 5$. In fact, $\mu(A_n) \to \infty$ as $n \to \infty$.

Proof. By [Pas92, p. 869] there are at least three primes p with $n/2 < p \leq n$ for $n \geq 17$. The same holds for $n = 13$ and $n = 14$. In these cases there are elements of distinct prime orders p_1, p_2, p_3 in A_n, where $n/2 < p_i \leq n$. Using the cycle decomposition of elements in A_n one sees that the corresponding maximal elements in $\mu(A_n)$ are distinct since $p_i p_j \geq p_i + p_j > n$. The other cases can be checked by a direct computation, see also Table A.1. The second claim is implied by the prime number theorem. □

Before we can prove Theorem A.0.2 we need to collect a couple of elementary number-theoretic lemmas. For p a prime number and $n \in \mathbb{N}$, we write $(n)_p$ for the largest power of p dividing n. Also recall that we denote by (n, m) resp. $[n, m]$ the greatest common divisor resp. the least common multiple of two natural numbers n, m.

Lemma A.0.5 ([Zav04, Lemma 6 (iii)])**.** For $q, n, m \in \mathbb{N}$ $(q > 1)$ the following formulas hold:

$$(q^n - 1, q^m - 1) = q^{(n,m)} - 1$$

$$(q^n + 1, q^m + 1) = \begin{cases} q^{(n,m)} + 1, & \text{if } (n)_2 = (m)_2 \\ (2, q+1), & \text{if } (n)_2 \neq (m)_2 \end{cases}$$

$$(q^n - 1, q^m + 1) = \begin{cases} q^{(n,m)} + 1, & \text{if } (n)_2 > (m)_2 \\ (2, q+1), & \text{if } (n)_2 \leq (m)_2 \end{cases}$$

Lemma A.0.6. For any $q \in \mathbb{N}$ and $n \in \mathbb{N}$ even we have

$$\left(q^{2n} - 1, q^{2n} - q^n + 1\right) = 1\,.$$

Proof. Using Euclid's algorithm we obtain that

$$\left(q^{2n} - 1, q^{2n} - q^n + 1\right) = (3, q^n + 1)$$

Now observe that for $n = 2k$ we get that $q^n + 1 \equiv (q \mod 3)^2 + 1$ which is congruent to 1 or 2 modulo 3. Hence $(3, q^n + 1) = 1$. □

Lemma A.0.7. For n odd an $q \geq 2$ we have

$$\left(\frac{q^n - 1}{q - 1}, \frac{q^n + 1}{q + 1}\right) = 1\,.$$

Proof. Observe that

$$\frac{q^n - 1}{q - 1} - \frac{q^n + 1}{q + 1} = 2 \cdot (q^{n-2} + q^{n-4} + \ldots + q)$$

As $({}^{q^n-1}/_{q-1}, 2) = 1$, it follows that

$$\begin{aligned}\left(\frac{q^n-1}{q-1}, \frac{q^n+1}{q+1}\right) &= \left(\frac{q^n-1}{q-1}, 2\cdot(q^{n-2}+q^{n-4}+\ldots+q)\right)\\ &= \left(\frac{q^n-1}{q-1}, (q^{n-2}+q^{n-4}+\ldots+q)\right)\\ &= \left(q^{n-1}+q^{n-3}+\ldots+q^2+1, q^{n-2}+q^{n-4}+\ldots+q\right)\\ &= \left(1, q^{n-2}+\ldots+q\right)\\ &= 1\,.\end{aligned}$$

□

Lemma A.0.8. Let $a \in \mathbb{N}$ with $a \geq 2$ and let $n \in \mathbb{N}$ and let d be a divisor of n.

(1) We always have
$$\left(\frac{a^n-1}{a^d-1}, a-1\right) = ({}^{n}/_{d}, a-1)\ .$$

(2) We have
$$\left(\frac{a^n-1}{a^d-1}, a+1\right) = \begin{cases} 1 & \text{if } n \text{ is odd}\\ a+1 & \text{if } n \text{ is even and } d \text{ is odd}\\ ({}^{n}/_{d}, a+1) & \text{if } n \text{ and } d \text{ are even}\end{cases}$$

(3) If n and ${}^{n}/_{d}$ are even, then
$$\left(\frac{a^n-1}{a^d+1}, a+1\right) = \begin{cases} a+1 & \text{if } d \text{ is even}\\ ({}^{n}/_{d}, a+1) & \text{if } d \text{ is odd}\end{cases}$$

(4) If n is odd, then
$$\left(\frac{a^n+1}{a^d+1}, a+1\right) = ({}^{n}/_{d}, a+1)\ .$$

Proof. Let $\mu = {}^{n}/_{d}$ and $z = a^d$. For proving (1) we let $b = a-1$ and note that ${}^{a^n-1}/_{a^d-1} = {}^{z^\mu-1}/_{z-1} = z^{\mu-1}+\ldots+z+1 = (b+1)^{d(\mu-1)}+\ldots+(b+1)^d+1$.

Thus $({}^{a^n-1}/_{a^d-1}, a-1) = \left((b+1)^{d(\mu-1)}+\ldots+(b+1)^d+1, b\right) = (\mu, b) = ({}^{n}/_{d}, a-1)$ as claimed.

For part (2) we let $b = a+1$, so $z = a^d = (b-1)^d$. Then $(z^{\mu-1}+\ldots+z+1, b) = \left((-1)^{d(\mu-1)}+\ldots+(-1)^d+1, b\right)$. If d is even, then $(-1)^{d(\mu-1)}+\ldots+(-1)^d+1 = \mu$. If d is odd and n is even, then $(-1)^{d(\mu-1)}+\ldots+(-1)^d+1 = 0$. If d and n are odd, then $(-1)^{d(\mu-1)}+\ldots+(-1)^d+1 = 1$.

For part (3) we can write ${}^{a^n-1}/_{a^d-1} = {}^{z^\mu-1}/_{z-1}$ as before. Note that we assumed μ to be even, hence
$$\frac{z^\mu-1}{z-1} = -\frac{(-z)^\mu-1}{(-z)-1} = -\left((-z)^{\mu-1}+\ldots+(-z)+1\right)\ .$$

If d is even we have $z = a^d \equiv 1 \mod (a+1)$, which implies that ${}^{z^\mu-1}/{}_{z-1} \equiv 0 \mod (a+1)$ as μ is even. If d is odd, then $z \equiv -1 \mod (a+1)$ and we obtain $({}^{z^\mu-1}/{}_{z-1}, a+1) = ({}^n/{}_d, a+1)$.

For (4) note that μ is odd, since n is odd. Hence

$$\frac{a^n+1}{a^d+1} = \frac{z^\mu+1}{z+1} = \frac{(-z)^\mu-1}{(-z)-1} = (-z)^{\mu-1} + \ldots + (-z) + 1$$

Also d is odd, thus $z = a^d \equiv (-1)^d \equiv -1 \mod (a+1)$. So $(-z)^{\mu-1} + \ldots + (-z) + 1 \equiv \mu \mod (a+1)$ and the claim follows. $\square$

Lemma A.0.9. Let $a \in \mathbb{N}$ with $a \geq 2$ and let $n, m \geq 1$, then:

(1)
$$\left(\frac{a^n-1}{a-1}, a^m-1\right) = \frac{a^{(n,m)}-1}{a-1} \cdot \left(\frac{n}{(n,m)}, a-1\right)$$

(2) Suppose n is even. Then

$$\left(\frac{a^n-1}{a+1}, a^m-1\right) = \begin{cases} \frac{a^{(n,m)}-1}{a+1} \cdot \left(\frac{n}{(n,m)}, a+1\right) & \text{if } m \text{ is even} \\ a^{(n,m)}-1 & \text{if } m \text{ is odd} \end{cases}$$

(3) Suppose n is even. Then

$$\left(\frac{a^n-1}{a+1}, a^m+1\right) = \begin{cases} (2, a+1) & \text{if } (n)_2 \leq (m)_2 \\ \frac{a^{(n,m)}+1}{a+1} \cdot \left(\frac{n}{(n,m)}, a+1\right) & \text{if } (n)_2 > (m)_2 = 0 \\ a^{(n,m)}+1 & \text{if } (n)_2 > (m)_2 > 0 \end{cases}$$

(4) If n is odd, then

$$\left(\frac{a^n+1}{a+1}, a^m-1\right) = \begin{cases} \frac{a^{(n,m)}+1}{a+1} \cdot \left(\frac{n}{(n,m)}, a+1\right) & \text{if } m \text{ is even} \\ 1 & \text{if } m \text{ is odd} \end{cases}$$

(5) If n is odd, then

$$\left(\frac{a^n+1}{a+1}, a^m+1\right) = \begin{cases} \frac{a^{(n,m)}+1}{a+1} \cdot \left(\frac{n}{(n,m)}, a+1\right) & \text{if } m \text{ is odd} \\ 1 & \text{if } m \text{ is even} \end{cases}$$

Proof. Let $d = (n,m)$, $z = a^d$, $\lambda = {}^m/{}_d$ and $\mu = {}^n/{}_d$. Then $a^n - 1 = (z-1) \cdot ({}^{z^\mu-1}/{}_{z-1})$ and $a^m - 1 = (z-1) \cdot ({}^{z^\lambda-1}/{}_{z-1})$. Thus

$$\left(\frac{a^n-1}{a-1}, a^m-1\right) = \frac{z-1}{a-1}\left(\frac{z^\mu-1}{z-1}, (a-1)\frac{z^\lambda-1}{z-1}\right)$$

Note that $\left({}^{z^\mu-1}/{}_{z-1}, {}^{z^\lambda-1}/{}_{z-1}\right) = {}^{z^{(\mu,\lambda)}-1}/{}_{z-1} = 1$ since $(\mu,\lambda) = 1$. Hence we are left to compute $({}^{z^\mu-1}/{}_{z-1}, a-1) = ({}^{a^n-1}/{}_{a^d-1}, a-1)$ which is provided by Lemma A.0.8. Hence

(1) follows. For (2) we first consider the case that d is even. Then $a+1$ divides $a^d-1=z-1$. We can then write

$$\frac{a^n-1}{a+1}=\frac{z-1}{a+1}\cdot\frac{z^\mu-1}{z-1}$$

and $a^m-1=({}^{z-1}\!/\!_{a+1})\cdot(a+1)\cdot({}^{z^\lambda-1}\!/\!_{z-1})$. Thus we obtain

$$\begin{aligned}\left(\frac{a^n-1}{a+1},a^m-1\right)&=\frac{z-1}{a+1}\left(\frac{z^\mu-1}{z-1},(a+1)\cdot\frac{z^\lambda-1}{z-1}\right)\\&=\frac{z-1}{a+1}\cdot\left(\frac{z^\mu-1}{z-1},a+1\right)\end{aligned}$$

And $({}^{z^\mu-1}\!/\!_{z-1},a+1)=({}^{a^n-1}\!/\!_{a^d-1},a+1)=(a+1,{}^{n}\!/\!_{d})$ by Lemma A.0.8.

If d is odd, then by Lemma A.0.8 we know that $a+1$ divides ${}^{z^\mu-1}\!/\!_{z-1}$, so that we can write

$$\frac{a^n-1}{a+1}=(z-1)\cdot\frac{z^\mu-1}{(z-1)(a+1)}$$

and $a^m-1=(z-1)\cdot({}^{z^\lambda-1}\!/\!_{z-1})$. Hence

$$\left(\frac{a^n-1}{a+1},a^m-1\right)=(z-1)\cdot\left(\frac{z^\mu-1}{(z-1)(a+1)},\frac{z^\lambda-1}{z-1}\right)$$

But the second factor equals one, as ${}^{z^\mu-1}\!/\!_{z-1}$ and ${}^{z^\lambda-1}\!/\!_{z-1}$ are already coprime.

For (3) first consider the case that $(n)_2\le(m)_2$. In this case we know by Lemma A.0.5 that $(a^n-1,a^m+1)=(2,a+1)$. If a is even, then certainly also $({}^{a^n-1}\!/\!_{a+1},a^m+1)=1=(2,a+1)$. So assume that a is odd. Since n is even we have

$$\frac{a^n-1}{a+1}=-\frac{(-a)^n-1}{(-a)-1}=-\left((-a)^{n-1}+\ldots+(-a)+1\right).$$

Thus we have a sum of n odd terms, thus ${}^{a^n-1}\!/\!_{a+1}$ is even. It follows that $({}^{a^n-1}\!/\!_{a+1},a^m+1)=2=(2,a+1)$.

So suppose now that $(n)_2>(m)_2=0$, in other words n is even and m is odd. Then $(a^n-1,a^m+1)=a^{(n,m)}+1$ and (n,m) is odd, so that $a+1$ divides $a^{(n,m)}+1$. We obtain

$$\begin{aligned}\left(\frac{a^n-1}{a+1},a^m+1\right)&=\frac{a^{(n,m)}+1}{a+1}\cdot\left(\frac{a^n-1}{a^{(n,m)}+1},(a+1)\cdot\frac{a^m+1}{a^{(n,m)}+1}\right)\\&=\frac{a^{(n,m)}+1}{a+1}\cdot\left(\frac{a^n-1}{a^{(n,m)}+1},a+1\right)\\&=\frac{a^{(n,m)}+1}{a+1}\cdot\left(\frac{n}{(n,m)},a+1\right),\end{aligned}$$

where in the last line we used Lemma A.0.8.

For the last claim assume that $(n)_2>(m)_2>0$. Observe that $d=(n,m)$ is even, hence $\left(a+1,a^d+1\right)=(2,a+1)$. Moreover, we still have that $(a^n-1,a^m+1)=a^d+1$. If a

is even, then $\Big(a+1, a^d+1\Big) = 1$ and so $(a+1)(a^d+1)$ divides a^n-1. If a is odd, then it follows that ${a^n-1}/{a^d+1}$ is even using that ${n}/{d}$ is even since we assume that $(n)_2 > (m)_2$. Hence also in this case $(a+1)(a^d+1)$ divides a^n-1. We can then compute

$$\begin{aligned}\left(\frac{a^n-1}{a+1}, a^m+1\right) &= (a^d+1)\cdot\left(\frac{a^n-1}{(a+1)(a^d+1)}, \frac{a^m+1}{a^d+1}\right)\\ &= a^d+1\end{aligned}$$

For (4) we first consider the case that m is odd. We know that $(a^n+1, a^m-1) = (2, a+1)$. If a is even, then $(a^n+1, a^m-1) = 1 = ({a^n+1}/{a+1}, a^m-1)$. If a is odd we know that

$$\frac{a^n+1}{a+1} = \frac{(-a)^n-1}{(-a)-1} = (-a)^{n-1} + \ldots + (-a) + 1$$

is odd as well since n is odd. Thus also in this case $({a^n+1}/{a+1}, a^m-1) = 1$. Suppose now that m is even, then $(a^n+1, a^m-1) = a^d+1$ where $d = (n,m)$. Also d is odd and thus $a+1$ divides a^d+1. So

$$\begin{aligned}\left(\frac{a^n+1}{a+1}, a^m-1\right) &= \frac{a^d+1}{a+1}\cdot\left(\frac{a^n+1}{a^d+1}, (a+1)\cdot\frac{a^m-1}{a^d+1}\right)\\ &= \frac{a^d+1}{a+1}\cdot\left(\frac{a^n+1}{a^d+1}, a+1\right)\\ &= \frac{a^d+1}{a+1}\cdot\left(\frac{n}{d}, a+1\right)\end{aligned}$$

by Lemma A.0.8.

For part (5), if m is even, then $(a^n+1, a^m+1) = (2, a+1)$. As in (4) we see that ${a^n+1}/{a+1}$ is odd if a is odd and thus $({a^n+1}/{a+1}, a^m+1) = 1$. If m is odd, so that $(a^n+1, a^m+1) = a^d+1$ we obtain

$$\begin{aligned}\left(\frac{a^n+1}{a+1}, a^m+1\right) &= \frac{a^d+1}{a+1}\cdot\left(\frac{a^n+1}{a^d+1}, (a+1)\cdot\frac{a^m+1}{a^d+1}\right)\\ &= \frac{a^d+1}{a+1}\cdot\left(\frac{a^n+1}{a^d+1}, a+1\right)\\ &= \frac{a^d+1}{a+1}\cdot\left(\frac{n}{d}, a+1\right)\end{aligned}$$

as in (4).

□

Lemma A.0.10. Let $q \in \mathbb{N}$. If q is odd an n is even, then $({q^n+1}/{2}, 2) = 1$. If q is odd and n is odd, then $(q^n+1)_{(2)} = (q+1)_{(2)}$. Moreover, for any $q \in \mathbb{N}$ and and any $n, m \in \mathbb{N}$ we have $(q^n+1)_{(2)} = (q^m+1)_{(2)}$ whenever $m \equiv n \mod 2$.

Proof. If n is even and q is odd, say $q = 2k+1$, then $q^n = 1+\binom{n}{1}(2k)+\binom{n}{n}(2k)^2+\ldots+\binom{n}{n}(2k)^n$. Hence ${q^n+1}/{2} \equiv 1 + n\cdot k \equiv 1 \mod 2$ since n is even. If q is odd and n is odd, then it is easy to see that $({}^{q^n+1}/_{q+1}, 2) = 1$, so $(q^n + 1)_{(2)} = (q + 1)_{(2)}$. If q is even, then certainly $(q^n + 1)_{(2)} = 0$. The last claim then follows. $\square$

It is also straightforward to see that

$$\left(\frac{q^n-1}{q-1}, 2\right) = \begin{cases} 2 & \text{if } n \text{ even and } q \text{ odd} \\ 1 & \text{otherwise} \end{cases}$$

Lemma A.0.11. Let $a \in \mathbb{N}$ with $a \geq 2$ and let $n \in \mathbb{N}$ be odd. Then

$$\left(\frac{a^n+1}{a+1}, a+1\right) = (n, a+1)\ .$$

Proof. As n is odd we have ${}^{a^n+1}/_{a+1} = {}^{(-a)^n-1}/_{(-a)-1} = (-a)^{n-1} + (-a)^{n-2} + \ldots + (-a) + 1$. The result follows. $\square$

Lemma A.0.12. Suppose $a \in \mathbb{N}$ is odd and $n \in N$. Then

(1)
$$\left(\frac{a^n-1}{2}, a-1\right) = \frac{a-1}{2} \cdot (n, 2)$$

(2)
$$\left(\frac{a^n+1}{2}, a-1\right) = \begin{cases} 1 & \text{if } n \text{ is even} \\ 1 & n \text{ is odd and } 4|(a-1) \\ 2 & \text{otherwise} \end{cases}$$

(3)
$$\left(\frac{a^n+1}{2}, a+1\right) = \begin{cases} 1 & \text{if } n \text{ is even} \\ {}^{(a+1)}/_2 & \text{if } n \text{ is odd} \end{cases}$$

(4)
$$\left(\frac{a^n-1}{2}, a+1\right) = \begin{cases} a+1 & \text{if } n \text{ is even} \\ 1 & \text{if } n \text{ is odd and } 4|(a+1) \\ 2 & \text{otherwise} \end{cases}$$

Proof. For (1) we write $a^n = ((a-1)+1)^n = \sum_{k=0}^{n} \binom{n}{k}(a-1)^k$. Then ${}^{a^n-1}/_2 = {}^{(a-1)}/_2 \cdot \left(\binom{n}{1} + \binom{n}{2}(a-1) + \ldots + \binom{n}{n}(a-1)^{n-1}\right)$, so that ${}^{a^n-1}/_2 \equiv {}^{a-1}/_2 \cdot n \mod (a-1)$. Hence $({}^{a^n-1}/_2, a-1) = ({}^{a-1}/_2 \cdot n, a-1) = {}^{(a-1)}/_2 \cdot (n, 2)$.

For (2) again write $a^n = ((a-1)+1)^n$ and observe that

$$\frac{a^n+1}{2} = 1 + \frac{a-1}{2} \cdot \left(\binom{n}{1} + \binom{n}{2}(a-1) + \ldots + \binom{n}{n}(a-1)^{n-1}\right)$$

so that ${}^{(a^n+1)}/_2 \equiv 1 + {}^{(a-1)}/_2 \cdot n \mod (a-1)$. If n is even, then ${}^{(a-1)}/_2 \cdot n \equiv 0 \mod (a-1)$, hence ${}^{(a^n+1)}/_2$ and $a-1$ are coprime. If n is odd, then ${}^{(a-1)}/_2 \cdot n \equiv {}^{(a-1)}/_2 \mod (a-1)$ and so $({}^{(a^n+1)}/_2, a-1) = (1 + {}^{(a-1)}/_2, a-1) = (1 + {}^{(a-1)}/_2, 2)$ and the claim follows.

For (3), we write $a^n = ((a+1)-1)^n = \sum_{k=0}^{n} \binom{n}{k}(a+1)^k(-1)^{n-k}$. If n is odd, then

$$\frac{a^n+1}{2} = \frac{a+1}{2}\left(\binom{n}{1}(-1)^{n-1} + \binom{n}{2}(a+1)(-1)^{n-2} + \ldots + \binom{n}{n}(a+1)^{n-1}\right)$$

So ${}^{(a^n+1)}/_2 \equiv {}^{(a+1)}/_2 \cdot n \mod (a+1)$ and the latter is equal to ${}^{(a+1)}/_2 \mod (a+1)$ as n is odd. Thus $({}^{(a^n+1)}/_2, a+1) = {}^{(a+1)}/_2$. If n is even, then

$$\frac{a^n+1}{2} = 1 + \frac{a+1}{2} \cdot \left(\binom{n}{1}(-1)^{n-1} + \binom{n}{2}(a+1)(-1)^{n-2} + \ldots + \binom{n}{n}(a+1)^{n-1}\right)$$

so that ${}^{(a^n+1)}/_2 \equiv 1 - {}^{(a+1)}/_2 \cdot n \mod (a+1)$ and since n is even we have ${}^{(a+1)}/_2 \cdot n \equiv 0 \mod (a+1)$. Thus ${}^{(a^n+1)}/_2$ and $a+1$ are coprime.

To prove (4), we write $a^n = ((a+1)-1)^n$ and obtain for n even

$$\begin{aligned}\frac{a^n-1}{2} &= \frac{a+1}{2}\left(\binom{n}{1}(-1)^{n-1} + \binom{n}{2}(a+1)(-1)^{n-2} + \ldots + \binom{n}{n}(a+1)^{n-1}\right)\\ &\equiv -\frac{a+1}{2} \cdot n \equiv 0 \mod (a+1)\end{aligned}$$

If n is odd, we obtain

$$\begin{aligned}\frac{a^n-1}{2} &= -1 + \frac{a+1}{2}\left(\binom{n}{1}(-1)^{n-1} + \binom{n}{2}(a+1)(-1)^{n-2} + \ldots + \binom{n}{n}(a+1)^{n-1}\right)\\ &\equiv -1 + \frac{a+1}{2} \cdot n \mod (a+1)\\ &\equiv -1 + \frac{a+1}{2} \mod (a+1)\,.\end{aligned}$$

So $({}^{(a^n+1)}/_2, a+1) = (-1 + {}^{(a+1)}/_2, a+1) = (2, 1 + {}^{(a+1)}/_2)$, which completes the proof. $\square$

Definition A.0.13. For a group G we denote by $\mathrm{meo}(G) = \sup\{\mathrm{ord}(g) \mid g \in G\}$ the maximum element order in G.

To estimate the maximum element order in a simple group of Lie type we often rely on:

Lemma A.0.14 ([VGM09, Lemma 1.3 (3)])**.** If S is a simple group of Lie type of rank n of a field of order q, then if S is distinct from Ree and Suzuki groups and $E_8(q)$, then element orders of S are at most ${}^{q^{n+1}}/_{q-1}$

The following is probably well-known. At least for q odd the result is given in [KS09, Table A.1].

Lemma A.0.15. The maximum element order in $\mathrm{PSL}_n(q)$ for $n \geq 2$ is given by

$$\mathrm{meo}(\mathrm{PSL}_n(q)) = \begin{cases} q & \text{if } n = 2 \text{ and } q \neq 2 \text{ is prime} \\ \frac{q^n-1}{(q-1)\cdot(n,q-1)} & \text{otherwise} \end{cases}$$

Proof. The spectrum of $\mathrm{PSL}_n(q)$ has been determined in [But08, Corollary 3]. For the convenience of the reader we will state the result here. Let $d = (n, q-1)$. Any element order in $\mathrm{PSL}_n(q)$ is a divisor of the following numbers:

(1) $\frac{q^n-1}{(q-1)d}$

(2) $\frac{[q^{n_1}-1, q^{n_2}-1]}{(n/(n_1,n_2), q-1)}$ where $n_1, n_2 > 0$ such that $n_1 + n_2 = n$.

(3) $[q^{n_1} - 1, q^{n_2} - 1, \ldots, q^{n_s} - 1]$ for $s \geq 3$ and $n_1, \ldots, n_s > 0$ such that $n_1+n_2+\ldots+n_s = n$.

(4) $p^k \cdot \frac{q^{n_1}-1}{d}$ where $k, n_1 > 0$ such that $p^{k-1} + 1 + n_1 = n$.

(5) $p^k \cdot [q^{n_1} - 1, q^{n_2} - 1, \ldots, q^{n_s} - 1]$ for $s \geq 2$ and $k, n_1, \ldots, n_s > 0$ such that $p^{k-1} + 1 + n_1 + n_2 + \ldots + n_s = n$.

(6) p^k if $p^{k-1} + 1 = n$ for $k > 0$.

By (1) and (6) the stated element order exists in $\mathrm{PSL}_n(q)$ in each case. We will first show that the numbers given in (2), ..., (5) do not exceed the number given in (1). For (2) note that $[q^{n_1} - 1, q^{n_2} - 1] = (q^{n_1}-1)(q^{n_2}-1)/(q^{(n_1,n_2)}-1)$. If $(n_1, n_2) = 1$, the claim follows. Otherwise $q^{(n_1,n_2)} - 1 \geq (q-1) \cdot q \geq (q-1) \cdot d$ as $d \leq q$. Since $(q^{n_1} - 1)(q^{n_2} - 1) \leq q^{n_1+n_2} - 1 = q^n - 1$ the claim follows in this case as well. For (3), observe that $[q^{n_1} - 1, q^{n_2} - 1, \ldots, q^{n_s} - 1] \leq (q^{n_1}-1)(q^{n_2}-1)\ldots(q^{n_s}-1)/(q-1)^2$ as $s \geq 3$. Now $(q-1)^2 \geq (q-1)d$ and so the given number does not exceed $(q^n-1)/d(q-1)$. To prove that (4) does not exceed (1) observe that $p^{k-1} = (1 + (p-1))^{k-1} \geq 1 + (k-1)(p-1) \geq k$ by Bernoulli's inequality. Hence $n \geq k + 1 + n_1$. It is also easy to see that $(q^m - 1)(q - 1) \leq q^{m+1} - 1$ for all $m, q \geq 1$. It follows that $p^k(q^{n_1} - 1)(q - 1) \leq q^k \cdot (q^{n_1+1} - 1) \leq q^{k+n_1+1} - 1 \leq q^n - 1$, which implies the claim. For (5) note that $p^k(q-1)d\,[q^{n_1} - 1, q^{n_2} - 1, \ldots, q^{n_s} - 1] \leq q^k(q-1)^2 \cdot (q^{n_1+n_2+\ldots+n_s}-1)/q-1 = q^k(q-1)(q^{n_1+n_2+\ldots+n_s} - 1) \leq q^k(q^{1+n_1+n_2+\ldots+n_2} - 1) \leq q^{k+1+n_1+n_2+\ldots+n_s} - 1$. As $p^{k-1}+1+n_1+n_2+\ldots+n_s = n$ we have $k+1+n_1+n_2+\ldots+n_s \leq n$, and hence $q^{k+1+n_1+n_2+\ldots+n_s} - 1 \leq q^n - 1$, which implies the claim.

We now show that (6) does not exceed (1) if $n \geq 3$ or if $n = 2$ and q is composite. We have $p^{k-1} + 1 = n$ for some $k > 0$, hence $p^k = p(n-1)$. Using the binomial expansion one checks that $q^n - 1 \geq (n-1)q(q-1)^2$ for $n \geq 4$. This implies that $dp(n-1)(q-1) \leq (n-1)q(q-1)^2 \leq q^n - 1$ for $n \geq 4$. If $n = 3$ one checks that $dp(n-1)(q-1) \leq 6q(q-1) \leq q^3 - 1 = q^n - 1$ for $q \geq 5$. If $n = 4$ and $q = 4$ or $q = 2$, an explicit calculation verifies that $p(n-1) \leq (q^n-1)/d(q-1)$. The case that $q = 3$ is impossible as we require that $p^{k-1} + 1 = n = 3$. So now suppose that $n = 2$ and q is composite, so $q = p^k$ for $k \geq 2$. We need to verify that $dp(q-1) \leq q^2 - 1 = q^n - 1$, which is equivalent to showing that $dp \leq q + 1 = p^k + 1$. Now, $dp \leq 2p \leq p^2 + 1 \leq p^k + 1$, which proves the claim.

If $n = 2$ and q is prime we now show that (1) is at most as big as (6) except in the case $q = 2$. If $n = 2$ and $q = 2$, we have $\mathrm{meo}(\mathrm{PSL}_2(2)) = 3 = q + 1$ as claimed. So suppose that $n = 2$ and $p = q > 2$, so p is odd. It is now easy to see that $(q^n-1)/(q-1)d = (p+1)/(2,p-1) = (p+1)/2$ does not exceed p. □

After these preparations are we now ready to prove the main theorem.

Proof of Theorem A.0.2. We dealt with the alternating groups in Proposition A.0.4 and the spectra of the sporadic simple groups are calculated in Section A.1. So we are left to show the claim for the finite simple groups of Lie type. Let us first consider the Chevalley groups:

$\boldsymbol{A_{n-1}(q) = \mathrm{PSL}_n(q), n \geq 2}$

Note that $\mathrm{PSL}_2(3) \cong A_4$ and $\mathrm{PSL}_2(2) \cong S_3$ are not simple. If $n = 2$ and $q > 3$, then $\mu(\mathrm{PSL}_2(q)) = \{p, {}^{q-1}/_{d}, {}^{q+1}/_{d}\}$ where $d = (q-1, 2)$ by [Hup67, Theorem 8.27].

So suppose that $n \geq 3$ and let $d = (n, q-1)$. We can choose the following element orders according to [But08, Corollary 3]:

$$a = \frac{q^n - 1}{d(q-1)}$$
$$b = \frac{[q-1, q^{n-1} - 1]}{d} = \frac{q^{n-1} - 1}{d}$$
$$c = p \cdot \frac{q^{n-2} - 1}{d}$$

Then $(b, c) = {}^{(q-1)}/_{d}$ so that

$$[b, c] = \frac{p(q^{n-1} - 1)(q^{n-2} - 1)}{d(q-1)}$$

We also have $(a, b) = 1$ by Lemma A.0.9 and

$$(a, c) = \frac{q^{(n,2)} - 1}{q - 1} \cdot \frac{({}^{n}/_{(n,2)}, q-1)}{d}$$

We have $[a, b] = {}^{(q^n-1)(q^{n-1}-1)}/_{d^2(q-1)}$. We claim that $[a, b] > {}^{q^n}/_{d(q-1)}$, which is equivalent to $(q^n - 1)(q^{n-1} - 1) > q^n d$. Note that $(q^n - 1)(q^{n-1} - 1) > q^{2n-3}$ and $q^n d \leq q^{n+1}$. If $n \geq 4$ the claim follows as $q^{2n-3} > q^{n+1}$. For $q \geq 3$ we have $(q^n - 1)(q^{n-1} - 1) > q^{2n-2}$ as $(q-1)^2 > q$ so that the inequality holds for all $n \geq 3$ in this case. The only case that remains is $q = 2$ and $n = 3$ which can be checked explicitly.

We show that $[b, c] > {}^{q^n}/_{d(q-1)}$, or equivalently $p(q^{n-1} - 1)(q^{n-2} - 1) > q^n$ as long as $n \neq 3$ or $q \neq 2$. Note that $p(q^{n-1} - 1)(q^{n-2} - 1) > q^{2n-5}$ so that the inequality is clearly satisfied if $n \geq 5$. If $n = 4$ one sees that $(q^3 - 1)(q^2 - 1) > q^4$ for $q \geq 3$. If $n = 4$ and $q = 2$ an explicit computation again shows that $(q^3 - 1)(q^2 - 1) > q^4$. If $n = 3$, we have $[b, c] > {}^{q^n}/_{d(q-1)}$ as long as $q \geq 3$ by a straightforward computation. The remaining case that $n = 3$ and $q = 2$ has been excluded in the beginning and an explicit computation of the spectrum yields $\mu(\mathrm{PSL}(3, 2)) = \{3, 4, 7\}$.

For showing that $[a, c] > {}^{q^n}/_{d(q-1)}$ we need to show that $p(q^n - 1)(q^{n-2} - 1)(q - 1) > q^n(q^{(n,2)} - 1)\,({}^{n}/_{(2,n)}, q - 1)$. If n is odd, we need to prove that $p(q^n - 1)(q^{n-2} - 1) > q^n d$. Note that $p(q^n - 1)(q^{n-2} - 1) > q^{2n-4}$ and $q^n d \leq q^{n+1}$, so that the inequality holds for $n \geq 5$. If $n = 3$ and $q \geq 3$ a simple calculation shows that $p(q^n - 1)(q^{n-2} - 1) \geq 2(q^n - 1)(q^{n-2} - 1) > q^{n+1}$. The remaining case that $n = 3$ and $q = 2$ is then easily verified. If n is even, we need to verify that $p(q^n - 1)(q^{n-2} - 1) > q^n(q + 1)\,({}^{n}/_{2}, q - 1)$. Certainly, $p(q^n - 1)(q^{n-2} - 1) > q^{2n-4}$ whereas $q^n(q+1)\,({}^{n}/_{2}, q-1) \leq q^{2n} \cdot 2q \cdot q \leq q^{n+3}$, so that the inequality holds for $n \geq 7$.

If $n = 6$, certainly $(n/2, q-1) \leq 3$ and a computation shows that $p(q^n-1)(q^{n-2}-1) \geq 2(q^n-1)(q^{n-2}-1) > 3q^n(q+1)$. If $n = 4$, so that $(n/2, q-1) \leq 2$, a similar computation shows the claim for $q \geq 3$. If $n = 4$ and $q = 2$ a direct calculation verifies the inequality.

$\boldsymbol{B_n(q) = \Omega_{2n+1}(q), n \geq 2}$

We first consider the case that q is odd and $n \geq 3$. The case that $n = 2$ and q is odd will be dealt with below since $\Omega_5(q) \cong \mathrm{PSp}_4(q)$ (see e.g. [Wil09, Section 3.11]). The spectrum $\Omega_{2n+1}(q)$ for $n \geq 3$ has been determined in [But10, Corollary 6] and so we can choose the following element orders:

$$\begin{aligned} a &= \frac{q^n+1}{2} \\ b &= \left[q-1, q^{n-1}+1\right] = \frac{(q-1)(q^{n-1}+1)}{2} \\ c &= p\frac{q^{n-1}-1}{2} \end{aligned}$$

We have $(a, b) = (2, {(q^n+1)}/2)$,

$$(a, c) = \begin{cases} (q+1)/2 & \text{if } n \text{ is odd} \\ 1 & \text{if } n \text{ is even} \end{cases}$$

and using Lemma A.0.12 one shows that $(b, c) = (q-1)/2 \cdot (n-1, 2)$. We are now going to show that $[a, b], [a, c]$ and $[b, c]$ are larger than $q^{n+1}/q-1$. Note that $[a, b] = (q^n+1)(q^{n-1}+1)(q-1)/4(a,b)$ and we thus need to show that $(q^n+1)(q^{n-1}+1)(q-1)^2 > 4\,(a, b)\,q^{n+1}$. We have $(q^n+1)(q^{n-1}+1)(q-1)^2 > q^{2n-1}$, whereas $4\,(a, b)\,q^{n+1} \leq 8q^{n+1} \leq q^{n+3}$ since $q \geq 3$. Thus the inequality certainly holds if $n \geq 4$. If $n = 3$ a more careful analysis shows that $(q^n+1)(q^{n-1}+1)(q-1)^2 > q^{n+3}$ for $q \geq 3$.

To show that $[a, c] > q^{n+1}/q-1$ we distinguish whether n is odd or even. If n is odd, then $[a, c] = p/2 \cdot (q^n+1)(q^{n-1}+1)/q+1$ and thus we need to prove that $p/2 \cdot (q^n+1)(q^{n-1}-1)(q-1) > q^{n+1}(q+1)$. Now, $p/2 \cdot (q^n+1)(q^{n-1}-1)(q-1) > q^{2n-2}$ and $q^{n+1}(q+1) < q^{n+3}$ so that the inequality holds for $n \geq 5$. If $n = 3$, we see that $(q^3+1)(q-1)^2 > q^3 \cdot q = q^4$ for $q \geq 3$ which shows the claim. If n is even, $[a, c] = p/4 \cdot (q^n+1)(q^{n-1}-1)$ and we need to show that $p/2 \cdot (q^n+1)(q^{n-1}-1)(q-1) > 2q^{n+1}$, which is easily seen to be the case for $n \geq 4$.

We compute $[b, c] = p/2 \cdot (n-1, 2) \cdot (q^{n-1}+1)(q^{n-1}-1)$. It is easy to see that $(q-1) \cdot [b, c] > q^{n+1}$ whenever $n \geq 4$. If $n = 3$, one checks that $(q-1)p/4 \cdot (q^{n-1}+1)(q^{n-1}-1) > q^{n+1}$ for $q \geq 4$ using that $p \geq 2$. If $n = 3$ and $p = 3 = q$, a direct computation verifies the inequality.

Now suppose that q is a power of 2 and $n \geq 2$. For example, we can compute using GAP:

$$\begin{aligned} \mu(\Omega_5(2)) &= \{4, 5, 6\} \\ \mu(\Omega_5(4)) &= \{4, 6, 10, 15, 17\} \end{aligned}$$

By [But10, Corollary 3] we can pick the following element orders

$$a = q^n + 1$$
$$b = q^n - 1$$
$$c = 2(q^{n-1} + 1)$$

We have $(a, b) = (2, q+1) = 1 = (a, c)$ and

$$(b, c) = \begin{cases} q+1 & \text{if } n \text{ is even} \\ 1 & \text{if } n \text{ is odd} \end{cases}$$

If n is even, we now show that $(q-1)[b, c] > q^{n+1}$ except if $n = 2$ and $q = 2$. In this exceptional case we computed above that $|\mu(\Omega_5(2))| = 3$. We have $[b, c] = {}^{2(q^n-1)(q^{n-1}+1)}/_{(q+1)}$ and we need to show that $2(q^n - 1)(q^{n-1} + 1)(q - 1) > q^{n+1}(q + 1)$. We easily see that this inequality is satisfied for $n \geq 5$. As before, one verifies that the inequality also holds for $n = 4$ and for $n = 2$ and $q \geq 4$. It is easy to see that $[a, b]$ and $[a, c]$ exceed ${}^{q^{n+1}}/_{q-1}$ in all cases.

$C_n(q) = \mathbf{PSp}_{2n}(q), n \geq 2$

Since $C_n(2^k) = B_n(2^k)$ and as we analyzed the spectrum of $B_n(q)$ already, we only need to consider the case that q is odd. By [But10, Corollary 2] we can then choose the following element orders:

$$a = \frac{q^n + 1}{2}$$
$$b = \frac{q^n - 1}{2}$$
$$c = p(q^{n-1} + 1)$$

We evaluate $(a, b) = {}^1/_2 \cdot (q^n + 1, q^n - 1) = 1$. Then $(q-1)[a, b] = ({}^{q-1}/_2)^2 \cdot (q^n + 1)(q^n - 1) \geq ({}^{q-1}/_2)^2 \cdot (q^n + 1) \cdot q^{n-1} > q^{2n-1} \geq q^{n+1}$ for $n \geq 2$.

We have $(a, c) \leq \left(q^n + 1, q^{n-1} + 1\right) \leq 2$. Then $(q-1)\,[a, c] \geq {}^{p(q-1)}/_4 \cdot (q^n + 1)(q^{n-1} + 1) > q^{2n-1} \geq q^{n+1}$ for $n \geq 2$.

Note that $(b, c) \leq \left(q^n - 1, q^{n-1} + 1\right) \leq q + 1$, so that $[b, c] \geq {}^p/_2 \cdot {}^{(q^n-1)(q^{n-1}+1)}/_{q+1}$. Observe that $(q-1)(q^n-1)(q^{n-1}+1) > q^{n+1}(q+1)$ for $n \geq 4$ as $(q-1)(q^n-1) \geq q^n$ for $q \geq 3$ and $q^{n+1}(q+1) \leq q^{n+3}$. A slightly more careful analysis shows that the inequality also holds for $n = 3$. Suppose now that $n = 2$. As q is odd, we have $p \geq 3$. One then shows that ${}^3/_2 \cdot (q-1)(q^n-1)(q^{n-1}+1) > q^{n+1}(q+1)$ for $q \geq 4$. If $n = 2$ and $q = 3$, we can explicitly compute $\mu(\mathrm{PSp}(4, 3)) = \{5, 9, 12\}$.

$D_n(q) = P\Omega^+_{2n}(q), n > 3$

The spectrum has been determined in [But10, Corollary 8, Corollary 9] for q odd and in [But10, Corollary 4] for q even. A computation with GAP shows that $\mu(P\Omega_8^+(3)) = \{8, 12, 13, 14, 15, 18, 20\}$. We will first consider the case that q is odd. The center of $\Omega^+_{2n}(q)$ is non-trivial if and only if $(4, q^n - 1) = 4$. For example, if $n = 4$, then $(4, q^4 - 1) = 4$ as $q^4 - 1 = (q^2 - 1)(q^2 + 1)$. If $q \geq 5$, then [KS09, Table A.5] yields for the largest element order $m_1 = {}^{(q^4-1)}/_4$.

Suppose now that n and q are such that $(4, q^n - 1) = 4$. Then we can choose the following element orders according to [But10, Corollary 9]:

$$a = \frac{q^n - 1}{4}$$
$$b = \frac{[q-1, q^{n-1} - 1]}{d} = \frac{q^{n-1} - 1}{d}$$
$$c = p \cdot \frac{q^{n-2} + 1}{2}$$

Here, $d = 2$ if $(q-1)_{(2)} = (q^{n-1} - 1)_{(2)}$ and $d = 1$ otherwise. Note that

$$\left(q^n - 1, q^{n-2} + 1\right) = \begin{cases} q^2 + 1 & \text{if } (n, 4) = 4 \\ 2 & \text{else} \end{cases}$$

So, if $(n, 4) = 4$, then $(a, c) \leq {}^{q^2+1}/_2$ thus $[a, c] \geq {}^{p}/_{4} \cdot {}^{(q^n-1)(q^{n-2}+1}/_{q^2+1}$. It is easy to see that $[a, c] > {}^{q^{n+1}}/_{q-1}$ for $n \geq 7$. As $(6, 4) = 2$ and $(5, 4) = 1$ we only need to consider the case that $n = 4$. But then, for $q \geq 5$, $m_1 = {}^{(q^4-1)}/_{q-1}$ is the maximal order element and it is again not hard to verify that $[a, c] > m_1$. If $(n, 4) \neq 4$, we know that $(a, c) = 1$ and thus $[a, c] = {}^{p(q^n-1)(q^{n-2}+1)}/_8 > {}^{q^{n+1}}/_{q-1}$ for all $n \geq 5$.

As $\left(q^n - 1, q^{n-1} - 1\right) = q - 1$ we have $(a, b) \leq q - 1$ so that $[a, b] \geq {}^{(q^n-1)(q^{n-1}-1)}/_{8(q-1)}$. We show that $[a, b] > {}^{q^{n+1}}/_{q-1}$ or equivalently $(q^n - 1)(q^{n-1} - 1) > 8q^{n+1}$. The claim follows for $n \geq 5$ from the fact that $(q^n - 1)(q^{n-1} - 1) > q^{2n-2}$ for $q \geq 2$ and $8 \cdot q^{n+1} \leq q^{n+3}$ since $q \geq 3$. One also easily checks that the inequality holds for $n = 4$.

Observe that $\left(q^{n-1} - 1, q^{n-2} + 1\right)$ equals $q+1$ if n is odd an equals 2 if n is even. Thus, for n odd, we have $(b, c) \leq q+1$ so that $[b, c] \geq {}^{(q^{n-1}-1)(q^{n-2}+1)}/_{4(q+1)}$ which exceeds ${}^{q^{n+1}}/_{q-1}$ for $n \geq 7$. If $n = 5$ and $q \geq 6$ we still have ${}^{(q^{n-1}-1)(q^{n-2}+1)}/_{4(q+1)} > {}^{q^{n+1}}/_{q-1}$. For $n = 5$ and $q \in \{3, 5\}$ one verifies that $[b, c] > {}^{q^{n+1}}/_{q-1}$ by a direct computation. If n is even we can assume that $n \leq 7$. If $n = 6$ one shows that $[b, c] \geq {}^{(q^{n-1}-1)(q^{n-2}+1)}/_8 > {}^{q^{n+1}}/_{q-1}$. If $n = 4$ and $q \geq 5$ we know the maximal element order m_1 explicitly and we can easily show that $[b, c] > {}^{(q^4-1)}/_4 = m_1$. For $n = 4$ and $q = 3$ we know the spectrum completely.

We now consider the case that $(4, q^n - 1) \neq 4$, so that $P\Omega^+_{2n}(q) = \Omega^+_{2n}(q)$ and thus [But10, Corollary 8] applies. Also note that in this case $n \geq 5$. By [But10, Corollary 8] we can choose the following element orders:

$$a = \frac{q^n - 1}{2}$$
$$b = q^{n-1} - 1$$
$$c = p \cdot \left[q - 1, \frac{q^{n-2} - 1}{2}\right] = \frac{p}{(n, 2)} \cdot (q^{n-2} - 1)$$

Since $\left(q^{n-1} - 1, q^{n-2} - 1\right) = q - 1$, we have $(b, c) \leq q - 1$, and thus we obtain that $[b, c] \geq {}^{p}/_{2} \cdot {}^{(q^{n-1}-1)(q^{n-2}-1)}/_{q-1}$. As $(q^{n-1} - 1)(q^{n-2} - 1) > q^{2n-4}$ it follows that $[b, c] > {}^{q^{n+1}}/_{q-1}$ for all $n \geq 5$.

We have $(a, b) \leq \left(q^n - 1, q^{n-1} - 1\right) = q - 1$, so that $[a, b] \geq {}^{(q^n-1)(q^{n-1}-1}/_{2(q-1)}$. It is then easy to see that $(q - 1)[a, b] > q^{n+1}$. It is also straightforward to verify that $(q - 1)[a, c] > q^{n+1}$ using that $(a, c) \leq q^2 - 1$.

We now consider the case that q is even. Then we choose the following element orders according to [But10, Corollary 4].

$$\begin{aligned} a &= q^n - 1 \\ b &= q^{n-1} - 1 \\ c &= 2(q^{n-2} - 1) \end{aligned}$$

One sees that $(a,b) = q - 1 = (b,c)$ and $(a,c) = q^{(n,2)} - 1$. By Lemma A.0.14 we know that the element orders are bounded by ${q^{n+1}}/{q-1}$. It is now straightforward to check that $[a,b],[a,c]$ and $[b,c]$ each exceed the maximal element order. For example, if n is even we show that $[a,c] = {2(q^n-1)(q^{n-2}-1)}/{q^2-1} > {q^{n+1}}/{q-1}$ if $n \neq 4$ or $q \neq 2$. If $n \geq 7$, the inequality follows since $(q^n-1)(q^{n-2}-1) > q^{n-1} \cdot q^{n-3} = q^{2n-4} \geq q^{n+3} \geq q^{n+1} \cdot (q^2-1)$. For $n = 6$ and $q \geq 2$ and for $n = 4$ and $q \geq 4$ a more careful analysis shows that the inequality holds. For $n = 4$ and $q = 2$ we can determine the spectrum explicitly:

$$\mu(P\Omega_8^+(2)) = \{7, 8, 9, 10, 12, 15\}$$

Let us consider the exceptional Chevalley groups:

$E_6(q)$

Let $d = (3, q-1)$. By [KS02, Section 2] there are semisimple elements in $E_6(q)$ of orders $a' = {a}/{d}, b' = {b}/{d}, c' = {c}/{d}$ where

$$\begin{aligned} a &= (q+1)(q^5-1) \\ b &= (q^2+q+1)(q^4-q^2+1) \\ c &= q^6 + q^3 + 1\,. \end{aligned}$$

In the following we show that $(a,b) = (a,c) = (b,c) = (3, q-1) = d$. We first compute that

$$(q^2+q+1, q^4-q^2+1) = (q^2+q+1, 2(q+1)) = (q^2+q+1, q+1) = 1$$

as q^2+q+1 is odd for all $q \in \mathbb{N}$. Thus

$$(a,b) = (a, q^2+q+1) \cdot (a, q^4-q^2+1)$$

Observe that

$$(a, q^4-q^2+1) = (q, q^2+2q+1) = (q, 1) = 1$$

And

$$\begin{aligned} \Big(a, q^2+q+1\Big) &= \Big(-a + (q^4-q^2+q) \cdot (q^2+q+1), q^2+q+1\Big) \\ &= \Big(2q+1, q^2+q+1\Big) \\ &= (2q+1, q(q-1)) \\ &= (2q+1, q) \cdot (2q+1, q-1) \\ &= (3, q-1) \end{aligned}$$

Hence we see that $(a,b) = (3, q-1)$. A direct computation also shows that $(a,c) = (3, q-1)$. We now compute

$$\begin{aligned}(q^2+q+1,c) &= \Big(q^2+q+1, c + (-q^4+q^3-2q+2)(q^2+q+1)\Big) \\ &= (q^2+q+1,3) \\ &= (q^2-2q+1,3) \\ &= \Big((q-1)^2,3\Big) \\ &= (q-1,3)\end{aligned}$$

Another direct computation shows that $(q^4-q^2+1,c) = (q,1) = 1$. Since q^2+q+1 and q^4-q^2+1 are coprime by the above computation, we obtain that $(b,c) = (q-1,3)$. Thus it follows that a', b' and c' are pairwise coprime.

By Lemma A.0.14 the maximum element order is at most $q^7/q-1$. Note that $a > q^5, b > q^4$ and $c > q^6$. If we let $d = (q-1,3)$ then note that $q/d > 1$ for any prime number q. It follows that $[a',b'] = a' \cdot b' = ab/d^2 > q^2/d^2 \cdot q^7$, which exceeds the maximum element order. Similarly, also $[a',c']$ and $[b',c']$ are larger than maximum element order.

$E_7(q)$

Let us choose the following numbers

$$\begin{aligned}a &= q^7-1 \\ b &= (q-1)(q^6+q^3+1) \\ c &= (q^5-1)(q^2+q+1)\,.\end{aligned}$$

According to [KS02, Section 2] these are element orders of semisimple elements in $E_7(q)$ up to a scaling factor of $(2, q-1)$. A straightforward computation shows that $(a,b) = (q^2-1, q-1) = q-1$. Moreover, one sees that $(a,c) = (q-1) \cdot (2q^2+3q+2, (q+1)(q^2+q+1))$. As $(q+1, q^2+q+1) = 1$ it follows that

$$\begin{aligned}\Big(2q^2+3q+2,(q+1)(q^2+q+1)\Big) &= \Big(2q^2+3q+2, q+1\Big)\cdot\Big(2q^2+3q+2, q^2+q+1\Big) \\ &= (q+2,q+1)\cdot\Big(q, q^2+q+1\Big) \\ &= 1\end{aligned}$$

Hence $(a,c) = q-1$. Note that $\big((q^5-1)/q-1, q^2+q+1\big) = \big(q^5-1/q-1, q^3-1/q-1\big) = \big(q^5-1, q^3-1\big)/q-1 = 1$. since $\big(q^5-1, q^3-1\big) = q^{(5,3)}-1 = q-1$. Thus $(b,c) = (q-1)\cdot \big(q^6+q^3+1, (q^5-1)/q-1\big)\cdot\big(q^6+q^3+1, q^2+q+1\big)$. We have $\big(q^6+q^3+1, (q^5-1)/q-1\big) = \big(q, 1+q^3\big) = 1$. Moreover,

$$\begin{aligned}\Big(q^6+q^3+1, q^2+q+1\Big) &= \Big(q^6+q^3+1+(-q^4+q^3-2q+2)(q^2+q+1), q^2+q+1\Big) \\ &= \Big(3, q^2+q+1\Big) \\ &= \Big(3, q^2-2q+1\Big) \\ &= (3, q-1)\ .\end{aligned}$$

Hence $(b,c) = (q-1)\cdot(3,q-1)$.

Observe that the product of any two elements of $\{a,b,c\}$ exceeds q^{12}. By Lemma A.0.14 the maximum element order is bounded by $q^8/q-1$. However, the least common multiple of any two semisimple element orders corresponding to a, b or c exceeds $q^{12}/(2,q-1)\cdot(3,q-1)\cdot(q-1)$, which is strictly larger than $q^8/q-1$.

$E_8(q)$
By [VGM09, Lemma 1.3 (2)] we know that the element orders are bounded by $q+1/q-1 \cdot q^8 \le q^{10}$. We choose the following element orders according to the table of [KS02, Section 2]:

$$\begin{aligned} a &= q^8 - 1 \\ b &= q^8 - q^4 + 1 \\ c &= q^6 + q^3 + 1\,. \end{aligned}$$

By Lemma A.0.6 we obtain that $(a,b) = 1$. A direct computation using Euclid's algorithm yields that $(b,c) = \left(q^3+q^2+q+1, q^3\right) = 1$ and $(a,c) = (3,q-1)$. Moreover, $a > q^7$, $b > q^4$ and $c > q^6$, so the least common multiple of any two of $\{a,b,c\}$ exceeds the maximum order of $E_8(q)$.

$F_4(q)$
We choose the following semisimple element orders [KS02, Section 2]

$$\begin{aligned} a &= (q^3-1)(q+1) \\ b &= q^4 + 1 \\ c &= q^4 - q^2 + 1\,. \end{aligned}$$

Note that according to [KS09] the element a is even of largest order as soon as q is composite. In any way by Lemma A.0.14 we know that the element orders are bounded by $q^5/q-1$.

It is easy to see that for all $n \in \mathbb{N}$ we have $\left(q^{2n}+1, q^{2n}-q^n+1\right) = 1$. In particular, $(b,c) = 1$. We have $(a,b) = (2q, q^2+1) = \left(2q,(q-1)^2\right) = (2,q-1)$. Using Euclid's algorithm we also compute that $(a,c) = \left(2, 1+q+q^2\right) = 1$.

We have $ab = (q^4+1)(q-1)(q^2+q+1)(q+1) > q^7$, and thus $[a,b] > q^6$. Certainly $q^4 - q^2 + 1 \ge q^2$, hence $ac = (q-1)(q^2+q+1)(q+1)(q^4-q^2+1) > q^2\cdot q\cdot q^2 = q^5$ and $bc > q^6$. So $[a,b]$, $[a,c]$ and $[b,c]$ all exceed the maximum element order. One also easily checks that a, b, c are pairwise distinct for all q.

It is also noteworthy that the reduced spectrum of $F_4(2^m)$ has been completely determined in [Cao+04], here $q = 2^m$:

$$\begin{aligned} \mu(F_4(2^m)) = \{&16, 8(q-1), 8(q+1), 4(q^2-1), 4(q^2+1), 4(q^2-q+1), \\ &4(q^2+q+1), 2(q-1)(q^2+1), 2(q+1)(q^2+1), 2(q^3-1), 2(q^3+1), \\ &(q^2-1)(q^2-q+1), (q^2-1)(q^2+q+1), q^4-1, q^4+1, q^4-q^2+1\} \end{aligned}$$

$G_2(q)$
First note that $G_2(q)$ is not simple for $q = 2$. However, its derived subgroup $G_2(2)' \cong$

$^3A_2(3)$ is simple. By [Con+] or a direct computation with GAP we obtain

$$\mu(G_2(2)') = \{7, 8, 12\}\,.$$

So in the following we suppose that $q > 2$. As G_2 has rank 2, Lemma A.0.14 yields that the element orders are bounded by $q^3/q-1 \le q^3$. There are semisimple elements of the following orders by [KS02, Section 2]:

$$\begin{aligned} a &= q^2 + q + 1 \\ b &= q^2 - q + 1 \\ c &= q^2 - 1\,. \end{aligned}$$

Note that according to [KS09, Table A.7] the element a is of largest order, at least if q is odd. By Lemma A.0.7 it follows that $(a, b) = 1$. A straightforward computation shows that $(a, c) = (3, q - 1)$ and $(b, c) = (3, q - 2)$.

One also observes that $[a, b] = a \cdot b > q^3$ as $b \ge q$ and $a > q^2$. Since $c > q$ and $(3, q - 1) \le q - 1$ we obtain that $[a, c] = ac/(3,q-1) > q^3/q-1$. Moreover, one sees that $bc > q^3$ for all $q \ge 2$ and $(3, q - 2) \le q - 2 \le q - 1$. Thus $[b, c] > q^3/q-1$. Also note that the elements a, b, c are not distinct if and only if $q = 2$, in which case $b = c$.

Let us now consider the Steinberg groups:

$^2A_{n-1}(q) = \mathrm{PSU}_n(q), n > 2$ In [But08, Corollary 3] the spectrum was determined, where the notation $\mathrm{PSU}_n(q) = \mathrm{PSL}^-(n, q)$ was used. An explicit computation shows that

$$\begin{aligned} \mu(\mathrm{PSU}_4(2)) &= \{5, 9, 12\} \\ \mu(\mathrm{PSU}_4(3)) &= \{5, 7, 8, 9, 12\} \end{aligned}$$

Also, by Lemma A.0.14 we know that the maximum element order is bounded by $q^n/q-1$. For n even, so $n \ge 4$ and $p = 2$ we choose the following element orders, where $d = (n, q + 1)$.

$$\begin{aligned} a &= \frac{q^n - 1}{d(q+1)} \\ b &= \frac{[q - 1, q^{n-1} + 1]}{d} = \frac{(q-1)(q^{n-1} + 1)}{d} \\ c &= p\frac{q^{n-2} - 1}{d} \end{aligned}$$

The second equality follows from Lemma A.0.5 since $\left(q - 1, q^{n-1} + 1\right) = (2, q + 1) = 1$ as q is even. We then obtain

$$\begin{aligned} (b, c) &= \frac{\left((q-1)(q^{n-1} + 1), p(q^{n-2} - 1)\right)}{d} \\ &= \frac{\left((q-1)(q^{n-1} + 1), (q^{n-2} - 1)\right)}{d} \\ &= \frac{\left(q - 1, q^{n-2} - 1\right) \cdot \left(q^{n-1} + 1, q^{n-2} - 1\right)}{d} \\ &= \frac{(q-1)(q+1)}{d} \end{aligned}$$

where we have again used Lemma A.0.5. Hence we get that

$$[b,c] = p\frac{(q^{n-1}+1)(q^{n-2}-1)}{d(q+1)}$$

Now we compute using Lemma A.0.9

$$\begin{aligned}(a,c) &= \frac{\left({(q^n-1)}/{q+1}, p(q^{n-2}-1)\right)}{d}\\ &= \frac{\left({(q^n-1)}/{q+1}, q^{n-2}-1\right)}{d}\\ &= \frac{q-1}{d}\cdot\left(q+1,\frac{n}{2}\right)\end{aligned}$$

It follows that

$$[a,c] = p\frac{(q^n-1)(q^{n-2}-1)}{d(q+1)(q-1)(\frac{n}{2},q+1)}$$

Moreover, again using Lemma A.0.9,

$$\begin{aligned}(a,b) &= \frac{\left({(q^n-1)}/{q+1}, (q-1)\cdot(q^{n-1}+1)\right)}{d}\\ &= \frac{\left({(q^n-1)}/{q+1}, q-1\right)\cdot\left({(q^n-1)}/{q+1}, q^{n-1}+1\right)}{d}\\ &= \frac{(q-1)\cdot(n,q+1)}{d} = q-1\end{aligned}$$

Thus

$$[a,b] = \frac{(q^n-1)\cdot(q^{n-1}+1)}{d^2\cdot(q+1)}$$

We now show that $[a,b] > {q^n}/{q-1}$, which is equivalent to showing that $(q-1)(q^n-1)(q^{n-1}+1) > q^n d^2(q+1)$. Observe that $(q-1)(q^n-1)(q^{n-1}+1) > q^{n-1}\cdot q^{n-1} = q^{2n-2}$. And $d = (n,q+1) \leq q+1 \leq 2q \leq q^2$, hence $q^n d^2(q+1) \leq q^{n+6}$. For $n \geq 8$ we have $q^{2n-2} \geq q^{n+6}$ so that the claim follows in this case. If $n = 6$ and $q \geq 4$, then $d = (3,q+1) \leq 3 \leq q$. So $q^n d^2(q+1) \leq 2q^9 \leq q^{10} = q^{2n-2}$. If $n = 6$ and $q = 2$, then a direct computation shows the inequality. The remaining case is $n = 4$. Then $d = (4,q+1) = 1$ since q is even, hence $q^n d^2(q+1) \leq 2q^5 \leq q^6 = q^{2n-2}$.

In a similar fashion one shows that $[b,c]$ and $[a,c]$ also exceed ${q^n}/{q-1}$.

Suppose now that n is even, but p is odd. We choose the same values for a,b,c as above. However note that $\left(q-1,q^{n-1}+1\right) = (2,q+1) = 2$, so that

$$\begin{aligned}a &= \frac{q^n-1}{d(q+1)}\\ b &= \frac{[q-1,q^{n-1}+1]}{d} = \frac{(q-1)(q^{n-1}+1)}{2d}\\ c &= p\frac{q^{n-2}-1}{d}\end{aligned}$$

We then compute

$$(b,c) = \frac{2}{d}\left(\frac{q-1}{2}\cdot\frac{q^{n-1}+1}{2}, \frac{q^{n-2}-1}{2}\right) = \frac{(q-1)(q+1)}{2d}$$

so that

$$[b,c] = \frac{p(q^{n-1}+1)(q^{n-2}-1)}{d(q+1)}$$

The previous computation for $[a,c]$ is unchanged, so

$$[a,c] = p\frac{(q^n-1)(q^{n-2}-1)}{d(q+1)(q-1)(\frac{n}{2},q+1)}$$

Note that since n is even and q is odd, we know that ${q^n-1}/{q+1}$ is divisible by 2. It follows that

$$\begin{aligned}
(a,b) &= \frac{1}{d}\cdot\left(\frac{q^n-1}{q+1}, \frac{(q-1)(q^{n-1}+1)}{2}\right)\\
&= \frac{2}{d}\cdot\left(\frac{q^n-1}{2(q+1)}, \frac{(q-1)}{2}\cdot\frac{(q^{n-1}+1)}{2}\right)\\
&= \frac{2}{d}\cdot\left(\frac{q^n-1}{2(q+1)}, \frac{(q-1)}{2}\right)\cdot\left(\frac{q^n-1}{2(q+1)}, \frac{q^{n-1}+1}{2}\right)\\
&= \frac{({q^n-1}/{q+1}, q-1)\cdot({q^n-1}/{q+1}, q^{n-1}+1)}{2d}\\
&= \frac{q-1}{2}
\end{aligned}$$

Hence we obtain

$$[a,b] = \frac{(q^n-1)\cdot(q^{n-1}+1)}{d^2\cdot(q+1)}$$

We now show that for $n\neq 4$ and $q\neq 3$ the least common multiple $[a,b]$ exceeds ${q^n}/{q-1}$. As noted above, we have to show that $(q-1)(q^n-1)(q^{n-1}+1) > q^n d^2(q+1)$ where $d=(n,q+1)$. We know that $(q-1)(q^n-1)(q^{n-1}+1) > q^{2n-2}$ and as above we can argue in the case that $n\geq 8$. If $n=6$, then $q^n d^2(q+1)\leq q^{n+2}d^2\leq 6^2q^8$ which is at most $q^{10}=q^{2n-2}$ if $q\geq 6$. If $q=3$, then $d=2\leq q$ and $q^n d^2(q+1)\leq q^{10}$ and if $q=5$ then $d=6$ and $q^6d^2(q+1)=q^6(q+1)^3\leq q^{10}$. We are left to show the claim if $n=4$. Note that ${(q-1)(q^n-1)(q^{n-1}+1)}/{q+1} = (q-1)^2(q^2+1)(q^3+1) > q^6$ for all $q\geq 3$. It thus suffices to show that $q^2\geq d^2$. Now $d=(4,q+1)\leq 4$, so the claim follows for $q>3$. Similar arguments show that also $[b,c]$ and $[a,c]$ exceed ${q^n}/{q-1}$ in the same cases. If $n=4$ and $q=3$, we computed the spectrum of $\mathrm{PSU}_4(3)$ explicitly, see above.

In the following we deal with the case that n is odd. Note that $\mathrm{PSU}_3(2)$ is not simple and hence will be excluded. According to [But08, Corollary 3] there are elements of the following orders if n is odd, where again $d = (n, q+1)$:

$$a = \frac{q^n + 1}{d(q+1)}$$
$$b = \frac{[q+1, q^{n-1}-1]}{d} = \frac{q^{n-1}-1}{d}$$
$$c = p\frac{q^{n-2}+1}{d}$$

Here we have used that $\big(q+1, q^{n-1}-1\big) = q+1$ as n is odd. Using Lemma A.0.9 we compute $(a,b) = 1 = (a,c)$ and $(b,c) = {}^{q+1}/_{d}$. We obtain that

$$[b,c] = {}^{p(q^{n-1}-1)\cdot(q^{n-2}+1)}/_{d(q+1)} \, .$$

In the following we will show that $[b,c] > {}^{q^n}/_{q-1}$ or equivalently that $p(q-1)(q^{n-1} - 1)(q^{n-2}+1) > q^n \cdot d \cdot (q+1)$ except in the case that $p = 2$ and $n = 3$. Observe that $p(q-1)(q^{n-1}-1)(q^{n-2}+1) > q^{2(n-2)}$ and $q^n \cdot d \cdot (q+1) \leq q^n \cdot (q+1)^2 \leq q^{n+4}$. For $n \geq 8$ we have $q^{2(n-2)} > q^{n+4}$. If $n = 7$ and $(n, q+1) = 1$, then $q^n \cdot d \cdot (q+1) \leq q^7 \cdot q^2 = q^9 \leq q^{10} = q^{2(n-2)}$. If $d = (n, q+1) = (7, q+1) = 7$, then we must have $q \geq 7$ so that $d \leq q$. Then $q^n \cdot q \cdot (q+1) \leq q^8 \cdot (q+1) \leq q^{10}$. If $n = 5$, note that as above ${}^{(q-1)(q^4-1)(q^3+1)}/_{q+1} = (q-1)^2(q^2+1)(q^3+1) > q^6$. If $q \geq 5$, then $q \geq d$ and we are done. If $q \in \{2,3,4\}$ we can show the inequality by a direct computation. We are thus left to show the inequality for $n = 3$. A more careful analysis shows that $2(q^2-1)(q-1) > q^3$ for $q \geq 3$, which implies that the inequality holds for $n = 3$ and those $q \geq 3$ such that $d = (3, q+1) = 1$. If $n = 3$ and $p \geq 7$ then we also see that $p(q^2-1)(q-1) > 3 \cdot q^n \geq d \cdot q^n$. So we are left to verify the inequality in the case that $p \in \{2,3,5\}$ and q is such that $d = (3, q+1) = 3$. Note that we excluded the case $n = 3$ and $p = 2$ in the beginning and also observe that $p = 3$ and $(3, q+1) = 3$ is never simultaneously possible. Hence the only case remaining is $p = 5$, which again can be checked easily.

In the following we prove that $[a,b] > {}^{q^n}/_{q-1}$ or equivalently $(q^n+1)(q^{n-1}-1)(q-1) > q^n d^2(q+1)$. Note that $(q^n+1)(q^{n-1}-1)(q-1) > q^n \cdot q^{n-2} = q^{2n-2}$ and $q^n d^2(q+1) \leq q^n \cdot q^4 \cdot q^2 = q^{n+6}$. For $n \geq 8$ we have $2n-2 \geq n+6$ so that the inequality is satisfied. If $n = 7$ and $d = (n, q+1) = 1$, then $q^n d^2(q+1) \leq q^7 \cdot q^2 = q^9 < q^{12} = q^{2n-2}$. If $d = 7$, then $q \geq 7$ so that $d = 7 \leq q$ and thus $q^n d^2(q+1) \leq q^{11} < q^{12}$ as desired. If $n = 5$, one checks that $(q^n+1)(q^{n-1}-1)(q-1) > q^n \cdot 5^2 \cdot (q+1) \geq q^n d^2(q+1)$ for all $q \geq 3$. If $n = 5$ and $q = 2$, $d = (n, q+1) = 1$ and an explicit computation yields that the inequality is satisfied. If $n = 3$ we have $q > 2$ and a computation shows that $(q^n+1)(q^{n-1}-1)(q-1) > q^n \cdot 3^2 \cdot (q+1) \geq q^n d^2(q+1)$ for all $q \geq 4$. If $q = 3$, then $d = (3, q+1) = 1$, and again one checks that the inequality is satisfied by a direct computation.

Now we are left to show that $[a,c] = {}^{p(q^n+1)(q^{n-2}+1)}/_{d^2(q+1)} > {}^{q^n}/_{q-1}$ or equivalently $p(q^n+1)(q^{n-2}+1)(q-1) > q^n d^2(q+1)$. Note that $p(q^n+1)(q^{n-2}+1)(q-1) > q^{2n-2}$ and $q^n d^2(q+1) \leq q^n(q+1)^3 \leq q^{n+5}$ as $(q+1)^3 \leq q^5$ for $q \geq 5$. As $2n-2 \geq n+5$ for $n \geq 7$, the inequality is satisfied in this case. If $n = 5$, one checks that $p(q^n+1)(q^{n-2}+1)(q-1) \geq 2(q^n+1)(q^{n-2}+1)(q-1) > q^n 5^2(q+1) \geq q^n d^2(q+1)$ for all

$q \geq 3$. An explicit computation yields the claim for $n = 5$ and $q = 2$. If $n = 3$, one sees that $p(q^n+1)(q^{n-2}+1)(q-1) \geq 2(q^n+1)(q^{n-2}+1)(q-1) > q^n \cdot 3^2 \cdot (q+1) \geq q^n d^2(q+1)$ for all $q \geq 6$. If $q \in \{3, 4, 5\}$ a direct computation shows that $(q-1)[a, c] > q^n$.

We thus have completed the proof that $|\mu(\mathrm{PSU}(n, q))| \geq 3$ except in the case that $n = 3$ and $p = 2$. By [But08, Corollary 3] there exists an element of order 4. We choose a and b as above and we let $c = 4$. Then $[a, c] = 4a$ and $[b, c] = 4b$. But again according to [But08, Corollary 3] the spectrum of $\mathrm{PSU}(3, q)$ does not contain elements $4a$ or $4b$. Moreover, the computation above shows that $[a, b] = a \cdot b$ exceeds the maximum element order. Hence the claim also holds in this case.

$\boldsymbol{{}^2D_n(q) = P\Omega^-_{2n}(q), n > 3}$ The group ${}^2D_n(q)$ is also known as $P\Omega^-_{2n}(q)$. We first analyze the spectrum in the case that q is odd and $(4, q^n + 1) = 4$. It is not hard to see that $(4, q^4 + 1) = 2$, so that we can assume in the following that $n \geq 5$.

According to [But10, Corollary 9] there are elements in $P\Omega^-_{2n}(q)$ of the following orders:

$$
\begin{aligned}
a &= \frac{q^n + 1}{4} \\
b &= \frac{[q-1, q^{n-1}+1]}{d} = \frac{(q-1)(q^{n-1}+1)}{2d} \\
c &= p \cdot \frac{q^{n-2}+1}{2}
\end{aligned}
$$

Here, $d = 2$ if $(q-1)_{(2)} = (q^{n-1}+1)_{(2)}$ and $d = 1$ otherwise. We have $(b, c) \leq {}^1/_2 \cdot (q-1, q^{n-2}+1) \cdot \left(q^{n-1}+1, q^{n-2}+1\right) = 2$. We can now estimate $[b, c] \geq {}^p/_{8d} \cdot (q-1)(q^{n-1}+1)(q^{n-2}+1) \geq {}^1/_{q^2} \cdot (q-1)(q^{n-1}+1)(q^{n-2}+1)$. For $n \geq 6$ one easily sees that $(q-1)^2(q^{n-1}+1)(q^{n-2}+1) > q^{n+3}$ and with a bit more one can show that the inequality also holds if $n = 5$. This implies that $[b, c] > {}^{q^{n+1}}/_{q-1}$.

We now estimate $[a, c]$. First observe that $(a, c) \leq {}^1/_2 \cdot (q^n+1, q^{n-2}+1) \leq {}^1/_2 \cdot (q^2 + 1)$. Thus $[a, c] \geq {}^p/_4 \cdot {}^{(q^n+1)(q^{n-2}+1)}/_{q^2+1}$. Further estimating $p \geq 2$, we show that ${}^{q-1}/_2(q^n+1)(q^{n-2}+1) > q^{n+1}(q^2+1)$ for $n \geq 5$. If $n = 5$, one sees that inequality holds for $q \geq 4$. If $n = 5$ and $q = 3$ an explicit computation shows that $[a, c] > {}^{q^{n+1}}/_{q-1}$. If $n \geq 6$, we estimate ${}^{q-1}/_2(q^n+1)(q^{n-2}+1) > q^{2n-2}$ and $q^{n+1}(q^2+1) \leq q^{n+4}$, which is enough to show the inequality. Hence in all cases $[a, c] > {}^{q^{n+1}}/_{q-1}$.

Next, we compute

$$
(a, b) = {}^1/_2 \cdot \left({}^{q^n+1}/_2, {}^{(q-1)(q^{n-1}+1)}/_d\right) \leq {}^1/_2 \cdot (q^n+1, q-1) \cdot \Big(q^n+1, q^{n-1}+1\Big) = 2\,.
$$

Now, using that $d \leq 2$, observe that $(q-1)[a, b] \geq {}^{(q-1)^2}/_{32} \cdot (q^n+1)(q^{n-1}+1) \geq {}^1/_8 \cdot (q^n+1)(q^{n-1}+1) \geq {}^1/_{q^2} \cdot (q^n+1)(q^{n-1}+1)$. We then easily see that $(q-1)[a, b] > q^{n+1}$ for $n \geq 4$.

Now suppose that q is odd and $(q^n+1, 4) = 2$. Then the center of $\Omega^-_{2n}(q)$ is trivial, i.e. $P\Omega^-_{2n}(q) = \Omega^-_{2n}(q)$. We can then choose the following element orders according to

[But10, Corollary 8]:

$$a = \frac{q^n + 1}{2}$$
$$b = \left[q + 1, q^{n-1} - 1\right]$$
$$c = p\left[q + 1, \frac{q^{n-2} + 1}{2}\right]$$

Suppose in the following that n is odd. Then $\left(q + 1, q^{n-1} - 1\right) = q + 1$ and hence $b = q^{n-1} - 1$. Moreover, $\left(q + 1, {(q^{n-2}+1)}/{2}\right) = {(q+1)}/{2}$ by Lemma A.0.12, so that $c = p \cdot (q^{n-2} + 1)$. We then obtain that $(b, c) = q + 1$, $(a, c) \leq q^{(n,2)} = q + 1$ and $(a, b) \leq \left(q^n + 1, q^{n-1} - 1\right) = q + 1$. A quick computation shows that $[a, b], [a, c]$ and $[b, c]$ each are larger than ${q^{n+1}}/{q-1}$.

If n is even, then $\left(q - 1, q^{n-1} + 1\right) = 2$ and $\left(q + 1, {(q^{n-2}+1)}/{2}\right) = 1$ so that $b = {(q-1)(q^{n-1}+1)}/{2}$ and $c = {p}/{2} \cdot (q + 1)(q^{n-2} + 1)$. We then compute $(b, c) = q + 1$, $(a, b) = 1$ since $\left({(q^n+1)}/{2}, {(q+1)}/{2}\right) = 1$ and $\left({(q^n+1)}/{2}, q + 1\right) = 1$ and $(a, c) = 1$ as $\left(q^n + 1, q^{n-2} + 1\right) = 2$. With these results it is then easy to verify that $[a, b], [a, c]$ and $[b, c]$ exceed ${q^{n+1}}/{q-1}$.

Finally, we analyze the spectrum if q is even. According to [But10, Corollary 4] we can choose the following element orders:

$$a = q^n + 1$$
$$b = [q - 1, q^{n-1} + 1] = (q - 1) \cdot (q^{n-1} + 1)$$
$$c = 2(q^{n-2} + 1)$$

One now easily verifies using Lemma A.0.5 that a, b and c are pairwise coprime and $[a, b], [a, c]$ and $[b, c]$ exceed ${q^{n+1}}/{q-1}$.

$\boldsymbol{{}^2E_6(q)}$ According to [KS02, Section 2.8] the maximal tori for ${}^2E_6(q)$ can be obtained from those of $E_6(q)$ by replacing q by $-q$. This way we obtain the following orders of semisimple elements up to multiplication by $(3, q + 1)$:

$$a = (q - 1)(q^5 + 1)$$
$$b = (q^2 - q + 1)(q^4 - q^2 + 1)$$
$$c = q^6 - q^3 + 1$$

As before, we obtain $(a, b) = (a, c) = (b, c) = (3, q + 1)$. A simple calculation shows that ${ac}/{3}$, ${ab}/{3}$ and ${bc}/{3}$ each exceed q^7 for $q \geq 2$.

$\boldsymbol{{}^3D_4(q)}$ By [KS02, Section 2] there are semisimple elements of orders a, b, c where

$$a = (q^3 + 1)(q - 1)$$
$$b = (q^3 - 1)(q + 1)$$
$$c = q^4 - q^2 + 1\,.$$

Note that by Lemma A.0.14 we have that the element orders in ${}^3D_4(q)$ are bounded by ${}^{q^5}\!/_{q-1} \leq q^5$ since ${}^3D_4$ is of rank 4.

Also for abitrary integers q we have

$$\begin{aligned}
\Big(q^4 - q^2 + 1, (q^3+1)(q-1)\Big) &= (2, q^2 - q - 1) = 1 \\
\Big(q^4 - q^2 + 1, (q^3-1)(q+1)\Big) &= (2, q^2 + q - 1) = 1 \\
\Big((q^3+1)(q-1), (q^3-1)(q+1)\Big) &= (q-1)\cdot(q+1)
\end{aligned}$$

The first and second equations follow as $q^2 - q = q(q-1)$ and $q^2 + q = q(q+1)$ are always even, so that $(2, q^2 - q - 1) = 1 = (2, q^2 + q - 1)$. The last equation follows from the fact that $q^3 - 1 = (q-1)\cdot(q^2+q+1)$ and $q^3 + 1 = (q+1)\cdot(q^2-q+1)$ and $(q^2+q+1, q^2-q+1) = (2q, q^2-q+1) = 1$ as $q^2 - q + 1$ is odd and $(q, q^2-q+1) = 1$. We then obtain

$$\begin{aligned}
[a,b] &= \frac{ab}{(a,b)} = (q^3+1)(q^3-1) > q^5 \\
[a,c] &= ac > q^5 \\
[b,c] &= bc > q^5
\end{aligned}$$

Finally, we deal with the Ree and Suzuki groups:

Suzuki groups ${}^2B_2(q)$ where $q = 2^{2n+1}$ for $n \geq 1$

In [HBb, XI Theorem 3.10] it was shown that

$$\mu({}^2B_2(2^{2n+1})) = \{4, 2^{2n+1} - 1, 2^{2n+1} - 2^{n+1} + 1, 2^{2n+1} + 2^{n+1} + 1\}\,,$$

thus $|\mu({}^2B_2(2^{2n+1}))| = 4$.

Tits group ${}^2F_4(2)'$

By the ATLAS [Con+] this group of order 17971200 has $\mu({}^2F_4(2)') = \{10, 12, 13, 16\}$.

Ree groups of type ${}^2F_4(q)$ for $q = 2^{2n+1}, n \geq 1$

The element orders of these groups have been determined in [DS99, Lemma 3]. The two largest element orders are

$$\begin{aligned}
m_1 &= q^2 + \sqrt{2}q^{3/2} + q + \sqrt{2q} + 1 \\
m_2 &= (q-1)(q + \sqrt{2q} + 1)
\end{aligned}$$

whereas the largest order of a 2-element equals 2^4. Note that m_1 and m_2 are odd and m_2 does not divide m_1. These facts imply that $|\mu({}^2F_4(q))| \geq 3$.

Ree group ${}^2G_2(3)'$

We compute via GAP or consult [Con+] and obtain $\mu({}^2G_2(3)') = \{2, 3, 7, 9\}$.

Ree groups of type ${}^2G_2(3^{2n+1})$ for $n \geq 1$

By [KS09, Table A.7] the two largest element orders are given by

$$\begin{aligned}
m_1 &= 3^{2n+1} + 3^{n+1} + 1 \\
m_2 &= 3^{2n+1} - 1\,.
\end{aligned}$$

We see that $m_2 \nmid m_1$ and neither m_1 nor m_2 are divisible by 3, so that $|\mu({}^2G_2(3^{2n+1})| \geq 3$.

□

A.1. Sporadic Simple Groups

In order to determine the (reduced) spectrum of the sporadic simple groups, we rely on the ATLAS [Con+] resp. GAP [GAP]. If the group order is not too big we also calculate the number of conjugacy classes of maximal subgroups with the help of GAP.

	$\mu(-)$	$\lvert\mu(-)\rvert$	$\gamma(-)$
M_{11}	5, 6, 8, 11	4	4
M_{12}	6, 8, 10, 11	4	6
M_{22}	5, 6, 7, 8, 11	5	6
M_{23}	6, 8, 11, 14, 15, 23	6	6
M_{24}	8, 10, 11, 12, 14, 15, 21, 23	8	9

Table A.2.: Spectra and number of conjugacy classes of maximal cyclic subgroups of the Mathieu groups

	$\mu(-)$	$\lvert\mu(-)\rvert$	$\gamma(-)$
J_1	6, 7, 10, 11, 15, 19	6	6
J_2	7, 8, 10, 12, 15	5	7
J_3	8, 9, 10, 12, 15, 17, 19	7	?
J_4	16, 23, 24, 28, 29, 30, 31, 35, 37, 40, 42, 43, 44, 66	14	?

Table A.3.: Spectra and number of conjugacy classes of maximal cyclic subgroups of the Janko groups

	$\mu(-)$	$\lvert\mu(-)\rvert$
Co_1	16, 22, 23, 24, 26, 28, 33, 35, 36, 39, 40, 42, 60	13
Co_2	11, 16, 18, 20, 23, 24, 28, 30	8
Co_3	14, 18, 20, 21, 22, 23, 24, 30	8

Table A.4.: Spectra of the Conway groups

	$\mu(-)$	$\lvert\mu(-)\rvert$
Fi_{22}	13, 14, 16, 18, 20, 21, 22, 24, 30	9
Fi_{23}	16, 17, 22, 23, 24, 26, 27, 28, 35, 36, 39, 42, 60	13
Fi'_{24}	16, 17, 22, 23, 24, 26, 27, 28, 29, 33, 35, 36, 39, 42, 45, 60	16

Table A.5.: Spectra of the Fischer groups

	$\mu(-)$	$\lvert\mu(-)\rvert$
Higman-Sims group HS	7, 8, 11, 12, 15, 20	6
McLaughlin group McL	8, 9, 11, 12, 14, 30	6
Held group He	8, 10, 12, 15, 17, 21, 28	7
Rudvalis group Ru	14, 15, 16, 20, 24, 26, 29	7
Suzuki sporadic group Sz	11, 13, 14, 15, 18, 20, 21, 24	8
O'Nan group $O'N$	11, 12, 15, 16, 19, 20, 28, 31	8
Harada-Norton group HN	9, 12, 14, 19, 21, 22, 25, 30, 35, 40	10
Lyons group Ly	18, 22, 24, 25, 28, 30, 31, 33, 37, 40, 42, 67	12
Thomspon group Th	19, 20, 21, 24, 27, 28, 30, 31, 36, 39	10
Baby Monster group B	25, 27, 31, 32, 34, 36, 38, 39, 40, 42, 44, 46, 47, 48, 52, 55, 56, 60, 66, 70	20
Monster group M	32, 36, 38, 40, 41, 45, 48, 50, 51, 54, 56 57, 59, 60, 62, 66, 68, 69, 70, 71, 78, 84, 87, 88, 92, 93, 94, 95, 104, 105, 110, 119	32

Table A.6.: Spectra of the remaining sporadic groups

B. Computer Algebra with GAP

We used the computer algebra system GAP [GAP] at the beginning of the work on understanding the groups in the class Γ_2, i.e. the finite groups with two conjugacy classes of maximal cyclic subgroups, by listing all those groups of order at most 2000 that belong to Γ_2 and formulating suitable conjectures regarding the structure of those groups. We were able to verify these conjectures afterwards, see Section 5.2.3. The function `NumWitnesses` computes the number of conjugacy classes of maximal cyclic subgroups of a finite group. The function `Witnesses` returns representatives of the conjugacy classes of the maximal cyclic subgroups of a finite group. For the computation of the (reduced) spectra in Appendix A we sometimes relied on the function `ReducedSpectrum`. These functions and the functions that they depend on are defined as follows:

```
# Given a list of orbits of cyclic subgroups (under the
# conjugation action) removes an orbit if it corresponds to
# a non-maximal cyclic subgroup
RemoveNonMaximalOrbit := function(orbs)
  local n, m, pivot, cyclic;

  for n in [1..Size(orbs)] do
    for m in [1..Size(orbs)] do
      if n = m then
        continue;
      fi;
      # pick a cyclic in orbs[n] and see whether it
      # is containd in a cyclic in orbs[m]
      pivot := orbs[n][1];
      for cyclic in orbs[m] do
        if IsSubgroup(cyclic, pivot) then
          Remove(orbs, n);
          return orbs;
        fi;
      od;
    od;
  od;

  return orbs;
end;
```

```
# Given a list of orbits of cyclic subgroups (under the
# conjugation action) remove those orbits that do not
# correspond to maximal cyclic subgroups
RemoveNonMaximalOrbits := function(orbs)
  local s;

  s := Size(orbs);

  while s > Size(RemoveNonMaximalOrbit(orbs)) do
    s := Size(orbs);
  od;

  return orbs;
end;

# Given a finite group, returns a list of representatives of the
# conjugacy classes of maximal cyclic subgroups
Witnesses := function(group)
  local cl, cyclic_subgroups, action, orbits, maximal_orbits;

  cl := List(ConjugacyClasses(group), Representative);
  cyclic_subgroups := Set(cl, g -> Subgroup(group, [g]));

  action := function(subgroup, g)
    return ConjugateSubgroup(subgroup, g); end;

  orbits := Orbits(group, cyclic_subgroups, action);
  maximal_orbits := ShallowCopy(orbits);

  RemoveNonMaximalOrbits(maximal_orbits);

  # pick a representative in each orbit
  return List(maximal_orbits, o -> o[1]);
end;

# Given a finite group, returns the number of conjugacy classes
# of maximal cyclic subgroups
NumWitnesses := function(group)
  return Size(Witnesses(group));
end;
```

```
# Given a list of natural numbers, returns a list of those
# numbers that are maximal with respect to the divisbility
# relation
MaximalNumbers := function(li)
  local maximals, non_maximal, i, j;

  maximals := [];

  for i in li do
    non_maximal := false;

    for j in li do
      if i = j then
        continue;
      fi;

      if RemInt(j,i) = 0 then
        non_maximal := true;
        break;
      fi;
    od;

    if not non_maximal then
      Add(maximals, i);
    fi;
  od;

  return Unique(maximals);
end;

# Computes the maximal element orders of a group
# with respect to the divisbility relation
ReducedSpectrum := function(group)
  return MaximalNumbers( Set(ConjugacyClasses(group),
    c -> Order(Representative(c))) );
end;
```

Bibliography

[BLR08] Bartels, A., Lück, W. & Reich, H. On the Farrell-Jones conjecture and its applications. *J. Topol.* **1,** 57–86 (2008).

[Bas72] Bass, H. The degree of polynomial growth of finitely generated nilpotent groups. *Proc. Lond. Math. Soc. (3)* **25,** 603–614 (1972).

[Ber08] Berkovich, Y. *Groups of prime power order. Vol. 1.* xx + 512 (Berlin: Walter de Gruyter, 2008).

[Ber12] Bernays, P. *Über die Darstellung von positiven, ganzen Zahlen durch die primitiven, binären quadratischen Formen einer nicht-quadratischen Diskriminante* PhD thesis (Göttingen, 1912).

[Bha09] Bhargava, M. Groups as unions of proper subgroups. *Am. Math. Mon.* **116,** 413–422 (2009).

[BS05] Borisov, A. & Sapir, M. Polynomial maps over finite fields and residual finiteness of mapping tori of group endomorphisms. *Invent. Math.* **160,** 341–356 (2005).

[BS09] Borisov, A. & Sapir, M. Polynomial maps over p-adics and residual properties of mapping tori of group endomorphisms. *Int. Math. Res. Not.* **2009,** 3002–3015 (2009).

[Bow12] Bowditch, B. H. Relatively hyperbolic groups. *Int. J. Algebra Comput.* **22,** 1250016, 66 (2012).

[Bra81] Brandl, R. A covering property of finite groups. *Bull. Aust. Math. Soc.* **23,** 227–235 (1981).

[Bd10] Breuillard, E. & de Cornulier, Y. On conjugacy growth for solvable groups. *Ill. J. Math.* **54,** 389–395 (2010).

[Bre+13] Breuillard, E., de Cornulier, Y., Lubotzky, A. & Meiri, C. On conjugacy growth of linear groups. *Math. Proc. Camb. Philos. Soc.* **154,** 261–277 (2013).

[BH99] Bridson, M. R. & Haefliger, A. *Metric spaces of non-positive curvature.* (Berlin: Springer, 1999).

[Bro82] Brown, K. S. *Cohomology of groups.* Graduate Texts in Mathematics, 87. New York-Heidelberg-Berlin: Springer-Verlag. X. 1982.

[Bry81] Bryukhanova, E. Automorphism groups of 2-automorphic 2-groups. *Algebra Logic* **20,** 1–12 (1981).

[But08] Buturlakin, A. Spectra of finite linear and unitary groups. *Algebra Logika* **47,** 157–173 (2008).

[But10] Buturlakin, A. Spectra of finite symplectic and orthogonal groups. *Mat. Tr.* **13,** 33–83 (2010).

[CFP96] Cannon, J., Floyd, W. & Parry, W. Introductory notes on Richard Thompson's groups. *Enseign. Math. (2)* **42,** 215–256 (1996).

[Cao+04] Cao, H., Chen, G., Grechkoseeva, M., Mazurov, V., Shi, W. & Vasil'ev, A. Recognition of the finite simple groups $F_4(2^m)$ by the spectrum. *Sib. Mat. Zh.* **45,** 1256–1262 (2004).

[CS11] Caprace, P.-E. & Sageev, M. Rank rigidity for CAT(0) cube complexes. *Geom. Funct. Anal.* **21,** 851–891 (2011).

[Car61] Carter, R. Nilpotent self-normalizing subgroups of soluble groups. *Math. Z.* **75,** 136–139 (1961).

[Coh94] Cohn, J. On n-sum groups. *Math. Scand.* **75,** 44–58 (1994).

[Con+] Conway, J., Curtis, R., Norton, S., Parker, R. & Wilson, R. *Atlas of finite groups. Maximal subgroups and ordinary characters for simple groups. With comput. assist. from J. G. Thackray.* Oxford: Clarendon Press. XXXIII, 252 p. (1985).

[CK02] Coornaert, M. & Knieper, G. Growth of conjugacy classes in Gromov hyperbolic groups. *Geom. Funct. Anal.* **12,** 464–478 (2002).

[CJ09] Costantini, M. & Jabara, E. On finite groups in which cyclic subgroups of the same order are conjugate. *Commun. Algebra* **37,** 3966–3990 (2009).

[DP13] Degrijse, D. & Petrosyan, N. Commensurators and classifying spaces with virtually cyclic stabilizers. *Groups Geom. Dyn.* **7,** 543–555 (2013).

[DS99] Deng, H. & Shi, W. The characterization of Ree groups ${}^2F_4(q)$ by their element orders. *J. Algebra* **217,** 180–187 (1999).

[Far98] Farb, B. Relatively hyperbolic groups. *Geom. Funct. Anal.* **8,** 810–840 (1998).

[FH94] Fel'shtyn, A. & Hill, R. The Reidemeister zeta function with applications to Nielsen theory and a connection with Reidemeister torsion. *K-Theory* **8,** 367–393 (1994).

[FT15] Fel'shtyn, A. & Troitsky, E. Aspects of the property R_∞. *J. Group Theory* **18,** 1021–1034 (2015).

[FN13] Fluch, M. G. & Nucinkis, B. E. On the classifying space for the family of virtually cyclic subgroups for elementary amenable groups. *Proc. Am. Math. Soc.* **141,** 3755–3769 (2013).

[Fou69] Foulser, D. Solvable primitive permutation groups of low rank. *Trans. Am. Math. Soc.* **143,** 1–54 (1969).

[Fro01] Frobenius, G. Über auflösbare Gruppen. IV. *Berl. Ber.* **1901,** 1216–1230 (1901).

[GAP] *GAP – Groups, Algorithms, and Programming, Version 4.8.8* The GAP Group (2017). `https://www.gap-system.org`.

[Gon75] Gonzalez-Acuna, F. Homomorphs of knot groups. *Ann. Math. (2)* **102,** 373–377 (1975).

[GW13] Groves, J. & Wilson, J. S. Soluble groups with a finiteness condition arising from Bredon cohomology. *Bull. Lond. Math. Soc.* **45,** 89–92 (2013).

[Gru57] Gruenberg, K. Residual properties of infinite soluble groups. *Proc. Lond. Math. Soc. (3)* **7,** 29–62 (1957).

[GS10] Guba, V. & Sapir, M. On the conjugacy growth functions of groups. *Ill. J. Math.* **54,** 301–313 (2010).

[Hig63] Higman, G. Suzuki 2-groups. *Ill. J. Math.* **7,** 79–96 (1963).

[Hil91] Hillman, J. A. Elementary amenable groups and 4-manifolds with Euler characteristic 0. *J. Aust. Math. Soc., Ser. A* **50,** 160–170 (1991).

[HL92] Hillman, J. A. & Linnell, P. A. Elementary amenable groups of finite Hirsch length are locally-finite by virtually-solvable. *J. Aust. Math. Soc., Ser. A* **52,** 237–241 (1992).

[HO13] Hull, M. & Osin, D. Conjugacy growth of finitely generated groups. *Adv. Math.* **235,** 361–389 (2013).

[Hup67] Huppert, B. *Endliche Gruppen. I.* Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen. 134. Berlin-Heidelberg-New York: Springer-Verlag. XII, 793 S. mit 15 Abb. 1967.

[HBa] Huppert, B. & Blackburn, N. *Finite groups. II.* Grundlehren der Mathematischen Wissenschaften, Bd. 242. Berlin-Heidelberg-New York: Springer-Verlag. XIII, 531 p. (1982).

[HBb] Huppert, B. & Blackburn, N. *Finite groups. III.* Grundlehren der Mathematischen Wissenschaften, 243. Berlin-Heidelberg-New York: Springer-Verlag. IX, 454 p. (1982).

[Isa08] Isaacs, I. *Finite group theory.* xi + 350 (Providence, RI: American Mathematical Society (AMS), 2008).

[Iwa43] Iwasawa, K. Einige Sätze über freie Gruppen. *Proc. Imp. Acad. Tokyo* **19,** 272–274 (1943).

[JL06] Juan-Pineda, D. & Leary, I. J. *On classifying spaces for the family of virtually cyclic subgroups.* in *Recent developments in algebraic topology. A conference to celebrate Sam Gitler's 70th birthday, San Miguel de Allende, México, December 3–6, 2003* 135–145 (Providence, RI: American Mathematical Society (AMS), 2006).

[jHal] Jun. Hall, M. *The theory of groups.* New York: The Macmillan Company. xiii, 434 p. (1959).

[KS09] Kantor, W. M. & Seress, Á. Large element orders and the characteristic of Lie-type simple groups. *J. Algebra* **322,** 802–832 (2009).

[KS02] Kantor, W. M. & Seress, Á. Prime power graphs for groups of Lie type. *J. Algebra* **247,** 370–434 (2002).

[Kap00] Kapovich, I. Mapping tori of endomorphisms of free groups. *Commun. Algebra* **28,** 2895–2917 (2000).

[KM98] Kharlampovich, O. & Myasnikov, A. Hyperbolic groups and free constructions. *Trans. Amer. Math. Soc.* **350,** 571–613 (1998).

[KM93] Kim, G. & McCarron, J. On amalgamated free products of residually p-finite groups. *J. Algebra* **162,** 1–11 (1993).

[KMN11] Kochloukova, D., Martínez-Pérez, C. & Nucinkis, B. Cohomological finiteness conditions in Bredon cohomology. *Bull. Lond. Math. Soc.* **43,** 124–136 (2011).

[KMT14] Krempa, J., Macedońska, O. & Tomaszewski, W. On finite number of conjugacy classes in groups. *Commun. Algebra* **42,** 5170–5179 (2014).

[Küh96] Kühnlein, S. Partial solution of a conjecture of Schmutz. *Arch. Math.* **67,** 164–172 (1996).

[Kur55] Kurosh, A. G. *The theory of groups. Vol. I* Translated and edited by K. A. Hirsch, 272 (Chelsea Publishing Co., New York, N.Y., 1955).

[Kut76] Kutzko, P. On groups of finite weight. *Proc. Am. Math. Soc.* **55,** 279–280 (1976).

[LN01] Leary, I. J. & Nucinkis, B. E. Every CW-complex is a classifying space for proper bundles. *Topology* **40,** 539–550 (2001).

[Lüc09] Lück, W. On the classifying space of the family of virtually cyclic subgroups for CAT(0)-groups. *Münster J. Math.* **2,** 201–214 (2009).

[Lüc05] Lück, W. *Survey on classifying spaces for families of subgroups.* in *Infinite groups: geometric, combinatorial and dynamical aspects. Based on the international conference on group theory: geometric, combinatorial and dynamical aspects of infinite groups, Gaeta, Italy, June 1–6, 2003.* 269–322 (Basel: Birkhäuser, 2005).

[Lüc00] Lück, W. The type of the classifying space for a family of subgroups. *J. Pure Appl. Algebra* **149,** 177–203 (2000).

[Lüc89] Lück, W. *Transformation groups and algebraic K-theory.* xii + 443 (Berlin etc.: Springer-Verlag, 1989).

[Lüc+17] Lück, W., Reich, H., Rognes, J. & Varisco, M. Assembly maps for topological cyclic homology of group algebras. *J. Reine Angew. Math.* (2017).

[LW12] Lück, W. & Weiermann, M. On the classifying space of the family of virtually cyclic subgroups. *Pure Appl. Math. Q.* **8,** 497–555 (2012).

[LS62] Lyndon, R. & Schützenberger, M. The equation $a_M = b^N c^P$ in a free group. *Mich. Math. J.* **9,** 289–298 (1962).

[LS] Lyndon, R. C. & Schupp, P. E. *Combinatorial group theory.* Ergebnisse der Mathematik und ihrer Grenzgebiete. 89. Berlin-Heidelberg-New York: Springer-Verlag. XIV, 339 p. (1977).

[Mal83] Mal'cev, A. On homomorphisms onto finite groups. *Transl., Ser. 2, Am. Math. Soc.* **119,** 67–79 (1983).

[MS02] Meintrup, D. & Schick, T. A model for the universal space for proper actions of a hyperbolic group. *New York J. Math.* **8,** 1–7 (2002).

[MO06] Moree, P. & Osburn, R. Two-dimensional lattices with few distances. *Enseign. Math. (2)* **52,** 361–380 (2006).

[New68] Newman, B. Some results on one-relator groups. *Bull. Am. Math. Soc.* **74,** 568–571 (1968).

[Ols91] Ol'shanskij, A. Y. *Geometry of defining relations in groups.* (Dordrecht etc.: Kluwer Academic Publishers, 1991).

[Ont05] Ontaneda, P. Cocompact CAT(0) spaces are almost geodesically complete. *Topology* **44,** 47–62 (2005).

[Osi06] Osin, D. Relatively hyperbolic groups: intrinsic geometry, algebraic properties, and algorithmic problems. *Mem. Amer. Math. Soc.* **843,** 100 (2006).

[Osi10] Osin, D. Small cancellations over relatively hyperbolic groups and embedding theorems. *Ann. of Math. (2)* **172,** 1–39 (2010).

[Pas92] Passman, D. The adjoint representation of group algebras and enveloping algebras. *Publ. Mat., Barc.* **36,** 861–878 (1992).

[Pla68] Platonov, V. A certain problem for finitely generated groups. *Dokl. Akad. Nauk BSSR* **12,** 492–494 (1968).

[Qui10] Quillen, D. *Higher algebraic K-theory. I.* in *Cohomology of groups and algebraic K-theory. Selected papers of the international summer school on cohomology of groups and algebraic K-theory, Hangzhou, China, July 1–3, 2007* 413–478 (Somerville, MA: International Press; Beijing: Higher Education Press, 2010).

[Ram18] Ramras, D. A. A note on orbit categories, classifying spaces, and generalized homotopy fixed points. *J. Homotopy Relat. Struct.* **13,** 237–249 (2018).

[Rob12] Robinson, D. *A Course in the Theory of Groups* 481 (Springer Science & Business Media, 2012).

[Rob] Robinson, D. J. *Finiteness conditions and generalized soluble groups. Part 1.* Ergebnisse der Mathematik und ihrer Grenzgebiete. Band 62. Berlin-Heidelberg-New York: Springer-Verlag. XIV, 210 p. (1972).

[SW02] Sapir, M. & Wise, D. T. Ascending HNN extensions of residually finite groups can be non-Hopfian and can have very few finite quotients. *J. Pure Appl. Algebra* **166,** 191–202 (2002).

[Sax88] Saxl, J. On a question of W. Jehne concerning covering subgroups of groups and Kronecker classes of fields. *J. Lond. Math. Soc., II. Ser.* **38,** 243–249 (1988).

[Sez14] Sezer, S. On finite solvable groups whose cyclic p-subgroups of equal order are conjugate. *J. Algebra* **415,** 214–233 (2014).

[Shu69a] Shult, E. On finite automorphic algebras. *Ill. J. Math.* **13,** 625–653 (1969).

[Shu69b] Shult, E. On the triviality of finite automorphic algebras. *Ill. J. Math.* **13,** 654–659 (1969).

[Sis16] Sisto, A. Contracting elements and random walks. *J. reine angew. Math.* (2016).

[Tit72] Tits, J. Free subgroups in linear groups. *J. Algebra* **20,** 250–270 (1972).

[Tom97] Tomkinson, M. Groups as the union of proper subgroups. *Math. Scand.* **81,** 191–198 (1997).

[VGM09] Vasil'ev, A., Grechkoseeva, M. & Mazurov, V. Characterization of the finite simple groups by spectrum and order. *Algebra Logic* **48,** 385–409 (2009).

[Vdo08] Vdovin, E. Carter subgroups of finite groups. *Mat. Tr.* **11,** 20–106 (2008).

[vW17] von Puttkamer, T. & Wu, X. Linear groups, conjugacy growth, and classifying space for families of subgroups. *Int. Math. Res. Not. IMRN* **0.** arXiv: `1704.05304` (2017).

[vW] von Puttkamer, T. & Wu, X. *On the finiteness of the classifying space for the family of virtually cyclic subgroups* arXiv: `1607.03790`.

[Wil81] Williams, J. Prime graph components of finite groups. *J. Algebra* **69,** 487–513 (1981).

[Wil09] Wilson, R. A. *The finite simple groups.* xv + 298 (London: Springer, 2009).

[Win72] Winter, D. L. The automorphism group of an extraspecial p-group. *Rocky Mt. J. Math.* **2,** 159–168 (1972).

[Zap91] Zappa, G. The papers of Gaetano Scorza on group theory. *Atti Accad. Naz. Lincei, Cl. Sci. Fis. Mat. Nat., IX. Ser., Rend. Lincei, Mat. Appl.* **2,** 95–101 (1991).

[Zav04] Zavarnitsine, A. V. Recognition of the simple groups $L_3(q)$ by element orders. *J. Group Theory* **7,** 81–97 (2004).

[Zha89] Zhang, G. On self-normalizing cyclic subgroups. *J. Algebra* **127,** 255–258 (1989).