Effective conjugacy separability of finitely generated nilpotent groups

Mark Pengitore

February 20, 2015

Abstract

We make effective conjugacy separability for finitely generated nilpotent groups using work of Blackburn and Mal’tsev. More precisely, we give polynomial upper and lower bounds for the asymptotic behavior of an associated complexity function introduced by Lawton, Louder, and McReynolds that measures how large the needed quotients are in separating pairs of conjugacy classes of bounded word length.

1 Introduction

In 1911, Dehn [13] posed the following question. Can one determine in finite time whether a word is trivial or not in a given finitely generated group? Formally, the above question is known as the word problem. A solution to the word problem will reflect geometric properties of the group as well as shed light on properties of geometric objects that the group is an algebraic invariant of. When the group under consideration is the fundamental group of a manifold, for instance, a solution to the word problem implies that we can determine in finite time when a closed loop is homotopically trivial.

Mal’tsev [31] was the first to consider solving the word problem for a group \( \Gamma \) using finite quotients of \( \Gamma \). More specifically, one can ask if for each non-trivial word \( \gamma \in \Gamma \) does there exists a finite index normal subgroup \( \Delta \) such that \( \gamma \neq 1 \) in \( \Gamma / \Delta \). When the above question has an affirmative answer for each such \( \gamma \), we say that \( \Gamma \) is residually finite. It was observed by Mal’tsev that if \( \Gamma \) is residually finite and finitely presentable, there exists a solution to the word problem.

Dehn asked an analogous question for conjugacy classes. Specifically, can one determine whether two elements are conjugate in a group in finite time? This problem is referred to as the conjugacy problem and it is a simple matter to see that a solution to the conjugacy problem implies that there exists a solution to the word problem. Subsequently one can try to provide a solution to the conjugacy problem using finite quotients. If for each pair of non-conjugate elements \( \gamma, \eta \in \Gamma \) there exists a finite index normal subgroup \( \Delta \) such that the images of \( \gamma \) and \( \eta \) in \( \Gamma / \Delta \) are not conjugate, we say that \( \Gamma \) is conjugacy separable. Mal’tsev [31] also proved that for any finitely presentable, conjugacy separable group, there exists a solution to the conjugacy problem.

One can see that every conjugacy separable group is residually finite; however, there is a rich collection of finitely presented groups that are residually finite but not conjugacy separable. Mal’tsev [31] proved that all finitely generated linear groups are residually finite. On the other hand, Stebe [39] demonstrated that \( GL_n(\mathbb{Z}) \) and \( SL_n(\mathbb{Z}) \) are conjugacy separable if and only if \( n = 1, 2 \) and since then Stebe’s results have been vastly generalized (see [55, Proposition 8.26]). Moreover, conjugacy separability is not well behaved with respect
to group operations. For example, conjugacy separability is closed under free products but is not closed with respect to finite index subgroups or finite extensions [17]. This, many of the tools one uses when studying residual finiteness are ineffective in the study of conjugacy separability. In this way, one can see that the collection of conjugacy separable groups form a complicated class of groups.

Conjugacy separability, residual finiteness, subgroup separability, and other residual properties have been extensively studied and used to great effect in resolving important conjectures in geometry, such as the work of Agol on the Virtual Haken conjecture. Much of the work in the literature has been to understand which groups satisfy various residual properties. For example, free groups, polycyclic groups, and surface groups have all been shown to be residually finite and conjugacy separable [2], [10], [32], [37]. However, there is an active area of research into making many of these residual properties effective. Therefore a natural question one may ask is quantifying the extent to which a given group satisfies these residual properties. In particular we are interested in how complex distinguishing conjugacy classes is via a quantification of conjugacy separability for finitely generated nilpotent groups.

For a finitely generated group $\Gamma$ and fixed finite generating set $S$, Lawton–Louder–McReynolds [24] introduced a function $\text{Conj}_{\Gamma,S}(n)$ on the natural numbers (see Section 2.1) that quantifies conjugacy separability. Specifically, the value on a positive integer $n$ is the maximum order of the minimal finite quotient needed to distinguish pairs of non-conjugate elements as one varies over the $n$-ball. This function is analogous to a function introduced by Bou–Rabee [4] that quantifies residual finiteness. Following Bou-Rabee, we denote this function as $F_{\Gamma,S}(n)$. Numerous authors have studied the asymptotic behavior of $F_{\Gamma,S}$ for a wide collection of groups $\Gamma$, (see [3], [4], [6], [10], [11], [21], [34], [36]), and has been useful in improving our understanding of interesting classes of groups. One can see that $F_{\Gamma,S}(n)$ is always bounded above by $\text{Conj}_{\Gamma,S}(n)$ for any group $\Gamma$ and finite generating set $S$ (see [24] Lemma 2.1), which further illustrates the more complicated nature of conjugacy separability versus residual finiteness.

For finitely generated nilpotent groups $\Gamma$, our two results demonstrate that the function $\text{Conj}$ reflects the polynomial structure of $\Gamma$, as seen in the work of Gromov, Lubotzky, Milnor, and others [1], [14], [18], [27], [33], [40]. To be more specific $\text{Conj}$ has polynomial upper and lower bounds asymptotically as a function of word length; we refer the reader to Section 2.1 for a precise definition of $\prec$.

**Theorem 1.1.** Let $\Gamma$ be a finitely generated nilpotent group with finite generating set $S$. If $\Gamma$ is not virtually abelian, then there exists an integer $D_1 > 0$ such that $n^{D_1} \preceq \text{Conj}_{\Gamma,S}(n)$.

**Theorem 1.2.** Let $\Gamma$ be a finitely generated nilpotent group with finite generating set $S$. Then there exists an integer $D_2 > 0$ such that $\text{Conj}_{\Gamma,S}(n) \preceq n^{D_2}$.

Additionally $D_1$ and $D_2$ can be determined explicitly from the structure of $\Gamma$.

Bou-Rabee [4] demonstrated that

$$F_{\Gamma,S}(n) \preceq (\log(n))^{D'}$$

for some integer $D' > 0$. Subsequently our work is the first to establish dramatically different growth rates between the residually finiteness function and the conjugacy separability function.

Blackburn [2] was the first to prove conjugacy separability of finitely generated nilpotent groups. Given two non-conjugate words of length at most $n$, our task is to find a homomorphism to a finite group $Q$ where our given words have non-conjugate image and the cardinality of $Q$ is no bigger than $Cn^{D_2}$ for some constant $C > 0$. Moreover, the degree $D_2$ and the constant $C$ must be independent of the given words. Our strategy is to make effective the conjugacy separability of these groups by following [2] and translating that to a Lie algebra setting using work of Mal’tsev. One technical hurdle is relating the word length of group elements to the structure of a naturally associated Lie algebra.
1.1 Acknowledgements

I would like to thank my advisor Ben McReynolds for all his help and my mentor Priyam Patel for her guidance. I am indebted to Karel Dekimpe for his suggestions for Proposition 5.3. Finally I want to thank Nick Miller, Artur Jackson, Alex Barrios, Rachel Davis, and Brooke Davisson for conversations on this work.

2 Background

We divide the background into a number of sections. The first two sections introduce the group theoretic prerequisites required for our article. The next section introduce the Lie theoretic tools which we use throughout our article. The last section packages all of these tools together.

Notation. The following notation is utilized throughout this article.

- $\Gamma$ is a finitely generated group and $S$ is a finite generating set. Often times $\Gamma$ will be a nilpotent group. $\gamma, \eta \in \Gamma$ are distinct elements of $\Gamma$ and $||\gamma||_S$ is the word length of $\gamma$ in $\Gamma$ with respect to the generating set $S$. We denote the n-ball of $\Gamma$ with respect to the generating set $S$ as $B_{\Gamma,S}(n)$.
- $[\gamma, \eta]$ is the commutator of $\gamma$ and $\eta$ and $[H,K]$ is the commutator subgroup of $H$ and $K$ for subgroups $H, K \leq \Gamma$.
- $\pi_H : \Gamma \rightarrow \Gamma/H$ to be the canonical projection.
- We denote $Z(\Gamma), \Gamma^i, \Gamma_i$ as the center, $i$th step of the upper central series and $i$th step of the lower central series of $\Gamma$ respectively.
- $C_\Gamma(\gamma)$ to be the centralizer of $\gamma$.
- $\pi_H : \Gamma \rightarrow \Gamma/H$ to be the canonical projection.
- $\pi_H : \Gamma \rightarrow \Gamma/H$ to be the canonical projection.
- $c_\Gamma$, $h_\Gamma$ and $d_\Gamma$ as the nilpotent step size, Hirsch length and the homogeneous dimension of $\Gamma$ respectively when $\Gamma$ is nilpotent.
- For a group $\Gamma$ and elements $\gamma, \eta$ of $\Gamma$, we write $\gamma$ is conjugate to $\eta$ in $\Gamma$ as $\gamma \sim \eta$. We denote the $\Gamma$ conjugacy class of $\gamma$ as $[\gamma]_\Gamma$.
- $\Delta_i \big|_{h_i}$ as a torsion-free central series, $\{\xi_i\}_{i=1}^{h_i}$ as a compatible set of generators, and $\{v_i\}_{i=1}^{h_i}$ as an induced basis for $\Gamma$.
- For a group $\Gamma$ we denote $T_\Gamma$ to be the subgroup generated by torsion elements of $\Gamma$. When $\Gamma$ is clear from context we write $T$.
- $G$ is a Lie group and $\mathfrak{g}$ is a Lie algebra.
- For a Lie algebra $\mathfrak{g}$ we denote $X$ as a basis for $\mathfrak{g}$. We denote $||A||_X$ as the length of the vector in respect to the basis $X$. We denote the n-ball as $B_{\mathfrak{g},X}(n)$.
- $\pi_\mathfrak{h} : \mathfrak{g} \rightarrow \mathfrak{g}/\mathfrak{h}$ as the canonical projection.
- $\pi_\mathfrak{h} : \mathfrak{g} \rightarrow \mathfrak{g}/\mathfrak{h}$ as the canonical projection.
- $\pi_\mathfrak{h} : \mathfrak{g} \rightarrow \mathfrak{g}/\mathfrak{h}$ as the canonical projection.
- $\pi_\mathfrak{h} : \mathfrak{g} \rightarrow \mathfrak{g}/\mathfrak{h}$ as the canonical projection.
2.1 Finitely generated groups and the conjugacy problem

For \( f, g : \mathbb{N} \to \mathbb{N} \), we write \( f \preceq g \) if there exists a natural number \( C \) such that \( f(n) \leq Cg(cn) \) for all \( n \). Additionally, we write \( f \approx g \) if \( f \preceq g \) and \( g \preceq f \).

For a group \( \Gamma \) and an element \( \gamma \in \Gamma \), we define the \( \Gamma \)-conjugacy class of \( \gamma \) to be

\[ [\gamma]_\Gamma \overset{\text{def}}{=} \{ \lambda^{-1} \gamma \lambda : \lambda \in \Gamma \} . \]

When \( [\gamma]_\Gamma = [\eta]_\Gamma \), we say that \( \gamma \) is conjugate to \( \eta \) and write \( \gamma \sim_c \eta \). For \( \gamma, \eta \in \Gamma \), we denote the commutator bracket as \( [\gamma, \eta] = \gamma^{-1} \eta^{-1} \gamma \eta \). For subgroups \( H, K \subseteq \Gamma \), we define \([H, K]\) as the subgroup generated by commutators of the elements of \( H \) and \( K \).

Following [24], we define

\( \text{CD}_\Gamma : \Gamma \times \Gamma \to \mathbb{N} \cup \{\infty\} \)

as

\[ \text{CD}_\Gamma (\gamma, \eta) = \min \{ [\Gamma : \Delta] : \Delta \triangleleft \Gamma \text{ and } g \sim_c h \text{ in } \Gamma / \Delta \} \]

with the understanding that \( \text{CD} (\gamma, \eta) = \infty \) if \( \gamma \sim_c \eta \) in every finite quotient of \( \Gamma \). We define

\[ \text{Conj}_{\Gamma, S} : \mathbb{N} \to \mathbb{N} \cup \{\infty\} \]

as

\[ \text{Conj}_{\Gamma, S} (n) = \max \{ \text{CD}_\Gamma (\gamma, \eta) : \gamma, \eta \in B_{\Gamma, S} (n), \gamma \sim_c \eta \} . \]

Asymptotically, this function is independent of the generating set as exhibited by the following lemma (see [24] Lemma 2.1).

**Lemma 2.1.** For any finite generating sets \( S_1, S_2 \) of \( \Gamma \)

\[ \text{Conj}_{\Gamma, S_1} (n) \approx \text{Conj}_{\Gamma, S_2} (n) \]

The proof of the previous lemma follows along the same lines as the proof seen in [4] Lemma 1.1.

When \( \Gamma \) is conjugacy separable then \( \text{Conj}_{\Gamma, S} (n) < \infty \) for all positive integers \( n \) thus establishing the connection between the complexity of solving the conjugacy problem via finite quotients and the asymptotic behavior of \( \text{Conj}_{\Gamma, S} (n) \).

2.2 Nilpotent groups

We require a few different well known normal series of \( \Gamma \). First, the lower central series of \( \Gamma \) is defined inductively by letting \( \Gamma_0 = \Gamma \) and \( \Gamma_i = [\Gamma, \Gamma_{i-1}] \). Second, we define the upper central series of \( \Gamma \) similarly by defining \( \Gamma^0 = \{1\} \) and \( \Gamma^i = \pi_{\Gamma}^{-1}(Z(\Gamma^i)) \). We say \( \Gamma \) is nilpotent if there exists an integer \( c \) such that \( \Gamma_n = \{1\} \) for \( n \geq c \). We refer to the smallest such integer, denoted \( c_{\Gamma} \), as the nilpotent step size of \( \Gamma \). A straightforward observation connecting the upper and lower central series is that \( \Gamma^0 = \Gamma \) for \( n \geq c_{\Gamma} \). Additionally, both \( \Gamma_i / \Gamma_{i+1} \) and \( \Gamma^i / \Gamma^{i+1} \) are abelian for all \( i \).

For a finitely generated nilpotent group \( \Gamma \), we define the homogeneous dimension of \( \Gamma \) to be

\[ d_{\Gamma} = \sum_{i=1}^{c_{\Gamma}} i \cdot \text{rank}_\mathbb{Z} (\Gamma_{i-1} / \Gamma_i) , \]

and the Hirsch length as

\[ h_{\Gamma} = \sum_{i=1}^{c_{\Gamma}} \text{rank}_\mathbb{Z} (\Gamma^i / \Gamma^{i+1}) . \]
In the event $\Gamma$ is torsion-free, we can refine the upper central series of $\Gamma$ by defining inductively $\{\Delta_i\}_{i=0}^{h_\Gamma}$ with $\Delta_0 = 1$ and the $\Delta_i$ satisfying the conditions

$$\Delta_i/\Delta_{i-1} \leq Z(\Gamma/\Delta_{i-1})$$

and

$$\Delta_i/\Delta_{i-1} \cong \mathbb{Z}.$$

In addition, we can pick a compatible set of generators associated to $\{\Delta_i\}_{i=0}^{h_\Gamma}$ in the following way: choose $\xi_1 \in \Gamma$ such that $\langle \xi_1 \rangle = \Delta_1$ then, assuming that $\xi_j$ has already been chosen for $j < i$, we select $\xi_i$ such that $\langle \xi_j \rangle_{j=1}^i = \Delta_i$. Following [14], we call $\{\Delta_i\}_{i=0}^{h_\Gamma}$ a torsion-free central series and $\{\xi_i\}_{i=0}^{h_\Gamma}$ a compatible set of generators to $\{\Delta_i\}_{i=0}^{h_\Gamma}$. We write $h_i, d_i,$ and $c_i$ for $h_{\Gamma/\Delta_i}, d_{\Gamma/\Delta_i}$, and $c_{\Gamma/\Delta_i}$ respectively when $\Gamma$ and the series are clear. We note that $\{\xi_i\}_{i=1}^{h_{\Gamma}}$ generates $\Gamma$ where $\xi_i = h_{\Gamma_i}$. Additionally, by [19] we can uniquely express $\gamma \in \Gamma$ as

$$\gamma = \prod_{i=1}^{h_\Gamma} \xi_{a_i}^d.$$ 

Finally if $\gamma$ is a word of length at most $n$, then by [11],

$$\sum_{i=1}^{h_\Gamma} |a_i| \leq h_{\Gamma} n^{d_{\Gamma}}.$$ 

### 2.3 Lie algebras and groups

A Lie algebra $\mathfrak{g}$ over a commutative ring $R$ with identity is an $R$-module with an alternating, bilinear map $[\cdot, \cdot] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$ satisfying the identity

$$[A, [B, C]] + [B, [C, A]] + [C, [A, B]] = 0$$

for all $A, B, C \in \mathfrak{g}$. We have the adjoint map $\text{ad} : \mathfrak{g} \to \text{End}(\mathfrak{g})$ defined by

$$\text{ad}(A) = [A, \cdot].$$

For simplicity, we denote $\text{ad}(A) = \text{ad}_A$. If $X = \{E_j\}_{j=1}^n$ is a basis for $\mathfrak{g}$, then we denote the structure constants of $\mathfrak{g}$ as $\delta_{i,j}^k$ where

$$[E_i, E_j] = \sum_{k=1}^n \delta_{i,j}^k E_k.$$ 

We denote the $n$-ball for $\mathfrak{g}$ by

$$B_{\mathfrak{g},X}(n) = \left\{ \sum_{i=1}^n r_i E_i : \sum_{i=1}^n |r_i| \leq n \right\}.$$ 

One can define similar notions of centers and nilpotency of a Lie algebra $\mathfrak{g}$ by defining

$$Z(\mathfrak{g}) = \{ A \in \mathfrak{g} : [A, B] = 0 \text{ for all } B \in \mathfrak{g} \}.$$ 

We define the lower central series of $\mathfrak{g}$ via $\mathfrak{g}_0 = \mathfrak{g}$ and $\mathfrak{g}_i = [\mathfrak{g}_{i-1}, \mathfrak{g}]$. We also define the upper central series of $\mathfrak{g}$ as $\mathfrak{g}^0 = 0$ and $\mathfrak{g}^i = \pi_{\mathfrak{g}^{i-1}}(Z(\mathfrak{g}/\mathfrak{g}^{i-1}))$. We state a few facts without proof for reference later.

**Lemma 2.2.** Let $\mathfrak{g}$ be a nilpotent Lie algebra and let $A \in \mathfrak{g}^i$ and $B \in \mathfrak{g}^j$ for $i, j \geq 1$. Then $[A, B] \in \mathfrak{g}^{\min(i,j)-1}$

**Lemma 2.3.** Let $\mathfrak{g}$ be a nilpotent Lie algebra and let $A \in \mathfrak{g}^i$. For any $j \geq i - 1$, then for any $B \in \mathfrak{g}$ we have $A \in \ker((\text{ad}_B)^j).$
Unless stated otherwise, we assume that our Lie algebras are finite dimensional \( \mathbb{R} \)-modules.

If \( G \) is a real, \( n \)-dimensional Lie group, then the tangent space at the identity \( T_1 (G) \) is naturally a Lie algebra over \( \mathbb{R} \), where \( T_1 (G) \) is identified with the vector space of left-invariant vector fields with the Lie bracket of vector fields. We write \( \mathfrak{g} = T_1 (G) \) and call \( \mathfrak{g} \) the associated Lie algebra for \( G \). We define the adjoint representation of \( G \) as \( \text{Ad} : G \to \text{Aut} (\mathfrak{g}) \), where \( \text{Ad} (\gamma) \) is the derivative at the identity of the Lie isomorphism given by \( \Psi_\gamma (x) = \gamma x \gamma^{-1} \).

We introduce some notation related to the Baker-Campbell-Hausdorff formula. Let \( G \) be a simply connected, connected nilpotent Lie group with Lie algebra \( \mathfrak{g} \). It is well known that the exponential map, written \( \exp : \mathfrak{g} \to G \), is a diffeomorphism (see [22, Pg 67]). As is customary, we denote the inverse by \( \log \). It follows from the Baker-Campbell-Hausdorff formula that

\[
\log (\exp A \cdot \exp B) = \sum_{j \geq 0} \frac{(-1)^{j-1}}{j} \sum_{\sum_{i} \alpha_i + \beta_i \leq j, \alpha_i, \beta_i \geq 0} \left( \sum_{i} \alpha_i + \beta_i \right)^{-1} \left[ A^{\alpha_1} B^{\beta_1} \ldots A^{\alpha_j} B^{\beta_j} \right]
\]

for any \( A, B \in \mathfrak{g} \), where

\[
[A^{\alpha_1} B^{\beta_1} \ldots A^{\alpha_j} B^{\beta_j}] = \left[ A, [A, [A, [A, [A, [A, [A, \ldots [A, B, B, \ldots B, B, \ldots B]]]]] \ldots] \right].
\]

We set \( A * B = \log (\exp A \cdot \exp B) \) for any \( A, B \in \mathfrak{g} \).

### 2.4 Lattices and Lie Ring Groups

Let \( G \) be a \( n \)-dimensional Lie group with Lie algebra \( \mathfrak{g} \). A subgroup \( \Gamma \) of \( G \) is called a lattice if \( \Gamma \) is a discrete subgroup of \( G \) such that \( G/\Gamma \) has finite volume with the induced Haar measure. Additionally if \( G/\Gamma \) is compact, then we call \( \Gamma \) a cocompact lattice. By [30], a simply connected, connected nilpotent Lie group \( G \) admits a cocompact lattice \( \Gamma \) if and only if \( \mathfrak{g} \) admits a basis \( \{ v_i \}_{i=1}^{r} \) with rational structure constants. For any such basis, we can clear denominators and so we may assume that \( \mathfrak{g} \) has integer structure constants. Note that the dimension of \( G \) is the Hirsch length of \( \Gamma \) which we denote as \( h_G \). We also have that the nilpotent step size of \( G \) and \( \Gamma \) agree i.e. \( c_G = c_\Gamma \). As that will come up a lot, we say that a simply connected, connected nilpotent Lie group that admits a cocompact lattice is \( \mathbb{Q} \)-defined.

Let \( G \) be a \( \mathbb{Q} \)-defined group with Lie algebra \( \mathfrak{g} \). We are interested in a special class of lattices within \( G \) which naturally sit as Lie algebras over \( \mathbb{Z} \) in \( \mathfrak{g} \). We call such a lattice \( \Gamma \leq G \) a Lie ring group if \( \log (\Gamma) \) is a Lie algebra over \( \mathbb{Z} \) in \( \mathfrak{g} \). We denote that by \( n \) and call \( n \) the associated Lie algebra of \( \Gamma \). A finitely generated, torsion-free nilpotent group is not far from being a Lie ring group. For every finitely generated, torsion-free nilpotent group \( \Gamma \), there exists a Lie ring group \( \Gamma^{1,\text{c}} \), unique up to isomorphism, in which \( \Gamma \) sits as a finite index subgroup (see [38 Chapter 6, Section B]). We call \( \Gamma^{1,\text{c}} \) the Lie ring hull of \( \Gamma \).

Let \( \Gamma \) be a finitely generated, torsion-free nilpotent group. By [29], there exists a \( \mathbb{Q} \)-defined group \( G \), unique up to isomorphism, with Lie algebra \( \mathfrak{g} \) in which \( \Gamma \) embeds as a cocompact lattice. We denote \( G \) as the Mal’cev completion of \( \Gamma \). Let \( \{ \Delta_i \}_{i=0}^{k} \) be a torsion-free central series of \( \Gamma \) and \( \{ \xi_i \}_{i=0}^{k} \) a compatible generating set. Associated with each \( \xi_i \), there exists a 1-parameter family of group elements \( \{ \xi_i^{r_i} : r_i \in \mathbb{R} \} \) satisfying

\[
G = \left\{ \xi_1^{r_1} \ldots \xi_k^{r_k} : r_i \in \mathbb{R} \right\}
\]

(see [22 Corollary 1.126]). Additionally, \( \xi_1^{r_1} \ldots \xi_k^{r_k} \in \Gamma \) if and only if \( r_i \in \mathbb{Z} \) for all \( i \). We also have that the vectors \( v_i = \log (\xi_i) \) span \( \mathfrak{g} \). We call \( \{ v_i \}_{i=1}^{k} \) an induced basis.
Suppose $\Gamma$ is a Lie ring group and let $\{\Delta_i\}_{i=0}^{h_G}$ be a torsion-free central series of $\Gamma$ with compatible generating set $\{\xi_i\}_{i=1}^{h_G}$ and induced basis $\{\eta_i\}_{i=1}^{h_G}$. We observe that many properties of $\Gamma$ are shared by $n$. We have that $c_n = c_\Gamma$, rank$_Z(n) = h_G$, and that $\{\eta_i\}_{i=1}^{h_G}$ is a $Z$-basis for $n$. Additionally, $n' = n \cap g'$ and $n_i = n \cap g_i$.

One can also see that rank$_Z(n') = \ell_i$ and that $\{\Delta_i\}_{i=0}^{h_G}$ induces a filtration by Lie ideals of $n$, namely $\{\log(\Delta_i)\}_{i=0}^{h_G}$. These ideals satisfy similar properties to a torsion-free central series of a finitely generated nilpotent group in the following way: let $h = \log(\Delta_i)$, then

$$h_i/h_{i-1} \subset Z(n/h_{i-1})$$

and $h_i/h_{i-1} \cong Z$. One can see that $\{\eta_i\}_{i=1}^{h_G}$ is compatible in a natural way with $\{\eta_i\}_{i=1}^{h_G}$. Subsequently we call $\{\eta_i\}_{i=1}^{h_G}$ an induced central Lie series of $n$ (for a more detailed account of the above, we refer the reader to [14] Chapter 1).

A choice of Lie ring group $\Gamma$, Mal’tsev completion $G$, associated Lie algebra $n$, torsion-free central series $\{\Delta_i\}_{i=0}^{h_G}$ of $\Gamma$, compatible generating set $\{\xi_i\}_{i=1}^{h_G}$, and induced basis $\{\eta_i\}_{i=1}^{h_G}$ will be called an admissible 6-tuple and we denote it as $\{\Gamma, G, n, \Delta_i, \xi_i, \eta_i\}$.

### 3 Blackburn’s proof and a simple example

We start with a review Blackburn’s proof of the conjugacy separability of finitely generated nilpotent groups. This section will provide motivation for estimates we give in the following sections and how one obtains effective upper bound for the conjugacy separability function for finitely generated nilpotent groups (see [2] for a more thorough account of Blackburn’s methods).

We first restrict to the torsion-free case. Let $\Gamma$ be a finitely generated, torsion-free nilpotent group and let $\{\Delta_i\}_{i=0}^{h_G}$ be a torsion-free central series of $\Gamma$ with compatible generating set $\{\xi_i\}_{i=1}^{h_G}$. We proceed by induction on the Hirsch length of $\Gamma$ with the observation that the base case $\Gamma = Z$ is clear. Assume that $\Gamma$ has Hirsch length $h_\Gamma > 1$ and let $\gamma$ and $\eta$ be two non-conjugate words of $\Gamma$. If $\gamma$ and $\eta$ are non-conjugate in $\Gamma/\Delta_i$, then by induction we are done. Otherwise we have that $\gamma$ is conjugate to an element of the form $\gamma_{\xi_1}^{k_{\gamma, \eta}}$. Blackburn then introduces the following map which we will take as a definition.

**Definition 3.1.** Let $\Gamma$ be a finitely generated, torsion-free nilpotent group with torsion-free central series $\{\Delta_i\}_{i=0}^{h_G}$ and compatible generating set $\{\xi_i\}_{i=1}^{h_G}$. Let $\gamma \in \Gamma$ and define the map

$$\varphi_{\Gamma, \gamma} : \pi^{-1}(C_{/\Delta_i}(\gamma)) \rightarrow \Delta_i$$

to be given by $\varphi_{\Gamma, \gamma}(\eta) = [\gamma, \eta]$. Let $\tau_{\gamma, \gamma}$ satisfy $\left(\xi_{\tau_{\gamma}}^{\gamma} \right) = \text{Im}(\varphi_{\Gamma, \gamma})$, and let $z_{\gamma, \gamma} \in \Gamma$ satisfy $\varphi_{\Gamma, \gamma}(z_{\gamma, \gamma}) = \xi_{\tau_{\gamma}}^{\gamma}$. We now choose a prime power $p^m$ such that $p^m$ divides $\tau_{\gamma}$ but does not divide $k$. There are two integers of importance that Blackburn constructs that we need to reference. There exists an integer $w_{p, \gamma}$ such that if $\alpha \geq w_{p, \gamma}$, then for each $g \in \Gamma^{\alpha}$ there exists $h \in \Gamma$ satisfying $h^{p^{\alpha-w_{p, \gamma}}} = g$ (see [2] Lemma 2), Proposition 5.7 (for more details). There also exists an integer $e_{\Gamma, \gamma}$ such that if $\alpha \geq e_{\Gamma, \gamma}$, then

$$C_{/\Delta_i}(\gamma) \subseteq C_{/\Delta_i}(\gamma) \cdot \Gamma^{p^m} \cdot \left(\gamma \cdot \Gamma^{p^m} \right)$$

(see [2] Lemma 3], Proposition 5.8 (for more details). We set $\beta = m + w_{p, \gamma} + e_{\Gamma, \gamma}$, and Blackburn demonstrates that $\gamma$ is not conjugate to $\eta$ in $\Gamma/\Gamma^{p^m}$. So to obtain an asymptotic upper bound for $\text{Conj}_{/\Delta_i}(n)$ we need to provide bounds in terms of word length for $\tau_{\gamma}$, $p^m$, $w_{p, \gamma}$, and $k_{\gamma, \eta}$. 

For a finite generated nilpotent group possibly with torsion \( \Gamma \) we proceed by induction on the order of the torsion subgroup which in our case is always a finite characteristic subgroup. Let \( T \) be the torsion subgroup of \( \Gamma \). We note that if \( |T| = 1 \), then \( \Gamma \) is torsion-free which has been accounted for by our previous discussion. For the inductive step we have two different cases. If \( T \) is a \( p \)-group, we let \( p^m \) be the exponent of \( T \) and set \( \alpha = m + eT, \eta + \varphi_{p,T} \). Blackburn then demonstrates that \( \gamma \) and \( \eta \) are not conjugate in \( \Gamma / \Gamma^\alpha \). When \( T \) is not a \( p \)-group, Blackburn demonstrates that one can reduce to when \( T \) is a \( p \)-group. We note that the exponent of a finite group is always bounded by the order of the group. Thus to give an estimate for this case we use the bounds determined for the torsion-free case.

Before we start developing the tools necessary for our two results we give an example of an application to lattices in the 3-dimensional Heisenberg group to give a sense of the structure of Blackburn’s work (see [14] for a general treatment of lattices in nilpotent Lie groups along with a classification of lattices in the 3-dimensional Heisenberg group). In particular, we are interested in the following lattice:

\[
UT_3(\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} : x, y, z \in \mathbb{Z} \right\}.
\]

If \( \gamma \in UT_3(\mathbb{Z}) \), we write

\[
\gamma = \begin{pmatrix} 1 & x_{\gamma} & y_{\gamma} \\ 0 & 1 & z_{\gamma} \\ 0 & 0 & 1 \end{pmatrix}.
\]

We evaluate the conjugacy class of \( \gamma \) using matrix multiplication and write

\[
\begin{pmatrix} 1 & x_{\gamma} & y_{\gamma} \\ 0 & 1 & z_{\gamma} \\ 0 & 0 & 1 \end{pmatrix}_{UT_3(\mathbb{Z})} = \left\{ \begin{pmatrix} 1 & x_{\gamma} & lt + y_{\gamma} \\ 0 & 1 & z_{\gamma} \\ 0 & 0 & 1 \end{pmatrix} : l_{\gamma} = \text{gcd}(x_{\gamma}, z_{\gamma}) \text{ and } t \in \mathbb{Z} \right\}.
\]

One final observation is that if \( \gamma \in B_{UT_3(\mathbb{Z})}(n) \), then \(|x_{\gamma}|, |z_{\gamma}| \leq Cn\) and \(|y_{\gamma}| \leq Cn^2\) for some constant \( C > 0 \) (see [15] Chapter VII, Section C for more details).

**Proposition 3.2.** \( \text{Conj}_{UT_3(\mathbb{Z})}(n) \leq n^6 \)

**Proof.** Consider the following elements of \( UT_3(\mathbb{Z}) \):

\[
a = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, c = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.
\]

We choose a torsion-free central series for \( UT_3(\mathbb{Z}) \) in the following way. We set \( \Delta_1 = \langle c \rangle, \Delta_2 = \langle b, c \rangle \), and \( \Delta_3 = UT_3(\mathbb{Z}) \). Subsequently a compatible generating set can be given by \( S = \{ \xi_1, \xi_2, \xi_3 \} \) where \( \xi_1 = c, \xi_2 = b, \) and \( \xi_3 = a \).

Suppose \( \gamma, \eta \in B_{UT_3(\mathbb{Z})}(n) \) where \( \gamma \sim_c \eta \). We first observe that \( UT_3(\mathbb{Z})/\Delta_1 \cong \mathbb{Z}^2 \). Thus if \( \tilde{\gamma} \sim_c \tilde{\eta} \) in \( UT_3(\mathbb{Z})/\Delta_1 \), then either \( x_{\gamma} \neq x_{\eta} \) or \( z_{\gamma} \neq z_{\eta} \). Subsequently we may assume \( x_{\gamma} \neq x_{\eta} \). By the Prime number theorem there exists a prime \( p \) such that \( p \) does not divide \( x_{\gamma} - x_{\eta} \) and \( p \leq \log |x_{\gamma} - x_{\eta}| \). For our finite quotient, we have the following series of maps:

\[
\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \rightarrow (x, y) \rightarrow x \rightarrow (\text{ mod } p).
\]

\( \gamma \) and \( \eta \) do not have the same image in the quotient and so are not conjugate. We have

\[|x_{\gamma} - y_{\gamma}| \leq 2Cn.\]
There are two possibilities. If

\[ \gamma \sim c \gamma_1 \text{ but } \gamma \sim c \gamma_2 \]  

and subsequently

\[ \gamma \sim c \gamma_1 \]  

where \( k_{\gamma, \tau} \) to be the minimum such integer.

By direct computation one can show that \( \gamma_1 \sim c \gamma_2 \) but \( \gamma \sim c \gamma_1 \), where \( k_{\gamma/\tau} \) is the minimum such integer.

As before we assume that \( \gamma_1, \gamma_2 = 0 \), then \( \gamma \) and \( \eta \) are central and thus one can take \( k = z_\eta - z_\gamma \). Subsequently \( |k| \leq 2Cn^2 \) and thus we choose \( p \) such that \( p \leq 2 \log (2Cn) \) where \( p \) does not divide \( k \). Note that

\[ p^2 \leq 4 (2Cn)^2 \]  

and subsequently

\[ \text{CD}_{UT_3(\mathbb{Z})} (\gamma, \eta) \leq (4 \log (2Cn))^6. \]

Now suppose without loss of generality that \( \gamma \neq 0 \). Therefore we write

\[ p^{m+1} = p^m p^1 \leq l^2 \leq \max \{ (|\gamma|)_{\mathbb{S}}, (|\eta|)_{\mathbb{S}} \} \]

and thus \( \text{CD}_{UT_3(\mathbb{Z})} (\gamma, \eta) \leq n^6 \). Taking into account all cases we have

\[ \text{Conj}_{UT_3(\mathbb{Z}), \mathbb{S}} (n) \leq n^6. \]

One can obtain a tighter asymptotic upper bound for \( \text{Conj}_{UT_3(\mathbb{Z})} (n) \) by adjusting the proof of Proposition 3.2 in the following way. Consider two non-conjugate elements \( \gamma, \eta \in UT_3(\mathbb{Z}) \) such that \( \gamma \sim c \eta \) in \( UT_3(\mathbb{Z}) / \Delta_1 \).

As before we assume that \( z_\gamma = z_\eta \) and \( z_\gamma = z_\eta \) and subsequently \( l_\gamma = l_\eta \). In particular \( l > 1 \). We see that if we find \( m \in \mathbb{N} \) satisfying

\[ z_\gamma \notin \{ \gamma_\eta + lt : t \in \mathbb{Z} \} \text{ (mod } m \}, \]

then \( r_m (\gamma) \sim c r_m (\eta) \). Equivalently, there is no solution to the equation

\[ \gamma_\eta - \gamma_\eta = lt \text{ (mod } m \} \]

for all \( t \in \mathbb{Z} \). Taking \( m = l \) we observe that \( l \leq \max \{ C ||\gamma||_{\mathbb{S}}, C ||\eta||_{\mathbb{S}} \} \leq Cn \). Subsequently \( \text{CD}_{UT_3(\mathbb{Z})} (\gamma, \eta) \leq (Cn)^3 \). Thus we improve Proposition 3.2 with the following result.

**Proposition 3.3.** \( \text{Conj}_{UT_3(\mathbb{Z}), \mathbb{S}} (n) \leq n^3 \)

While following Blackburn will provide an asymptotic upper bound for \( \text{Conj}_{\Gamma, \mathbb{S}} (n) \) it will not be sharp as the integral Heisenberg example demonstrates.

The following proposition and its proof will be a model for how we will approach Theorem 1.1.

**Proposition 3.4.** \( n^3 \leq \text{Conj}_{\mathbb{S}} (n) \)

**Proof.** Consider the following elements:

\[ \gamma_p = \begin{pmatrix} 1 & p & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \eta_p = \begin{pmatrix} 1 & p & 2 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \]
where $p$ is prime. By $\{12\}$ $UT_3 (\mathbb{Z})$ has the congruent subgroup property and therefore we reduce the problem of separating the conjugacy classes of $\gamma_p$ and $\eta_p$ via finite quotients to separating the conjugacy classes of $\gamma_p$ and $\eta_p$ via congruent subgroups. Since $r_P (\gamma_p)$ and $r_P (\eta_p)$ are non-equal central elements it follows that $\gamma_p$ and $\eta_p$ are not conjugate in $UT_3 (\mathbb{Z}/p\mathbb{Z})$. Suppose $m < p$. Then there exists $s$ such that $sp = 1 \mod m$. That implies $\gamma_p$ and $\eta_p$ are conjugate in $UT_3 (\mathbb{Z}/m\mathbb{Z})$ and subsequently

$$p^3 \leq \text{CD}_{UT_3 (\mathbb{Z})} (\gamma_p, \eta_p).$$

Note that $\|\gamma_p\| = p + 1$ and $\|\eta_p\| = p + 2$ with respect to our chosen generating set.

**Corollary 3.5.** Let $UT_3 (\mathbb{Z})$ be the group of upper triangular unipotent matrices in $SL_3 (\mathbb{Z})$. Then

$$\text{Conj}_{UT_3 (\mathbb{Z})} (n) \approx n^3.$$

### 4 Relating complexity in groups and Lie algebras

Let $\{\Gamma, G, n, \Delta, \xi, \upsilon\}$ be an admissible 6-tuple and let $\gamma = \prod_{i=1}^{hG} \xi^{r_i}$. We write

$$\text{Log} \left( \prod_{i=1}^{hG} \xi^{r_i} \right) = \sum_{i=1}^{hG} f_i \upsilon_i.$$

We will demonstrate that each $f_i$ can be realized as a polynomial in variables $\{r_j\}_{j=1}^{hG}$ of bounded degree determined by $G$. We will also explicitly compute $\text{Ad}(\gamma)$ for $\gamma \in G$. We do both of these tasks by considering $m$-fold Lie brackets. First we need the following lemma regarding iterated compositions of $\text{ad}_A$ for some $A \in \mathfrak{n}$. The proof of Lemma 4.1 is a straightforward application of the Baker–Campbell–Hausdorff formula and so will be omitted for sake of brevity.

**Lemma 4.1.** Let $\{\Gamma, G, n, \Delta, \xi, \upsilon\}$ be an admissible 6-tuple and let

$$A = \sum_{i=1}^{hG} a_i \upsilon_i \quad \text{and} \quad B = \sum_{i=1}^{hG} b_i \upsilon_i.$$

Then

$$\left(\text{ad}_A\right)^n (B) = \sum_{i=1}^{\ell_G - n} \left( \prod_{j=i+1}^{hG} f_{i,j} b_j \right) \upsilon_i$$

where each $f_{i,j}$ is a homogeneous polynomial in variables $\{a_j\}_{j=1}^{hG}$ of degree at most $n$.

Via repeated applications of Lemma 4.1 we obtain a similar result for $m$-fold brackets.

**Lemma 4.2.** Let $\{\Gamma, G, n, \Delta, \xi, \upsilon\}$ be an admissible 6-tuple and let

$$A = \sum_{i=1}^{hG} a_i \upsilon_i \quad \text{and} \quad B = \sum_{i=1}^{hG} b_i \upsilon_i.$$

Let $\{\alpha_i\}_{i=1}^{j}$ and $\{\beta_i\}_{i=1}^{j}$ be a sequence of natural numbers and set $n = \sum_{i=1}^{j} \alpha_i + \beta_i$. Then

$$[A^\alpha_1 B^\beta_1 \ldots A^\alpha_j B^\beta_j] = \sum_{i=1}^{\ell_G - n + 1} f_i \upsilon_i$$

where each $f_i$ is a polynomial in variables $\{a_i\}_{i=1}^{hG}$ and $\{b_i\}_{i=1}^{hG}$ of degree at most $n$. 


Effective conjugacy separability of finitely generated nilpotent groups

11

One can see that the Baker-Campbell-Hausdorff formula and Lemma 4.3 together imply Lemma 4.4 which is the main tool in relating the word length of an element in a finitely generated, torsion-free nilpotent group with the length of its image in the Lie algebra of its Mal’tsev completion.

**Lemma 4.3.** Let \( \{ \Gamma, G, n, \Delta, \xi, v_1 \} \) be an admissible 6-tuple. Let

\[
A = \sum_{i=1}^{h_G} a_i v_i \quad \text{and} \quad B = \sum_{i=1}^{h_G} b_i v_i
\]

where \( A \in \mathfrak{n}' \) and \( B \in \mathfrak{n}' \). Then

\[
A \ast B = \sum_{i=1}^{\ell_G+1} f_i v_i,
\]

where each \( f_i \) is a polynomial in variables \( \{ a_j \}_{j=1}^{h_G} \) and \( \{ b_j \}_{j=1}^{h_G} \) whose degrees are bounded by \( \max \{ t, s \} \).

We are now ready to prove our assertion above. Namely, that each \( f_i \) is a polynomial in variables \( \{ a_j \}_{j=1}^{h_G} \).

**Proposition 4.4.** Let \( \{ \Gamma, G, n, \Delta, \xi, v_1 \} \) be an admissible 6-tuple. Then we have

\[
\text{Log} \left( \prod_{i=1}^{h_G} \xi_i^{a_i} \right) = \sum_{i=1}^{h_G} f_i v_i
\]

where each \( f_i \) is a polynomial in variables \( \{ a_j \}_{j=1}^{h_G} \) of degree at most \( d_\Gamma \).

**Proof.** We proceed by induction on the dimension of \( G \) and observe that the base case is clear. Now suppose \( G \) has dimension \( h_G > 1 \) and set

\[
\gamma = \prod_{i=1}^{h_G} \xi_i^{a_i} \quad \text{and} \quad \eta = \sum_{i=1}^{h_G} \xi_i^{a_i}.
\]

Using the Baker-Campbell-Hausdorff formula, we write \( \text{Log} (\gamma) = \text{Log} (\eta) \ast \text{Log} \left( \xi_i^{a_i h_G} \right) \).

There exists an \( \mathbb{Q} \)-defined group \( N \) which sits as Lie subgroup of \( G \) with cocompact lattice \( N \cap \Gamma \) and Lie algebra \( \mathfrak{t} \) such that the following diagram commutes (see [22, Corollary 1.126], [14, Chapter 1]):

\[
\begin{array}{c}
1 \downarrow N \xrightarrow{\text{Log}} G \xrightarrow{\pi} \mathbb{R} \xrightarrow{d\pi} \mathfrak{t} \xrightarrow{dN} 0
\end{array}
\]

Thus \( \{ N \cap \Gamma, N, \mathfrak{n} \cap \mathfrak{t}, \Delta, \xi, v_1 \} \) is an admissible 6-tuple and by induction we have

\[
\text{Log}_N (\eta) = \sum_{i=1}^{h_G-1} f'_i v_i
\]

where each \( f'_i \) is a polynomial in the variables \( \{ a_j \}_{j=1}^{h_G-1} \) of degree at most \( d_{N \cap \Gamma} \). By inspection of the Baker-Campbell-Hausdorff formula one can show \( \text{Log}_G \left( \xi_i^{a_i h_G} \right) = a_i v_i h_G \). Lemma 4.3 implies that we can write

\[
\text{Log}_G (\gamma) = \left( \sum_{i=1}^{h_G-1} f'_i v_i \right) \ast a_i v_i h_G = \sum_{i=1}^{h_G} f_i v_i,
\]

where each \( f_i \) can be express as a polynomial of degree at most \( c_N \) in variables \( \{ f'_j \}_{j=1}^{h_G-1} \) and \( a_i h_G \). Since each \( f'_j \) is polynomial in \( \{ a_k \}_{k=1}^{h_G} \) of degree at most \( d_{N \cap \Gamma} \) we have our result. \( \square \)
Ad(γ) has a matrix representative with respect to our chosen basis because it is a Lie algebra endomorphism. Using Lemma 4.1 we have control over the matrix coefficients of Ad(γ) in terms of the word length of γ which will be an essential aspect of our estimation of the choice our prime p.

**Lemma 4.5.** Let \( \{ \Gamma, G, n, \Delta, \xi, v_1 \} \) be an admissible 6-tuple and let \( \gamma = \prod_{i=1}^{h_G} \xi_i^{a_i} \). Then the matrix representation of Ad(γ) − I, with respect to the basis \( \{ v_j \}_{j=1}^{h_G} \), can be written as \( (\beta_{i,j}) \) where for rows \( \ell_{m-1} + 1 \leq i \leq \ell_m \) we have

\[
\beta_{i,j} = \begin{cases} 
\sum_{k=1}^{m} f_{i,j,k} \frac{k!}{k} & \text{if } \ell_m + 1 \leq j \leq h_G \\
0 & \text{otherwise}
\end{cases}
\]

where each \( f_{i,j,k} \) is a polynomial of degree at most \( k \) in the variables \( \{ a_s \}^{h_G}_{s=1} \).

## 5 Preliminary estimates for Theorem 1.2

### 5.1 Exponent control

Let \( \{ \Gamma, G, n, \Delta, \xi, v_1 \} \) be an admissible 6-tuple. Having a matrix representative of Ad(expA) − I allows us to understand solutions to linear systems of the form \( (\text{Ad}(\exp A) - I)(B) = C \) for \( A, B, C \in n \). We relate the entries of \( B \) to each other via polynomials in the entries of \( A \) and the distribution of the non-zero coefficients of \( B \) will affect the degree of the polynomial estimate for \( \tau_r \). We need to take into account the ranks of the upper central series of \( n \) and what terms of the upper central series the non-zero coefficients of \( B \) land. Proposition 5.1 takes that into account and proceeds by induction on the number of terms of the upper central series of \( n \) in which the non-zero coefficients fall into.

**Proposition 5.1.** Suppose \( \{ \Gamma, G, n, \Delta, \xi, v_1 \} \) is an admissible 6-tuple and let \( \{ h_i \}^{h_G}_{i=1} \) be an induced central Lie series of \( n \). Let \( A \in n \) and define \( \mathfrak{t}_A = \pi^{-1}(\epsilon_n/h_1(\mathfrak{A})) \). Consider the map

\[
\text{Ad}(\exp A) - I : \mathfrak{t} \to h_1.
\]

Suppose \( B \in \mathfrak{t} \) satisfies \( (\text{Ad}(\exp A) - I)(B) = \tau v_1 \) where \( \tau = \text{Im}((\text{Ad}(\exp A) - I)) \). Suppose \( \{ i_t \}^{s}_{t=1} \) is a strictly increasing sequence of indices where \( h_i \neq 0 \) and let

\[
\{ j_m \}^{n}_{m=1} \subset \{ 2, 3, \ldots, c_G \}
\]

be a strictly increasing sequence. Set \( \kappa_{n+1} = s \) and let \( \{ \kappa_m \}^{n}_{m=1} \) satisfy

\[
\ell_{h-1} + 1 \leq i_0 < i_{h+1} < \ldots < i_{h+1-1} \leq \ell_{h_i}.
\]

Then there exist polynomials \( \omega \) and \( \{ \Xi_z \}^{s}_{z=2} \) of degree at most \( s \) in \( \{ a_\alpha \}^{h} \) where

\[
s = \sum_{t=1}^{n} 2^{\kappa_{t+1} - \kappa_t} (c_G - j_t + 1)
\]

such that \( \omega b_{i_z} = \Xi_z b_{j_z} \) for each \( z \).

In the proof of Proposition 5.1, we will make repeated use of the following result.

**Proposition 5.2.** For \( 1 \leq z \leq m \) let \( b_z, c_z \in \mathbb{Q} \) and suppose for all \( z \) that \( b_z \neq 0 \). Suppose there exist polynomials \( f_{\alpha, \beta} \) of degree \( \alpha \) in variables \( \{ a_\alpha \}^{n}_{\alpha=1} \) such that for each \( 1 \leq \alpha \leq m \) we have \( \sum_{z=1}^{m} f_{\alpha, z} b_z = c_\alpha \). Then there
exist polynomials \( \{w_l\}_{l=1}^{m-1} \) of degree that satisfy the following: For each \( t, s \) where \( 1 \leq t \leq s \leq m \) there exist polynomials \( \lambda_{t,z} \) for \( 1 \leq z \leq t-1 \) and polynomials \( \rho_{t,s,k} \) for \( 1 \leq k \leq m \) in variables \( \{a_\alpha\}_{\alpha=1}^n \) satisfying

\[
\left( \prod_{l=t}^m w_l \right) b_s = \sum_{z=1}^{t-1} \lambda_{t,z} b_z + \sum_{k=1}^m \rho_{t,s,k} c_k.
\]

Moreover \( \deg(w_l) = 2^{t-1} \alpha \).

We defer the proof of Proposition 5.2 until after the proof of Proposition 5.1.

**Proof of Proposition 5.1.** Let \( M = (\beta_{m,n}) \) be the matrix representative of \( \text{Ad}_A - I \). We proceed by induction by applying Proposition 5.2 to construct our polynomials using the entries of \( M \).

Observe for \( 1 \leq t \leq n \) that

\[
\ell_{i_t} + 1 \leq \ell_{i_{t+1}} < \ldots < \ell_{i_{k+1}} - 1 < \ell_{i_t}.
\]

For \( t < \kappa_n \) and rows \( i_{\kappa_n} \leq \alpha \leq h_G \) we have that \( \beta_{i_{\kappa_n}, t} = 0 \). Proposition 5.2 implies that there exist polynomials \( \{w_m\}_{m=1}^{t-\kappa} \) and \( \lambda_{t,i_{\alpha}} \) such that

\[
\left( \prod_{l=t}^m w_l \right) b_{i_{\alpha}} = \sum_{z=1}^{t-1} \lambda_{t,i_{\alpha}} b_z + \sum_{k=1}^m \rho_{t,i_{\alpha},k} c_k.
\]

for \( \kappa_n + 1 \leq t \leq s \). Additionally, \( \deg(w_l) = 2^{t-\kappa_{n-1}} \). We let \( \omega_{\alpha} = \prod_{l=t}^s w_l \) and note

\[
\deg(\omega_{\alpha}) = 2^{s-\kappa_{n-1}} (c_G - j_n + 1).
\]

Multiplying row \( \kappa_n - 1 \) of our linear system by \( \omega_{\alpha} \) we write

\[
0 = \sum_{z=1}^s \beta_{\kappa_n-1,i_{\alpha}} \omega_{\alpha} b_{i_{\alpha}} = \sum_{z=1}^{s-\kappa_n} \beta_{\kappa_n-1,i_{\alpha}} \omega_{\alpha} b_z + \left( \sum_{\zeta=s-\kappa_n}^s \Xi_{\zeta,n} \beta_{\kappa_n-1,i_{\alpha}} \right) b_{i_{\kappa_n}}.
\]

Let

\[
\Xi_{\alpha,n} = -\sum_{\alpha=1}^s \Xi_{\alpha,n} \beta_{i_{\kappa_n-1,i_{\alpha}}}
\]

and for \( \kappa_n \leq z \leq s \) one can see

\[
\Xi_{\alpha,n} \omega_{\alpha} b_{i_{\alpha}} = \sum_{\alpha=1}^s \beta_{i_{\kappa_n-1,i_{\alpha}}} \Xi_{\zeta,n} b_{i_{\alpha}}
\]

where \( \deg(\Xi_{\alpha,n} \omega_{\alpha}) \) is at most

\[
2^{s-\kappa_{n-1}} (c_G - j_n + 1) + c_G - j_{n-1} + 1.
\]

That implies multiplying rows \( \alpha \) where \( i_{\kappa_n-1} \leq \alpha \leq i_{\kappa_n} \) by \( \omega_{\alpha} \) allows one to obtain a system of equations of the form for which we can apply Lemma 5.2 again. We construct polynomials \( \omega_{n-1}, \Xi_{z,n-1} \) for \( \kappa_{n-1} \leq z \leq s \), such that

\[
\omega_{n-1} b_{i_{\alpha}} = \sum_{\alpha=1}^{\kappa_{n-1}} \Xi_{\alpha,n-1} b_{i_{\alpha}}
\]

where

\[
\deg(\omega_{n-1}), \deg(\Xi_{z,n-1}) = 2^{s-\kappa_{n-1}} (c_G - j_n + 1) + 2^{\kappa_n-\kappa_{n-1}-1} (c_G - j_{n-1} + 1).
\]

By induction, we arrive with polynomials \( \omega \) and \( \Xi \) for \( 2 \leq z \leq s \) of degree at most

\[
\sum_{t=1}^n 2^{\kappa_{t-1} - \kappa_{t-1}} (c_G - j_t + 1).
\]

\( \square \)
Proof of Proposition 5.2 We proceed by induction on $l$. For the base case of $l = m$ we set $w_m = 1$ and set $\lambda_{m,m} = -f_{m,m}$ for each $z$. We also set $\rho_{m,m} = 1$ and $\rho_{m,m-1} = 0$ and one can see that we have our desired result. Now suppose that $w_{l+1}, w_{l+2}, \ldots, w_m, \lambda_{l+1,l}, \ldots, \eta_{l,j,k}$, and $\rho_{l+1,t}$, for $l + 1 \leq t \leq j \leq m$ have been constructed. We write
\[
\sum_{z=1}^{m} f_{l+1,k} b_z = c_l
\]
Now we multiply the above by $\prod_{k=l+1}^{m} w_k$ and by induction we write
\[
\prod_{k=l+1}^{m} w_k c_l = \sum_{z=1}^{m} \left( \sum_{s=l+1}^{m} \left( \prod_{k=l+1}^{s} w_k \right) \rho_{l+1,s,z} \right) c_z + \sum_{z=1}^{l} \left( \sum_{s=l+1}^{m} \left( \prod_{k=l+1}^{s} w_k f_{l+1,k} + f_{l+1,k} \lambda_{l+1,s,z} \right) \right) b_z.
\]
We define
\[
w_l = \sum_{s=l+1}^{m} \left( \prod_{k=l+1}^{s} w_k f_{l+1,k} + f_{l+1,k} \lambda_{l+1,s,z} \right)
\]
and
\[
\lambda_{l+1,l,z} = -\sum_{s=l+1}^{m} \left( \prod_{k=l+1}^{s} w_k f_{l+1,k} + f_{l+1,k} \lambda_{l+1,s,z} \right).
\]
We also define
\[
\rho_{l+1,t} = -\sum_{s=l+1}^{m} \left( \prod_{k=l+1}^{s} w_k \right) \rho_{l+1,s,z}
\]
for $z > l$. For $z = l$ we define
\[
\rho_{l+1,l} = \prod_{k=l+1}^{m} w_k - \sum_{s=l+1}^{m} \left( \prod_{k=l+1}^{s} w_k \right) \rho_{l+1,s,l}.
\]
To finish we need to define $\lambda_{l+1,t,z}$ and $\rho_{l+1,t,k}$ for $l + 1 \leq t$. We write
\[
\left( \prod_{s=1}^{l+1} w_s \right) b_l = \sum_{z=1}^{l+1} w_l \lambda_{l+1,t,z} b_z + \sum_{k=l+1}^{m} w_l \rho_{l+1,t,k} c_k.
\]
We set $\lambda_{l+1,t,z} = w_l \lambda_{l+1,t,z}$ and $\rho_{l+1,t,k} = w_l \rho_{l+1,t,k}$ giving our desired result. One can see that $\deg (w_l) = 2^{l-1} \alpha$ by computation.

Let $\Gamma$ be a finitely generated, torsion-free nilpotent group with torsion-free central series $\{\Delta_i\}_{i=0}^{h_{\eta}}$ and compatible generating set $S = \{\xi_i\}_{i=1}^{h_{\eta}}$. Let $\gamma, \eta \in \Gamma$ be non-conjugate words of length at most $n$. We are interested in using $\{\Delta_i\}_{i=0}^{h_{\eta}}$ in an inductive method to prove conjugacy separability of $\Gamma$ and to give asymptotic upper bounds for $\text{Conj}_{\Gamma,S}$. Specifically if $\tilde{\gamma}$ is non-conjugate to $\tilde{\eta}$ in $\Gamma/\Delta_1$, we can proceed by induction to get a bound on the size of the quotient of $\Gamma$. However if $\tilde{\gamma}$ is conjugate to $\tilde{\eta}$ in $\Gamma/\Delta_1$, then there are technical considerations that we need to account for.

Assume that $\eta \sim_{c} \gamma \in S_{\tilde{\gamma} \tilde{\eta}}^{k_{\tilde{\gamma},\tilde{\eta}}}$. By inspection of $\tau_\gamma$ one can see that $\tau_\gamma$ is an invariant of the conjugacy class of $\gamma$ and that $\gamma$ is conjugate to $\gamma^{2^t}$ for all $t \in \mathbb{Z}$. To find a prime power $p^m$ such that $\tilde{\gamma}$ and $\tilde{\eta}$ remain non-conjugate in $\Gamma/\Gamma_{p^m}$ we need to ensure that $\gamma^{2^t} \in S_{\tilde{\gamma} \tilde{\eta}}$ do not become conjugate in our quotient. So to bound the size of the quotient we need to bound $\tau_\gamma$ as a function of word length. We also need to consider the degenerate case of when $\tau_\gamma, \tau_\eta = 0$. In that case we have that any prime $p$ that does not divide $k_{\tilde{\gamma},\tilde{\eta}}$ will work and thus we want to bound a minimal choice of prime $p$ that does not divide $k_{\tilde{\gamma},\tilde{\eta}}$. We do that by bounding the minimal choice for $k_{\tilde{\gamma},\tilde{\eta}}$. Hence we have the following definitions and proposition.

Proposition 5.3. Let $\Gamma$ be a finitely generated, torsion-free nilpotent group with torsion-free central series $X = \{\Delta_i\}_{i=0}^{h_{\eta}}$ and compatible generating set $S = \{\xi_i\}_{i=1}^{h_{\eta}}$. We define
\[
\sigma_{\Gamma,S}(n) = \max \{ \sigma_{\Gamma,S}(n) : \eta \in B_{\Gamma,S}(n) \}.
\]
Then \(\sigma_{\Gamma,S}(n) \leq n^a\) where
\[
\alpha = d_1^2 \left( c_G + \sum_{i=1}^{c_G} 2^{h_{\Gamma_G} - 1 + h_{B_{\Gamma}}} (c_G - 1 + 1) \right).
\]

Proof. Let \(\gamma \in \Gamma\). Let \(\Gamma_{\text{Lie}}\) be the Lie ring hull of \(\Gamma\) with torsion-free central series \(\{K_i\}_{i=0}^{h_{\Gamma}}\) and compatible generating set \(S = \{\xi_i\}_{i=1}^{h_{\Gamma}}\). Observe that \(K_i \cap \Gamma = \Delta_i\) and that there exists integers \(\alpha_i\) such that \(\xi_i^{\alpha_i} = \xi_i\). Assume \(\tau_{\Gamma,\gamma} \neq 0\) Let
\[
H_\Gamma = \pi_{\alpha_i}^{-1}(C_{\Gamma/\Delta_i}(\gamma)) \quad \text{and} \quad H_{\Gamma_{\text{Lie}}} = \pi_{K_i}^{-1}(C_{\Gamma_{\text{Lie}}/K_i}(\gamma)).
\]
We have \([H_{\Gamma_{\text{Lie}}} : H_\Gamma] \leq l\) where \(l = [\Gamma_{\text{Lie}} : \Gamma]\) and
\[
H_{\Gamma_{\text{Lie}}} \cap \Gamma = \left\langle C_{\Gamma_{\text{Lie}}} (\gamma), \zeta_{\Gamma_{\text{Lie}},\gamma} \right\rangle \cap \Gamma = \left\langle C_\Gamma (\gamma), \zeta_{\Gamma,\gamma} \right\rangle = H_\Gamma
\]
That implies \(\tau_{\Gamma_{\text{Lie}},\beta} = \tau_{\Gamma,\gamma}\) where \(\beta \leq l\). Thus we need only give asymptotic estimates for \(\sigma_{\Gamma,S}\) when \(\Gamma\) is a Lie ring group.

Assume that \(\Gamma\) is a Lie ring group. Then \(\Gamma\) fits into an admissible 6-tuple \(\{\Gamma, G, n, \Delta_i, \xi_i, \eta_i\}\). Let \(\gamma \in B_{\Gamma,S}(n)\) where \(S = \{\xi_i\}_{i=1}^{h_{\Gamma}}\). Define \(\eta : G \to G\) as \(\eta(x) = \gamma^{-1}x^{-1}\gamma\).

We have \((d\eta)^i(X) = (\text{Ad}(\gamma^{-1}) - I)(X)\). Writing
\[
\gamma = \prod_{i=1}^{h_G} x_{\xi_i}^{a_i} \quad \text{and} \quad \zeta_{\Gamma,\gamma} = \prod_{i=1}^{h_G} x_{\eta_i}^{b_i},
\]
we have by Proposition 4.4 that
\[
\log(\gamma) = \sum_{i=1}^{h_G} f_i v_i \quad \text{and} \quad \log(\eta) = \sum_{i=1}^{h_G} g_i v_i
\]
where each \(f_i\) and \(g_i\) is a polynomial in variables \(\{a_{\alpha}\}_{\alpha=1}^{h_{\Gamma}}\) and \(\{b_{\alpha}\}_{\alpha=1}^{h_{\Gamma}}\) respectively of degree at most \(d_{\Gamma}\).

Let \(A_{\gamma} = \log(\gamma)\) and \(B_\gamma = \log(\zeta_\gamma)\). By \([13]\), we have \((\text{Ad}(\gamma^{-1}) - I)(B) = \tau_{\Gamma,\gamma}\).

To bound \(\tau_{\Gamma,\gamma}\) we need to understand how the entries of \(B_{\gamma}\) relate to one another. By Proposition 5.1, there exist polynomials \(\omega, \Xi\) for \(1 \leq \varepsilon \leq \delta \leq s\) of degree \(m\) in \(\{a_{\alpha}\}_{\alpha=1}^{h_{\Gamma}}\) where
\[
m = \sum_{i=1}^{n} 2^{\kappa_{i+1} - \kappa_i - 1} (c_G - j_i + 1)
\]
such that \(\omega y_i = \Xi g_i\) for \(2 \leq z \leq s\) where
\[
j_i \in \{2, 3, \ldots, c_G\} \quad \text{and} \quad \kappa_i \in \{1, 2, \ldots, s - 1\}.
\]

Multiplying \(\tau_{\Gamma,\gamma}\) by \(\omega\), we write
\[
|\omega_{\tau_\gamma}| \leq \sum_{\varepsilon=1}^s |\omega_{\beta_{1,\varepsilon} b_{1,\varepsilon}}| = \sum_{\varepsilon=1}^s |\Xi_{z} b_{1,\varepsilon} b_{1,\varepsilon}|
\]
Thus \(|\tau_\gamma| \leq C n^m\) for some constant \(C > 0\) where
\[
m = c_G + \sum_{i=1}^{n} 2^{\kappa_{i+1} - \kappa_i - 1} (c_G - j_i + 1).
\]
To maximize over all cases consider the case where all \( b_i \neq 0 \) for \( i > \ell_1 \). We have
\[
\{i_1, i_2, \ldots, i_k\} = \{\ell_1 + 1, \ell_1 + 2, \ldots, h_G\}
\]
where \( s = h_G - h_Z(\Gamma) \). We also have that \( j_i = t \) for \( 2 \leq t \leq c_G \) and subsequently \( \kappa_i = \ell_t - \ell_1 \). Thus, we have
\[
\sigma_{\alpha, \delta}(n) \leq n^\alpha
\]
where
\[
\alpha = d_1^2 \left( c_G + \sum_{i=1}^{c_G} 2^{h_{\Gamma - t - 1} - h_Z(\Gamma)} (c_G - t + 1) \right).
\]

As we will reference this estimate throughout this article, we introduce the following definition for notational simplicity.

**Definition 5.4.** Let \( \Gamma \) be a finitely generated, torsion-free nilpotent group with torsion-free central series \( \{\Delta_i\}_{i=0}^{h_\Gamma} \). We let
\[
u_\Gamma = d_1^2 \left( c_\Gamma + \sum_{i=1}^{c_\Gamma} 2^{h_{\Gamma - t - 1} - h_Z(\Gamma)} (c_\Gamma - t + 1) \right)
\]
and write \( u_i = \nu_{\Gamma / \Delta_i} \) whenever \( \Gamma \) and \( \{\Delta_i\}_{i=0}^{h_\Gamma} \) are clear from context.

We finish with the following definition and proposition.

**Definition 5.5.** Let \( \Gamma \) be a finitely generated, torsion-free nilpotent group with a torsion-free central series \( \{\Delta_i\}_{i=0}^{h_\Gamma} \) and compatible generating set \( \{\xi_i\}_{i=1}^{h_\Gamma} \). Let \( \gamma, \eta \in \Gamma \) be two non-conjugate elements. If \( \bar{\gamma} \sim_c \bar{\eta} \) in \( \Gamma / \Delta_1 \) we set
\[
k_{\bar{\gamma}, \bar{\eta}} = \min \left\{ |k| : \gamma \sim_c \gamma_{\xi_1}^k \text{ and } \eta \sim_c \gamma_{\xi_1}^k \right\}.
\]
If \( \bar{\gamma} \sim_c \bar{\eta} \) in \( \Gamma / \Delta_1 \), then we set \( k_{\bar{\gamma}, \bar{\eta}} = 0 \).

**Proposition 5.6.** Let \( \Gamma \) be a finitely generated, torsion-free nilpotent group with torsion-free central series \( \{\Delta_i\}_{i=0}^{h_\Gamma} \) and compatible generating set \( S = \{\xi_i\}_{i=1}^{h_\Gamma} \). We define
\[
\psi_{\Gamma, S}(n) = \max \left\{ k_{\bar{\gamma}, \bar{\eta}} : \gamma, \eta \in B_{\Gamma, S}(n) \text{ and } \gamma \sim_c \eta \right\}.
\]
Then there exists an integer \( D \) such that \( \psi_{\Gamma, S}(n) \leq n^D \).

**Proof.** As with the proof of Proposition 5.3 we can assume that \( \Gamma \) is a Lie ring group. Thus \( \Gamma \) fits into an admissible 6-tuple \( \{\Gamma, G, n, \Delta_i, \xi_i, v_i\} \). Let \( \gamma, \eta \in \Gamma \) be non-conjugate words of length at most \( n \) such that \( k_{\bar{\gamma}, \bar{\eta}} \neq 0 \). There exists an \( x \in \Gamma \) such that \( x^{-1} \eta x = \gamma_{\xi_1}^{k_{\bar{\gamma}, \bar{\eta}}} \). Then we have \( \eta^{-1} x^{-1} \eta x = \eta^{-1} \gamma_{\xi_1}^{k_{\bar{\gamma}, \bar{\eta}}} \). Writing
\[
\gamma = \prod_{i=1}^{h_\Gamma} \xi_i^{a_i} \text{ and } \eta = \prod_{i=1}^{h_\Gamma} \xi_i^{b_i},
\]
we have by Proposition 4.4 that
\[
\log(\gamma) = \sum_{i=1}^{h_\Gamma} f_i v_i, \quad \log(x) = \sum_{i=1}^{h_\Gamma} g_i v_i, \quad \text{and } \log(\eta^{-1} \gamma) = \sum_{i=1}^{h_\Gamma} \Xi_i v_i.
\]
where each $f_i$ is a polynomial in variables $\{a_j\}_{j=1}^{h_T}$ and each $\Xi_i$ is a polynomial in variables $\{a_j\}_{j=1}^{h_T}$ and $\{b_j\}_{j=1}^{h_T}$ of degree at most $d_T$. Let $A_{\gamma} = \log(\eta)$, $B_{\tau} = \log(x)$ and $C = \log(\eta^{-1}\gamma)$. By \cite{14}, we have
\[
(\text{Ad}(\eta^{-1}) - I)(B) = k_{\gamma, \eta}v_1 + C.
\]
As before in the proof of Proposition 5.3 we want to see how the entries of $B_{\tau}$ relate to one another. We proceed by taking into account the distribution of non-zero coefficients of $B_{\tau}$ in the terms of the upper central series of $n$. Following the proof of Proposition 5.1 we assume there exists a set of strictly increasing indices $i_z$ such that $g_{i_z} \neq 0$. We then construct polynomials $\omega$, $\lambda_{\tau}$, and $\rho_{\tau, r}$ in variables $\{a_j\}_{j=1}^{h_T}$ and $\{b_j\}_{j=1}^{h_T}$ satisfying
\[
\omega g_{i_z} = \lambda_{\tau} g_{i_z} + \sum_{t=1}^{c_T} \rho_{\tau, r} z_i.
\]
There exist integers $j \in \{2, 3, \ldots, c_T\}$ and $\alpha$ such that
\[
\ell_2 \leq i_1 < i_2 \leq \ldots < i_{\alpha} \leq i_{\alpha+1} < i_2 \leq \ldots < i_\ell \leq \ell_j.
\]
If there does not exist a $s > 1$ such that $\Xi_{i_s} \neq 0$ we apply Proposition 5.3 to get a polynomial bound for $k_{\gamma, \eta}$. Otherwise we write
\[
\sum_{t=1}^{c_T} \beta_i_{s, i_t} g_{i_t} = \Xi_{i_s}
\]
where $(\beta_{m, n})$ is the matrix representative of $\text{Ad}(\eta^{-1}) - I$. We write
\[
\omega \Xi_{i_s} = \sum_{t=1}^{c_T} \beta_i_{s, i_t} \omega g_{i_t} = \sum_{t=1}^{c_T} \lambda_{i_t} \beta_i_{s, i_t} g_{i_t} + \left(\sum_{t=1}^{c_T} \rho_{s, i_t} \beta_i_{s, i_t}\right) \Xi_{i_s}.
\]
Therefore $|\Xi_{i_s}|$ is bounded by a polynomial in word length. We now write
\[
\omega k_{\gamma, \eta} = -\omega \Xi_1 + \omega \sum_{t=1}^{c_T} \beta_i_{1, i_t} g_{i_t} = -\omega \Xi_1 + \sum_{t=1}^{c_T} \lambda_{i_t} \beta_i_{1, i_t} g_{i_t} + \left(\sum_{t=1}^{c_T} \rho_{1, i_t} \beta_i_{1, i_t}\right) \Xi_{i_s}.
\]
Noting that $\eta^{-1}\gamma$ is a word of length at most $2n$ we have that $\Xi_{i_s} \leq 2^{d_T} h_T n^{d_F}$. We also note that each $\beta_{m, n}$ is a polynomial in variables $\{b_j\}_{j=1}^{h_T}$. Thus $|k_{\gamma, \eta}|$ is bounded by a polynomial in word length. We maximize over every case to obtain our polynomial bound $D$. Therefore $\Psi_{\gamma, \delta}(n) \leq n^D$. \hfill \Box

One may notice in the statement of Proposition 5.6 that we do not determine explicitly the degree of the bounding polynomial. The reason being is that we want to bound over the $n$-ball the minimal prime that does not divide $\tau_{\gamma, \eta}$. Once we have a polynomial bound we have by the Prime Number Theorem there exists a prime $p \leq \log(\tau_{\gamma, \eta})$ such that $p$ does not divide $\tau_{\gamma, \eta}$. Subsequently the minimal prime $p$ is bounded by $D \log(Cn)$ for constants $C, D > 0$.

### 5.2 Applications to Blackburn

With the results of the previous sections we can now give asymptotic bounds for the values used in Blackburn’s proof.

Let $p$ be prime and let $\Gamma$ be a finitely generated nilpotent group. We intend to separate conjugacy classes of $\Gamma$ in finite quotients of the form $\Gamma/\Gamma^{p^n}$ so a technical issue that we will encounter regards elements of $\Gamma^{p^n}$. We would like that if $\gamma \in \Gamma^{p^n}$, then there exists an element $\eta \in \Gamma$ such that $\eta^{p^n} = \gamma$. Unfortunately that is not always the case for every power of $p$. The following proposition allows us to avoid this issue (see \cite{2} Lemma 2)).
Proposition 5.7. Let $\Gamma$ be a finitely generated nilpotent group and let $p$ be prime. There exists an integer $w_{p,\Gamma}$ such that if $m \geq w_{p,\Gamma}$, then for each $\gamma \in \Gamma^{\Gamma^m}$ there exists $\eta \in \Gamma$ such that $\gamma = \eta^{p^{\leq w_{p,\Gamma}}}$}. Moreover, for all primes $p$ we have

$$w_{p,\Gamma} \leq \frac{1}{2} c_{\Gamma} (c_{\Gamma} + 1).$$

Proof. Let $a_i$ be the largest power of $p$ such that $p^{a_i} \leq i$ and define $w_{p,\Gamma} = \sum_{i=1}^{c_{\Gamma}} a_i$. We demonstrate that $w_{p,\Gamma}$ is the integer we are looking for.

We proceed by induction on $c_{\Gamma}$. The result is clear for $c_{\Gamma} = 1$. Now assume $c_{\Gamma} > 1$ and let $\gamma_1, \gamma_2, \ldots, \gamma_e \in \Gamma$. For $n \leq w_{p,\Gamma}$, we consider

$$\gamma_1^{p^n} \gamma_2^{p^n} \cdots \gamma_e^{p^n} \in \Gamma^{p^n}.$$  

By [19, 6.3], we write

$$\gamma_1^{p^n} \gamma_2^{p^n} \cdots \gamma_e^{p^n} = (\gamma_1 \cdots \gamma_e)^{p^n} x_2^{\left(\frac{p^n}{2}\right)} x_3^{\left(\frac{p^n}{3}\right)} \cdots x_p^{p^n}$$

where $x_i \in \Gamma_i$. Consider $(p^{a_i})$ where $(u, p) = 1$. Observe that $x_i = 1$ for $c_{\Gamma} \leq i$. For $i \leq c_{\Gamma}$, we have $l \leq a_{c_{\Gamma}}$ and $p^{l' u} \leq c_{\Gamma}$. Letting $a = (p^{a_i})$ it follows that $x_i^{a}$ is always a $p^{a_{c_{\Gamma}}}$ power. We write

$$\gamma_1^{p^n} \gamma_2^{p^n} \cdots \gamma_e^{p^n} = \zeta_1^{p^{a_{c_{\Gamma}}}} \zeta_2^{p^{a_{c_{\Gamma}}}} \cdots \zeta_{c_{\Gamma}}^{p^{a_{c_{\Gamma}}}}.$$  

Observe that $\zeta_i \in [\Gamma, \Gamma]$ for $i > 1$. By [19, Lemma 1.3] the group generated by $\langle \zeta_i \rangle_{i=1}^{c_{\Gamma}}$ is a nilpotent group of step size at most $c - 1$. By induction, there exists a $\eta \in \Gamma$ such that

$$\gamma_1^{p^n} \gamma_2^{p^n} \cdots \gamma_e^{p^n} = \eta^{p^{a_{c_{\Gamma}}-w_{p,\Gamma}}} = \eta^{p^{a_{c_{\Gamma}}-w_{p,\Gamma}}}.$$  

\[\square\]

Let $\Gamma$ be a finitely generated, torsion-free nilpotent group. Let $p$ be prime and let $\gamma, \eta \in \Gamma$ be non-conjugate words. When considering quotients of form $\Gamma/\Gamma^{p^n}$ there may be elements that centralize $\eta$ that are not contained $C_{\Gamma}(\eta)/\Gamma^{p^n}$. That is problematic because we then loose control over the conjugacy class of $\gamma$ in $\Gamma/\Gamma^{p^n}$. To circumvent this technicality Blackburn constructs an integer $e_{\Gamma, \gamma}$ such that

$$C_{\Gamma/\Gamma^{p^n}}(\gamma) \leq C_{\Gamma}(\gamma)/\Gamma^{p_{e_{\Gamma, \gamma}}}.$$  

(for more details see [2, Lemma 3]). The following proposition gives an asymptotic upper bound on the $p^{e_{\Gamma, \gamma}}$ as $\gamma$ varies over the $n$-ball.

Proposition 5.8. Let $\Gamma$ be a finitely generated, torsion-free nilpotent group with a torsion-free central series $\{\Delta_i\}_{i=0}^{h_{\Gamma}}$ and compatible generating set $S = \{\xi_i\}_{i=1}^{h_{\Gamma}}$. Let $p$ be prime and let $\gamma \in \Gamma$. Then there exists an integer $e_{\Gamma, \gamma}$ such that if $m \geq e_{\Gamma, \gamma}$, then

$$C_{\Gamma/\Gamma^{p^m}}(\gamma) \leq C_{\Gamma}(\gamma)^{p^{m-e_{\Gamma, \gamma}}}.$$  

Moreover, we let

$$\Phi_{\Gamma, S, p}(n) = \max\{p^{e_{\Gamma, \gamma}} : \gamma \in B_{\Gamma, S}(n)\}.$$  

Then $\Phi_{\Gamma, S, p} \leq n^{a_1 p^{a_2}}$ where

$$\alpha_1 = \sum_{i=0}^{h_{\Gamma, \Gamma^1} - 1} d_i^2 \cdot u_i \quad \text{and} \quad \alpha_2 = \frac{1}{2} \sum_{i=0}^{h_{\Gamma, \Gamma^1} - 1} c_i + c_i^2.$$  

**Proof.** We proceed by induction on the Hirsch length of \( \Gamma \). If \( h_\Gamma = 1 \), we then set \( e_\gamma = 0 \) for all \( \gamma \). For the inductive hypothesis assume for \( \gamma \in \Gamma \) there exists \( e_{\Gamma / \Delta_1, \gamma} \) such that if \( e_{\Gamma / \Delta_1, \gamma} \leq m \), then

\[
C_{\Gamma / \Gamma^m \Delta_1}(\bar{\gamma}) \leq H_{\gamma} \Gamma^{m-e_\gamma} / \Gamma^m \Delta_1
\]

where \( H_{\gamma} = \pi^{-1}(C_{\Gamma / \Delta_1}(\bar{\gamma})) \).

Consider the homomorphism \( \varphi_\gamma \) as in Definition 3.1 and the associated value \( \tau_{\Gamma, \gamma} \). If \( \tau_{\Gamma, \gamma} = 0 \), we set \( e_{\Gamma, \gamma} = e_{\Gamma / \Delta_1, \gamma} \). In that case \( H_{\gamma} = C_{\Gamma}(\gamma) \). Letting \( m \geq e_\gamma \) and \( \eta \in C_{\Gamma / \Gamma^m}(\bar{\gamma}) \) we have \( \eta \gamma \eta^{-1} = \gamma \bar{\gamma}^k \) for some integer \( k \). That implies

\[
\eta \gamma \eta^{-1} = \gamma \left( \text{mod } \Gamma^m \Delta_1 \right).
\]

By assumption,

\[
\bar{\eta} \in C_{\Gamma}(\gamma) \Gamma^{m-e_\gamma} / \Gamma^m \Delta_1
\]

which implies

\[
\bar{\eta} \in C_{\Gamma}(\gamma) \Gamma^{m-e_\gamma} \gamma / \Gamma^m \Delta_1.
\]

Now suppose \( \tau_{\Gamma, \gamma} \neq 0 \). Let \( \alpha \) be the largest power of \( p \) such that \( p^\alpha \) divides \( \tau_{\Gamma, \gamma} \) and let \( w_{p, \alpha} \) be given by Lemma 5.7. Set

\[
e_{\Gamma, \gamma} = e_{\Gamma / \Delta_1, \gamma} + \alpha + w_{p, \alpha}.
\]

For \( m \geq e_{\Gamma, \gamma} \), let \( \bar{\eta} \in C_{\Gamma / \Gamma^m}(\bar{\gamma}) \). That implies \( \eta \gamma \eta^{-1} = \gamma \) where \( \gamma \in \Gamma^m \). Therefore \( \bar{\eta} \in C_{\Gamma / \Gamma^m \Delta_1}(\bar{\gamma}) \). By induction, we have

\[
\bar{\eta} \in H_{\gamma} \Gamma^{m-e_\gamma} / \Gamma^m \Delta_1.
\]

That implies \( \eta = t \mu \) where \( t \in H_{\gamma} \) and \( \mu \in \Gamma^{m-e_\gamma} \).

Letting \( t = \eta \xi_{\Gamma, \gamma}^k \) where \( \eta \in C_{\Gamma}(\gamma) \), we write

\[
[\gamma, \xi_{\Gamma, \gamma}^k] = [\gamma, \eta^{-1} t] = [\gamma, \eta t] \in \Gamma^{m-e_\gamma} \gamma \bar{\gamma} \Delta_1, \gamma.
\]

By definition of \( \varphi_{\Gamma, \gamma} \), \( [\gamma, \xi_{\Gamma, \gamma}^k] = \xi_{\varphi_{\Gamma, \gamma}}^k \). Lemma 5.7 implies

\[
\xi_{\varphi_{\Gamma, \gamma}}^k = w_{p, \alpha}^{m+e_\gamma} \gamma / \Gamma^m \Delta_1, \gamma
\]

for some \( \xi \in \Gamma \). Since \( \Delta_1 \) is torsion-free, we have \( \xi \in \Delta_1 \) and so \( p^{m+e_\gamma + \alpha} \mid \xi_{\Gamma, \gamma} \). Since \( \alpha \) is the largest power of \( p \) that divides \( \tau_{\Gamma, \gamma} \) we have \( p^{m+e_\gamma} \) divides \( k \) and thus \( \xi_{\Gamma, \gamma}^k \in \Gamma^{m+e_\gamma} \gamma \bar{\gamma} \Delta_1, \gamma \). Therefore \( t \in C_{\Gamma}(\gamma) \Gamma^{m-e_\gamma} \) giving our desired result.

For the effective bound we make the following definitions for notational simplicity. Let \( S_i \) be the image of the generating set \( S \) in \( \Gamma / \Delta_1 \). Let \( \gamma \in \Gamma \) and let \( \bar{\gamma} \) be the image of \( \gamma \) in \( \Gamma / \Delta_1 \). Let \( e_{\gamma} = e_{\Gamma / \Delta_1, \gamma} \). If \( \tau_{\Gamma / \Delta_1, \gamma} = 0 \), we define \( m_i, k_i = 0 \). Otherwise, let \( m_i \) be the largest power of \( p \) that divides \( \tau_{\Gamma / \Delta_1, \gamma} \), and let \( k_i = w_{p, e_{\gamma}} \). For \( i \geq h_{\Gamma, \Gamma} \), it follows that \( e_{\Gamma / \Delta_1, \gamma} = 0 \). Subsequently

\[
e_{\Gamma, \gamma} = \sum_{i=0}^{h_{\Gamma, \Gamma} - 1} m_i + k_i \leq \sum_{i=0}^{h_{\Gamma, \Gamma} - 1} m_i + \sum_{i=0}^{h_{\Gamma, \Gamma} - 1} w_{p, e_{\gamma}}.
\]

Observe that \( p^{m_i} \leq \sigma_{\Gamma / \Delta_1, S_i}(n) \) and by Lemma 5.7 we have \( w_{p, e_{\gamma}} \leq \frac{1}{2} (c_\gamma^2 + e_{\gamma}) \). Therefore

\[
p^{e_{\Gamma, \gamma}} \leq \prod_{i=0}^{h_{\Gamma, \Gamma} - 1} \sigma_{\Gamma / \Delta_1, S_i}(n) \prod_{i=0}^{h_{\Gamma, \Gamma} - 1} p^{\frac{1}{2} (c_\gamma^2 + e_{\gamma})}.
\]

\( \square \)
6 Proof of Theorem 1.1

Proof. We first specialize to when \( \Gamma \) is a finitely generated, torsion-free nilpotent group. Let \( \Gamma \) be the Lie ring hull with a torsion-free central series \( \{ \Delta_i \}_{i=0}^{h_{\Gamma}} \) and compatible generating set \( \{ \xi_i \}_{i=1}^{h_{\Gamma}} \). By [38], we have \( h_{\Gamma} = h_{\Gamma} \). Notice \( \{ \Delta_i \cap \Gamma \}_{i=0}^{h_{\Gamma}} \) is a torsion-free central series of \( \Gamma \) with compatible generating set given by \( \{ \xi_i \}_{i=1}^{h_{\Gamma}} \) where \( \alpha_i \) is a non-zero integer.

We have that \( \Gamma \) fits into an admissible 6-tuple \( \{ \Gamma, G, n, \Delta_i, \xi_i, v_i \} \). Let \( \gamma, \eta \in \Gamma, A = \exp(\gamma), \) and \( B = \exp(\eta) \). We claim that \( \gamma \sim_{\epsilon} \eta \) if and only if there exists \( x \in \Gamma \) such that \( \Ad(x)(A) = B \). Suppose \( \gamma \sim_{\epsilon} \eta \), i.e. there exists \( x \in \Gamma \) where \( x^\gamma x^{-1} = \eta \). We have, by [14], that is equivalent to \( \Ad(x)(A) = B \). If \( \gamma \sim_{\epsilon} \eta \), then we have for every \( x \in \Gamma \) that \( x^\gamma x^{-1} \neq \eta \). Since \( \Log \) is a bijective map, we have \( \Ad(x)(A) \neq B \) for all \( x \) as desired.

Since \( \Gamma \) is a finitely generated, torsion-free nilpotent group, we have by [12] that \( \Gamma \) has the congruent subgroup property. Thus we can reduce the problem of distinguishing conjugacy classes of \( \Gamma \) via finite quotients to separating conjugacy classes via congruent subgroups. By inspection of iterated \( m \)-fold commutators, we observe that \( \Log(\Gamma^m) \subseteq kn \). If \( x^\gamma x^{-1} = \gamma \eta \) where \( \eta \in \Gamma^k \), then one can see by examination of \( \Log \) map by \( m \)-fold Lie brackets that \( \Ad(x)(A) = B + kC \) for some \( C \in n \). Similarly, if \( x^\gamma x^{-1} \neq \eta \) for \( x \in \Gamma^k \), then there exists \( x \in \Gamma \) such that

\[
\Ad(x)(A) = B \mod {kn}.
\]

Let \( S = \{ \xi_i \}_{i=1}^{h_{\Gamma}} \). We want to construct an infinite sequence of elements \( A_n, B_n \in n \) such that \( A_n, B_n \in \Log(\Gamma) \),

\[
\|\exp(A_n)\|_S, \|\exp(B_n)\|_S \approx n,
\]

and where

\[
\text{CD}(\exp(A_n), \exp(B_n)) = n^{h_{\Gamma} - h_{\Gamma(\gamma)}} + 1.
\]

Let \( p \) be a prime integer and define \( A_p = \alpha \xi_1 + b p v_{i_2} \) where \( b = \text{Lcm}(\alpha_1, \alpha_2, \ldots, \alpha_{h_{\Gamma}}) \). Using the matrix representation for \( \operatorname{ad}_x \) given by Lemma [4.5] we write an arbitrary element of the orbit of \( A_p \) as

\[
\begin{pmatrix}
\alpha_1 + pb \sum_{i=1}^{h_{\Gamma}} \delta_{i, \xi_2} a_i
\end{pmatrix} v_1 + \sum_{i=2}^{\ell_2 - 1} \left( pb \sum_{i=1}^{h_{\Gamma}} \delta_{i, \xi_2} a_i \right) v_i + \left( pb + pb \sum_{i=1}^{h_{\Gamma}} \delta_{i, \xi_2} a_i \right) v_{i_2}.
\]

Since \( v_{i_2} \notin Z(n) \) there is a \( v_m \), where \( \ell_1 + 1 \leq m \leq h \), such that \( [v_m, v_{i_2}] \neq 0 \). Since \( [v_m, v_{i_2}] \in Z(n) \), we have \( \delta_{m, \xi_2} \neq 0 \) for some \( 1 \leq j \leq \ell_1 \). That motivates our choice for \( B_p \). We define

\[
B_p = \alpha_1 v_1 + \sum_{i=1}^{\ell_1} \delta_{i, \xi_2} b^2 v_i + b p v_{i_2}.
\]

Since \( A_p \neq B_p \) and \( A_p \in Z(n/pn) \), we have

\[
\tilde{A}_p \sim \tilde{B}_p \mod {pn},
\]

which implies that \( A_p \sim \tilde{B}_p \) in \( n \). We also have that

\[
A_p = B_p \mod {Z(n)}.
\]

We claim that \( A_p \) and \( B_p \) are conjugate in \( n/h + kn \) for \( k < p \) by an element in \( \Log(\Gamma) \) where \( h \) the Lie subalgebra generated by \( \{ v_i \}_{i=1, i \neq j}^{\ell_1} \). Since \( \gcd(p, k) = 1 \), there exists \( a_i \in Z \) such that

\[
a_i p \equiv 1 \mod {t}.
\]
Let \( C_i = a_i bv_i \). We have

\[
(I + \text{ad}_{C_i})(A_p) \equiv \alpha_i v_i + a_i p \sum_{i=1}^{\ell_i} b_i^2 \delta_{m/2}^i v_i + p v_i \equiv B_p \pmod{h + kn}.
\]

That implies

\[ A_p \sim_b B_p \pmod{h + kn}. \]

Observe that \( \exp(C_i) \in \Gamma \) for \( t < n \) and thus

\[ \exp(A_p) \sim_c \exp(B_p) \pmod{\Gamma} \]

where \( t < p \). Since \( \{v_i, v_i\} \) pairwise commute for \( i \leq \ell_1 \) we have

\[ \exp(A_p) = \xi_1^p \quad \text{and} \quad \exp(B_p) = \xi_1^p \prod_{i=1}^{\ell_1} \xi_i^p \beta_{m/2}^{i} \cdot \xi_i^p \]

as desired.

Now suppose \( \Gamma \) is an infinite finitely generated nilpotent group and let \( H = \Gamma / T \). Since \( \Gamma \) is a polycyclic group, we have, by [38], that there exists a central series of the form \( \{ \Delta_i \}_{i=0}^k \) where

\[ \Delta_i / \Delta_{i-1} \subset Z(\Gamma / \Delta_{i-1}) \]

is cyclic. We choose a generating set \( S = \{ \xi_i \}_{i=1}^k \) satisfying \( \langle \Delta_{i-1}, \xi_i \rangle = \Delta_i \). Since \( \Gamma \) is infinite, we have that there exists at least one \( \xi_i \) such that \( \gamma \) has infinite order. Let \( \{i_1, i_2, \ldots, i_{h_\gamma}\} \) be the increasing set of indices, where \( \xi_{i_s} \) has infinite order. We note that \( \{ \xi_{i_s} \}_{s=1}^{h_\gamma} \) is a torsion-free central series of \( H \) with compatible generating set \( \{ \xi_{i_s} \}_{s=1}^{h} \). There exists a sequence of non-conjugate elements \( \tilde{\gamma}_p \) and \( \tilde{\eta}_p \) in \( H \) where \( \| \tilde{\gamma}_p \| \cdot \| \tilde{\eta}_p \| = p \) and

\[
CD_H(\tilde{\gamma}_p, \tilde{\eta}_p) = p^{h_H - h_Z(H) + 1}.
\]

We write

\[ \tilde{\gamma}_p = \prod_{s=1}^{h_\gamma} \xi_{i_s}^{a_s} \quad \text{and} \quad \tilde{\eta}_p = \prod_{s=1}^{h_\gamma} \xi_{i_s}^{b_s}. \]

Then the elements

\[ \gamma_p = \prod_{s=1}^{h_\gamma} \xi_{i_s}^{a_s} \quad \text{and} \quad \eta_p = \prod_{s=1}^{h_\gamma} \xi_{i_s}^{b_s} \]

satisfy \( \| \gamma_p \| \cdot \| \eta_p \| = p \) and \( CD_{\Gamma}(\gamma_p, \eta_p) = p^{h_H - h_Z(H) + 1} \). \( \square \)

### 7 Proof of Theorem 1.2

**Proof.** We first assume \( \Gamma \) is torsion-free with torsion-free central series \( \{ \Delta_i \}_{i=0}^{h_\gamma} \) and compatible generating set \( S = \{ \xi_i \}_{i=1}^{h_\gamma} \). We proceed by induction on the Hirsch length of \( \Gamma \), and for \( h_{\Gamma} = 1 \) our result follows.

Now suppose \( h_{\Gamma} > 1 \) and let \( \gamma, \eta \in B_{\Gamma, S}(n) \), where \( \gamma \sim_c \eta \). If \( \gamma \sim_c \eta \) in \( \Gamma / \Delta_i \), then by induction we have our result. Otherwise let \( \gamma \sim_c \eta \) in \( \Gamma / \Delta_1 \). There exists \( g \in \Gamma \) such that \( g \eta g^{-1} = \gamma_{S_1}^{x_{k_\gamma \eta}} \). Hence \( \gamma \sim_c \gamma_{S_1}^{x_{k_\gamma \eta}} \).

Consider the map \( \phi_{\Gamma, \gamma} \) given by Definition 3.1. There exists a prime \( p_{\gamma}^{m_{\gamma}} \) that divides \( \tau_{\Gamma, \gamma} \) but does not divide \( k_{\Gamma, \eta} \). For notational simplicity we suppress subscripts and write \( p^m \) and \( k \).

Let

\[ \omega = m_{\Gamma / \Delta_i} \tilde{\gamma} + w_{p, \gamma}. \]
where \( e_{\Gamma/\Delta_1} \) is given by Proposition 5.8 for \( \Gamma/\Delta_1 \) and \( w_{p,\gamma} \) is given by Lemma 5.7. We claim that \( \bar{\gamma} \sim_c \bar{\eta} \) in \( \Gamma/\Gamma^p \). Suppose otherwise. Then \( \bar{\gamma} \not\sim_c \bar{\eta} \) in \( \Gamma/\Gamma^p \). That implies \( \gamma \sim_c \gamma \bar{z}^{k_1,\eta} \) in \( \Gamma/\Gamma^p \). Thus there exists \( x \in \Gamma \) satisfying
\[
x \bar{\gamma} x^{-1} = \gamma \pmod{\Gamma^p \Delta_1}.
\]
That implies \( x \in C_{\Gamma/\Delta_1} (\bar{\gamma}) \), and by Proposition 5.8 we have
\[
x \in \pi^{-1} \left( C_{\Gamma/\Delta_1} (\bar{\gamma}) \right) \Gamma^p \sim \gamma \pmod{\Gamma^p \Delta_1}.
\]
Therefore \( x \in \pi^{-1} \left( C_{\Gamma/\Delta_1} (\bar{\gamma}) \right) \Gamma^p \sim \gamma \pmod{\Gamma^p \Delta_1} \). That implies that there exists \( t \in \pi^{-1} \left( C_{\Gamma/\Delta_1} (\bar{\gamma}) \right) \) such that
\[
\gamma^{-1} t^{-1} \bar{\gamma} = \xi_1^{k_1,\gamma} \pmod{\Gamma^p \Delta_1}.
\]
However, \( \gamma^{-1} t^{-1} \bar{\gamma} = \xi_1^{k_1,\gamma} \pmod{\Gamma^p \Delta_1} \). By Lemma 5.7, there exists \( y \in \Gamma \) such that \( \xi_1^{k_1,\gamma} = y \pmod{\Gamma^p \Delta_1} \) and since \( \Gamma \) is torsion-free, \( y \in \Delta_1 \). Therefore we have \( \xi_1^{k_1,\gamma} = \xi \bar{\gamma}^m \) for some integer \( b \). Since \( \bar{\gamma}^m \) divides \( \gamma \), \( \bar{\gamma}^m \) divides \( k_1,\gamma \), which is a contradiction. Therefore \( \gamma \sim_c \bar{\eta} \) in \( \Gamma/\Gamma^p \).

For the effective conjugacy separability of finitely generated nilpotent groups 22
Suppose first that $T$ is a $p$-group. If $\gamma \sim_c \eta$ in $\Gamma/T$, then by induction we are done. Thus we will assume that $\chi\eta x^{-1} = \gamma y$ where $y \in T$. It follows that $\gamma \sim_c \gamma y$.

Let $p^m$ be the exponent of $T$, $e_{\Gamma/T,\tilde{r}}$ be the value given by Proposition 5.8, and $w_{p,\Gamma}$ be the value given by Proposition 5.7. Set

$$\omega = m + e_{\Gamma/T,\tilde{r}} + w_{p,\Gamma}$$

and suppose $\tilde{r} \sim_c \tilde{t}$ in $\Gamma/\Gamma^{p\omega}$. There exists $\zeta \in \Gamma$ and $\lambda \in \Gamma$ such that

$$\zeta^{-1} \gamma \zeta = \eta \lambda \pmod{\Gamma^{p\omega}}.$$

That implies $\tilde{z} \in C_{\Gamma/\Gamma^{p\omega}}(\tilde{y})$. Let $H = \pi^{-1}(C_{\Gamma/\Gamma} (\tilde{y}))$. By Proposition 5.8,

$$\tilde{z} \in \left( H\Gamma^{p_{\tilde{r}} - 1, \tilde{r}} \right) \setminus \left( T\Gamma^{p\omega} \right)$$

and subsequently $\zeta = z\zeta$ for $z \in H$ and $\zeta \in \Gamma^{p_{\tilde{r}} - 1, \tilde{r}}$. Thus

$$z^{-1} \gamma z = \zeta^{-1} \gamma \zeta \zeta^{-1} = \zeta \gamma \zeta^{-1} = \eta \lambda \pmod{\Gamma^{p_{\tilde{r}} - 1, \tilde{r}}}.$$

In particular, $[\gamma, z] \lambda^{-1} \in \Gamma^{p_{\tilde{r}} - 1, \tilde{r}}$ and since $z \in H$, we have $[\gamma, z] \in T$ and that

$$[\gamma, z] \lambda^{-1} \in T \cap \Gamma^{p_{\tilde{r}} - 1, \tilde{r}}.$$

By Lemma 5.7, $[\gamma, z] \lambda^{-1} = \mu^{p^m}$ for some $\mu \in \Gamma$. That implies $\mu \in T$ and so $\mu^{p\omega} = 1$. We have $z^{-1} \gamma z = \gamma y$, a contradiction.

Now suppose there exists another prime $q$ which divides $|T|$. Let $K$ be a subgroup of $Z(\Gamma)$ of order $q$. We claim $\gamma \sim_c \eta$ in $\Gamma/K$. Suppose otherwise, then $\gamma \sim_c \gamma y$ in $\Gamma/K$. There exists a generator $\zeta$ of $\Delta$ and $x \in \Gamma$ such that $\chi x^{-1} \gamma x = \gamma y \zeta$ and so we have $x^{-q} \gamma x^q = \gamma^q$. Since there exist integers $s$ and $r$ such that $ps + qr = 1$, we write

$$x^{-q} \gamma x^q = \gamma^q \gamma^{-1} \zeta^q = \gamma y^1 = \gamma y,$$

a contradiction. Therefore $\gamma \sim_c \eta$ in $\Gamma/K$.

To finish we note that $T = \prod_{i=1}^n P_i$, where $P_i$ are $p_i$-groups for primes $p_i$. Our choice $p^m$ is the exponent of a quotient of $P_i$, which is always less than $|T|$. We have

$$p^\omega = p^{m + e_{\Gamma/T,\tilde{r}} + w_{p,\Gamma}} \leq |T|^{\frac{1}{2}(c^2 + c) + 1} p^{e_{\Gamma/T,\tilde{r}}},$$

Our choice of prime $p$ is bounded for any $\gamma$. Thus there exists a constant $C > 0$ satisfying

$$p^{e_{\Gamma/T,\tilde{r}}} \leq \Psi_{\Gamma/T,\tilde{r}, p}(n) \leq C n^{k_1} p^{k_2} \leq C |T|^{k_2 n^{k_1}}$$

where $k_1$ and $k_2$ are given by Proposition 5.8. That implies

$$p^{\omega} \leq D |T|^{\frac{1}{2}(c^2 + c) + k_2} n^{k_1},$$

for some constant $D > 0$. We write

$$|\Gamma/\Gamma^{p\omega}| \leq D |T|^{h_{\Gamma/T}} \Gamma^{p_{\tilde{r}} \left( 1 + \frac{1}{2} (c_1 + c_2) \right) + k_2} n^{k_1},$$

and so we have our desired result. \qed
8 Final Comments

More generally one can ask about the asymptotic behavior of conjugacy separability for virtually nilpotent group and virtually polycyclic groups. Since conjugacy classes are not preserved in finite extensions, one does not automatically obtain estimates for virtually nilpotent groups from this work. However, for a virtually nilpotent group $\Gamma$ with fitting subgroup $\Delta$, we expect that

$$n^{k_1} \preceq \text{Conj}_{\Gamma,S}(n) \preceq n^{k_2},$$

where $k_1 = h_\Delta$ and $k_2 = h_\Delta \cdot [\Gamma : \Delta]$. Part of this expectation comes from the explicit asymptotic behavior for conjugacy separability of the integral Heisenberg example as seen in Corollary 3.5. One would hope to be able to use similar methods to obtain better bounds for the asymptotic behavior of conjugacy separability for nilpotent and virtually nilpotent groups through the use of a faithful representation into $\text{GL}_n(\mathbb{Z})$. Unfortunately discerning conjugacy invariants become computationally intensive for finitely generated nilpotent groups of higher Hirsch length.

For non-virtually nilpotent, virtually polycyclic groups $\Gamma$ we expect that

$$\text{Conj}_{\Gamma,S}(n) \approx 2^n.$$

That will give a characterization of virtually nilpotent groups within the collection of virtually polycyclic groups via the asymptotic behavior of conjugacy separability which we intend to address in a future paper.

References

[1] H. Bass, *The degree of polynomial growth of finitely generated nilpotent groups*, Proc. London Math. Soc. (3) 25 (1972), 603–614.

[2] N. Blackburn, *Conjugacy in nilpotent groups*, Proc. Amer. Math. Soc. 16 1965 143–148.

[3] K. Bou-Rabee, *Approximating a group by its solvable quotients*, New York J. Math. 17 (2011), 699–712.

[4] K. Bou-Rabee, *Quantifying residual finiteness*, J. Algebra 323 (2010), no. 3, 729–737.

[5] K. Bou-Rabee and A. Hadari, *Simple closed curves, word length, and nilpotent quotients of free groups*, Pacific J. Math. 254 (2011), no. 1, 67–72.

[6] K. Bou-Rabee and T. Kaletha, *Quantifying residual finiteness of arithmetic groups*, Compos. Math. 148 (2012), no. 3, 907–920.

[7] K. Bou-Rabee and D. B. McReynolds, *Bertrand’s postulate and subgroup growth*, J. Algebra 324 (2010), no. 4, 793–819.

[8] K. Bou-Rabee and D. B. McReynolds, *Asymptotic growth and least common multiples in groups*, Bull. Lond. Math. Soc. 43 (2011), no. 6, 1059–1068.

[9] K. Bou-Rabee and D. B. McReynolds, *Extremal behavior of divisibility functions*, Geom. Dedicata (2) 2014, 1–9

[10] K. Bou-Rabee, M. Hagen and P. Patel, *Residual finiteness growths of virtually special groups*, to appear in Math. Zeit. [http://front.math.ucdavis.edu/1402.6974](http://front.math.ucdavis.edu/1402.6974).

[11] N. V. Buskin, *Efficient separability in free groups*, Sib. Math. J. 50 (2009), no. 4, 603–608.
[12] J. S. Chahal, *Solution of the congruence subgroup problem for solvable algebraic groups*, Nagoya Math. J. 79 (1980), 141–144.

[13] M. Dehn, *Über unendliche diskontinuierliche Gruppen*, Math. Ann. 71 (1911), no. 1, 116–144.

[14] K. Dekimpe, *Almost-Beiberbach groups: Affine and polynomial structures*, Springer–Verlag, Berlin, 1996.

[15] P. de la Harpe, *Topics in geometric group theory*, University of Chicago Press, Chicago, IL, 2000.

[16] E. Formanek, *Conjugate separability in polycyclic groups*, J. Algebra 42 (1976), no. 1, 1–10.

[17] A. V. Goryaga, *Example of a finite extension of an FAC-group that is not an FAC-group* (Russian) Sibirsk. Mat. Zh. 27, no. 3, 203–205, 225.

[18] M. Gromov, *Groups of polynomial growth and expanding maps*, Inst. Hautes Études Sci. Publ. Math., (1981), no. 53 (1981), 53–73.

[19] P. Hall, *The Edmonton notes on nilpotent groups*, Queen Mary College Math. Notes. Math. Dept., Queen Mary College, London 1969.

[20] J. Humphreys, *Linear Algebraic Groups*, Graduate Texts in Mathematics, No. 21., Graduate Texts in Mathematics, no. 21. Springer–Verlag, New York–Heidelberg, 1975.

[21] M. Kassabov and F. Matucci, *Bounding the residual finiteness of free groups*, Proc. Amer. Math. Soc. 139 (2011), no. 7, 2281–2286.

[22] A. W. Knapp, *Lie groups beyond an introduction*, Second edition. Progress in Mathematics, 140. Birkhäuser Boston, Inc., Boston, MA, 2002.

[23] G. Kozma and A. Thom, *Divisibility and laws in finite simple groups*, http://front.math.ucdavis.edu/1403.2324.

[24] S. Lawton, L. Louder and D. B. McReynolds, *Decision problems, complexity, traces, and representations*, http://front.math.ucdavis.edu/1312.1261.

[25] M. Larsen, *How often is 84/(g – 1) achieved?* Israel J. Math. 126 (2001), 1–16.

[26] R. C. Lyndon and P. E. Schupp, *Combinatorial group theory*, Springer–Verlag, Berlin, 2001.

[27] A. Lubotzky and D. Segal, *Subgroup growth*, Birkhäuser-Verlag, Basel, 2003.

[28] J. Malestein and A. Putman, *On the self-intersections of curves deep in the lower central series of a surface group*, Geom. Dedicata 149 (2010), 73–84.

[29] A. I. Mal’tsev, *On a class of homogeneous spaces*, Amer. Math. Soc. Translation 1951, (1951), no. 39, 33 pp.

[30] A. I. Mal’tsev, *On homomorphisms onto finite groups*, Uchen. Zap. Ivanovskogo Gos. Ped. Inst. 18 (1958), 49–60.

[31] A. I. Mal’tsev, *On isomorphic matrix representations of infinite groups*, Amer. Math. Soc. Transl. (2) 45 (1965), 1–18.

[32] A. Martino and A. Minasyan, *Conjugacy in normal subgroups of hyperbolic groups*, Forum Math. 24 (2012), no. 5, 889–910.

[33] J. Milnor, *Growth of finitely generated solvable groups*, J. Differential Geometry 2 (1968), 447–449.

[34] P. Patel, *On a theorem of Peter Scott*, Proc. Amer. Math. Soc. 142 (2014), no. 8, 2891–2906.
[35] V. Platonov and A. Rapinchuk, *Algebraic groups and number theory*, Academic Press, Inc., Boston, MA, 1994.

[36] I. Rivin, *Geodesics with one self-intersection, and other stories*, Adv. Math. 231 (2012), no. 5, 2391–2412.

[37] V. N. Remeslennikov, *Finite approximability of groups with respect to conjugacy*, Siberian Math. J. 23 (1971) 783–792.

[38] D. Segal, *Polycyclic Groups*, Cambridge University Press, Cambridge, 1983.

[39] P. Stebe, *Conjugacy separability of groups of integer matrices*, Proc. Amer. Math. Soc. 32 (1972), 1–7.

[40] J. Wolf, *Growth of finitely generated solvable groups and curvature of Riemannian manifolds*, J. Differential Geometry 2 (1968), 421–446.