Decision problems, complexity, traces, and representations

Sean Lawton, Larsen Louder, and D. B. McReynolds

March 6, 2014

Abstract

In this article, we study connections between representation theory and the complexity of the conjugacy problem on finitely generated groups. The main focus is on the conjugacy problem in conjugacy separable groups.

1 Introduction

The present article focuses on the interplay between three somewhat different topics in geometric group theory. We begin by introducing each.

1. Decision problems and residual properties. Given an infinite, finitely presented group $\Gamma$, two basic decision problems posed by Dehn [19] in 1911 are the word and conjugacy problems. In 1927, in solving the word problem for free groups, Schreier [50] proved that free groups are residual finite. That seems to be the first concrete connection between decision problems and residual properties. In 1958, Mal’cev [40] noted a similar connection between the conjugacy problem and conjugacy separability. We will discuss conjugacy separability more momentarily.

2. Algorithmic complexity. Once an algorithm for the word or conjugacy problem is found, one can study the complexity of the algorithm. For free groups, it is straightforward to see that both problems have linear algorithms as a function of word length via cyclic reduction. Bou-Rabee [7] introduced a complexity function $F_T(n)$ that quantified the efficiency of the algorithm for the word problem on $\Gamma$ given by residual finiteness (see [14] for instance on how residual finiteness relates to the word problem for finitely presented groups). Recall that a group $\Gamma$ is residually finite if for each $\gamma \in \Gamma$ with $\gamma \neq 1$, there exists a homomorphism $\varphi: \Gamma \to Q$ with $|Q| < \infty$ and $\varphi(\gamma) \neq 1$. The function introduced by Bou-Rabee measures how big the finite quotients must be over all the words of length at most $n$ in the verification of residual finiteness. Several papers have addressed the growth rate of this complexity function for various classes of groups; [7], [8], [9], [10], [11], [12], [17], [28], [29], [30], [43], and [49]. One interesting feature of this complexity function is that it relates the word growth and normal
subgroup growth (see [11]). That connection is clear in the following sense. If \( \Gamma \) has a rich supply of words of length \( n \), then we have a greater chance of making \( F_\Gamma(n) \) larger. On the other hand, if \( \Gamma \) has a rich supply of normal subgroups of bounded index, we have a greater chance of making \( F_\Gamma(n) \) smaller. We will return shortly to this relation with normal subgroup growth.

3. Linear representations of groups. In 1940, Mal’cev [39] proved that any finitely generated linear group is residually finite. The proof is not difficult and is based on the simple observation that a matrix that is not the identity is visibly not the identity in the sense that some coefficient cannot be zero. In [12], using an algorithmic proof of [39], the complexity function \( F_\Gamma(n) \) for finitely generated linear groups was shown to have a polynomial upper bound \( n^d \) where \( d \) depends only on a linear realization of \( \Gamma \). The reader should view linearity as an uniform solution to the word problem whereas residually finiteness is a case-by-case solution, providing for each word, a map to a finite group where the word has non-trivial image. This, of course, provides additional freedom as we are permitted to change \( \rho_\gamma \) and \( n_\gamma \) to custom for each word \( \gamma \). Work of Larsen [31] further emphasizes the connection between linear representations and residual properties. Specifically, if \( I(\Gamma) \) is the set of distinct indices of finite index, normal subgroups, then the abscissa of convergence \( s_\Gamma \) of the function \( \zeta_{I(\Gamma)}(s) = \sum_{i \in I(\Gamma)} i^{-s} \) is related to the representation theory of \( \Gamma \). To that end, let \( \mathcal{R}(\Gamma) \) be the set of representations \( \rho: \Gamma \to \text{GL}(n, \mathbb{C}) \) such that \( \rho(\gamma) \) is not the identity matrix. This, of course, provides additional freedom as we are permitted to change \( \rho_\gamma \) and \( n_\gamma \) to custom for each word \( \gamma \). Work of Larsen [31] further emphasizes the connection between linear representations and residual properties. Specifically, if \( I(\Gamma) \) is the set of distinct indices of finite index, normal subgroups, then the abscissa of convergence \( s_\Gamma \) of the function

\[
\zeta_{I(\Gamma)}(s) = \sum_{i \in I(\Gamma)} i^{-s}
\]

is related to the representation theory of \( \Gamma \). To that end, let \( \mathcal{R}(\Gamma) \) be the set of representations \( \rho: \Gamma \to \text{GL}(n, \mathbb{C}) \) such that \( |\rho(\Gamma)| \) is infinite. Note that in \( \mathcal{R}(\Gamma) \), the dimension \( n \) ranges over all possible natural numbers. Next, define

\[
d_\Gamma = \min \left\{ \dim \overline{\rho(\Gamma)} : \rho \in \mathcal{R}(\Gamma) \right\},
\]

where \( \overline{\rho(\Gamma)} \) is the Zariski closure of \( \rho(\Gamma) \). With this setup, the relationship established by Larsen is simply \( d_\Gamma = s_\Gamma^{-1} \). Passing from the representation to the \( \zeta \)–function is the easier direction. The converse is more difficult and employs the classification of finite simple groups. In [11], the authors proved that if a group \( \Gamma \) has an infinite linear representation, then the average behavior of \( F_\Gamma(n) \) is finite. All of these results are meant to convey the connection between linear representations and the complexity of the word problem. This connection will be further elaborated on in the forthcoming article [13].

1.1 Conjugacy separability via linear representations

Recall that \( \Gamma \) is conjugacy separable if for any pair of non-conjugate words \( \gamma, \eta \in \Gamma \), there exists a homomorphism \( \varphi: \Gamma \to Q \) with \( \varphi(\gamma), \varphi(\eta) \) not conjugate in \( Q \) and \( |Q| < \infty \). One of the goals of this article is to extend some of the above results with conjugacy separability in place of residual finiteness. Unfortunately, issues arise immediately. Stebe [52] proved that the linear groups \( \text{SL}(n, \mathbb{Z}) \) are not conjugacy separable for \( n > 2 \). For groups like \( \text{SL}(n, \mathbb{Z}) \), namely groups of integer points of a semi-simple \( \mathbb{Q} \)–algebraic group, conjugacy separability can be related to generalized class numbers, at least when the group of integer points satisfies a congruence subgroup property; see [45], Chapter 8. What
the reader can gleam from those results is that conjugacy separability is rare for groups in a large and natural class of finitely presented linear groups. Nevertheless, free groups \[52\] and finitely generated polycyclic groups \[20\] are conjugacy separable.

As in the case of residual finiteness, we seek a uniform solution to the conjugacy problem or a case-by-case solution via the representation theory of the group. It is worth noting that a linear representation reduces the non-triviality of a word to a finite check and thus an algorithmically implementable solution. We seek a similar finite reduction and must replace the coefficients of the matrix by conjugacy invariants. In this article, we focus largely on trace as trace is the simplest conjugacy invariant; other conjugacy invariants could be used, though we suspect that the general theory presented here would not greatly change. We can ask for separate levels of uniformity in our solution of the conjugacy problem:

(A) There exists an integer \( n \) and representation

\[
\rho : \Gamma \to \text{SL}(n, \mathbb{C})
\]

such that for any non-conjugate pair \( \gamma, \eta \in \Gamma \), we have

\[
\text{Tr}(\rho(\gamma)) \neq \text{Tr}(\rho(\eta)).
\]

(B) For each word \( \gamma \in \Gamma \), there exists a representation

\[
\rho_\gamma : \Gamma \to \text{SL}(n_\gamma, \mathbb{C})
\]

such that if \( \eta \in \Gamma \) is not conjugate to \( \gamma \), then

\[
\text{Tr}(\rho_\gamma(\gamma)) \neq \text{Tr}(\rho_\gamma(\eta)).
\]

(C) For any finite set \( S = \{ \gamma_i \}_{i=1}^s \) of conjugacy classes in \( \Gamma \), there exists a representation

\[
\rho_S : \Gamma \to \text{SL}(n_S, \mathbb{C})
\]

such that

\[
\text{Tr}(\rho_S(\gamma_i)) \neq \text{Tr}(\rho_S(\gamma_j))
\]

for \( \gamma_i, \gamma_j \in S \) and \( i \neq j \).

(D) For each pair of non-conjugate words \( \gamma, \eta \in \Gamma \), there exists a representation

\[
\rho_{\gamma,\eta} : \Gamma \to \text{SL}(n_{\gamma,\eta}, \mathbb{C})
\]

such that

\[
\text{Tr}(\rho_{\gamma,\eta}(\gamma)) \neq \text{Tr}(\rho_{\gamma,\eta}(\eta)).
\]

By definition, we have

(A) \( \rightarrow \) \( \rightarrow \) \( \rightarrow \) \( \rightarrow \) (B)

(C) \( \rightarrow \) \( \rightarrow \) (D)
though it is possible that (B) does not imply (C). We say one of the above properties (B), (C), or (D) is uniformly satisfied if \( n_\gamma, n_\eta, n_S \) is bounded over all choices of \( \gamma, \eta \). That is, the dimension of the representations do not depend on \( \gamma, \{ \gamma, \eta \}, \) or \( S \). In those cases, we say \( \Gamma \) uniformly has property (B), (C), or (D). It was pointed out to us by Greg Kuperberg that (C) and (D) are equivalent. To prove this, one can use the matrix associated to the character table for finite groups and the observation that conjugacy separability for non-conjugate pairs is equivalent to conjugacy separability for arbitrary finite sets of non-conjugate words. It is less clear if uniform (C) and (D) are equivalent. It is precisely this reason that we introduced (C) (see Theorem 1.1 below). Finally, we will occasionally want to consider different classical conjugacy invariants like the characteristic polynomial with regard to these properties and will say a group has the given property with respect to a given invariant in that case. If not explicitly stated, trace will be understood to be the chosen invariant.

Our first basic result is:

**Theorem 1.1.** If \( \Gamma \) uniformly has property (C), then \( \Gamma \) has property (A).

In fact, if \( \Gamma \) uniformly has property (D) for some \( n_0 \) and \( \text{Hom}(\Gamma, \text{SL}(n_0, C)) \) is connected, then \( \Gamma \) has property (A). In particular, we have the following corollary:

**Corollary 1.2.** For a free group \( F_r \), uniform property (D) and property (A) are equivalent. Moreover, for any connected Lie group \( G < \text{SL}(n, C) \), the following are equivalent:

(a) For each representation \( \rho : F_r \to G \), there exists a non-conjugate pair \( \gamma, \eta \in F_r \) with \( \text{Tr}(\rho(\gamma)) = \text{Tr}(\rho(\eta)) \).

(b) There exists a non-conjugate pair \( \gamma, \eta \in F_r \) such that for each representation \( \rho : F_r \to G \), we have \( \text{Tr}(\rho(\gamma)) = \text{Tr}(\rho(\eta)) \).

Though it seems rather clear, we also record the following result that makes explicit the theme of this portion of the article. This result first appeared in the paper of Bass–Lubotzky \[3, Proposition 3.1\] where they also prove the converse.

**Theorem 1.3** (Bass–Lubotzky). If \( \Gamma \) satisfies property (D), then \( \Gamma \) is conjugacy separable.

Bass–Lubotzky exhibited many linear features for automorphisms of schemes of finite type. One sees the rich representation theory driving the separation for automorphism groups must produce especially rich separation in the group via these representations. Specifically, they established residual finiteness for automorphisms from the much more rare conjugacy separability of the group being acted upon. This philosophy is central to this paper. We emphasize though that our primary interest is in the interplay between the infinite representation theory of a group and how it interacts with the finite representation theory (the profinite topology); see Theorem 1.8 below or our proof of Theorem 1.6.

### 1.2 Complexity for conjugacy problems

Similar to the complexity function \( F_\Gamma(n) \) associated to the word problem using residual finiteness, one can define a complexity function \( \text{Conj}_\Gamma(n) \) for the conjugacy problem using conjugacy separability
(See Section 2 for the definition). Recall that [12] shows that linearity provides uniform control on the complexity of $F(\Gamma(n))$. In comparison, we have the following pair of results.

**Theorem 1.4.** If $\Gamma$ satisfies property (A), then $\text{Conj}_\Gamma(n) \preceq n^d$ for some $d \in \mathbb{N}$. Moreover, the finite quotients used in proving conjugacy separability are subgroups of $\text{SL}(n_0, F_p)$ for an infinite set of prime fields $F_p$ and a fixed $n_0$.

We can define a relative version of the complexity function $\text{Conj}_\Gamma(n)$ by fixing a conjugacy class $[\gamma]$ in $\Gamma$. If we denote this function by $\text{Conj}_{\Gamma, \gamma}(n)$, then our next result is:

**Theorem 1.5.** If $\Gamma$ satisfies property (B), then for each $\gamma \in \Gamma$, we have $\text{Conj}_{\Gamma, \gamma}(n) \preceq n^{d_\gamma}$ for some $d_\gamma \in \mathbb{N}$.

If we replace trace with another invariant like characteristic polynomial, then both Theorems 1.4 and 1.5 hold.

**Property A: Why or why not.** We now address the likelihood a group might satisfies (A), (B), (C), or (D). We begin with property (A).

The obvious test case to begin investigating with regard to property (A) is finitely generated free groups. For $n = 2$, Horowitz [26] proved that there exist non-conjugate $\gamma, \eta \in F_2$ such that for any representation $\rho : F_2 \to \text{SL}(2, \mathbb{C})$, we have $\text{Tr}(\rho(\gamma)) = \text{Tr}(\rho(\eta))$.

We say such words are $\text{SL}_2$–trace equivalent. It seems to have been, for some time now, a folklore question as to whether or not there exists $\text{SL}_n$–trace equivalent words in $F_2$ for $n > 2$. Indeed, even the case of $n = 3$ is currently open. We discuss whether or not the words constructed by Horowitz can be $\text{SL}_n$–trace equivalent. We see that if they are, an unexpected trace relation must hold. In particular, such relations seems unlikely and we view that as a little evidence that $F_2$ (more generally $F_r$) should have property (A). Anderson [2] provides a broader context for the construction of Horowitz and a conjectural picture for what such pairs of $\text{SL}_2$–trace equivalent words should look like. Additionally, Leininger [36] and Kapovich–Levitt–Schupp–Shpilrain [27] give a more geometric/topological take (see also [21], [33], [34], [35]). Of course, we have trivially that any $\text{SL}_3$–trace equivalent pair is also an $\text{SL}_2$–trace equivalent pair. The failure of Anderson’s general construction for $\text{SL}(3, \mathbb{C})$ would be considerably more compelling evidence for property (A).

When first encountering the possibility of $\text{SL}_n$–trace equivalent words, a typical reaction is to insist that the demand is too high. After all, free groups have a rich supply of representations into $\text{SL}(n, \mathbb{C})$ and we seek non-conjugate words that regardless of the choice of the representation, have the same trace. However, we see from Corollary 1.2 for a free group the following are equivalent:

1. For each representation $\rho : F_r \to \text{SL}(n, \mathbb{C})$, there exist non-conjugate words $\gamma, \eta \in F_r$ with $\text{Tr}(\rho(\gamma)) = \text{Tr}(\rho(\eta))$.

2. There exists non-conjugate words $\gamma, \eta \in F_r$ such that for each representation $\rho : F_r \to \text{SL}(n, \mathbb{C})$, we have $\text{Tr}(\rho(\gamma)) = \text{Tr}(\rho(\eta))$. 
In particular, for each representation, we simply need to find two non-conjugate words with the same trace opposed to finding two non-conjugate words that have the same trace for every representation into $\text{SL}(n, \mathbb{C})$.

Perhaps the most compelling argument against a free group having property (A) is Theorem 1.4. Indeed, we know that for free groups, by [28] and [7], the word complexity function satisfies the asymptotic inequalities

$$n^{2/3} \lesssim \mathcal{F}_F(n) \lesssim n^3.$$ 

It is our belief that the conjugacy complexity $\text{Conj}_F(n)$ should be considerably greater. After all, we seek a finite quotient $\varphi : F_r \to Q$ where for every element $\gamma'$ in the $F_r$–conjugacy class of $\gamma$, we have $\varphi(\gamma') \neq \varphi(\eta)$. In comparison, residual finiteness only seeks that $\varphi(\gamma) \neq \varphi(\eta)$ and so on face value, conjugacy separability demands infinitely more than residual finiteness. Indeed, it is this reason why many of the natural linear groups are not conjugacy separable. However, if $F_r$ has property (A), then by Theorem 1.4, we would have, for some fixed $d$, the asymptotic inequalities

$$n^{2/3} \lesssim \text{Conj}_F(n) \lesssim n^d.$$ 

In particular, $\text{Conj}_F(n)$ and $\mathcal{F}_F(n)$ would be of the same general complexity. As an example for comparison, the integral 3–dimensional Heisenberg group is defined to be

$$N_3(\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} : x, y, z \in \mathbb{Z} \right\}.$$ 

Bou-Rabee [7] proved that $\mathcal{F}_{N_3}(n) \approx (\log(n))^2$ whereas in [44], it is shown that $\text{Conj}_{N_3}(n) \approx n^3$. The integral 3–dimensional Heisenberg group is the first non-trivial example to compare the complexity of these two functions and it is dramatically different. This holds for all torsion free, finitely generated nilpotent groups (see [44]).

**Property B: why or why not.** The best evidence for property (B) being a more reasonable property is that free and surface groups have property (B).

**Theorem 1.6.** Let $\Gamma$ be a finitely generated free or surface group. Then $\Gamma$ has property (B).

From Theorem 1.5 and Theorem 1.6, we obtain:

**Corollary 1.7.** Let $\Gamma$ be a finitely generated free or surface group and $\gamma \in \Gamma$. Then there exists $d_\gamma \in \mathbb{N}$ such that

$$\text{Conj}_{\Gamma, \gamma}(n) \lesssim n^{d_\gamma}.$$ 

Moreover, one can take $d_\gamma \approx ||\gamma||^2$ and thus

$$\text{Conj}_\Gamma(n) \lesssim n^{9n^2-1}.$$ 

The proof of Theorem 1.6 is derived from a construction of Wehrfritz [53] in the case of free groups. We provide a geometric heuristic as well. In Corollary 1.7, that $d_\gamma$ can be taken to be roughly $||\gamma||^2$. 

follows from work of Patel [43] in combination with our argument. Specifically, $\sqrt{d_\gamma}$ can be taken, up to constants, to be the smallest cover where the curve associated to $\gamma$ has a simple lift. The specific exponent $9n^2 - 1$ follows from our method of proof. The algorithm we use in Corollary 1.7 necessarily has $d_\gamma$ unbounded as $\gamma$ varies over $F_r$. We conjecture that there is no uniform polynomial complexity algorithm for solving the conjugacy problem on $F_r$; it is unclear how close our upper bound for $\text{Conj}_r(n)$ is to optimal and we have no precise conjecture for the behavior. In tandem with Theorem 1.4, we thus conjecture:

**Conjecture 1.** Finitely generated free groups do not have property (A).

This is in contrast with the general geometric belief that multiplicities in either the eigenvalue spectrum or geodesic length spectrum should generically be multiplicity free in any sufficiently complicated space of metrics. For instance, the finite dimensional space of constant $-1$ curvature metrics on a closed surface of genus $g > 1$ have large multiplicities always by [48]. In contrast, in the infinite dimensional space of negatively curved metrics, the geodesic length spectrum has multiplicity 1 generically. It is likely that the space of finite dimensional representations is simply not large enough to force distinct traces, where the moment one permits infinite dimensional unitary representation, distinct conjugacy classes should have distinct traces generically.

### 1.3 A simple observation: Profinite via representations

In the final section, Section 7, we prove an elementary result that shows that one can recover the profinite topology on a free group using faithful representations of $F_r$ to $\text{SL}(n, \mathbb{Z})$ for fixed $r$ and varying $n$. Specifically, we prove:

**Theorem 1.8.** Let $\Delta$ be a finite index normal subgroup of $F_r$. Then there exists a faithful representation $\rho : F_r \to \text{SL}(n_\Delta, \mathbb{Z})$ and a prime $p$ such that the diagram

$$
\begin{array}{ccc}
F_r & \xrightarrow{\rho} & \text{SL}(n_\Delta, \mathbb{Z}) \\
\downarrow{\varphi_\Delta} & & \downarrow{r_p} \\
F_r/\Delta & \xrightarrow{\iota} & \text{SL}(n_\Delta, \mathbb{F}_p)
\end{array}
$$

commutes. Here $r_p$ is reduction modulo $p$, $\varphi_\Delta : F_r \to F_r/\Delta$ is the canonical epimorphism, and $\iota : F_r/\Delta \to \text{SL}(n_\Delta, \mathbb{F}_p)$ is an inclusion.

Recall that the profinite topology on a group $\Gamma$ is given by declaring the finite index subgroups of $\Gamma$ to be both an open and closed neighborhood basis at the identity. By further declaring left/right multiplication to be a homeomorphism, we get a topological group topology called the profinite topology.

The proof of Theorem 1.8 is fairly simple but provides an explicit example of a possible general phenomenon. In Section 7, we discuss implications of some conjectural generalizations of Theorem 1.8. Most notable of these implications would be the implication that super-rigid lattices satisfy the
congruence subgroup property. This implication, in turn, implies the existence of non-residually finite hyperbolic groups via Agol–Groves–Manning [1] and the super-rigidity of lattices in $\text{Sp}(n,1)$ due to Corlette [18] and Gromov–Schoen [24].

Acknowledgements. The authors would like to thank Nigel Boston, Khalid Bou-Rabee, Frank Calegari, Ted Chinburg, Kelly Delp, Nathan Dunfield, Patrick Eberlein, Carolyn Gordon, Adrian Ioana, Mike Jablonski, Ilya Kapovich, Greg Kuperberg, Chris Leininger, Darren Long, Alex Lubotzky, Dave Morris, Alan Reid, Mark Sapir, Juan Souto, and Pete Storm for stimulating conversations on the topics of this article. Special thanks is given to Dunfield who many years ago posed the question to the third author on the possibility of generalizing Horowitz’s construction. The first author was partially supported by NSF grant 1309376 and Simons grant 245642. The third author was partially supported by NSF grant 1105710.

2 Preliminaries

We begin with some preliminary material that will be useful throughout this article.

2.1 Complexity functions

For two functions $f, g: \mathbb{N} \to \mathbb{N}$, we say $f \preceq g$ if there exists a positive integer constant $C$ such that $f(n) \leq Cg(Cn)$ for all $n$. In the event $f \preceq g$ and $g \preceq f$, we write $f \approx g$. For a finitely generated group $\Gamma$ with a finite generating set $X$, we denote by $||\gamma||_X$, the word length of $\gamma$ with respect to the generating set $X$. The $n$–ball with respect to a fixed generating set $X$ will be denoted by $B_{\Gamma,X}(n)$. For any set $S \subset \Gamma$, we denote by $S^\star$, the set $S - \{1\}$ with the understanding that $S = S^\star$ in the event $1 \not\in S$.

2.1.1 Word problem

Given a residually finite group $\Gamma$, Bou-Rabee [7] introduced a function for quantifying the complexity of solving the word problem via finite quotients. Specifically, we have the normal divisibility function

$$D_{\Gamma}: \Gamma^* \longrightarrow \mathbb{N}$$

given by

$$D_{\Gamma}(\gamma) = \min \{[\Gamma : \Delta] : \gamma \notin \Delta, \Delta \triangleleft \Gamma\}.$$ 

In [7] and the papers [8], [9], [11], [12], [28], [29], and [43], the complexity of this function were investigated. Presently, our interest is in an $L^\infty$–norm of $D_{\Gamma}$ on balls $B_{\Gamma,X}(n)$ given via a finite generating set $X$ for $\Gamma$. Specifically, the $L^\infty$–norm function is defined to be

$$F_{\Gamma,X}(n) = \max_{\gamma \in B_{\Gamma,X}^\star(n)} D_{\Gamma}(\gamma).$$

For any two finite generating sets $X, Y$, we have $F_{\Gamma,X} \approx F_{\Gamma,Y}$ (see [7] Lemma 1.1). Consequently, we will suppress the dependence on $X$ in notation.
2.1.2 Conjugacy problem

For a finitely generated group $\Gamma$, let $C_\Gamma$ to be the set of $\Gamma$–conjugacy classes. We can topologize the set $C_\Gamma$ with the quotient topology induced from the profinite topology on $\Gamma$. In this topology, $C_\Gamma$ is Hausdorff if and only if $\Gamma$ is conjugacy separable. However, in the definition below, we do not require that $\Gamma$ be conjugacy separable. We will relax our notation on conjugacy classes and simply write $[\gamma]$ instead of $[\gamma]_\Gamma$. For a class $[\gamma] \in C_\Gamma$, we define

$$\| [\gamma] \|_X = \min \{ \| \gamma' \|_X : \gamma' \in [\gamma] \}.$$  

We define

$$CD_\Gamma : C_\Gamma \times C_\Gamma \rightarrow \mathbb{N} \cup \{\infty\}$$

by

$$CD_\Gamma([\gamma],[\eta]) = \min \{ |Q| : \phi : \Gamma \rightarrow Q, [\phi(\gamma)]_Q \neq [\phi(\eta)]_Q \}.$$  

The following basic lemma relates $CD_\Gamma$ with $D_\Gamma$ and is left to the reader.

Lemma 2.1. For $\gamma, \eta \in \Gamma$ with $[\gamma] \neq [\eta]$, we have

$$CD_\Gamma([\gamma],[\eta]) \geq \max \{ D_\Gamma(\gamma^{-1}\eta') : \eta' \in [\eta] \}.$$  

Lemma 2.1 certainly shows that the complexity of the conjugacy problem is at least as great as the complexity of the word problem.

We define

$$B_X(C_\Gamma, n) = \{ [\gamma] : \| [\gamma] \|_X \leq n \}$$

and

$$\text{Conj}_{\Gamma,X} : \mathbb{N} \rightarrow \mathbb{N} \cup \{\infty\}$$

via

$$\text{Conj}_{\Gamma,X}(n) = \max_{[\gamma],[\eta] \in B_X(C_\Gamma, n), [\gamma] \neq [\eta]} CD_\Gamma([\gamma],[\eta]).$$

For a fixed class $[\gamma] \in C_\Gamma$, we define

$$CD_{\Gamma,\gamma} : C_\Gamma - \{[\gamma]\} \rightarrow \mathbb{N} \cup \{\infty\}$$

to be

$$CD_{\Gamma,\gamma}([\eta]) = CD_\Gamma([\gamma],[\eta]).$$

Similarly, we set

$$\text{Conj}_{\Gamma,\gamma,X}(n) = \max_{[\eta] \in B_X(C_\Gamma, n), [\eta] \neq [\gamma]} CD_{\Gamma,\gamma}([\eta]).$$

The proof of the following lemma follows that for the function $F_\Gamma(n)$ (see [7] Lemma 1.1).

Lemma 2.2. For any two finite generating sets $X, Y$ of $\Gamma$, we have

$$\text{Conj}_{\Gamma,X}(n) \approx \text{Conj}_{\Gamma,Y}(n), \quad \text{Conj}_{\Gamma,\gamma,X}(n) \approx \text{Conj}_{\Gamma,\gamma,Y}(n).$$

As a result, we will suppress the dependence on the generating set $X$ in our notation.
2.2 Representation theory

We refer the reader to [16, Section 5], [22, Section 2], and [47, Chapter V] for the material in this subsection.

We will be interested in the set $\text{Hom}(\Gamma, G)$ for a pair of groups $\Gamma, G$. When $G$ is a Lie group and $\Gamma = \mathbb{F}$, then $\text{Hom}(\mathbb{F}, G) = G'$ is obviously an analytic space. More generally, when $\Gamma$ is finitely generated of rank $r$, then $\text{Hom}(\Gamma, G)$ will be an analytic subvariety of $\text{Hom}(\mathbb{F}, G)$ (see [16, Section 5]). For each $\gamma \in \Gamma$, we have an analytic function

$$\text{Hom}(\Gamma, G) \to G$$

given by

$$\rho \mapsto \rho(\gamma).$$

In addition, if $G < \text{GL}(n, \mathbb{C})$, the function

$$\text{Tr}_\gamma : \text{Hom}(\Gamma, G) \to \mathbb{C}$$

given by

$$\text{Tr}_\gamma(\rho) = \text{Tr}(\rho(\gamma))$$

is analytic. If $G$ is a $K$–algebraic group with $K$ a characteristic zero field, then $\text{Hom}(\Gamma, G)$ is a $K$–algebraic set (not necessarily irreducible). Consequently, $\text{Hom}(\Gamma, G)$ has finitely many connected components. In particular, for $G = \text{SL}(n, \mathbb{C})$, the space $\text{Hom}(\Gamma, \text{SL}(n, \mathbb{C}))$ is a complex analytic variety with finitely many connected components. Moreover, the $\overline{Q}$–points are Zariski dense.

Though we will not require this result in the sequel, we include the following result on algebraic points of character varieties. Recall that for a connected, reductive algebraic group $G$, the $G$–character variety $X(\Gamma, G)$ is the geometric invariant theory quotient of $\text{Hom}(\Gamma, G)$ by the $G$–conjugation action. Below, for $\Gamma = \mathbb{F}$, we set $X(\mathbb{F}, G)$ to be $X(F, G)$.

**Theorem 2.3.** Let $G$ be a connected reductive affine algebraic group over $\mathbb{C}$. Then $X(\mathbb{F}, G(\mathbb{Q}))$ is classically dense in $X(\mathbb{F}, G)$.

**Proof.** To begin, $\text{Hom}(\mathbb{F}, G) \cong G'$ by evaluation. According to [6] p. 220], $G(K)$ is Zariski dense in $G$ for any infinite subfield $K \subset \mathbb{C}$. Since Cartesian products inherit this property, $\text{Hom}(\mathbb{F}, G(K))$ is Zariski dense in $\text{Hom}(\mathbb{F}, G)$ for any infinite $K \subset \mathbb{C}$. However, since

$$\text{Hom}(\mathbb{F}, G(K)) \subset \text{Hom}(\mathbb{F}, G),$$

we conclude $\text{Hom}(\mathbb{F}, G(K))$ is Zariski dense in $\text{Hom}(\mathbb{F}, G)$ for infinite fields $K \subset \mathbb{C}$. However, Zariski dense implies classically dense over algebraically closed fields. Thus, $\text{Hom}(\mathbb{F}, G(\overline{\mathbb{Q}}))$ is classically dense in $\text{Hom}(\mathbb{F}, G)$.

Now consider

$$X(\mathbb{F}, G) = \text{Spec}(\mathbb{C}[\text{Hom}(\mathbb{F}, G)]^G).$$

Let $f_1, \ldots, f_N$ be a set of generators for $\mathbb{C}[\text{Hom}(\mathbb{F}, G)]^G$ and define

$$F : \text{Hom}(\mathbb{F}, G) \to \mathbb{C}^N$$
by
\[ F(g_1, \ldots, g_r) \overset{\text{def}}{=} (f_1(g_1, \ldots, g_r), \ldots, f_N(g_1, \ldots, g_r)). \]

Geometric invariant theory tells us that
\[ X_r(G) = F(\text{Hom}(F_r, G)) \] (see [51]). Since
\[ C[\text{Hom}(F_r, G)]^G \subset C[\text{Hom}(F_r, G)] = C[G]^\otimes r \]
\[ C[G] = Q[G] \otimes Q C, \]
we conclude that \( f_1, \ldots, f_N \) may be chosen to have only coefficients over \( Q \). Thus,
\[ F(\text{Hom}(F_r, G(\overline{Q}))) \subset X_r(G(\overline{Q})). \]

Finally, as \( F \) is a continuous surjective function in the classical topology and the image of a classically dense set under a continuous surjective function is classically dense, we conclude that \( F(\text{Hom}(F_r, G(\overline{Q}))) \) is classically dense in \( X_r(G) \). Hence, \( X_r(G(\overline{Q})) \) is classically dense in \( X_r(G) \) as it contains the dense set \( F(\text{Hom}(F_r, G(\overline{Q}))) \).

**Corollary 2.4.** If \( G = \text{SL}(n, C) \), the integral points are infinite in \( X_r(G) \).

**Proof.** Since the group schemes and invariant rings are defined over \( Z[1/n] \), the result follows from the above proof.

In the work of Long and Reid [37], one can infer that this is false for \( \text{SL}(2, C) \) and closed surface groups.

### 3 Property (C): Proof of Theorem 1.1 and Theorem 1.3

In this section, we prove Theorems 1.1 and 1.3.

#### 3.1 Proof of Theorem 1.1 and Corollary 1.2

In the following, we need something slightly more than property (D) in order to recover property (A). Specifically, we need either (C) or that \( \text{Hom}(\Gamma, \text{SL}(n, C)) \) is connected. In this subsection, we prove that either uniform (C), or uniform (D) with the connectivity of \( \text{Hom}(\Gamma, \text{SL}(n, C)) \) imply property (A).

**Proof of Theorem 1.1** We assume first that \( \Gamma \) uniformly has property (C). Note that if \( \Gamma \) is finite, then the equivalence of (A) and (C) is obvious. Thus, we shall assume that \( \Gamma \) is infinite; indeed, the reader should always assume \( \Gamma \) is infinite throughout this article. We enumerate the conjugacy classes of \( \Gamma \) by \( \{ [\gamma_1], [\gamma_2], \ldots \} \). For each \( r \), let \( S_r = \{ [\gamma_i] \}_{i=1}^r \) be the set of the first \( r \) conjugacy classes. By assumption, there exists \( n \in N \) and for each \( r \), we have a representation
\[ \rho_r : \Gamma \rightarrow \text{SL}(n, C) \]
such that
\[ \text{Tr}(\rho(\gamma_i)) \neq \text{Tr}(\rho(\gamma_j)) \]
for all \( i \neq j \). As \( \text{Hom}(\Gamma, \text{SL}(n, \mathbb{C})) \) is a complex analytic variety, there are only finitely many connected components. By the Pigeon Hole Principle, there exists a component that contains infinitely many of the representations \( \rho_r \), say \( V_0 \subset \text{Hom}(\Gamma, \text{SL}(n, \mathbb{C})) \). By selection, the trace functions \( \text{Tr}_\gamma \) restricted to \( V_0 \) are distinct analytic functions for each conjugacy class \([\gamma]\). In particular,
\[ \text{Tr}_{\gamma_i} - \text{Tr}_{\gamma_j} \neq 0 \]
is a non-constant analytic function on \( V_0 \) for each pair \( i \neq j \). In particular, the sets
\[ Z_{i,j} = \{ \rho \in V_0 : \text{Tr}_{\gamma_i}(\rho) - \text{Tr}_{\gamma_j}(\rho) = 0 \} \]
are proper analytic subvarieties of \( V_0 \). By the Baire Category Theorem,
\[ V = V_0 - \bigcup_{i,j} Z_{i,j} \]
is a dense, a thus non-empty, subset. By construction, any \( \rho \in V \) has the property that
\[ \text{Tr}(\rho(\gamma)) = \text{Tr}(\rho(\eta)) \]
if and only if \( \gamma, \eta \) are conjugate in \( \Gamma \). In particular, \( \Gamma \) has property (A).

In the case we uniformly have (D) and \( \text{Hom}(\Gamma, \text{SL}(n, \mathbb{C})) \) is connected, we know that by assumption that for each pair of conjugacy classes \( \gamma, \eta \in \Gamma \), we have a representation \( \rho : \Gamma \to \text{SL}(n, \mathbb{C}) \) with \( \text{Tr}(\rho(\gamma)) \neq \text{Tr}(\rho(\eta)) \). Since \( \text{Hom}(\Gamma, \text{SL}(n, \mathbb{C})) \) is connected, we can proceed as before with \( V_0 = \text{Hom}(\Gamma, \text{SL}(n, \mathbb{C})) \).

\[ \square \]

Proof of Corollary 1.2. The first part of Corollary 1.2 follows immediate from the connectivity of
\[ \text{Hom}(F_r, \text{SL}(n, \mathbb{C})) = (\text{SL}(n, \mathbb{C}))^F. \]
The second part, the equivalence of (a) and (b), of Corollary 1.2 follows from the Baire Category Theorem. Specifically, we argue as follows. We must prove that the following two statements are equivalent:

(a) There exists two non-conjugate words \( \gamma, \eta \in F_r \) that have \( \text{Tr}(\rho(\gamma)) = \text{Tr}(\rho(\eta)) \) for every \( \rho : F_r \to \text{SL}(n, \mathbb{C}) \).

(b) For each representation \( \rho : F_r \to \text{SL}(n, \mathbb{C}) \), there exist two non-conjugate words \( \gamma, \eta \in F_r \) such that \( \text{Tr}(\rho(\gamma)) = \text{Tr}(\rho(\eta)) \).

It is clear that (a) implies (b). To prove that (b) implies (a), we assume that (b) holds but not (a) and derive a contradiction. Since (a) does not hold, then for each pair of non-conjugate words \( \gamma, \eta \in F_r \), the function
\[ \text{Tr}_\gamma - \text{Tr}_\eta \]
on \( \text{Hom}(F_r, \text{SL}(n, \mathbb{C})) \) is a non-constant analytic function. Thus
\[
V_{\gamma, \eta} = \left\{ \rho \in \text{Hom}(F_r, \text{SL}(n, \mathbb{C})) : \text{Tr}_\gamma(\rho) - \text{Tr}_\eta(\rho) = 0 \right\}
\]
is nowhere dense. Taking
\[
V = \bigcup_{|\gamma| \neq |\eta|} V_{\gamma, \eta},
\]
by the Baire Category Theorem, \( V \) is nowhere dense. Let \( \rho \in \text{Hom}(F_r, \text{SL}(n, \mathbb{C})) - V \) and note that by construction, no two non-conjugate elements have the same trace under \( \rho \). This contradicts our assumption that (b) holds for every \( \rho \in \text{Hom}(F_r, \text{SL}(n, \mathbb{C})) \). Thus, we see that (b) implies (a). \( \square \)

### 3.2 Proof of Theorem 1.3

The proof of this result is not too difficult. However, as we will use some of the setup later, we will be particularly careful at the cost of possibly belaboring the point of the proof. We refer the reader to [42] for some background material number fields, their ring of integers, and ideal theory in such rings.

**Proof of Theorem 1.3** Given a pair of non-conjugate words \( \gamma, \eta \in \Gamma \), we seek a homomorphism
\[
\varphi : \Gamma \rightarrow Q
\]
where \( Q \) is a finite group such that \( \varphi(\gamma), \varphi(\eta) \) are not conjugate in \( Q \). By assumption, \( \Gamma \) has property (D) and so we have a representation
\[
\rho : \Gamma \rightarrow \text{SL}(n, \mathbb{C})
\]
such that \( \text{Tr}(\rho(\gamma)) \neq \text{Tr}(\rho(\eta)) \). Our goal now will be to use this representation \( \rho \) to produce a homomorphism
\[
\varphi : \Gamma \rightarrow \text{SL}(n, \mathbb{F}_q)
\]
such that \( \text{Tr}(\varphi(\gamma)) \neq \text{Tr}(\varphi(\eta)) \) where \( \mathbb{F}_q \) is a finite field of order \( q \). To that end, since \( \Gamma \) is finitely generated, the field \( L \) generated over \( \mathbb{Q} \) by the coefficients of the elements \( \rho(\lambda) \) as we vary over all \( \lambda \in \Gamma \) has the form
\[
L = K(x_1, \ldots, x_r)
\]
where \( K/\mathbb{Q} \) is a finite extension and \( x_1, \ldots, x_r \) are indeterminants. At the cost of introducing a fixed finite number of new indeterminants, we can ensure that \( \rho(\Gamma) < \text{SL}(n, R) \) where
\[
R = S[x_1, \ldots, x_r],
\]
where \( S = \mathcal{O}_K[1/\beta_1, \ldots, 1/\beta_t] \) and \( \mathcal{O}_K \) is the ring of \( K \)-integers. We see then that \( \text{Tr}(\rho(\lambda)) \in R \) for each \( \lambda \in \Gamma \). Now, we know that
\[
\text{Tr}(\rho(\gamma)) - \text{Tr}(\rho(\eta)) = F(x_1, \ldots, x_{r'}) \in R
\]
is a non-zero polynomial in the variables \( x_1, \ldots, x_{r'} \) with coefficients in \( S \). Since \( F \) is non-zero, we can find \( \alpha_1, \ldots, \alpha_{r'} \in S \) such that
\[
\alpha = F(\alpha_1, \ldots, \alpha_{r'}) \neq 0, \quad \alpha \in S.
\]
We know that there are only finitely many prime ideals \( p \) in \( S \) such that \( \alpha = 0 \mod p \). Specifically, the primes for which \( \alpha = 0 \mod p \) are precisely those prime ideals that occur in the primary decomposition of the ideal \( (\alpha) \). Note also that all prime ideals in \( R \) are maximal and that for every non-trivial ideal \( \alpha \) of \( S \), \( S/\alpha \) is finite. In particular, when \( p \) is a prime ideal, \( S/p \) will be a finite field. We select a prime \( p \) for which 
\[
\alpha \neq 0 \mod p.
\]
This yields a sequence of maps of rings
\[
R \xrightarrow{\text{Eval}} S \xrightarrow{\alpha} S/p \cong F_q
\]
and a sequence of homomorphisms
\[
\Gamma \to SL(n, R) \to SL(n, S) \to SL(n, F_q).
\]
Set
\[
\varphi : \Gamma \to SL(n, F_q)
\]
to be the resulting map. By construction
\[
\text{Tr}(\varphi(\gamma)) \neq \text{Tr}(\varphi(\eta))
\]
and so \( \varphi(\gamma), \varphi(\eta) \) are not conjugate in \( SL(n, F_q) \).

4 Complexity: Proof of Theorem 1.4 and Theorem 1.5

In this section, we show how property (A) and (B) give bounds on the growth rate of \( \text{Conj}_\Gamma(n) \)

4.1 Proof of Theorem 1.4

We will assume that \( \Gamma \) has property (A) for some integer \( m \in \mathbb{N} \). Namely, we have a representation
\[
\rho : \Gamma \to SL(m, \mathbb{C})
\]
such that for any non-conjugate pair \( \gamma, \eta \in \Gamma \), we have \( \text{Tr}(\rho(\gamma)) \neq \text{Tr}(\rho(\eta)) \). We will assume that \( \rho(\Gamma) \subset SL(m, \overline{Q}) \). The alternative is \( \rho(\Gamma) \subset SL(m, K[x_1, \ldots, x_r]) \) where \( K/\mathbb{Q} \) is a finite extension is handled similarly (see [12]). The plan for the proof is to follow the proof of Theorem 1.3 but additionally control the process. Our task is to prove that for any pair of non-conjugate words \( \gamma, \eta \in \Gamma \) with \( ||\gamma||, ||\eta|| \leq n \), that
\[
\text{CD}_\Gamma(\gamma, \eta) \leq Cn^{m^2-1}
\]
for a constant \( C \) that is independent of \( \gamma, \eta \). To begin, we have our representation
\[
\rho : \Gamma \to SL(m, \overline{Q}).
\]
We can find a finite extension $K/Q$ and finite extension $S/O_K$ such that $\rho(\Gamma) < \text{SL}(m,S)$. With this setup, we know for any two non-conjugate elements $\gamma, \eta$ that

$$\text{Tr}(\rho(\gamma)) - \text{Tr}(\rho(\eta)) \in S$$

and also is non-zero. We seek an ideal $\alpha$ of $S$ such that

$$\text{Tr}(\rho(\gamma)) - \text{Tr}(\rho(\eta)) \neq 0 \mod \alpha$$

and with $|S/\alpha|$ small. We achieve this goal using the methods of [7] (or [12]). First, we control the size of the coefficients of $\rho(\gamma), \rho(\eta)$ as a function of word length. To that end, it follows (see [7] or [12] Proof of Theorem 1.1) that there exists constants $\alpha$ and $C_0$ depending only on the generators of $\Gamma$ such that

$$\max \{ \|(\rho(\gamma))_{i,j}\| : i,j \in \{1,\ldots,m\} \} \leq \alpha^{C_0||\gamma||}.$$ 

In particular, given two elements $\gamma, \eta \in \Gamma$ that are not conjugate and $||\gamma||, ||\eta|| \leq n$, we see that

$$|\text{Tr}(\rho(\gamma)) - \text{Tr}(\rho(\eta))| \leq |\text{Tr}(\rho(\gamma))| + |\text{Tr}(\rho(\eta))| \leq 2m\alpha^{C_0n}.$$ 

By [7, Theorem 2.4]), we can find a prime ideal $p$ with

$$|S/p| \leq C_1 \log(C_12m\alpha^{C_0n}) \leq C_1C_0n \log(C_12m\alpha)$$

such that

$$\text{Tr}(\rho(\gamma)) \neq \text{Tr}(\rho(\eta)) \mod p.$$ 

The constant $C_1$ depends only on the ring $S$. Let

$$r_p : \text{SL}(n,S) \rightarrow \text{SL}(n,S/p)$$

be the reduction modulo $p$ homomorphism and set

$$\rho_p : \Gamma \rightarrow \text{SL}(n,S/p)$$

by $\rho_p = r_p \circ \rho$. The elements $\gamma$ and $\eta$ have non-conjugate images since $\rho_p(\Gamma) < \text{SL}(n,S/p)$ and $\rho_p(\gamma), \rho_p(\eta)$ have different traces. We also have

$$|\rho_p(\Gamma)| \leq |\text{SL}(n,S/p)| \leq |S/p|^{m^2-1} \leq (C_1n \log(C_12m\alpha))^{m^2-1} = Cn^{m^2-1}$$

where $C$ is the constant $(C_1C_0 \log(C_12m\alpha))^{m^2-1}$. In particular, we have

$$\text{CD}_\Gamma([\gamma],[\eta]) \leq Cn^{m^2-1}$$

for some constant $C$ depending only $\Gamma$ and $\rho$. As this holds for all $[\gamma],[\eta] \in B(\Gamma,n)$, we see that

$$\text{Conj}_\Gamma(n) \leq n^{m^2-1}.$$ 

The assertion that one only needs subgroups of $\text{SL}(n_0,F_p)$ in proving conjugacy separability for $\Gamma$ follows via a direct application of the Cebotarev density theorem. Specifically, the prime $p$ can be selected to have prime residue field $S/p = F_p$. That claim, in turn, follows from the infinitude of inert
primes $p$ in $S$, a standard corollary of the Cebotarev density theorem. Note that we are also additionally using that there are only finitely many primes $p$ where

$$\text{Tr}(\rho(\gamma)) - \text{Tr}(\rho(\eta)) = 0 \mod p.$$ 

The method of proof for Theorem 1.5 is identical. In addition, we see that after applying corestriction from $L/\mathbb{Q}$, we obtain the following (in the statement of the result, $\mathbb{Z}_p$ is the $p$–adic integers):

**Corollary 4.1.** Let $\Gamma$ have property (A) and $\rho(\Gamma) < \text{SL}(n, \mathbb{Q})$. Then for all but finitely many primes $p$, there exists a representation $\rho : \Gamma \to \text{SL}(N, \mathbb{Z}_p)$ such that $\gamma, \eta \in \Gamma$ are conjugate in $\Gamma$ if and only if $\rho(\gamma), \rho(\eta)$ are conjugate in $\text{SL}(N, \mathbb{Z}_p)$. We can take $N = n \deg(K/\mathbb{Q})$ and the excluded set of primes $p$ is determined by $S$.

For the free group, the profinite (or pro–$p$ completion) $\widehat{F}_r$ is quite large. In particular, the homomorphism $\widehat{\rho} : \widehat{F}_r \to \text{SL}(N, \mathbb{Z}_p)$ induced by $\rho : F_r \to \text{SL}(N, \mathbb{Z}_p)$ has a large kernel. If $F_r$ has property (A) (or equivalent uniform property (D)), the map $\widehat{\rho}$ is injective on conjugacy classes coming from $F_r$ despite this large kernel. The existence of such a representation seems rather unlikely. Consequently, we view Corollary 4.1 as further evidence that free groups do not have property (A).

### 5 Horowitz’s construction

In this section we show that the cyclically reduced words constructed in Example 8.2 in [26] that do have the same trace over $\text{SL}(2, \mathbb{C})$ are not likely to have the same trace over $\text{SL}(n, \mathbb{C})$ for $n > 2$. Since $\text{SL}(n-1, \mathbb{C})$ embeds into $\text{SL}(n, \mathbb{C})$ it suffices to show that this failure occurs for $n = 3$.

Let $F_2 = \langle a, b \rangle$. Horowitz’s words are defined recursively by $w_0 = a$ and

$$w_m(\varepsilon_1, \ldots, \varepsilon_m) := \prod_{i=0}^{m-1} b^{2^i} w_i \prod_{i=0}^{m-1} b^{2^{-i}} w_i^{-1},$$

for $\varepsilon_i = \pm 1$. So for instance,

$$w_1(1) = a^{-1} b^2 a b a^{-1} b^2 a$$

and

$$w_1(-1) = a b^2 a^{-1} b a b a^{-1}.$$

Explicitly checking $w_1(\pm 1)$ for $\text{SL}(3, \mathbb{C})$ in *Mathematica*, using the a specific representation $\rho = (A, B) \in \text{SL}(3, \mathbb{C})^2$ gives

$$\text{Tr}(w_1(1)) - \text{Tr}(w_1(-1)) \neq 0,$$
since the 7th and 8th variables are in fact permuted (switching the roles of $u$ and $v$) and the first 6 are identical (just by cyclic permutation), and the 9th is cyclically equivalent to the trace of its inverse. The 9th word is $ubu^{-1}bub^{-1}ua^{-1}b^{-1}$. Note also that there is a polynomial $P$ in the 8 algebraically independent variables so that

$$\text{Tr}(w^{-1}) = P - \text{Tr}(w).$$

If we had equality we would have a non-trivial relation (symmetric in two variables), which is highly unlikely.
5.1 Candidates words

By Lemma 6.8 in [26] any two words in a free group of rank two that have the same $\text{SL}(2, \mathbb{C})$ trace, must have the same number of each generator represented in the word, up to plus or minus exponents. Thus, the same result holds for words that are $\text{SL}_n$–trace equivalent for any $n$.

Since $F_2 < F_r$ for $r \geq 2$, it suffices to find words in $F_2$. Conversely, as pointed out to us by Greg Kuperberg, if $s < r$, then $F_r$ is isomorphic to an equiconjugate subgroup of $F_s$ (a subgroup $H$ of a group $G$ is equiconjugate if every two elements $a$ and $b$ in $H$ that are conjugate in $G$, are already conjugate in $H$). Note that a malnormal subgroup is visibly equiconjugate and free groups have many finitely generated, malnormal subgroups. So, if there are non-conjugate pairs of words in $F_r$ ($r > 2$) that are $\text{SL}_n$–trace equivalent, then there are likewise $\text{SL}_n$–trace equivalent pairs in $F_2$. So we need only consider $F_2 = F_2(a, b)$.

It is easy to see that pairs of the form $(w, w^{-1})$ are $\text{SL}_2$–trace equivalent. However, by [5] the word map is dominant for non-trivial words, and so $(w, w^{-1})$ are never $\text{SL}_n$–trace equivalent for $n \geq 3$ since $\text{Tr}(A) \neq \text{Tr}(A^{-1})$ for all $A \in \text{SL}(3, \mathbb{C})$.

Along the same lines, we have:

**Lemma 5.1.** Let $r(w)$ be the palindrome of the word $w$, and assume $r(w)$ is not conjugate to $w$. Then $r(w)$ and $w$ are always $\text{SL}_n$–trace equivalent if and only if $n = 2$.

**Proof.** Since $\text{Tr}(w) = \text{Tr}(w^{-1})$ for $n = 2$, we obtain

$$\text{Tr}(w(a, b)) = \text{Tr}(w(a, b)^{-1}) = \text{Tr}(r(w(a^{-1}, b^{-1}))).$$

Therefore, $\text{Tr}(r(w(a, b))) = \text{Tr}(w(a^{-1}, b^{-1}))$. By the Fricke-Voigt Theorem (see for instance [23]), $\text{Hom}(F_2, \text{SL}(2, \mathbb{C})) / \text{SL}(2, \mathbb{C}) \cong \mathbb{C}^3$ parametrized by $(\text{Tr}(a), \text{Tr}(b), \text{Tr}(ab))$. Thus, there exists a (unique) polynomial $P \in \mathbb{C}[x, y, z]$ such that

$$\text{Tr}(w(a, b)) = P(\text{Tr}(a), \text{Tr}(b), \text{Tr}(ab)).$$

We conclude

$$\text{Tr}(r(w(a, b))) = P(\text{Tr}(a^{-1}), \text{Tr}(b^{-1}), \text{Tr}(a^{-1}b^{-1})) = P(\text{Tr}(a), \text{Tr}(b), \text{Tr}(ab)) = \text{Tr}(w(a, b)).$$

Conversely, $\text{Hom}(F_2, \text{SL}(3, \mathbb{C})) / \text{SL}(3, \mathbb{C})$ is a branched double cover of $\mathbb{C}^8$ (see [32]). The branch is exactly determined by $\text{Tr}(aba^{-1}b^{-1}) = \text{Tr}(b^{-1}a^{-1}ba)$; showing that for $r = 2$ the pairs $(w, r(w))$ are not generally $\text{SL}_n$–trace equivalent for $n \geq 3$.

Moreover, we expect that non-conjugate palindromic pairs are never $\text{SL}_3$–trace equivalent, although we do not yet have a proof. A more provocative conjecture is this; positive words have only non-negative powers of the generators occurring in a reduced representation:

**Conjecture 2.** Let $n \geq 2$. There exists $\text{SL}_n$–trace equivalent pairs $(u, v)$ if and only if there exists positive pairs $(u', v')$ that are $\text{SL}_n$–trace equivalent.
Sketch of Proof. As the reverse implication is obvious, we discuss only the direct implication. For \( n = 2 \), Lemma 5.1 establishes the statement. For \( n > 2 \) we describe an algorithm (that depends on \( n \)) that takes a non-conjugate \( SL_n \)-trace equivalent pair and produces a pair, that we expect that is positive, \( SL_n \)-trace equivalent, and not conjugate. We have implemented the algorithm for \( n = 2 \) and it does produce a positive pair \((u', v')\) that is \( SL_2 \)-trace equivalent but \( u' \) is conjugate to \( v' \); we expect this to be a problem only with \( n = 2 \).

In what follows, let \( \rho(a) = A \) be an \( n \times n \) matrix. Recall the Cayley–Hamilton formula gives

\[
0 = \sum_{k=0}^{n} (-1)^{n-k} C_k^n(A) A^k,
\]

where the coefficients \( C_k^n(A) \) arise from the characteristic equation \( \det(tI - A) = \sum_{k=0}^{n} (-1)^{n-k} C_k^n(A) t^k \). We know that \( C_0^n(A) = 1 \), \( C_1^n(A) = \text{Tr}(A) \) and \( C_0^n(A) = \det(A) \). By Newton’s trace formulas each \( C_k^n(A) \) is a polynomial in the traces of non-negative powers of the matrix \( A \). Since \( \det(A) = 1 \), we can multiply the Cayley–Hamilton formula by a word \( UA^{-1} := \rho(ua^{-1}) \) on the left and another word \( V := \rho(v) \) on the right. This results in

\[
UA^{a-1}V + \sum_{k=1}^{n-1} (-1)^{n-k} C_k^n(A) UA^{k-1}V = (-1)^{n+1} UA^{-1}V.
\]

Thus, by taking the trace of both sides, we have:

\[
\text{Tr}(UA^{a-1}V) = (-1)^{n+1} \text{Tr}(UA^{a-1}V) + \sum_{k=1}^{n-1} (-1)^{k-1} C_k^n(A) \text{Tr}(UA^{k-1}V).
\]

This shows that given any word \( w \) with negative exponents, one can iteratively apply the preceding formula in the coordinate ring \( \mathbb{C}[\text{Hom}(F_2, SL(n, \mathbb{C})) // SL(n, \mathbb{C})] \), which is generated by traces of words by results of Procesi [46], to obtain an expression for \( \text{Tr}(w) \) as a polynomial in traces of positive words.

Now, suppose \((u, v)\) is \( SL_n \)-trace equivalent but are not conjugate. After cyclically reducing \( u \) and \( v \), given results of Horowitz [26], we can assume that \( u \) and \( v \) have the same word length and the same (signed) multiplicity of each letter.

Then applying the preceding algorithm to \( \text{Tr}(u) \) and to \( \text{Tr}(v) \) results in polynomial expressions \( P_u \) and \( P_v \) in terms of traces of only positive words. By inspection of the replacement formula defining the algorithm, one sees that there will be a monic trace term with a longest word. That is \( P_u = \text{Tr}(u') + L \), and likewise \( P_v = \text{Tr}(v') + L' \) where both \( L, L' \) contain terms of products of traces of shorter positive words. We expect that \( \text{Tr}(u') = \text{Tr}(v') \) since \( \text{Tr}(u) = \text{Tr}(v) \) to begin with. Also, given that \( n \geq 3 \), we expect that \( u' \) is not conjugate to \( v' \) given that \( u \) is not conjugate to \( v \).

It is not presently clear to us how to complete the above argument, that is, to prove that the last two lines are valid. We thank Greg Kuperberg for conversations about the validity of the above sketch.

We now indicate our interest in this conjecture. For the free group \( F_2 = F_2(a, b) \), the smallest positive exponent \( SL_2 \)-trace equivalent pair is

\[
\{babba, abaabb\}.
\]
To find examples of $\text{SL}(3, \mathbb{C})$ words, if the conjecture is true, we need only check words with the same number of letters in each word having only positive exponents. Moreover, since by restricting, the trace equivalence must also hold for $\text{SL}(2, \mathbb{C})$, we need only check words of the above type that work for $\text{SL}(2, \mathbb{C})$. We expect that non-conjugate reverse pairs will never be $\text{SL}_3$–trace equivalent, and so we further wish to only consider positive non-conjugate pairs that are not palindromes but are $\text{SL}_2$–trace equivalent—the first example occurs at length 12:

$$\{aabbaabbab,aababbabaabb\}.$$ 

We end this section with two broad questions about such words.

**Question.**

1. What is a classification of these words, or generating families?
2. What is the growth rate of the length of these words? If it is slow enough, can we really expect there to be examples for all $n$?

As we expect $\text{SL}_n$–trace equivalent words exist, our guess is that the above words are rather plentiful, despite our exhaustive (unsuccessful) search for $\text{SL}_3$–equivalent pairs (not only positive pairs) up to length 20.

## 6 Complexity for the conjugacy problem: Free groups

In this section, we provide two different approaches to solving the conjugacy problem in free groups, neither of which are originally due to us. We give complexity bounds on these two different approaches by implementing them algorithmically.

### 6.1 Lower central and derived series methods

The lower central and derived series in a group $\Gamma$ are defined inductively by

$$\Gamma_0 = \Gamma, \quad \Gamma_j = [\Gamma, \Gamma_{j-1}], \quad \Gamma^j = [\Gamma^{j-1}, \Gamma^{j-1}].$$

The quotient groups $N_j(\Gamma) = \Gamma / \Gamma_j$ and $S_j(\Gamma) = \Gamma / \Gamma^j$ are universal for maps to nilpotent and solvable quotient groups of $\Gamma$ of step size $j$.

The following result can be found in [38, p. 27, Proposition 4.9]:

**Proposition 6.1.** $\gamma, \eta \in F_r$ are conjugate if and only if they have conjugate image in $S_j(F_r)$ (or $N_j(F_r)$) for all $j$.

The groups $S_j(F_r)$ and $N_j(F_r)$ are conjugacy separable for all $j$ (see [41] and [20]) and so one obtains an algorithm for deciding when two elements in $F_r$ are conjugate. We can associate several complexity
functions for various algorithms for deciding the conjugacy problem on a finitely generated group. For example, we know from [8] and [41] that one can ensure as a function of word length $|\gamma|$ when $\gamma$ will represent non-trivially in $S_j(F_r)$ and $N_j(F_r)$. Two algorithms for solving the conjugacy problem in $F_r$ can be given using $S_j(N_r)$ and $N_j(F_r)$. Indeed, it seems most proofs of the fact that free groups are conjugacy separable reduce the problem to two results:

(Step 1) Prove that given two non-conjugate words $\gamma, \eta \in F_r$, there exists $j_{\gamma, \eta}$ such that $\gamma, \eta$ have non-conjugate images in $N_j(F_r)$.

(Step 2) Prove that $N_j(F_r)$ is conjugacy separable.

One can instead take $S_j(F_r)$ in (Step 1) and then prove $S_j(F_r)$ is conjugacy separable. In fact, since $S_j(F_r)$ maps onto $N_j(S_r)$, we see that the same $j_{\gamma, \eta}$ from (Step 1) would work for $S_j(F_r)$.

In (Step 2), we know that $N_j(F_r)$ is conjugacy separable by Blackburn [4] and that $S_j(F_r)$ is conjugacy separable by Formanek [20].

In order to implement the above approach algorithmically, we must first estimate $j_{\gamma, \eta}$ as a function of the complexity of $\gamma, \eta$. Second, we must algorithmically solve the conjugacy problem in torsion free nilpotent or polycyclic groups. The work of Malestein–Putman [41] addresses the first problem. The forthcoming paper [44] addresses the second problem.

As our current goal is deciding whether or not the function $Conj_{F_r}(n)$ has a polynomial bound, we note that it is already known that the above method cannot work. Specifically, neither the lower central or derived series provides a polynomial complexity solutions of the word problem; see [7] and [8]. As such, we will not say more about these approaches and refer the reader to [44] for more on the complexity of these algorithms.

6.2 Representation theoretic methods: Theorem 1.6

In this subsection, we give a proof of Theorem 1.6. The proof uses a construction of Wehrfritz [53] who gave a different proof of the conjugacy separability of $F_r$. The statement of his result is as follows.

Theorem 6.2 (Wehrfritz). For $\gamma \in F_r$, there exists a faithful representation $\rho: \Gamma \to \text{GL}(3m, R)$ where $R$ is a residually finite integral domain such that $[\rho(\gamma)]_{\rho(F_r)}$ is Zariski closed in $\rho(F_r)$.

The Zariski closed condition permits one to separate the conjugacy class of $[\rho(\gamma)]$ using ideals in the ring $R$.

Before we provide an algorithm for conjugacy separability, we first give a more geometric, informal version of how to prove Theorem 6.2. This approach can be extended to surface groups and also be made fully rigorous. The algebraic proof following our geometric sketch is also easily extended to surface groups. We discuss this extension in greater detail below.

(Step 1) View $F_r$ as the fundamental group of a compact surface with boundary $\Sigma$. Identify $\gamma \in F_r$ with a closed curve on $\Sigma$. We say a loop on $\Sigma$ is simple if there is a loop in the free homotopy class
that is embedded. Via M. Hall [25], we can find a finite cover \( \Sigma \rightarrow \Sigma \) where \( \gamma \) is a simple closed loop. Patel [43] says that the degree of this cover can be taken to be approximately the length of the word \( \gamma \).

(Step 2) Double \( \Sigma \) along the boundary to produce a closed surface \( \Sigma_g \) where \( \gamma \) is a simple closed curve. As \( \gamma \) is simple, we can find a hyperbolic metric on \( \Sigma_g \) where the geodesic representative for \( \gamma \) is the unique shortest geodesic. This yields a faithful representation \( \rho : \pi_1(\Sigma_g) \rightarrow \text{SL}(2, \mathbb{R}) \),

where \( |\text{Tr}(\rho(\gamma))| < |\text{Tr}(\rho(\eta))| \) for all non-conjugate \( \eta \in \pi_1(\Sigma_g) \) with \( \eta \neq \gamma^{-1} \). In addition, we can arrange for the coefficients of the representation \( \rho \) to be in \( \mathbb{Q} \).

(Step 3) As \( \text{Tr}(\rho(\gamma)) = \text{Tr}(\rho(\gamma^{-1})) \), we must augment the representation \( \rho \). Since \( \gamma \) corresponds to a simple curve, we have an associated map \( \tau : \pi_1(\Sigma_g) \rightarrow \mathbb{Z} \) with \( \tau(\gamma) = 1 \); the map \( \tau \) is just projection onto the line in first (co)homology corresponding to the class \( [\gamma] \). We then obtain \( \rho' : \pi_1(\Sigma_g) \rightarrow \text{GL}(3, \mathbb{C}) \)

given by

\[ \rho' (\eta) = \begin{pmatrix} \rho(\eta) & 0 \\ 0 & e^{\tau(\eta)} \end{pmatrix}. \]

(Step 4) Via induction of representations, we get \( \text{Ind}_{\pi_1(\Sigma)}^{\pi_1(\Sigma_g)}(\rho'_{\pi_1(\Sigma_g)}) = \tilde{\rho} \) where

\[ \tilde{\rho} : \pi_1(\Sigma) \rightarrow \text{SL}(3|\pi_1(\Sigma) : \pi_1(\Sigma_g)|, \mathbb{C}). \]

The trace of \( \tilde{\rho}(\gamma) \) determines the conjugacy class of \( \gamma \) in \( \pi_1(\Sigma) \).

This terse argument is meant to serve as a geometric model of how to solve the conjugacy problem as after all conjugacy is nothing more than free homotopy. The point is that it is easy to deal with simple curves since we can find a pants decomposition of our surface containing our simple curve and freely assign geodesic lengths to the curves in the pants decomposition as it is a free variable in Fenchel–Nielsen coordinates. However, we cannot push this hyperbolic structure down to the base surface \( \Sigma \) and instead must induct to produce a higher dimensional representation. In particular, the complexity of this process is governed by a geometric/topology quantity measured by the failure to be simple. It would be interesting to determine how geometrically the associated flat vector bundle over \( \Sigma \) coming from \( \tilde{\rho} \) singles out the curve associated to \( \gamma \).

With the above serving as motivation, we give a more careful, more algebraic construction following explicitly [53]. For ease of reference, we largely maintain the notation used by Wehrfritz.

**Wehrfritz’s Construction.** We now provide a fairly detailed account of a construction due to Wehrfritz [53] that we will make substantial use of in our proof of Theorem 1.6. Given an element \( \gamma \in F_r \), by a theorem of M. Hall [25], we can find a finite index subgroup \( \Gamma \) of \( F_r \) of index \( m_\gamma = m \) such that

\[ \Gamma = \langle \gamma \rangle * \Delta. \]
More simply put, $\gamma$ is part of a free basis for $\Gamma$. We first build a family of representation

$$\tau_p : \Gamma \rightarrow \text{GL}(2,R_p),$$

where the ring $R_p$ is described as follows. Select a free basis $\{\lambda_1, \ldots, \lambda_r\}$ for $\Delta$ and for a prime $p$, let $S_p$ be $F_p$ if $p$ is finite and $Z$ when $p = \infty$. We have the tautological representation

$$\tau_p : \Delta \rightarrow \text{GL}(2,S_p[X_j,Y_j,W_j,Z_j])$$

given by

$$\tau_p(\lambda_j) = \begin{pmatrix} X_j & Y_j \\ W_j & Z_j \end{pmatrix}.$$ 

We know that

$$\det(\lambda_j) = X_jZ_j - Y_jW_j = D_j$$

and replace $Z_j$ with

$$Z_j = X_j^{-1}(D_j + Y_jW_j)$$

and then invert both $X_j$ and $D_j$. We thus obtain

$$\tau_p : \Delta \rightarrow \text{GL}(2,S_p[X_j,Y_j,W_j,D_j,X_j^{-1},D_j^{-1}]),$$

given by

$$\tau_p(\lambda_j) = \begin{pmatrix} X_j & Y_j \\ W_j & X_j^{-1}(D_j + Y_jW_j) \end{pmatrix}.$$ 

We extend $\tau_p$ to $\Gamma$ via

$$\tau_p(\gamma) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$ 

For future reference, set

$$R_p = S_p[X_j,Y_j,W_j,D_j,X_j^{-1},D_j^{-1}].$$

The above representation $\tau_p$ on $\Gamma$ has the feature that the unipotent elements in the image are precisely the conjugates of powers of $\gamma$. In particular, one can distinguish a power of $\gamma$ from an element that is not a conjugate of a power of $\gamma$ easily via specialization of the variables. In order to distinguish the various powers of $\gamma$, we enlarge the representation by one dimension via

$$\psi_p : \Gamma \rightarrow \text{GL}(3,R_p[T,T^{-1}])$$

defined by

$$\psi_p(\gamma) = \begin{pmatrix} \tau_p(\gamma) & 0 \\ 0 & T \end{pmatrix}, \quad \psi_p(\lambda_j) = \begin{pmatrix} \tau_p(\lambda_j) & 0 \\ 0 & 1 \end{pmatrix}.$$ 

This representation distinguishes the conjugacy class of $\gamma$ via traces as it is the unique class with trace $2 + T$ as the $\ell$th power of $\gamma$ will have trace $2 + T^\ell$.

To extend $\psi_p$ to a representation of $F_r$, we select distinct coset representative $\theta_1, \ldots, \theta_m$ and observe that for each $\theta \in F_r$, there exist $\alpha_{j,\theta} \in \Gamma$ and $\sigma_\theta \in \text{Sym}(m)$ such that

$$\theta_j \theta = \alpha_{j,\theta} \theta_{\sigma_\theta(j)}.$$
We then define a representation
\[ \rho_p : F_r \rightarrow GL(m, M(3, R_p[T, T^{-1}])) \]
by
\[ (\rho_p(\theta))_{i,j} = \begin{cases} \psi_p(\alpha, \theta), & \sigma_{\theta}(i) = j \\ 0_3, & \text{otherwise} \end{cases} \]
where
\[ 0_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}. \]

Note that
\[ GL(m, M(3, R_p[T, T^{-1}])) = GL(3m, R_p[T, T^{-1}]). \]

The representation \( \rho_\infty \) is faithful and by construction permits one to distinguish the conjugacy class \([\gamma]_{F_r}\) via ideal reductions. In essence, the representation reduces the problem of distinguishing the conjugacy class \([\gamma]_{F_r}\) from \([\eta]_{F_r}\) into three cases:

(Case 1) \( \eta \) is conjugate into \( \Gamma \) but not a conjugate of a power of \( \gamma \). In this case, we can consider just the first stage two-by-two block and distinguish \([\gamma], [\eta]\) via the fact the \([\gamma]\) is unipotent and \([\eta]\) is not unipotent.

(Case 2) \( \eta \) is conjugate into \( \Gamma \) and conjugate to a power of \( \gamma \). In this case, we can use the three-by-three block and the trace, as any power that is not zero will not have the same part of the trace involving the variable \( T \).

(Case 3) \( \eta \) is not conjugate into \( \Gamma \). Then we take the full representation into \( GL(3m, R_\infty[T, T^{-1}]) \) but the focus is on the top three-by-three block, which for \( \eta \) is \( 0_3 \) by construction.

The above representation is the desired one for Theorem 1.6 and Corollary 1.7. A few additional words are in order with regard to Theorem 1.6 to see that traces can be used.

Proof of Theorem 1.6. Our goal is to prove that \( \rho_\infty(\gamma) = \rho_\infty(\eta) \) if and only if \( \gamma, \eta \) are conjugate in \( F_r \). We start first by computing the trace of \( \gamma \). By construction, our given element \( \gamma \) has characteristic polynomial under the representation \( \rho_\infty \) given by
\[ c_{\rho_\infty(\gamma)}(t) = (t - 1)^{2m}(t - T)^m \]
and trace is
\[ \text{Tr}(\rho_\infty(\gamma)) = m(2 + T). \]

In what follows, we will show that \( \text{Tr}(\rho_\infty(\gamma)) \neq \text{Tr}(\rho_\infty(\eta)) \) when \( \gamma, \eta \) are not conjugate in \( F_r \). We will split into the three cases above.

Case 1. \( \eta \) is conjugate to a power \( \gamma^n \) of \( \gamma \).
The characteristic polynomial of an element $\eta \in \Gamma$ that is conjugate to a power $\gamma^\ell \eta$ of $\gamma$ is
\[ c_{\rho_\infty(\eta)}(t) = (t - 1)^{2m}(t - T^\ell \eta)^m \]
and the trace is
\[ \text{Tr}(\rho_\infty(\eta)) = m(2 + T^\ell \eta). \]
In particular, $\text{Tr}(\rho_\infty(\gamma)) = \text{Tr}(\rho_\infty(\eta))$ if and only if $\ell \eta = 1$.

**Case 2.** $\eta$ is conjugate into $\Gamma$ but not conjugate to a power of $\gamma$.

The characteristic polynomial of an element $\eta \in \Gamma$ that is not conjugate to a power of $\gamma$ is
\[ c_{\rho_\infty(\eta)}(t) = [C_\eta(t)]^m(t - T^{\tau(\eta)})^m, \]
where $C_\eta(t)$ is the characteristic polynomial of $\gamma$ under the initial 2–dimensional representation $\tau_\infty$. Here the function $\tau$ is the projection onto the line in (co)homology generated by $\gamma$ given by the homomorphisms
\[ \Gamma \rightarrow H_1(\Gamma, \mathbb{Z}) \rightarrow \mathbb{Z}[\gamma]. \]
The trace is
\[ \text{Tr}(\rho_\infty(\eta)) = m(T^{\tau(\eta)} + \text{Tr}_2(\eta)), \]
where $\text{Tr}_2(\eta)$ is the trace under the initial 2–dimensional representation $\tau_\infty$.

**Subcase 2.1.** $\tau(\eta) \neq 1$.

If $\tau(\eta) \neq 1$, then
\[ mT \neq mT^{\tau(\eta)} . \]
Since $\text{Tr}_2(\eta)$ does not involve $T$, we must have $\text{Tr}(\rho_\infty(\gamma)) \neq \text{Tr}(\rho_\infty(\eta))$.

**Subcase 2.2.** $\tau(\eta) = 1$.

Otherwise $\tau(\eta) = 1$ and we have
\[ \text{Tr}(\rho_\infty(\eta)) = mT + m\text{Tr}_2(\eta). \]
Since $\eta$ is not conjugate to a power of $\gamma$, we know that $\tau_\infty(\eta)$ is not unipotent and thus
\[ \text{Tr}_2(\eta) \neq 2. \]
Consequently,
\[ \text{Tr}(\rho_\infty(\eta)) = mT + m\text{Tr}_2(\eta) \neq mT + 2m = \text{Tr}(\rho_\infty(\gamma)). \]
In either subcase, if $\eta \in \Gamma$ but is not conjugate to a power of $\gamma$, we have $\text{Tr}(\rho_\infty(\eta)) \neq \text{Tr}(\rho_\infty(\gamma))$.

**Case 3.** $\eta$ is not conjugate into $\Gamma$.

For this case, recall that we have a permutation $\sigma_\eta$ that describes the action of $\eta$ on the $\Gamma$–cosets. We also have
\[ \theta_j \eta = \alpha_{j, \eta} \theta_{\sigma_\eta(j)}, \]
where \( \theta_j \) are distinct \( \Gamma \)-coset representatives and \( \alpha_{j, \eta} \in \Gamma \). We will utilize these things in this case. For an element \( \eta \) that is not conjugate into \( \Gamma \), set
\[
Q_\eta = \{ i : \sigma_\eta(i) = i \}.
\]
Note that since \( \eta \notin \Gamma \), we must have \( 1 \notin Q_\eta \) and so \( |Q_\eta| < m \). For each \( i \) with \( \sigma_\eta(i) = i \), \( \rho_\infty(\eta) \) will have a three by three diagonal block with the trace of the block given by
\[
\text{Tr}_2(\alpha_{i, \eta}) + T^\tau(\alpha_{i, \eta}).
\]
In particular, we get
\[
\text{Tr}(\rho_\infty(\eta)) = \sum_{i \in Q_\eta} \left( \text{Tr}_2(\alpha_{i, \eta}) + T^\tau(\alpha_{i, \eta}) \right).
\]
Set
\[
s_{\eta, j} = |\{ i \in Q_\eta : \tau(\alpha_{i, \eta}) = j \}|
\]
and note that
\[
\sum_{j \in \mathbb{Z}} s_{\eta, j} = |Q_\eta|.
\]
In this notation, we now have
\[
\text{Tr}(\rho_\infty(\eta)) = \sum_{i \in Q_\eta} \text{Tr}_2(\alpha_{i, \eta}) + \sum_{j \in \mathbb{Z}} s_{\eta, j} T^j. \tag{1}
\]
Now, since \( |Q_\eta| < m \), we must have
\[
\sum_{j \in \mathbb{Z}} s_{\eta, j} T^j \neq m T.
\]
Finally, since \( T \) only occurs in the second sum of (1), it must be that \( \text{Tr}(\rho_\infty(\gamma)) \neq \text{Tr}(\rho_\infty(\eta)) \).

In total, we see that if \( \text{Tr}(\rho_\infty(\gamma)) = \text{Tr}(\rho_\infty(\eta)) \), then \( \gamma, \eta \) are conjugate in \( F \). In particular, \( \rho_\infty \) is the desired representation for property (B).

Note that [12] efficiently solves the word problem in \( \text{GL}(m, R) \) for the above types of rings. In particular, the degree depends only on \( m \) and \( R \), both of which are constant for a fixed \( \gamma \). For this particular case of \( R \), the exponent \( d_\gamma \) in Corollary 1.7 will be \( 9m^2 - 1 \). Patel [43] proves that we can take \( m \approx \| \gamma \| \).

When \( \| \gamma \|, \| \eta \| \leq n \), we can take \( m = n \) and thus get
\[
\text{CD}_\Gamma(\gamma, \eta) \leq C n^{C(9n^2 - 1)}.
\]
In particular, from \( \rho_\infty \), we obtain Corollary 1.7 with the specified exponents. Namely,
\[
\text{Conj}_F(n) \leq n^{9n^2 - 1}.
\]

The index \( m_\gamma \) of \( \Gamma \) absolutely depends on \( \gamma \) in our proof and there is no uniform \( m \) that works over all \( \gamma \); simplicity of the associated curve for \( \gamma \) is essential as this condition allows us to treat \( \gamma \) as a free variable with regard to the construction of the representation \( \rho_\infty \). In fact, the measurement of how far an element is from being primitive (the associated curve is simple) is likely a reasonable coarse measurement on how difficult it is to distinguish the conjugacy class \([\gamma]_F \).
The production of $\rho_{\infty}$ can be extended to surface groups. Given a conjugacy class $[\gamma]$ in $\pi_1(\Sigma_g)$ for \(g > 1\), we first pass to a finite cover where $\gamma$ lifts to a simple curve. Taking the tautological representation $\tau_2$ of the corresponding finite index subgroup $\Gamma$ into $\text{SL}(2, \mathbb{C})$, the trace of $\gamma$ is unique up to conjugation and inverses. We extend this representation to $\text{SL}(3, \mathbb{C})$ as in the geometric sketch by taking the exponential of the projection onto the line in (co)homology corresponding to $\gamma$. Here, to follow the free case more closely, the three dimensional representation is given by

$$\rho_3(\eta) = \begin{pmatrix} \tau_2(\eta) & 0 \\ 0 & t \tau(\eta) \end{pmatrix},$$

where $t$ is a free variable. Recall that $\tau: \Gamma \to \mathbb{Z}$ is the projection map onto the (co)homology line spanned by $\gamma$. Specifically, $\tau$ is given by

$$\Gamma \longrightarrow H_1(\Gamma, \mathbb{Z}) \longrightarrow \mathbb{Z}[\gamma].$$

Finally, we extend the representation to the full group $\pi_1(\Sigma_g)$ via induction of representations. The same analysis of traces carried out in the case of the free group extends identically with $t$ playing the role of $T$. Note that instead of using that $\gamma$, up to powers and conjugation, is the unique unipotent, we instead use that $|\text{Tr}(\tau_2(\gamma))|$ is minimal, up to inverses. We could have used a representation where $\gamma$ is unipotent but that is less natural geometrically.

7 Proof of Theorem 1.8

Let $\Delta$ be a finite index normal subgroup of $F_r$. Recall that we seek a faithful representation $\rho: F_r \to \text{SL}(n_\Delta, \mathbb{Z})$ and a prime $p$ such that the diagram

$$
\begin{array}{ccc}
F_r & \xrightarrow{\rho} & \text{SL}(n_\Delta, \mathbb{Z}) \\
\downarrow{\varphi_\Delta} & & \downarrow{r_p} \\
F_r/\Delta & \xrightarrow{t} & \text{SL}(n_\Delta, F_p)
\end{array}
$$

commutes, where $r_p$ is reduction modulo $p$, $\varphi_\Delta: F_r \to F_r/\Delta$ is the canonical epimorphism, and $t: F_r/\Delta \to \text{SL}(n_\Delta, F_p)$ is an inclusion. To that end, set $Q_\Delta = F_r/\Delta$. First, observe that we have a faithful representation $Q_\Delta < \text{SL}(n_\Delta, F_p)$ where $n_\Delta \leq |Q_\Delta|$. This representation exists for all $p$. Set

$$r_p: \text{SL}(n, \mathbb{Z}) \longrightarrow \text{SL}(n, F_p)$$

to be the reduction modulo $p$ homomorphism. For a free basis $x_1, \ldots, x_r$ for $F_r$, let $q_1, \ldots, q_r$ be the images of this fixed free basis under the canonical epimorphism

$$\varphi_\Delta: F_r \longrightarrow Q_\Delta.$$

For each $q_j$, we have the fiber of the map $r_p$ over $q_j$ given by

$$\{ A_{j,k} \in \text{SL}(n, \mathbb{Z}) : r_p(A_{j,k}) = q_j \}.$$
Since the map \( r_p \) is onto, each of these fibers is infinite. In addition, if \( \ell_p = |\text{SL}(n, F_p)| \), we see that for each \( A_{j,k} \) in the fiber over \( q_j \), that \( A_{j,k}^{\ell_p+1} \) is also in the fiber since \( q_j^{\ell_p+1} = q_j \). Pick elements \( A_1, \ldots, A_r \) in the fibers of \( q_1, \ldots, q_r \) with infinite order and also such that they generate a non-virtually solvable group. For the latter, note that we can conjugate or left/right multiply our choices by any elements in \( \ker r_p \) which is a finite index subgroup of \( \text{SL}(n, Z) \). In addition, if the image is virtually solvable, then it is virtually conjugate into upper triangular matrices (see \cite{6} p. 137). Now, according to \cite{15}, we can take sufficiently high powers of \( A_{\ell_p+1} \), such that the resulting group is free. It follows that we can arrange for this power to be of the form \( m\ell_p + 1 \) and so we have the faithful representation

\[
\rho: F_r \longrightarrow \text{SL}(n, Z)
\]

generated by

\[
\rho(x_j) = A_j^{m\ell_p+1}.
\]

By construction, the diagram

\[
\begin{array}{ccc}
F_r & \xrightarrow{\rho} & \text{SL}(n, Z) \\
\downarrow{\phi_\Delta} & & \downarrow{r_p} \\
F_r/\Delta & \longrightarrow & \text{SL}(n, F_p)
\end{array}
\]

commutes.

The proof of Theorem \ref{1.8} has suitable generalizations to surface groups. However, to what extent this observation can be generalized is unclear. Set \( \text{Hom}_{\infty, n}(\Gamma, \text{GL}(n, \overline{Q})) \) to be the representations \( \rho: \Gamma \rightarrow \text{GL}(n, \overline{Q}) \) such that \( \rho(\Gamma) \) is an infinite group. For \( \rho \in \text{Hom}_{\infty, n}(\Gamma, \text{GL}(n, \overline{Q})) \), there exists \( K_p/Q \) and \( S_p/\mathcal{O}_{K_p} \) such that \( \rho(\Gamma) < \text{GL}(n, S_p) \). Reducing modulo ideals \( \alpha < S_p \), we obtain homomorphisms \( \rho_\alpha: \Gamma \rightarrow \text{GL}(n, S_p/\alpha) \). Varying \( n \), \( \rho \), and \( \alpha \), we obtain a group topology \( T_{\text{rep}, \infty} \) on \( \Gamma \) generated via \( \ker \rho_\alpha \). When \( \Gamma = F_r \), we see via Theorem \ref{1.8} that this topology is the profinite topology.

**Question 3.** For a finitely generated group \( \Gamma \), when is \( T_{\text{rep}, \infty} \) the profinite topology?

Question 3 in this generality seems difficult to say the least. It is worth noting that Larsen \cite{31} does relate the growth rate of normal subgroups in a finitely generated group \( \Gamma \) with the infinite representation theory of \( \Gamma \). In particular, there is certainly a connection. The Grigorchuk group is residually finite but has no infinite linear representations due to torsion. Consequently, there are groups with a positive answer to Question 3 (free groups, surface groups) and groups with a negative answer to Question 3 (Grigorchuk group). It seems reasonable to insist the group \( \Gamma \) be (virtually) torsion free or admit at least one infinite linear representation. An affirmative answer to Question 3 for finitely generated linear groups would be a major result as we would obtain a direct connection between super-rigidity and the congruence subgroup problem for arithmetic lattices. Even for fundamental groups of hyperbolic 3–manifolds, we do not at present know the answer to Question 3. The above mentioned generalization of Theorem \ref{1.8} to surface groups provides an affirmative answer to Question 3 when \( \Gamma \) is a surface group.
References

[1] I. Agol, D. Groves, and J. F. Manning, *Residual finiteness, QCERF and fillings of hyperbolic group*, Geom. Topol. 13 (2009), 1043–1073.

[2] J. W. Anderson, *Variations on a theme of Horowitz*, Kleinian groups and hyperbolic 3-manifolds (Warwick, 2001), 307–341, London Math. Soc. Lecture Note Ser., 299, Cambridge Univ. Press, Cambridge, 2003.

[3] H. Bass, A. Lubotzky, *Automorphism of schemes and of subgroups of finite type*, Israel J. of Math. 44 (1983), 1–22.

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

[5] A. Borel, *On free subgroups of semisimple groups*, Enseign. Math. (2), 29 (1983), 151–164.

[6] A. Borel, *Linear algebraic groups*, Springer-Verlag, 1991.

[7] K. Bou-Rabee, *Quantifying residual finiteness*, J. Algebra 323 (2010), 729–737.

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

[9] K. Bou-Rabee and T. Kaletha, *Quantifying residual finiteness of arithmetic groups*, Compos. Math. 148 (2012), 907–920.

[10] K. Bou-Rabee and D. B. McReynolds, *Bertrand’s postulate and subgroup growth*, J. of Algebra 324 (2010), 793–819.

[11] K. Bou-Rabee and D. B. McReynolds, *Asymptotic growth and least common multiples in groups*, Bull. Lond. Math. Soc. 43 (2011), 1059–1068.

[12] K. Bou-Rabee and D. B. McReynolds, *Extremal behavior of divisibility functions*, [http://arxiv.org/abs/1211.4727](http://arxiv.org/abs/1211.4727), to appear in Geom. Dedicata.

[13] K. Bou-Rabee and D. B. McReynolds, *Characterizing linear groups in terms of growth properties*, in preparation.

[14] K. Bou-Rabee and B. Seward, *Arbitrarily large residual finiteness growth*, [http://arxiv.org/abs/1304.1782](http://arxiv.org/abs/1304.1782), to appear in J. Reine Angew. Math.

[15] E. Breuillard and T. Gelander, *Uniform independence in linear groups*, Invent. Math. 173 (2008), 225–263.

[16] E. Breuillard, T. Gelander, J. Souto, and P. Storm, *Dense embeddings of surface groups*, Geom. Topol. 10 (2006), 1373–1389.

[17] N. V. Buskin, *Efficient separability in free groups*, Sibirsk. Mat. Zh. 50 (2009), 765–771.

[18] K. Corlette, *Archimedean superrigidity and hyperbolic geometry*, Ann. of Math. (2) 135 (1992), 165–182.
[19] M. Dehn, Über unendliche diskontinuierliche Gruppen, Math. Ann. 71 (1911), 116–144.
[20] E. Formanek, Conjugate separability in polycyclic groups, J. Algebra 42 (1976), 1–10.
[21] D. Ginzburg and Z. Rudnick, Stable multiplicities in the length spectrum of Riemann surfaces Israel J. of Math. 104 (1998), 129–144.
[22] W. M. Goldman, Topological components of spaces of representations, Invent. Math. 93 (1988), 557–607.
[23] W. M. Goldman, Trace coordinates on Fricke spaces of some simple hyperbolic surfaces, EMS Publishing House, Zürich, 2008. Handbook of Teichmüller theory II (A. Papadopoulos, editor).
[24] M. Gromov and R. Schoen, Harmonic maps into singular spaces and p-adic superrigidity for lattices in groups of rank one, Inst. Hautes Études Sci. Publ. Math. 76 (1992), 165–246.
[25] M. Hall, Coset representations of free groups, Trans. Amer. Math. Soc. 67 (1949), 421–432.
[26] R. Horowitz, Characters of free groups represented in the two-dimensional special linear group, Comm. Pure Appl. Math. 25 (1972), 635–649.
[27] I. Kapovich, G. Levitt, P. Schupp, and V. Shpilrain, Translation equivalence in free groups, Trans. Amer. Math. Soc. 359 (2007), 1527–1546.
[28] M. Kassabov and F. Matucci, Bounding the residual finiteness of free groups, Proc. Amer. Math. Soc. 139 (2011), 2281–2286.
[29] O. Kharlampovich, A. Myasnikov, and M. Sapir, Algorithmically complex residually finite groups, http://front.math.ucdavis.edu/1204.6506
[30] G. Kuperberg, Knottedness is in NP, modulo GRH, http://front.math.ucdavis.edu/1112.0845, to appear in Adv. Math.
[31] M. Larsen, How often is \(84(g - 1)\) achieved?, Israel J. of Math., 126 (2001), 1–16.
[32] S. Lawton, Generators, relations and symmetries in pairs of \(3 \times 3\) unimodular matrices, J. Algebra 313 (2007), 782–801.
[33] D. Lee, Translation equivalent elements in free groups, J. Group Theory 9 (2006), 809–814.
[34] D. Lee, An algorithm that decides translation equivalence in a free group of rank two, J. Group Theory 10 (2007), 561–569.
[35] D. Lee and E. Ventura, Volume equivalence of subgroups of free groups, J. Algebra 324 (2010), 195–217.
[36] C. J. Leininger, Equivalent curves in surfaces, Geom. Dedicata 102 (2003), 151–177.
[37] D. D. Long and A. W. Reid, Integral points on character varieties, Math. Ann. 325 (2003), 299–321.
[38] R. C. Lyndon and P. E. Schupp, *Combinatorial group theory*, Springer–Verlag, 1977.

[39] A. I. Mal’cev, *On the faithful representation of infinite groups by matrices*, Mat. Sb. 8 (1940), 405–422.

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

[41] 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.

[42] D. A. Marcus, *Number fields*, Springer–Verlag, 1977.

[43] P. Patel, *On a Theorem of Peter Scott*, [http://front.math.ucdavis.edu/1204.5135](http://front.math.ucdavis.edu/1204.5135) to appear in Proc. Amer. Math. Soc.

[44] M. Pengitore, *Conjugacy problems on solvable groups*, in preparation.

[45] V. Platonov and A. Rapinchuk, *Algebraic groups and number theory*, Academic Press, 1994.

[46] C. Procesi, *The invariant theory of $n \times n$ matrices*, Adv. Math. 19 (1976), 306–381.

[47] M. S. Raghunathan, *Discrete subgroups of Lie groups*, Springer–Verlag, 1972.

[48] B. Randol, *The length spectrum of a Riemann surface is always of unbounded multiplicity*, Proc. Amer. Math. Soc. 78 (1980), 455–456.

[49] I. Rivin, *Geodesics with one self-intersection, and other stories*, Adv. Math. 231 (2012), 2391–2412.

[50] O. Schreier, *Die Untergruppen der freien Gruppe*, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg 5 (1927), 161–183.

[51] G. W. Schwarz, *The topology of algebraic quotients*, Birkhäuser Boston, Progr. Math. 80 (1989), 135–151.

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

[53] B. A. F. Wehrfritz, *Conjugacy separating representations of free groups*, Proc. Amer. Math. Soc. 40 (1973), 52–56.

Lawton: University of Texas-Pan American, Edinburg, TX 78539. lawtonsd@utpa.edu
Louder: University College London, London, UK, WC1E 6BT. l.louder@ucl.ac.uk
McReynolds: Purdue University, West Lafayette IN 47907. dmcreyno@math.purdue.edu