Journal of Algebra 323 (2010) 729–737

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Quantifying residual finiteness

Khalid Bou-Rabee

The University of Chicago, Department of Mathematics, 5734 S. University Avenue, Chicago, IL, United States

ARTICLE INFO

Article history:
Received 29 July 2008
Available online 10 November 2009
Communicated by Martin Liebeck

Keywords:
Quantifying residual finiteness
Free groups
Grigorchuk group
Arithmetic groups
Finitely generated nilpotent groups
Asymptotic group theory
Cebotarëv's Density Theorem

ABSTRACT

We introduce the notion of quantifying the extent to which a finitely generated group is residually finite. We investigate this behavior for examples that include free groups, the first Grigorchuk group, finitely generated nilpotent groups, and certain arithmetic groups such as $\mathrm{SL}_n(\mathbb{Z})$. In the context of finite nilpotent quotients, we find a new characterization of finitely generated nilpotent groups.

Introduction

Given a finitely generated group G, one natural question that has attracted interest is the asymptotic growth of the number of subgroups of G of index n. Indeed, the subject of subgroup growth predates the study of word growth (see Lubotzky and Segal [5, p. xvi]). In this context, the class of residually finite groups is particularly interesting as they have a rich collection of finite index subgroups. Recall that such groups have the property that the intersection of all finite index subgroups is trivial. Given this property, one might ask how quickly this intersection becomes trivial or in the same vein, how well finite quotients of G approximate G. The goal of this article is to make precise and investigate this question for several classes of residually finite groups. Before stating our main results on this, some notation is required.

For a fixed finite generating set S of G and $g \in G$, let $\|g\|_S$ denote the word length of g with respect to S. Define

$$k_G(g) := \min\{|Q|: \ Q \text{ is a finite quotient of } G \text{ where } g \neq 1\},$$

E-mail address: khalid.math@gmail.com.

0021-8693/$ – see front matter © 2009 Elsevier Inc. All rights reserved.
doi:10.1016/j.jalgebra.2009.10.008

and

$$F_G^S(n) := \max\{k_G(g)\colon \|g\|_S \leqslant n\}.$$

The objective of this paper is to study the asymptotic properties of F_G^S and one of its variants.

Throughout the paper, we write $f_1 \preccurlyeq f_2$ to mean that there exists a C such that $f_1(n) \leqslant Cf_2(Cn)$ for all n, and we write $f_1 \simeq f_2$ to mean $f_1 \preccurlyeq f_2$ and $f_2 \preccurlyeq f_1$. The dependence of F_G on the generating set is mild, a fact that we will see in Section 1. Consequently, we will suppress the dependence of F_G on S for the remainder of the introduction. In that same section, we will also provide some general facts on the behavior of F_G under group extensions, passage to subgroups, and taking direct products.

Our first main result establishes the polynomial growth of F_G for certain arithmetic lattices – see Section 2 for the definition of $\mathcal{O}_L$.

Theorem 0.1. *Let L be a finite extension of $\mathbb{Q}$. If $k \geqslant 2$, then $F_{\mathrm{SL}_k(\mathcal{O}_L)}(n) \preccurlyeq n^{k^2-1}$. Moreover, if $k > 2$, then $F_{\mathrm{SL}_k(\mathcal{O}_L)}(n) \succcurlyeq n$.*

Notice that the asymptotic upper bound for F_G depends only on the dimension of the algebraic group $\mathrm{SL}_n(\mathbb{C})$ and not on the field L. Further, since $\mathbb{Z} * \mathbb{Z} \leqslant \mathrm{SL}_2(\mathbb{Z})$, we have, as a consequence of Theorem 0.1 and Lemma 1.1, that $F_F(n) \preccurlyeq n^3$ for any finitely generated non-abelian free group F. The author, unfortunately, does not know of a sharper upper bound for the growth of $F_F(n)$.

There are examples of groups with sub-polynomial and super-polynomial F_G growth. Let the *Hirsch number* of G, denoted $h(G)$, be the number of infinite cyclic factors in a series for G with cyclic or finite factors. In Section 3 we find a general bound for nilpotent groups of a given Hirsch number:

Theorem 0.2. *Let P be a finitely generated nilpotent group. Then $F_P(n) \preccurlyeq \log(n)^{h(P)}$.*

In Section 4, we present some calculations that show that the first Grigorchuk group has exponential F_G growth.

In the last section we restrict our attention to finite nilpotent quotients and the asymptotic growth of the associated function for these quotients. To be precise, let

$$k_G^{nil}(g) = \min\{|Q|\colon\ Q \text{ is a finite nilpotent quotient of } G \text{ where } g \neq 1\}$$

and

$$F_G^{nil}(n) = \max\{k_G^{nil}(g)\colon \|g\| \leqslant n\}.$$

Then we get the following characterization of finitely generated nilpotent groups in Section 5.

Theorem 0.3. *Let G be any finitely generated group. Then $F_G^{nil}(n)$ has growth which is polynomial in $\log(n)$ if and only if G is nilpotent.*

The ingredients used in the proofs of the above theorems include the prime number theorem, Cebotarëv's Density Theorem, the Strong Approximation Theorem, the congruence subgroup property of $\mathrm{SL}_k(\mathbb{Z})$ for $k > 2$, and Mal'cev's representation theorem for nilpotent groups.

1. Basic theory

In this first section, we lay out some basic lemmas for the sequel. Recall that a group G is *residually finite* if for any nontrivial g in G there exists a finite group Q and a homomorphism $\psi : G \to Q$ such that $g \notin \ker \psi$. We begin with a lemma that when applied twice with $G = H$, will let us drop the decoration S in $F_G^S(n)$.

Lemma 1.1. *Let G and $H \leqslant G$ be residually finite groups finitely generated by S and L respectively. Then $F_H^L(n) \preccurlyeq F_G^S(n)$.*

Proof. As any homomorphism of G to Q restricts to a homomorphism of H to Q, it follows that $k_H(h) \leqslant k_G(h)$ for all $h \in H$. Hence,

$$F_H^L(n) = \sup\{k_H(g)\colon \|g\|_L \leqslant n\} \leqslant \sup\{k_G(g)\colon \|g\|_L \leqslant n\}. \tag{1}$$

Further, there exists a $C > 0$ such that any element in L can be written in terms of at most C elements of S. Thus,

$$\{h \in H\colon \|h\|_L \leqslant n\} \subseteq \{g \in G\colon \|g\|_S \leqslant Cn\}. \tag{2}$$

So by (1) and (2), we have that

$$F_H^L(n) \leqslant \sup\{k_G(g)\colon \|g\|_L \leqslant n\} \leqslant \sup\{k_G(g)\colon \|g\|_S \leqslant Cn\} = F_G^S(Cn),$$

as desired. □

The previous lemma implies that the growth functions for all non-abelian finitely generated free groups are equivalent. The next lemma shows that F_G is well behaved under direct products. We leave the proof as an exercise to the reader, as it is straightforward.

Lemma 1.2. *Let G and H be residually finite groups generated by finite sets S and T respectively. Then*

$$\max\{F_G^S(n), F_H^T(n)\} = F_{G\times H}^J(n),$$

where $J = S \times T$.

The next lemma shows that growth under finite group extensions is moderately well-behaved. We leave the proof as an exercise to the reader, as it is also straightforward.

Lemma 1.3. *Let $H \leqslant G$ be two finitely generated groups with $[G : H] < \infty$. Then $F_G(n) \preccurlyeq (F_H(n))^{[G:H]}$.*

2. Arithmetic groups

In order to quantify residual finiteness for arithmetic groups, we require some auxiliary results concerning the ring analogue of growth for rings of algebraic integers $\mathcal{O}_L$.

2.1. The integers

Fix the generating set {1} for the integers $\mathbb{Z}$. For $\mathbb{Z}$ we can do much better than the obvious bound $F_{\mathbb{Z}}(n) \leqslant n+1$. In fact, the elements with the largest value of $k_{\mathbb{Z}}$ are of the form $\psi(r) := lcm(1, \ldots, r)$.

Lemma 2.1. *If $l_1 < \psi(m) < l_2 < \psi(m+1)$, then $k_{\mathbb{Z}}(\psi(m))$ is greater than or equal to $k_{\mathbb{Z}}(l_1)$ and $k_{\mathbb{Z}}(l_2)$.*

Proof. We prove this by induction on m. The base case with $\psi(2) = 2$ and $\psi(3) = 6$ are easily checked. For the inductive step, suppose the statement is true for $m < n$, and let $l_1 < \psi(m+1) < l_2 < \psi(m+2)$. By the inductive hypothesis, and the fact that $k_{\mathbb{Z}}(\psi(\cdot))$ is nondecreasing, we deduce that $k_{\mathbb{Z}}(\psi(m+1)) \geqslant k_{\mathbb{Z}}(l_1)$. In order for $k_{\mathbb{Z}}(\psi(m+1)) < k_{\mathbb{Z}}(l_2)$ we must have that l_2 satisfies $j|l_2$ for all $j = 1, \ldots, m+2$. Thus l_2 is a multiple of $1, \ldots, m+2$ and thus $l_2 \geqslant \psi(m+2)$, which is absurd. □

The function $\psi(x)$ is well-studied, as the asymptotic behavior of ψ is used to prove the prime number theorem in analytic number theory. In fact (see Proposition 2.1, p. 189, in Stein and Shakarchi [8]),

$$\lim_{x\to\infty} \frac{\log(\psi(x))}{x} = 1. \tag{3}$$

Since Lemma 2.1 shows that $F_{\mathbb{Z}}$ and ψ are related, it is no surprise that (3) is used to prove the following theorem.

Theorem 2.2. *We have $F_{\mathbb{Z}}(n) \simeq \log(n)$.*

Proof. Lemma 2.1 gives

$$\frac{F_{\mathbb{Z}}(n)}{\log(n)} = \frac{k_{\mathbb{Z}}(\psi(k_n))}{\log(n)},$$

where k_n is the maximum value of m with $\psi(m) \leqslant n$. Since log is increasing we have

$$\frac{k_{\mathbb{Z}}(\psi(k_n))}{\log(\psi(k_n+1))} \leqslant \frac{k_{\mathbb{Z}}(\psi(k_n))}{\log(n)} \leqslant \frac{k_{\mathbb{Z}}(\psi(k_n))}{\log(\psi(k_n))}. \tag{4}$$

The left-hand side of (4) with $k_{\mathbb{Z}}(\psi(k_n)) \geqslant k_n + 1$ and (3) gives

$$\lim_{n\to\infty} \frac{k_{\mathbb{Z}}(\psi(k_n))}{\log(n)} \geqslant 1.$$

The right-hand side of (4) with $k_{\mathbb{Z}}(\psi(k_n)) \leqslant 2k_n$ and (3) gives

$$\lim_{n\to\infty} \frac{k_{\mathbb{Z}}(\psi(k_n))}{\log(n)} \leqslant 2.$$

Thus $F_{\mathbb{Z}}(n) \simeq \log(n)$ as desired. □

Corollary 2.3. *We have $F_{\mathbb{Z}^d}(n) \simeq \log(n)$.*

Proof. This follows immediately from Lemma 1.2 and Theorem 2.2. □

2.2. Rings of integers

Let $L/\mathbb{Q}$ be a finite extension, and let $\mathcal{O}_L$ be the ring of integers. With these conditions and some work, it can be shown that $\mathcal{O}_L$ is a residually finite ring and a finitely generated abelian group. We need to define $F_{\mathcal{O}_L}$ while keeping the ring structure of $\mathcal{O}_L$ in mind, because $\mathrm{SL}_n(-)$ is a functor from the category of rings to the category of groups. Equip $\mathcal{O}_L$ with a word metric as a finitely generated abelian group and define

$$k_{\mathcal{O}_L}(g) := \min\bigl\{|Q|\colon\ \psi(g) \neq 1,\ \psi : \mathcal{O}_L \to Q\bigr\},$$

where the maps ψ are ring homomorphisms, and

$$F_{\mathcal{O}_L}(n) := \max\bigl\{k_{\mathcal{O}_L}(g)\colon\ \|g\| \leqslant n\bigr\}.$$

The obvious analogue of Lemma 1.1 holds for $F_{\mathcal{O}_L}(n)$.

To study the asymptotic behavior of $F_{\mathcal{O}_L}(n)$, we need some algebraic number theory. If $\mathfrak{p}$ is a prime ideal of $\mathbb{Z}$, then $\mathfrak{p}\mathcal{O}_L$ is an ideal of $\mathcal{O}_L$ and has factorization

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_c^{e_c},$$

where $\mathfrak{p}_i$ are distinct. Let $f_{\mathfrak{p}_i}$ be the degree of the field extension $[\mathcal{O}_L/\mathfrak{p}_i : \mathbb{Z}/\mathfrak{p}]$. If $e_i = 1$ and $f_{\mathfrak{p}_i} = 1$ for all i, we say that $\mathfrak{p}$ *splits* in $\mathcal{O}_L$. In the case where $\mathfrak{p} = (p)$ where p is a prime number in $\mathbb{Z}$, we have that $\mathfrak{p}$ splits only if each prime $\mathfrak{p}_i$ that appears in the factorization satisfies $\mathcal{O}_L/\mathfrak{p}_i = p$. Thus, the primes (p) that split are nice in that they then give small quotients for $\mathcal{O}_L$. These nice primes appear quite often. Indeed, the Cebotarëv Density Theorem (see Theorem 11, p. 414 in Lubotzky and Segal [5]) implies that the natural density of such primes is nonzero in the set of all primes. This implication, along with the prime number theorem, implies the following result:

Lemma 2.4. *There exists a constant $C > 0$ such that for any n large enough, there exists a prime q such that $n \leqslant q \leqslant Cn$ and (q) splits over $\mathcal{O}_L$.*

Proof. Let δ be the natural density of all the primes ideals in $\mathbb{Z}$ that split over $\mathcal{O}_L$. Then Cebotarëv's Density Theorem implies that δ is nonzero. Choose a real number $C > 1/\delta$. We claim that for any n large enough, there must exist a prime p such that (p) splits over $\mathcal{O}_L$ and $n \leqslant p \leqslant Cn$. Otherwise, the prime number theorem gives, for n large enough,

$$\delta \leqslant \frac{n/\log(n)}{(Cn)/\log(Cn)},$$

which, as $n \to \infty$, gives $\delta \leqslant 1/C$, an impossibility. □

This lemma will play a key role in the proof of the upper bound in the next theorem.

Theorem 2.5. *We have $F_{\mathcal{O}_L}(n) \simeq \log(n)$.*

Proof. The lower bound, $F_{\mathcal{O}_L}(n) \succcurlyeq \log(n)$, follows from Lemma 1.1 for rings and Theorem 2.2.

For the upper bound, the main idea is that we will first use the bound for $\mathbb{Z}$ to ensure that one of the coordinates in an integral basis for $\mathcal{O}_L$ will not vanish in a small quotient, then we will use Lemma 2.4 find an even smaller quotient where the element does not vanish. Let $S = \{b_1, \ldots, b_k\}$ be an integral basis for $\mathcal{O}_L$, and fix a nontrivial g in $\mathcal{O}_L$ with $\|g\|_S = n$. Then $g = \sum_{i=1}^n a_i b_i$ where $a_i \in \mathbb{Z}$ and $|a_i| \leqslant n$. Since $g \neq 0$ there exists k such that $a_k \neq 0$. Furthermore, by the proof of Theorem 2.2, and for n large enough, there exists a prime $p \in \mathbb{Z}$ such that $p \leqslant 2\log(n)$ and $a_k \neq 0 \bmod q$ for all primes $q \geqslant p$. We may further assume that all primes are sufficiently large so that Lemma 2.4 holds. And so by Lemma 2.4, there exists a $C > 0$, which does not depend on n, and a prime q such that $p \leqslant q \leqslant \frac{C}{2} p$ such that (q) splits over $\mathcal{O}_L$. Hence, we have that $(q) = \mathfrak{q}_1 \cdots \mathfrak{q}_c$ with $|\mathcal{O}_L/\mathfrak{q}_i| = q$. Further, since q does not divide a_k and since the integral basis S gets sent to a basis in $\mathcal{O}_L/(q)$, we have that $g \neq 1$ in $\mathcal{O}_L/(q)$. Hence, there exists one $\mathfrak{q}_i$ with $g \neq 1$ in $\mathcal{O}_L/\mathfrak{q}_i$. As the cardinality of $\mathcal{O}_L/\mathfrak{q}_i$ is equal to q which is no greater than $C \log(n)$, we have the desired upper bound. □

2.3. Proof of Theorem 0.1

Let $L/\mathbb{Q}$ be a finite extension, and let $\mathcal{O}_L$ be the ring of integers. With the results of the previous section, we can now obtain results for $\mathrm{SL}_k(\mathcal{O}_L)$. Note that $\mathrm{SL}_k(\mathcal{O}_L)$ is finitely generated, but this fact is highly nontrivial (see Platonov and Rapinchuk [9, Chapter 4]). For $A \in \mathrm{SL}_k(\mathcal{O}_L)$, let $\|A\|_2 = \max\{\|Ax\|/\|x\|\colon\ x \in \mathbb{R}^k - \{0\}\}$ be the L^2 operator norm of A.

Theorem 2.6. *If $k \geqslant 2$, we have $F_{\mathrm{SL}_k(\mathcal{O}_L)}(n) \preccurlyeq n^{k^2-1}$.*

Proof. The strategy in this proof is to bound the entries of a word of length n in $\mathrm{SL}_k(\mathcal{O}_L)$ and then to use this bound to approximate the group using the $F_{\mathcal{O}_{\mathbb{L}}}$ result. Let $A_1, \ldots, A_r$ be generators for $\mathrm{SL}_k(\mathcal{O}_L)$. Let $g \in \mathrm{SL}_n(\mathcal{O}_L)$ be a nontrivial element with word length less than or equal to n. The basic properties of $\|\cdot\|_2$ give that $\|g\|_2 \leqslant (\sqrt{\lambda})^n$ where λ is the absolute value of the largest eigenvalue of any of the $A_i A_i^T$, where $i = 1, \ldots, r$. Since $g \neq 1$ and $\|g\|_2 \leqslant (\sqrt{\lambda})^n$ we may find an off-diagonal nonzero entry, $a \neq 0$, or a diagonal entry $a \neq 1$ of the matrix g that is no greater than $(\sqrt{\lambda})^n$. For simplicity we assume that a is an off-diagonal entry, a similar argument to what we will give works otherwise. Since a is in $\mathcal{O}_L$, Theorem 2.5 gives a $D > 0$, depending only on L, and a ring homomorphism $\psi : \mathcal{O}_L \to \mathbb{Z}/d\mathbb{Z}$ where $d < D(\log((\sqrt{\lambda})^n))$ such that $a \notin \ker\psi$. The function ψ induces a map $\psi' : \mathrm{SL}_k(\mathcal{O}_L) \to \mathrm{SL}_k(\mathbb{Z}/d\mathbb{Z})$ where $g \notin \ker\psi'$. By our bound for d we have

$$d^{k^2-1} \leqslant D^{k^2-1}\bigl(\log\bigl((\sqrt{\lambda})^n\bigr)\bigr)^{k^2-1} \leqslant D^{k^2-1}\bigl(\log(\sqrt{\lambda})\bigr)^{k^2-1} n^{k^2-1},$$

giving $F_{\mathrm{SL}_k(\mathcal{O}_L)}(n) \preccurlyeq n^{k^2-1}$ as asserted. □

For the next theorem we need to introduce some definitions concerning certain subgroups of $\mathrm{SL}_k(\mathbb{Z}/n\mathbb{Z})$. A normal subgroup of $\mathrm{SL}_k(\mathbb{Z}/n\mathbb{Z})$ is said to be a *principal congruence subgroup* if it is the kernel of some map $\varphi : \mathrm{SL}_k(\mathbb{Z}/n\mathbb{Z}) \to \mathrm{SL}_k(\mathbb{Z}/d\mathbb{Z})$ induced from the natural ring homomorphism $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$, where d properly divides n. A subgroup in $\mathrm{SL}_k(\mathbb{Z}/n\mathbb{Z})$ which contains some principal congruence subgroup is said to be a *congruence subgroup*. A subgroup in $\mathrm{SL}_k(\mathbb{Z}/n\mathbb{Z})$ which does not contain any principal congruence subgroups is said to be *essential*.

Theorem 2.7. *If $k > 2$, then $F_{\mathrm{SL}_k(\mathcal{O}_L)}(n) \succcurlyeq n$.*

Proof. We first pick a candidate for the lower bound. By Lubotzky, Mozes and Raghunathan [4, Theorem A], there exists a finite generating set, S, for $\mathrm{SL}_k(\mathbb{Z})$ (see also Riley [6]) and a $C > 0$ satisfying

$$\|-\|_S \leqslant C \log\bigl(\|-\|_1\bigr),$$

where $\|-\|_1$ is the 1-operator norm for matrices. Thus, as $\log(\|E_{ij}(\psi(n))\|_1) \simeq \log(\psi(n)) \simeq n$, the elementary matrix $E_{ij}(\psi(n))$ may be written in terms of at most Cn elements from S. This elementary matrix is our candidate.

Now we show that our candidate, $E_{ij}(\psi(n))$, takes on the lower bound. Suppose that Q is the finite quotient with the smallest cardinality such that $E_{ij}(\psi(n))$ does not vanish. Since $\mathrm{SL}_k(\mathbb{Z})$ has the congruence subgroup property (see Bass, Lazard and Serre [10]), then for the map $\delta : \mathrm{SL}_k(\mathbb{Z}) \to Q$, we have an integer d such that the following diagram commutes.

$$\begin{tikzcd}
\mathrm{SL}_k(\mathbb{Z}) \arrow[r, "\delta"] \arrow[dr] & Q \\
 & \mathrm{SL}_k(\mathbb{Z}/d\mathbb{Z}). \arrow[u]
\end{tikzcd}$$

Hence, by our choice of $E_{ij}(\psi(n))$, we have that $Q = \mathrm{SL}_k(\mathbb{Z}/d\mathbb{Z})/N$ where $d \geqslant n$. In the case where N is a principal congruence subgroup, we see that the smallest finite quotient of $\mathrm{SL}_k(\mathbb{Z})$ where $E_{ij}(\psi(n))$ is nontrivial has size greater than $|\mathrm{SL}_k(\mathbb{Z}/n\mathbb{Z})| \succcurlyeq n$. If N is a congruence group, then taking the quotient by the largest principal congruence group N contains reduces to the case of N being an essential group. Then by Proposition 6.1.1 in Lubotzky and Segal [5], we have that there exists a $c > 0$, depending only on k, such that $|Q| \geqslant cn$. Since $\mathrm{SL}_k(\mathbb{Z})$ is contained in $\mathrm{SL}_k(\mathcal{O}_L)$, Lemma 1.1 gives the claim. □

3. Proof of Theorem 0.2

In the proof of Theorem 0.2, we require the following lemma.

Lemma 3.1. *Let U be the group of $d \times d$ integral upper triangular unipotent matrices. If $G \leqslant U$, then $F_G(n) \leqslant C\log(n)^{h(G)}$, where C does not depend on n.*

Proof. It is easy to see that entries of matrices of word length n in G are bounded by Cn^r for some fixed r. Take $g \in G$. Then Theorem 2.2 gives some $D > 0$, which does not depend on n, such that $p \leqslant D\log(n)$ and the natural map $\psi : U \to U_p$ has $g \notin \ker\psi$, where U_p is the image of U in $\mathrm{GL}_d(\mathbb{Z}/p\mathbb{Z})$ consisting of unipotent upper triangular matrices. So long as p is greater than d, we have that U_p has exponent p. Thus $|G| \leqslant p^{h(G)}$, giving $|G| \leqslant D^{h(G)}\log(n)^{h(G)}$. Setting $C = D^{h(G)}$ finishes the proof. □

In the following proof we will reduce the general case to the case in the previous lemma.

Proof of Theorem 0.2. To start, we may assume, without loss of generality, that G is a torsion-free, finitely generated nilpotent group. By Mal'cev's Theorem (see Segal [7, Chapter 5, §B, Theorem 2], or Hall [3, Theorem 7.5, p. 56]) there exists a canonical injective homomorphism $\beta_N : G \to U$, where U is a group of $d \times d$ integral upper triangular unipotent matrices. Hence, the bound given by Lemma 3.1 finishes the proof. □

4. The first Grigorchuk group

Let T be the collection of finite sequences of 1s and 0s of length $n \geqslant 0$. We will be interested in the automorphisms of T defined inductively by:

$$\begin{aligned}
a(\xi_1, \dots, \xi_n) &= (\overline{\xi_1}, \xi_2, \dots, \xi_n), \\
b(0, \xi_1, \dots, \xi_n) &= (0, \overline{\xi_1}, \dots, \xi_n), \\
b(1, \xi_1, \dots, \xi_n) &= \bigl(1, c(\xi_1, \dots, \xi_n)\bigr), \\
c(0, \xi_1, \dots, \xi_n) &= (0, \overline{\xi_1}, \dots, \xi_n), \\
c(1, \xi_1, \dots, \xi_n) &= \bigl(1, d(\xi_1, \dots, \xi_n)\bigr), \\
d(0, \xi_1, \dots, \xi_n) &= (0, \xi_1, \dots, \xi_n), \\
d(1, \xi_1, \dots, \xi_n) &= \bigl(1, b(\xi_1, \dots, \xi_n)\bigr),
\end{aligned}$$

where $\bar{1} = 0$ and $\bar{0} = 1$. Let the *first Grigorchuk Group* be $\Gamma := \langle a, b, c, d\rangle$ as in Grigorchuk [1] (see also de la Harpe [2, Chapter VIII]). In the case when $g \in \mathrm{Aut}(T)$ fixes the first k entries of any element in T, we will write $g = (\gamma_1, \ldots, \gamma_{2^k})_k$ in order to record the action beyond level k only. In this case, we say that g has *level* k. For example, $b = (a, c)_1$, $c = (a, d)_1$, and $d = (1, b)_1$ all have level 1.

Let $T(k)$ be the collection of sequences of length at most k. The truncation $T \to T(k)$ induces a map $\psi_k : \Gamma \to \mathrm{Aut}(T(k))$; a *principal congruence subgroup* is equal to $\ker \psi_k$ for some k. Let Γ_k be the image of ψ_k in $\mathrm{Aut}(T(k))$. We borrow from de la Harpe [2, p. 238]:

Lemma 4.1. *For $k \geqslant 3$, $|\Gamma_k| = 2^{5\cdot 2^{k-3}+2}$.*

Theorem 4.2. *We have $F_\Gamma(n) \preccurlyeq 2^n$.*

Proof. Let g be an element of word length $\leqslant n$. We will show that there exists a $C > 0$, not depending on g, such that $k_\Gamma(g) \leqslant C2^n$. To this end, we claim that there exists $k \leqslant \log(n)$ such that at level k there is an odd number of a symbols appearing in some coordinate of g. Hence $\psi_k(g) \neq 1$. Suppose g is in reduced word form. Then the relations $cb = bc = d$ and $dc = cd = b$ give that g must be in a form conjugate to $g = ae_1ae_2a \cdots e_kr$ where $e_i \in \{b, c, d, b^{-1}, c^{-1}, d^{-1}\}$ and $r \in \{1, a\}$. If $r = a$, then we are done, as $\psi_1(g) \neq 1$. Otherwise, we see that the number of the symbols describing g on some coordinate of level 2 is nonzero and no greater than $(|g| + 1)/2$. And so, by induction, the number of symbols describing g on some coordinate of level $k + 1$ is nonzero and no greater than $(((|g| + 1)/2 + 1)/2 + \cdots + 1)/2 = |g|2^{-k} + 2^{-1} + 2^{-2} + \cdots + 2^{-k} = 2^{-k}|g| + (1 - 2^{-k})$. Hence, we see that there is some k with $2^{-k}|g| \geqslant 1$, such that some coordinate of level $k + 1$ has an odd number of a symbols. And so $\psi_{k+2}(g) \neq 1$ where $|g| \geqslant 2^k$, giving some $C > 0$ such that $k_\Gamma(g) \leqslant C2^n$ by Lemma 4.1. □

Lemma 4.3. *There exists a $C > 0$ such that the element $(1, \ldots, 1, (ab)^2)_k$ is in Γ and has word length less than $C2^k$.*

Proof. We will prove this by induction on k. For the base case, observe that

$$(ab)_0^2 d^{-1} (ab)_0^{-2} d = (abad)_0^2 = (c, a)_1 (1, b)_1 (c, a)_1 (1, b)_1 = \bigl(1, (ab)^2\bigr)_1.$$

For the inductive step, let $g_k = (1, 1, \ldots, 1, (ab)^2)_k$. Then conjugating g_k by one of b, c or d yields $(1, 1, \ldots, 1, (ab)^2)_{k+1}$. □

Theorem 4.4. *We have $F_\Gamma(n) \succcurlyeq 2^n$.*

Proof. By Lemma 4.3 there exists a nontrivial element $g \in \Gamma$ of word length no greater than $C2^n$ such that any $k < n$ has $\psi_k(g) = 1$. Let N be the normal subgroup of Γ of smallest index such that $g \notin N$. If any element in N has level k, then by the proof of Theorem 42 on p. 239 in de la Harpe [2], N must contain $\ker \psi_{k+6}$. Hence, as $g \notin N$, the normal subgroup N must act trivially on the first $n - 6$ levels of the rooted binary tree. Thus, N is contained in $\ker \psi_{n-6}$ and so has index greater than or equal to $2^{5\cdot 2^{n-9}+2}$ when $n \geqslant 9$, by Lemma 4.1, giving the desired lower bound. □

5. Proof of Theorem 0.3

Theorem 0.3 follows from Lemma 5.1, below, and Theorem 0.2.

Lemma 5.1. *If G is a finitely generated group that is not nilpotent, then $n \preccurlyeq F_G^{nil}(n)$.*

Proof. Let S be a finite set of generators for G. It suffices to show that there exists a $C > 0$ such that for any n, there exists g with $\|g\|_S \leqslant C2^n$ and $k_G^{nil}(g) \geqslant 2^n$. Fix $n > 0$, then since G is not nilpotent, $\Gamma_n(G) \neq 1$. Recall that $\Gamma_n(G)$ is normally generated by elements of the form $[a_1, \ldots, a_n]$ where $a_i \in S$ or $a_i^{-1} \in S$ for every i. Since $\Gamma_n(G) \neq 1$, there exists some element $[a_1, \ldots, a_n]$ as above that is nontrivial. Hence, there exists some g with $\|g\|_S \leqslant C2^n$ with $g \in \Gamma_n(G)$. Any finite nilpotent quotient Q where $g \neq 1$ must be nilpotent of class $n + 1$ or more giving $|Q| \geqslant 2^n$. Thus $k_G^{nil}(g) \geqslant 2^n$, as desired. □

Acknowledgments

I would like to extend special thanks to my advisor, Benson Farb for suggesting this topic, providing encouragement, sound advice, good teaching, and many good ideas. I am also especially grateful to my coadvisor, Ben McReynolds, for his time, good ideas, and comments on the paper. I would also like to acknowledge Tom Church, Matt Day, Asaf Hadari, Justin Malestein, Aaron Marcus, Shmuel Weinberger, and Thomas Zamojski for reading early drafts of this paper and for stimulating conversations on this work. Finally, it is my pleasure to thank the excellent referee for making comments, suggestions, and a number of corrections on an earlier draft of this paper.

References

[1] R.I. Grigorchuk, Burnside's problem on periodic groups, Funct. Anal. Appl. 14 (1980) 41–43.
[2] P. de La Harpe, Topics in Geometric Group Theory, Chicago Lectures in Math., Chicago, 2000.
[3] P. Hall, The Edmonton notes on nilpotent groups, in: Queen Mary College Mathematics Notes, Mathematics Department, Queen Mary College, London, 1969.
[4] A. Lubotzky, Sh. Mozes, M.S. Raghunathan, The word and Riemannian metrics on lattices of semisimple groups, Publ. Math. Inst. Hautes Etudes Sci. 91 (2000) 5–53.
[5] A. Lubotzky, D. Segal, Subgroup Growth, Progr. Math., vol. 212, Birkhäuser Verlag, Basel, 2003.
[6] T.R. Riley, Navigating in the Cayley graphs of $\mathrm{SL}_N(\mathbb{Z})$ and $\mathrm{SL}_N(\mathbb{F}_p)$, Geom. Dedicata 113 (2005).
[7] D. Segal, Polycyclic Groups, Cambridge Tracts in Math., vol. 82, Cambridge University Press, 1983.
[8] E.M. Stein, R. Shakarchi, Complex analysis, in: Princeton Lectures in Analysis, II, Princeton University Press, Princeton, NJ, 2003.
[9] V.P. Platonov, A.S. Rapinchuk, Algebraic Groups and Number Theory, Pure Appl. Math., vol. 139, Academic Press, Boston, MA, 1994, translated from the 1991 Russian original by Rachel Rowen.
[10] H. Bass, M. Lazard, J.-P. Serre, Sous-groupes d'indice fini dans $\mathrm{SL}(n, \mathbb{Z})$, Bull. Amer. Math. Soc. (N.S.) 70 (1964) 385–392.