Approximating a group by its solvable quotients

Khalid Bou-Rabee

ABSTRACT. The solvable residual finiteness growth of a group quantifies how well the group is approximated by its finite solvable quotients. In this note we present a new characterization of polycyclic groups which are virtually nilpotent. That is, we show that a group has solvable residual finiteness growth which is at most polynomial in $\log(n)$ if and only if the group is polycyclic and virtually nilpotent. We also give new results concerning approximating oriented surface groups by nilpotent quotients. As a consequence of this, we prove that a natural number C exists so that any nontrivial element of the Ckth term of the lower central series of a finitely generated oriented surface group must have word length at least k. Here C depends only on the choice of generating set. Finally, we give some results giving new lower bounds for the solvable residual finiteness growth of some metabelian groups (including the Lamplighter groups).

CONTENTS

Introduction

Let $B_{\Gamma,\mathcal{X}}(n)$ denote the metric ball of radius n in a group Γ generated by a finite set $\mathcal{X}$ with respect to the word metric $\| \cdot \|_{\Gamma,\mathcal{X}}$. In this article we study the following question:

Question 1. *Let P be a property of groups. How large a finite group with property P do we need to detect elements in $B_{\Gamma,\mathcal{X}}(n)$? That is, what is the smallest integer $\mathrm{F}_{\Gamma,X}^{P}(n)$ such that each nontrivial element in $B_{\Gamma,X}(n)$ survives through some homomorphism to a group with property P of cardinality no greater than $\mathrm{F}_{\Gamma,X}^{P}(n)$?*

We will be focusing on two properties: nilpotent ($P = \text{nil}$) and solvable ($P = \text{sol}$). The asymptotic growth of F_{Γ}^{sol} is called the *solvable residual finiteness growth* of Γ, while the asymptotic growth of F_{Γ}^{nil} is called the *nilpotent residual finiteness growth*. When the property P is relaxed, we use the notation F_{Γ} and call the growth the *normal residual finiteness growth*.

It is known that any virtually nilpotent group has normal residual finiteness growth which is at most polynomial in $\log(n)$ [B10]. Further, any finitely generated linear group with normal residual finiteness growth which is polynomial in $\log(n)$ is virtually nilpotent [BM1]. The author has been unable to find any group that is not virtually nilpotent with such growth. Hence, this has lead the author to believe that there may be a positive answer to the following question.

Question 2. *Is it true that if a group Γ has normal residual finiteness growth which is at most polynomial in $\log(n)$, then Γ is virtually nilpotent?*

Our first result is the following, which resolves the question for a large class of groups. Our proof builds off of the methods in [BM1] (cf. Theorem 1.1 in that paper).

Theorem 1. *If Γ has a finite-index subgroup that is residually solvable and finitely generated then the following are equivalent:*

- *Γ has normal residual finiteness growth which is at most polynomial in $\log(n)$.*
- *Γ is virtually nilpotent.*

We also record the following result, which resolves the question for solvable groups, while providing a new characterization of solvable groups which are virtually nilpotent. Loosely speaking, the result shows that, except in the "obvious" cases, there is a new universal lower bound on the difficulty of detecting elements in finite solvable quotients.

Theorem 2. *Let Γ be finitely generated. Then the following are equivalent:*

- *Γ has solvable residual finiteness growth that is polynomial in $\log(n)$.*
- *Γ is solvable and virtually nilpotent.*

The proofs of Theorems 1 and 2 are in Section 2. In our proofs we use in an essential way the results of J. S. Wilson [Wi05].

On the other end of the growth spectrum, the first Grigorchuk group is known to have solvable, normal, and nilpotent residual finiteness growth which is exponential [B10]. Our next main result, proved in Section 3, shows that the fundamental group of an oriented surface has super-polynomial, but not super-exponential, nilpotent residual finiteness growth. The proof of the upper bound relies on the structure theory of the group $\mathrm{PSL}_2(\mathbb{Z}[i])$, while the lower bound uses a construction due to B. Bandman, G-M Greuel, F. Grunewald, B. Kunyavskiĭ, G. Pfsiter, and E. Plotkin [B06].

Theorem 3. *Let Γ be the fundamental group of an oriented surface. Then*
$$2^n \succeq \mathrm{F}_\Gamma^{\mathrm{nil}}(n) \succeq 2^{\sqrt{n}}.$$

From this theorem, we obtain the following corollary (proved in Section 3). Variants of the following corollary for free groups have been shown using different methods (cf. Theorem 1.2 in [MP]).

Corollary 4. *Let Γ be the fundamental group of an oriented surface with generating set $\mathcal{X}$. Then there exists a constant $C > 0$ such that any nontrivial $\gamma \in \Gamma$ satisfies $\gamma \notin \Gamma_{C\|\gamma\|_{\mathcal{X}}}$.*

We conclude, in Section 4, by showing new lower bounds for the normal residual finiteness growth for some wreath products of abelian groups (the Lamplighter groups). The proofs give explicit constructions of elements in $B_{\Gamma,\mathcal{X}}(n)$ that are not well-approximated by finite solvable quotients. These results suggest that a gap might exist for the normal residual finiteness growth of solvable groups that are not polycyclic.

1. Preliminaries

In this section we build up some notation and tools needed in the proofs of our theorems.

1.1. Some group theory. Let Γ be a group. Set $\Gamma^{(k)}$ to be the *derived series* of Γ, defined recursively by
$$\Gamma^{(0)} = \Gamma \text{ and } \Gamma^{(k)} = [\Gamma^{(k-1)}, \Gamma^{(k-1)}].$$

A group Γ is said to be *solvable* if $G^{(k)} = 1$ for some natural number k. The minimal such k is called the *solvable class* of Γ. If, in addition to Γ being solvable, each quotient $\Gamma^{(k)}/\Gamma^{(k+1)}$ is finitely generated, then Γ is said to be

polycyclic. Equivalently, a group Γ is polycyclic if and only if Γ is solvable and every subgroup of Γ is finitely generated. Set Γ_k to be the lower central series for Γ, defined recursively by

$$\Gamma_0 = \Gamma \text{ and } \Gamma_k = [\Gamma_{k-1}, \Gamma].$$

A group Γ is said to be *nilpotent* if $\Gamma_k = 1$ for some natural number k. The minimal such k is the *nilpotent class* of Γ.

We record the following elementary lemma:

Lemma 5. *Let Γ be a finitely generated group. Then the following are equivalent:*

(1) Γ *is polycyclic and virtually nilpotent.*
(2) Γ *is solvable and virtually nilpotent.*

Proof. The implication $(1) \Rightarrow (2)$ is immediate since polycyclic groups are solvable. We now show that $(2) \Rightarrow (1)$. Since Γ is virtually nilpotent, Γ contains some nilpotent subgroup, say Δ, of finite-index. It suffices to show that any subgroup Δ' of Γ is finitely generated. The group $\Delta' \cap \Delta$ is finite index in Δ' and is a subgroup of Δ. Since Δ is f.g. nilpotent and hence polycyclic, it follows that $\Delta \cap \Delta'$ is finitely generated. Hence Δ' is finitely generated as finite generation is inherited by finite group extensions. $\qquad \square$

1.2. Quantifying residual finiteness. Recall that a group is *residually finite* if the intersection of all its finite index subgroups is trivial. Let Γ be a finitely generated, residually finite group. Let P be a property of groups. For $\gamma \in \Gamma - \{1\}$ we define $Q(\gamma, \Gamma, P)$ to be the set of finite quotients of Γ with property P in which the image of γ is non-trivial. We say that these quotients *detect* γ. We define

$$D_\Gamma^P(\gamma) := \inf\{|Q| : Q \in Q(\gamma, G, P)\}.$$

For a fixed finite generating set $\mathcal{X} \subset \Gamma$ we define

$$F_{\Gamma, \mathcal{X}}^P(n) := \max\{D_\Gamma^P(\gamma) \ : \ \gamma \in \Gamma - \{1\}, \|\gamma\|_\mathcal{X} \leq n\}.$$

For two functions $f, g : \mathbb{N} \to \mathbb{N}$ we write $f \preceq g$ if there exists a natural number M such that $f(n) \leq Mg(Mn)$, and we write $f \approx g$ if $f \preceq g$ and $g \preceq f$. In the case when $f \approx g$ does not hold we write $f \not\approx g$. When $f \preceq g$ does not hold we write $f \not\preceq g$. We will also write $f \succeq g$ for $g \preceq f$ and $f \not\succeq g$ for $g \not\preceq f$. If there exists a natural number M such that $f(n) \leq Mg(Mn)$ for infinitely many n, we say that $f(n) \preceq g(n)$ *for infinitely many n.*

It was shown in [B10] that if $\mathcal{X}, \mathcal{Y}$ are two finite generating sets for the residually finite group Γ, then $F_{\Gamma, \mathcal{X}} \approx F_{\Gamma, \mathcal{Y}}$. This result actually holds for the more general F_Γ^P function when the property P is always inherited by subgroups:

Lemma 6. *Let Γ be a finitely generated group and P be a property of groups that is always inherited by subgroups. If Δ is a finitely generated subgroup of Γ and $\mathcal{X}, \mathcal{Y}$ are finite generating sets for Γ, Δ respectively, then $F_{\Delta, \mathcal{Y}}^P \preceq F_{\Gamma, \mathcal{X}}^P$.*

Proof. As any homomorphism of Γ to Q, with Q having property P, restricts to a homomorphism of Δ to a subgroup of Q, it follows that $D_\Delta^P(h) \leq D_\Gamma^P(h)$ for all $h \in \Delta$. Hence,

$$(1) \qquad F_{\Delta,\mathcal{Y}}^P(n) = \sup\{D_\Delta^P(g) \ : \ \|g\|_\mathcal{Y} \leq n, g \neq 1\}$$
$$\leq \sup\{D_\Gamma^P(g) \ : \ \|g\|_\mathcal{Y} \leq n, g \neq 1\}.$$

Further, there exists a $C > 0$ such that any element in $\mathcal{Y}$ can be written in terms of at most C elements of $\mathcal{X}$. Thus,

$$(2) \qquad \{h \in \Delta : \|h\|_\mathcal{Y} \leq n, h \neq 1\} \subseteq \{g \in \Gamma : \|g\|_\mathcal{X} \leq Cn, g \neq 1\}.$$

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

$$F_{\Delta,\mathcal{Y}}^P(n) \leq \sup\{D_\Gamma^P(g) : \|g\|_\mathcal{Y} \leq n, g \neq 1\}$$
$$\leq \sup\{D_\Gamma^P(g) : \|g\|_\mathcal{X} \leq Cn, g \neq 1\} = F_{\Gamma,\mathcal{X}}^P(Cn),$$

as desired. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Since we will only be interested in asymptotic behavior, we let F_Γ^P be the equivalence class (with respect to $\approx$) of the functions $F_{\Gamma,\mathcal{X}}^P$ for all possible finite generating sets $\mathcal{X}$ of Γ. Sometimes, by abuse of notation, F_Γ^P will stand for some particular representative of this equivalence class, constructed with respect to a convenient generating set.

1.3. Connections to word growth and normal subgroup growth.
Given a finitely generated group Γ with generating set $\mathcal{X}$, recall that *word growth* involves studying the asymptotics of the following function:

$w_\Gamma(n)$
$:= |\{\gamma \in \Gamma : \text{ the word length of } \gamma \text{ with respect to } \mathcal{X} \text{ is no more than } n\}|.$

Subgroup growth is the asymptotic growth of

$$s_\Gamma(n) := |\{\Delta \leq \Gamma : [\Gamma : \Delta] = n\}|.$$

Normal subgroup growth is the asymptotic growth of

$$s_\Gamma^\triangleleft(n) := |\{\Delta \triangleleft \Gamma : [\Gamma : \Delta] = n\}|.$$

Gromov's Polynomial Growth theorem [G81] equates virtual nilpotency to having polynomial word growth. The following lemma is a slight improvement of Proposition 2.3 in [BM1].

Lemma 7. *Let Γ be a finitely generated, residually finite group generated by $\mathcal{X}$. If*

$$\exp(\exp([\log\log(n)]^3)) \preceq w_{\Gamma,\mathcal{X}}(n),$$

for infinitely many n, then $F_{\Gamma,X}(n) \not\preceq (\log(n))^r$ for any $r \in \mathbb{R}$.

Proof. We first recall a basic inequality from [BM1] (Inequality (1) in that paper) that relates word growth, normal subgroup growth, and normal residual finiteness growth:

$$(3) \qquad \log(\mathrm{w}_{\Gamma,\mathcal{X}}(n)) \leq \mathrm{s}_{\Gamma}^{\lhd}(\mathrm{F}_{\Gamma,\mathcal{X}}(2n)) \log(\mathrm{F}_{\Gamma,\mathcal{X}}(2n)).$$

To prove the theorem with this inequality, assume to the contrary that there exists $r \in \mathbb{R}$ such that $\mathrm{F}_{\Gamma,\mathcal{X}} \preceq (\log(n))^r$. In terms of $\preceq$ notation, inequality (3) becomes:

$$\log(\mathrm{w}_{\Gamma,\mathcal{X}}(n)) \preceq \mathrm{s}_{\Gamma}^{\lhd}(\mathrm{F}_{\Gamma,\mathcal{X}}(n)) \log(\mathrm{F}_{\Gamma,\mathcal{X}}(n)).$$

Taking the log of both sides, we obtain

$$\log\log(\mathrm{w}_{\Gamma,\mathcal{X}}(n)) \preceq \log(\mathrm{s}_{\Gamma}^{\lhd}(\mathrm{F}_{\Gamma,\mathcal{X}}(n))) + \log(\log(\mathrm{F}_{\Gamma,\mathcal{X}}(n))).$$

This inequality, in tandem with the assumptions

$$\exp(\exp([\log\log(n)]^3)) \preceq \mathrm{w}_{\Gamma,\mathcal{X}}(n) \text{ for infinitely many } n,$$
$$\mathrm{F}_{\Gamma,\mathcal{X}}(n) \preceq (\log(n))^r,$$

and $\log(\mathrm{s}_{\Gamma}^{\lhd}(n)) \preceq (\log(n))^2$ (see [LS03, Corollary 2.8]) gives

$$[\log\log(n)]^3 \preceq (\log\log(n))^2 + \log\log\log(n),$$

for infinitely many n, which is impossible. $\qquad\square$

Following the proofs in [BM1], we achieve the following two corollaries.

Corollary 8. *Any finitely generated solvable group has normal residual finiteness growth which is at most polynomial in* $\log(n)$ *if and only if the group is virtually nilpotent.* $\qquad\square$

Proof. Since virtually nilpotent groups are linear [A67], any virtually nilpotent group has polynomial in $\log(n)$ normal residual finiteness growth (see [B10]). If suffices to show that any finitely generated solvable group that has normal residual finiteness growth which is at most polynomial in $\log(n)$ is virtually nilpotent. Milnor's Theorem in [M68] states that any finitely generated solvable group which is not virtually nilpotent must have exponential word growth. This fact along with the normal residual finiteness growth assumption on Γ contradicts Lemma 7. $\qquad\square$

Corollary 9. *Any finitely generated solvable group* Γ *that is virtually nilpotent has solvable residual finiteness growth bounded above by* $(\log(n))^k$ *for some* k. $\qquad\square$

2. The Proofs of Theorems 1 and 2

Proof of Theorem 1. It follows, from Theorem 0.2 in [B10], that if Γ is virtually nilpotent then $\mathrm{F}_\Gamma(n)$ is at most polynomial in $(\log(n))$. Hence, it suffices to show that Γ is virtually nilpotent if $\mathrm{F}_\Gamma(n)$ is at most polynomial in $\log(n)$. Let Δ be a finite-index subgroup of Γ that is residually solvable and finitely generated. If Δ is virtually nilpotent, then Γ is virtually nilpotent.

Further, by Lemma 6, $F_\Delta(n)$ is at most polynomial in $\log(n)$. Hence, we may assume that Γ is residually solvable and finitely generated. Suppose Γ is not virtually nilpotent, then by Theorem 1.1 in [Wi05], it follows that Γ must have word length greater than

$$\exp\exp([\log(n)]^{1/3})$$

for infinitely many n. But we claim that having such word growth contradicts Lemma 7. Indeed, the assumption in Lemma 7 is satisfied if

$$\exp(\exp([\log\log(n)]^3)) \preceq \exp(\exp([\log(n)]^{1/3})),$$

which is clearly true.   □

Proof of Theorem 2. If Γ is virtually nilpotent and residually solvable, then by Lemma 0.4 in [LM91], Γ is solvable. So by Corollary 9, we see that Γ must have solvable residual finiteness growth which is at most polynomial in $\log(n)$. This completes one direction of the proof. To finish, we must show that if Γ has solvable residual finiteness growth which is at most polynomial in $\log(n)$, then Γ is virtually nilpotent and solvable. By Theorem 1, Γ is virtually nilpotent. Hence, as Γ is residually solvable, Γ must be solvable by Lemma 0.4 in [LM91].   □

3. Proof of Theorem 3

Let Γ be the fundamental group of a compact surface. Since Γ contains a free group, the lower bound of the theorem follows from the following claim and Lemma 6.

Claim 1. *We have* $F^{\mathrm{nil}}_{\mathbb{Z}*\mathbb{Z}}(n) \succeq \exp[\sqrt{n}]$.

Proof. Let x and y be generators for $\mathbb{Z}*\mathbb{Z}$. Let $u_1(x,y) = x^{-2}y^{-1}x$ and

$$u_{n+1}(x,y) = [xu_n(x,y)x^{-1}, yu_n(x,y)y^{-1}].$$

By Theorem 1.1 in [B06], $u_n(x,y) \neq 1$ for all n. Moreover, $u_n \in \Gamma^{(n)}$ and $\|u_n\| \leq C4^n$ for some natural number C. By a well-known result of Hall, $\Gamma^{(n)} \subset \Gamma_{2^n}$ (see, for example, Lemma 2.7 in [MP]). Further recall that if Q is a finite group of nilpotence class 2^n, then $|Q| > 2^{2^n}$. Drawing all this together gives

$$F^{\mathrm{nil}}_\Gamma(C4^n) \geq 2^{2^n}.$$

Let $m = [\log_2(\sqrt{n})]$, where $[\cdot]$ denote the floor function and n is large enough to ensure that m is positive. We have

$$F^{\mathrm{nil}}_\Gamma(C4^m) \geq 2^{2^m}.$$

Since $[\log_2(\sqrt{n})] \geq \log_2(\sqrt{n})$, we have $2^{2^m} \geq 2^{\sqrt{n}}$. Further, $[\log_2(\sqrt{n})] < \log_2(\sqrt{n}) + 1$, so because F^{nil}_Γ is a nondecreasing function in n,

$$F^{\mathrm{nil}}_\Gamma(C2^{2[\log(\sqrt{n})]}) \leq F^{\mathrm{nil}}_\Gamma(C2^{2\log_2(\sqrt{n})+2}) \leq F^{\mathrm{nil}}_\Gamma(4Cn).$$

Hence,

$$\mathrm{F}_\Gamma^{\mathrm{nil}}(4Cn) < 2^{\sqrt{n}}.$$

Since $4C$ is greater than one, we get

$$\mathrm{F}_\Gamma^{\mathrm{nil}}(n) \preceq 2^{\sqrt{n}}. \qquad \square$$

Before proving the upper bound in Theorem 3, we first prove some preliminary results.

Claim 2. *Let Δ be the kernel of the group homomorphism*

$$\phi : \mathrm{PSL}_2(\mathbb{Z}[i]) \to \mathrm{SL}_2(\mathbb{Z}/2\,\mathbb{Z})$$

induced by the ring homomorphism

$$\mathbb{Z}[i] \to \mathbb{Z}[i]/\langle(1-i)\rangle = \mathbb{Z}/2\,\mathbb{Z}.$$

Then $\mathrm{F}_\Delta^{\mathrm{nil}}(n) \preceq 2^n$.

Proof. Before starting the proof, we construct a filtration for the kernel which will help us find small nilpotent quotients. Set $G_0 = \Delta$ and

$$G_k = \ker[\mathrm{PSL}_2(\mathbb{Z}[i]) \to \mathrm{SL}_2((\mathbb{Z}/2^k\,\mathbb{Z})[i])/\{\pm 1\}] \text{ for } k \geq 1.$$

Then, because $2 = (1-i)(1+i)$, we have the following filtration of normal subgroups for G_0:

$$G_0 \geq G_1 \geq G_2 \geq G_3 \geq \cdots$$

We first claim that each quotient G_0/G_k is a 2-group of order less than 2^{8k}. We write $[A]$ for the equivalence class in $\mathrm{PSL}_2(\mathbb{Z}[i])$ containing an element $A \in \mathrm{SL}_2(\mathbb{Z}[i])$. The first quotient G_0/G_1 is

$$\{[A] \in \mathrm{PSL}_2(\mathbb{Z}[i]) : A \equiv 1 \mod (1-i)\,\mathbb{Z}[i]\}/\sim,$$

where $[A] \sim [B]$ if $A \equiv \pm B \equiv B \mod 2\,\mathbb{Z}[i]$. Denote by $M_2(\mathbb{Z}/2\,\mathbb{Z}[i])$ the set of all 2×2 matrices with coefficients in $\mathbb{Z}/2\,\mathbb{Z}[i]$. Let $h : G_0/G_1 \to (M_2(\mathbb{Z}/2\,\mathbb{Z}[i]), +)$ be given by $[A]G_1 \mapsto (A - 1)$. The map is well-defined: indeed if $[A] \sim [B]$ then $[A] = [B + 2N]$ for some N in $M_2(\mathbb{Z}[i])$. So setting $M_A = A - 1$ gives

$$[B] = [A + 2N] = [1 + M_A + 2N].$$

Hence, $h([A]G_1) = M_A$ and $h([B]G_1) = M_A + 2N$ which is equal to M_A in $M_2(\mathbb{Z}[i]/2\,\mathbb{Z}[i])$. Further, the map is a homomorphism: indeed, if $[A] = [1 + (1-i)M]$ and $[B] = [1 + (1-i)N]$, then

$$[A][B] = [1 + (1-i)(M+N) - 2iMN] \sim [1 + (1-i)(M+N)].$$

Finally, the map h is injective since matrices that get mapped to 1 under h must satisfy $A \equiv 1 \mod 2\,\mathbb{Z}[i]$. It follows that G_0/G_1 is a 2-group of order at most $|M_2(\mathbb{Z}/2\,\mathbb{Z}[i])| = 2^8$.

For $k > 1$ we write

$$G_k/G_{k+1} = \{[A] \in \mathrm{PSL}_2(\mathbb{Z}[i]) : A \equiv 1 \mod 2^k\,\mathbb{Z}[i]\}/\sim,$$

where $[A] \sim [B]$ if $A \equiv \pm B \mod 2^{k+1} \mathbb{Z}[i]$. Define a map

$$g : G_k/G_{k+1} \to (M_2(\mathbb{Z}/2\,\mathbb{Z}[i]), +)$$

by $[A] \mapsto (A - 1)2^{-k}$. It is well-defined: indeed if $[A] \sim [B]$ then $A = \pm(B - 2^{k+1}N)$ for some N in $M_2(\mathbb{Z}[i])$. So setting $M_A = (A-1)2^{-k}$ gives

$$\pm B = A \pm 2^{k+1}N = 2^k M_A + 1 \pm 2^{k+1}N = 1 + 2^k(M_A \pm 2N).$$

Hence, $h([A]G_{k+1}) = M_A$ and $h([B]G_{k+1}) = M_A + 2N$ which is equal to M_A in $M_2(\mathbb{Z}[i]/2\,\mathbb{Z}[i])$.

Further, g is a homomorphism: Indeed, if $[A] = [1 + 2^k M]$ and $[B] = [1 + 2^k N]$, then $[A][B] = [AB]$ becomes

$$[(1 + 2^k M)(1 + 2^k N)] = [1 + 2^k M + 2^k N + 2^{2k} MN] \sim [1 + 2^k(M + N)],$$

which maps to $M + N$. Finally, the map is injective, as $g([A]G_{k+1}) = 0$ implies that $[A] = [1 + 2^{k+1}N] \sim [1]$. It follows that G_k/G_{k+1} is a two group with order bounded above by 2^8. This gives that G_0/G_k is a 2-group of order bounded above by 2^{8k}, as claimed.

Let $\mathfrak{X}$ be a finite set of generators for Δ as a semigroup and set $S = \{1, i\}$. We claim that there exists $\lambda > 0$ such that for any $[A] \in \Delta$ with $\|[A]\|_{\mathfrak{X}} \leq n$ and any non-zero entry $a \in \mathbb{Z}[i]$ of $A \pm 1$ we have

$$\|a\|_S \leq \lambda^n.$$

To prove the claim, let a' be the entry of A in the same spot as a in $A \pm 1$. We have, by the triangle inequality,

$$\|a\|_S \leq \|a'\|_S + \|1\|_S.$$

This reduces the above claim to the following. There exists $\mu > 0$ such that for any $A \in G_0$ with $\|A\|_{\mathfrak{X}} \leq n$ and any non-zero entry $a \in \mathbb{Z}[i]$ of A we have

$$\|a\|_S \leq \mu^n.$$

We claim that if β denotes the maximum of $\|x\|_S$, where x ranges over all entries of all elements of $\mathfrak{X}$, then $\mu := m\beta$ satisfies the last statement. To see this, consider first the case $A = XY$ with $X, Y \in \mathfrak{X}$. The entries of A are scalar products of the rows of X and the columns of Y. Thus we are led to study $\|x \cdot y\|_S$ for $x, y \in \mathbb{Z}[i]^m$, where $\cdot$ denotes scalar product. Clearly we have $\|x \cdot y\|_S \leq m \max\{\|x_j y_j\|_S : 1 \leq i \leq m\}$. In terms of the basis S we can write

$$x_j = a_x + b_x i \qquad \text{and} \qquad y_j = a_y + b_y i$$

where each a_x, b_x, a_y, b_y belongs to $\mathbb{Z}$. One computes

$$\|x_j y_j\|_S \leq \|x_j\|_S \|y_j\|_S.$$

This formula and induction on n complete the proof of the claim.

We now finish the proof. Let $[A]$ be an element in Δ of word length at most n in terms of $\mathcal{X}$. Then, by the above, there exists a $C > 0$ such that any nonzero entry a of $A - 1$ or $A + 1$ satisfies

$$\|a\|_S \leq 2^{Cn}.$$

However, by the definition of G_k: if A is nontrivial and in G_k, then any nonzero entry a of $A-1$ and $A+1$ has $\|a\|_S \geq 2^k$. It follows that $[A] \notin G_{Cn}$, hence, as G_0/G_{Cn} is a 2-group of order at most 2^{8Cn}, we have

$$\mathrm{D}^{\mathrm{nil}}([A]) \leq 2^{8Cn},$$

giving

$$\mathrm{F}_{G_0}^{\mathrm{nil}}(n) \preceq 2^n. \qquad \square$$

Claim 3. *Let Δ be the kernel of the group homomorphism*

$$\phi : \mathrm{PSL}_2(\mathbb{Z}[i]) \to \mathrm{SL}_2(\mathbb{Z}/2\,\mathbb{Z})$$

induced by the ring homomorphism

$$\mathbb{Z}[i] \to \mathbb{Z}[i]/\langle (1-i) \rangle = \mathbb{Z}/2\,\mathbb{Z}.$$

Then Δ contains the fundamental group of a genus 2 surface.

Proof. Let d be a square-free postive integer, $\mathcal{O}_d$ the ring of integers of the quadratic imaginary number field $\mathbb{Q}(\sqrt{-d})$ and Γ_d the Bianchi group $\mathrm{PSL}_2(\mathcal{O}_d)$. It was shown by Maclachlan (see Chapter 9.6 of [MR03]) that for any circle $\mathcal{C}$ with equation:

$$a|z|^2 + Bz + \overline{B}\overline{z} + c = 0, \ \text{ with } a, c \in \mathbb{Z}, B \in \mathcal{O}_d$$

the group

$$\mathrm{Stab}(\mathcal{C}, \Gamma_d) = \{\gamma \in \Gamma_d : \gamma(\mathcal{C}) = \mathcal{C} \text{ and } \gamma \text{ preserves components of } \mathbf{C} \setminus \mathcal{C}\}$$

is an arithmetic Fuchsian subgroup of Γ_d. Moreover, all such arithmetic Fuchsian subgroups occur like this.

We now fix attention on the case of $d = 1$ and the circle $\mathcal{C}$ with equation

$$2|z|^2 + (1+i)z + (1-i)\overline{z} - 2 = 0.$$

Denote the group $\mathrm{Stab}(\mathcal{C})$ by F. It is shown in [MR91] Theorem 8 that this is an arithmetic Fuchsian group of signature $(0; 2, 2, 3, 3; 0)$. With a bit of effort, explicit generators for F can be computed, namely:

$$x_1 = \begin{pmatrix} i & 1+i \\ 0 & -i \end{pmatrix}, \qquad x_2 = \begin{pmatrix} -1+2i & 3+i \\ 1+i & 1-2i \end{pmatrix},$$

$$x_3 = \begin{pmatrix} 2i & 3+2i \\ 1 & 1-2i \end{pmatrix}, \qquad x_4 = \begin{pmatrix} 1+2i & 2+3i \\ -i & -2i \end{pmatrix}.$$

Now let Γ denote the principal congruence subgroup of Γ_1 of level $\langle (1+i) \rangle$. To determine the group $F \cap \Gamma$ we consider the reduction of the generators

of F modulo $\langle (1+i) \rangle$. It is easily seen that (projectively) x_1 and x_2 map trivially with x_3 and x_4 mapping to the elements

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},$$

respectively. We deduce from this that the image of F under the reduction homomorphism is cyclic of order 3, and so it follows that since each of x_1 and x_2 is killed, they determine 3 conjugacy classes of cyclic groups of order 2 in $F \cap \Gamma$. Given that the index $[F : F \cap \Gamma] = 3$, we deduce that the signature of the Fuchsian group $F \cap \Gamma$ is $(0; 2, 2, 2, 2, 2, 2; 0)$. Any such group has a genus 2 surface group. In summary we have shown that the level $\langle (1+i) \rangle$ principal congruence subgroup of $\mathrm{PSL}_2(\mathcal{O}_1)$ contains a genus 2 surface group. $\qquad \square$

We now prove the upper bound in Theorem 3:

Corollary 10. *Let Γ be the fundamental group of an oriented surface. Then* $\mathrm{F}_\Gamma^{\mathrm{nil}}(n) \preceq 2^n$.

Proof. By Claim 3, the kernel in Claim 2 contains Γ. Hence the corollary follows from Lemma 6. $\qquad \square$

Corollary 11. *Let Γ be the fundamental group of an oriented surface with generating set $\mathcal{X}$. Then there exists a constant $C > 0$ such that any $\gamma \in \Gamma$ satisfies $\gamma \notin \Gamma_{C\|\gamma\|_\mathcal{X}}$.*

Proof. By the previous corollary, we have that there exists $C > 0$ such that $\mathrm{F}_{\Gamma, \mathcal{X}}^{\mathrm{nil}}(n) < 2^{Cn}$ for all n. Hence, for any $\gamma \in \Gamma - \{1\}$, we have $\mathrm{D}_\Gamma^{\mathrm{nil}}(\gamma) \leq 2^{C\|\gamma\|_\mathcal{X}}$. But any finite group of nilpotent class no less than $C\|\gamma\|_\mathcal{X}$, must have order no less than $2^{C\|\gamma\|_\mathcal{X}}$, hence $\gamma \notin \Gamma_{C\|\gamma\|_\mathcal{X}+1}$, which is sufficient. $\qquad \square$

4. Some examples

In this section we show that better lower bounds can be found for some groups Γ where $[\Gamma, \Gamma]$ is not finitely generated.

Example 1. *Let p be a prime number. Let Γ be the group $\mathbb{Z}/p\mathbb{Z} \wr \mathbb{Z}$. Set $\Delta = \oplus_{i \in \mathbb{Z}} \mathbb{Z}/p\mathbb{Z}$ to be the base group of Γ so $\Gamma/\Delta \cong \mathbb{Z}$. We claim that $\mathrm{F}_\Gamma(n) \succeq \sqrt{n}$.*

Proof. We begin with a linear algebraic construction of candidates for a lower bound. Let A be the $2m \times m$ matrix with entries in $\mathbb{Z}/p\mathbb{Z}$ given by

$$(4) \qquad \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & \cdots \\ 1 & 0 & 1 & 0 & 1 & \cdots \\ 0 & 1 & 0 & 1 & 0 & \cdots \\ 1 & 0 & 0 & 1 & 0 & \cdots \\ 0 & 1 & 0 & 0 & 1 & \cdots \\ 0 & 0 & 1 & 0 & 0 & \cdots \\ 1 & 0 & 0 & 0 & 1 & \cdots \\ & & \vdots & & & \end{pmatrix}.$$

Set $m = n(n + 1)/2$. This matrix gives a linear transformation from $(\mathbb{Z}/p\mathbb{Z})^{2m}$ to $(\mathbb{Z}/p\mathbb{Z})^m$. Since the cardinality of $(\mathbb{Z}/p\mathbb{Z})^{2m}$ is greater than that of $(\mathbb{Z}/p\mathbb{Z})^m$, we have that $\ker(A)$ is nontrivial. Fix $w = (w_1, \ldots, w_{2m})$ to be a nontrivial element in $\ker(A)$. Let δ_i be the Dirac delta function giving an element in Δ. Set v to be the element

$$\sum_{i=1}^{2m} w_i \delta_i.$$

This element v is our candidate.

Let t be the generator for $\mathbb{Z}$ in the wreath product of $\mathbb{Z}/p\mathbb{Z} \wr \mathbb{Z}$. It is straightforward to see that the element v has word length less than $2m(p+2)$. Let $\phi : \Gamma \to Q$ be a map onto a finite Q such that $v \notin \ker \phi$. Then, supposing that $\phi(t^r) = 1$ for $r < n$ gives

$$\phi(v) = \phi\left(\sum_{i=1}^{2m} w_i \delta_i\right) = \phi\left(\sum_{i=1}^{r-1}(w_i + w_{i+r} + w_{i+2r} + \cdots)\delta_i\right) = 0.$$

Hence, $r \geq n$, and so $|Q| \geq n$, giving $\mathrm{F}_\Gamma(n^2) \succeq n$ and hence $\mathrm{F}_\Gamma(n) \succeq n^{1/2}$ as desired. $\qquad\square$

The above method strengthens Example 2.3 in [BK10].

Example 2. Let Γ be the wreath product $\mathbb{Z} \wr \mathbb{Z}$. Set $\Delta = \oplus_{i \in \mathbb{Z}} \mathbb{Z}$ to be the base group of Γ so $\Gamma/\Delta \cong \mathbb{Z}$. We claim that $\mathrm{F}_\Gamma(n) \succeq n^{1/4}$.

Proof. We begin with a linear algebraic construction of candidates for a lower bound. As in the above proof, let A be the $2m \times m$ matrix, this time with entries in $\mathbb{Z}$ given by Expression 4. Set $m = n(n + 1)/2$, for n even. This matrix gives a map from $V := \mathbb{Z}^{2m}$ to $W := \mathbb{Z}^m$. Let $\|\cdot\|_{\mathbb{Z}^\ell}$ be the supremum norm on $\mathbb{Z}^\ell$. By the triangle inequality and the definition of A, one sees that for any $v \in V$, we have

$$\|Av\|_W \leq m\|v\|_V.$$

Further, if we let $B_{\mathbb{Z}^\ell}(k) = \{v \in \mathbb{Z}^\ell : \|v\|_{\mathbb{Z}^\ell} \leq k\}$, then $AB_V(k) \subseteq B_W(mk)$ for all k. Moreover, for all even $k \in \mathbb{N}$,

$$\begin{aligned}
|B_W(k/2)| &= (k+1)^m, \text{ and} \\
|B_V(k/2)| &= (k+1)^{2m}.
\end{aligned}$$

If $k = (m + 2)$, then

$$\begin{aligned}
|B_V(k/2)| = (k+1)^{2m} &> ((m+3)k)^m = (km + 3k)^m \\
&> (mk + 1)^m = |B_W(mk/2)|.
\end{aligned}$$

Hence, as $AB_V(k/2) \subseteq B_W(mk/2)$, there must exist $w \in \ker(A) \cap B_V(k)$ that is nontrivial. Fix such a w, and write $w = (w_1, \ldots, w_{2m})$. Let δ_i be the

Dirac delta function giving an element in Δ. Set v to be the element

$$\sum_{i=1}^{2m} w_i \delta_i.$$

This element v is our candidate. It is straightforward to show that the element v has word length less than $2m(k+2)$.

Let t be the canonical generator for the wreath product of $\mathbb{Z} \wr \mathbb{Z}$ whose image generates Γ/Δ. Let $\phi : \Gamma \to Q$ be a map onto a finite Q such that $v \notin \ker \phi$. Then, supposing that $\phi(t^r) = 1$ for $r < n$ gives

$$\phi(v) = \phi\left(\sum_{i=1}^{2m} w_i \delta_i\right) = \phi\left(\sum_{i=1}^{r-1}(w_i + w_{i+r} + w_{i+2r} + \cdots)\delta_i\right) = 0.$$

Hence, $r \geq n$, and so $|Q| \geq n$, giving $\mathrm{F}_\Gamma(n^4) \succeq n$ and hence $\mathrm{F}_\Gamma(n) \succeq n^{1/4}$ as desired. $\qquad\square$

References

[A67]   AUSLANDER, LOUIS. On a problem of Philip Hall. *Ann. of Math.* (2) **86** (1967), 112–116. MR0218454 (36 #1540), Zbl 0149.26904.

[B06]   BANDMAN, TATIANA; GREUEL, GERT-MARTIN; GRUNEWALD, FRITZ; KUNYAVSKIĬ, BORIS; PFISTER, GERHARD; PLOTKIN, EUGENE. Identities for finite solvable groups and equations in finite simple groups. *Compositio Math.* **142** (2006), 734–764. MR2231200 (2007d:20027), Zbl 1112.20016.

[B10]   BOU-RABEE, KHALID. Quantifying residual finiteness. *J. Algebra* **323** (2010), 729–737. MR2574859 (2011d:20087), Zbl pre05681238.

[BK10] BOU-RABEE, KHALID; KALETHA, TASHO. Quantifying residual finiteness of arithmetic groups. To appear in *Compositio Math.*

[BM1]   BOU-RABEE, KHALID; MCREYNOLDS, DAVID BEN. Asymptotic growth in groups and generalized least common multiples. To appear in *Bull. London Math. Soc.*

[G81]   GROMOV, MIKHAEL. Groups of polynomial growth and expanding maps. *Inst. Hautes Études Sci. Publ. Math.* **53** (1981), 53–73. MR0623534 (83b:53041), Zbl 0474.20018. Appendix, TITS, JACQUES. *Inst. Hautes Études Sci. Publ. Math.* **53** (1981), 74–78. MR0623535 (83b:53042).

[G89]   GRIGORCHUK, R. I. On the Hilbert-Poincaré series of graded algebras associated with groups. *Math. Sb.* **180** (1989) 207–225 (Russian). *Math. USSR Sb.* **66** (1990), 211–229 (English). MR0993455 (90j:20063), Zbl 0695.16009.

[LM91] LUBOTZKY, ALEXANDER; MANN, AVINOAM. On groups of polynomial subgroup growth. *Invent. Math.* **104** (1991), 521–533. MR1106747 (92d:20038), Zbl 0743.20040.

[LS03] LUBOTZKY, ALEXANDER; SEGAL, DAN. Subgroup growth, Progress in Mathematics, 212. *Birkhäuser Verlag, Basel*, 2003. xxii+453 pp. ISBN: 3-7643-6989-2. MR1978431 (2004k:20055), Zbl 1071.20033.

[MR91] MACLACHLAN, COLIN; REID, ALAN W. Parametrizing Fuchsian subgroups of the Bianchi groups. *Canadian J. Math.* **43** (1991), 158–181. MR1108918 (92d:11040), Zbl 0739.20020.

[MR03] MACLACHLAN, COLIN; REID, ALAN W. The arithmetic of hyperbolic 3-manifolds. Graduate Texts in Mathematics, 219. *Springer-Verlag, New York*, 2003. xiv+463 pp. ISBN: 0-387-98386-4. MR1937957 (2004i:57021), Zbl 1025.57001.

[MP]   Malestein, Justin; Putman, Andrew. On the self-intersections of curves deep in the lower central series of a surface group. *Geom. Dedicata* **149** (2010), 73–84. MR2737679, Zbl 1210.57001.

[M68]   Milnor, John. Growth of finitely generated solvable groups. *J. Differential Geometry* **2** (1968), 447–449. MR0244899 (39 #6212), Zbl 0176.29803.

[R93]   Robinson, Derek J. S. A course in the theory of groups. Graduate Texts in Mathematics, 80. *Springer, New York*, 1993. xviii+481 pp. ISBN: 0-387-94092-8. MR1261639 (94m:20001), Zbl 0483.20001.

[Wi05] Wilson, John S. On the growth of residually soluble groups. *J. London Math. Soc.* (2) **71** (2005), 121–132. MR2108251 (2006a:20069), Zbl 1073.20031.

Department of Mathematics, The University of Michigan, 2074 East Hall, Ann Arbor, MI 48109-1043
khalidb@umich.edu

This paper is available via `http://nyjm.albany.edu/j/2011/17-30.html`.