Extremal behavior of divisibility functions

Khalid Bou-Rabee* and D. B. McReynolds†

May 5, 2014

Abstract

In this short article, we study the extremal behavior $F_\Gamma(n)$ of divisibility functions $D_\Gamma$ introduced by the first author for finitely generated groups $\Gamma$. These functions aim at quantifying residual finiteness and bounds give a measurement of the complexity in verifying a word is non-trivial. We show that finitely generated subgroups of $\text{GL}(m,K)$ for an infinite field $K$ have at most polynomial growth for the function $F_\Gamma(n)$. Consequently, we obtain a dichotomy for the growth rate of $\log F_\Gamma(n)$ for finitely generated subgroups of $\text{GL}(n,C)$. We also show that if $F_\Gamma(n) \preceq \log \log n$, then $\Gamma$ is finite. In contrast, when $\Gamma$ contains an element of infinite order, $\log n \preceq F_\Gamma(n)$. We end with a brief discussion of some geometric motivation for this work.

1 Introduction

A group is residually finite if the intersection of all the finite index subgroups is trivial. We continue the study of quantifying residual finiteness, started in [B10] and furthered in [B11], [BM10] [BM11], and [KM11]. This venue is concerned with the asymptotic growth of variants of the normal divisibility function $D_\Gamma$: $\Gamma \to \mathbb{N}$ defined by

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

The asymptotic or $L^\infty$–behavior of this function is measured by

$$F_{\Gamma,X}(n) = \max\{D_\Gamma(g) : g \in B_{\Gamma,X}^*(n)\},$$

where $B_{\Gamma,X}^*(n)$ is the ball of radius $n$ minus the identity for $\Gamma$ with respect to some fixed finite generating set $X$. The function $F_{\Gamma,X}(n)$ is related to both the word growth $w_{\Gamma,X}(n)$ and normal subgroup growth function $s_\Gamma(n)$ via a basic inequality established in [BM10] (see (3) below).

It is a classical theorem of Mal’cev [M40] that any finitely generated linear group is residually finite [M40]. In [BM11] Theorem 1.1], we proved that for finitely generated linear groups,

*University of Michigan, Ann Arbor, MI 48109. E-mail: khalidb@umich.edu
†Purdue University, West Lafayette, IN 47907. E-mail: dmcreyno@math.purdue.edu
Extremal behavior of divisibility functions

For some $r > 0$ if and only if $\Gamma$ is virtually nilpotent; a similar result with restrictions on finite quotients was established in [B11 Theorem 2] without the linearity assumption. In [B10 Theorem 0.1] and the substantial generalization [BK12 Theorem 1.3], the growth rate of the function $F_{\Gamma,X}(n)$ was established for a large class of arithmetic lattices. Our first main result completes our goal of determining the growth of $F_{\Gamma}(n)$ for finitely generated linear groups $\Gamma$. Specifically, we prove the following:

**Theorem 1.1.** Let $\Gamma$ be a finitely generated subgroup of $GL(m, K)$, where $K$ is an infinite field. Then $F_{\Gamma,X}(n) \leq n^d$ for some $d$ depending only on $m$ and $K$.

The chief difficulty in proving Theorem 1.1 versus what was done in [B10 Theorem 0.1] and [BK12 Theorem 1.3] (also the general methods used in [BM10]) is the possibility that the field of coefficients for the group is transcendental over $\mathbb{Q}$ or $\mathbb{F}_p$. Geometrically, this issue is dealt with via a deformation of the representation in the variety of representations to a representation with coefficients in $\overline{\mathbb{Q}}$ or $\mathbb{F}_p$ since such a point cannot be locally rigid by work of Weil; the resulting representation need not be faithful but a fixed non-trivial word will have non-trivial image generically. Algebraically, this deformation equates to employing evaluation maps on function fields to the field of coefficients. We will take the geometrically less intuitive algebraic approach here as it is better suited for quantitative analysis. Combining Theorem 1.1 with [B10 Theorem 0.2] and [BM11 Theorem 1.1], we have the following dichotomy which was a main goal of the study of the function $F_{\Gamma,X}(n)$.

**Corollary 1.2.** Let $\Gamma$ be a finitely generated subgroup of $GL(m, \mathbb{C})$. Then there exists a positive integer $b$ such that

(i) $F_{\Gamma,X}(n) \leq (\log n)^b$, or

(ii) $F_{\Gamma,X}(n) \leq n^b$.

Moreover, (i) holds if and only if $\Gamma$ is virtually nilpotent.

Our second main result concerns the growth rate of $F_{\Gamma,X}(n)$ and how it relates to the threshold between finite and infinite groups. It is straightforward to see that for an infinite group, $w_{\Gamma,X}(n) \geq n$. However, the existence of infinite simple groups precludes such a growth threshold result for subgroup growth. As the function $F_{\Gamma,X}$ relates these two functions, it is not clear if such a growth threshold result should hold for $F_{\Gamma,X}$. That said, our final result exhibits that $F_{\Gamma,X}$ does enjoy a growth threshold. Specifically,

**Theorem 1.3.** Let $\Gamma$ be a finite generated group. If $F_{\Gamma,X}(n) \leq \log \log n$, then $\Gamma$ is finite.

It was established in [B10 Lemma 1.1, Theorem 2.2] that if $\Gamma$ contains an element of infinite order, than $\log n \leq F_{\Gamma,X}(n)$. We give a slight improvement of Theorem 1.3 (see Scholium 4.2) in Section 4. The proof of Theorem 1.3 uses the above mentioned basic inequality relating $F_{\Gamma,X}(n)$ with the word growth function $w_{\Gamma,X}(n)$ and the normal subgroup growth function $s_{\Gamma}(n)$ established earlier in [BM11 Equation 1].
We conclude with some geometric motivation for the study of the functions \( D_\Gamma, F_{\Gamma,X} \), and some related functions from [BM11].

Acknowledgements. We are immensely grateful to the excellent referee for pointing out errors in an earlier draft of this paper. We thank Martin Kassabov for asking us a question that led us to find Theorem 1.3. The first author was partially supported by NSF RTG grant DMS-0602191. The second author was partially supported by NSF DMS-1105710.

Notation and Conventions. We write \( f \preceq g \) to mean that there exists \( C > 0 \) such that \( f(n) \leq C(g(Cn)) \). If \( f \preceq g \) and \( g \preceq f \), then we write \( f \approx g \). The growth of \( F_{\Gamma,X}(n) \) is, up to this equivalence, independent of \( X \) (see [B10, Lemma 1.1]). Hence, we typically drop \( X \) from the notation.

2 A short algebraic excursion

In the proof of Theorem 1.1 we require some results on divisibility functions for rings. This section contains a pair of lemmas for just this task. Throughout, \( S \) will be either the ring \( \mathbb{Z}[T] \) or \( \mathbb{F}_p[T] \), where \( T = \{x_1, \ldots, x_s\} \) is a finite set of indeterminants. The divisibility function for \( S \)

\[
D_S: S - \{0\} \longrightarrow \mathbb{N}
\]

is given by

\[
D_S(f) = \min \{|S/p| : f \neq 0 \mod p, S/p \text{ is a field}\}.
\]

The next few results provide the needed control of this function in the characteristic zero and positive characteristic cases. We start with a lemma that allows us to reduce to the single variable case:

**Lemma 2.1.** Let \( S = R[T] \) where \( R = \mathbb{F}_p \) or \( R = \mathbb{Z} \) and \( T = \{x_1, \ldots, x_s\} \). Let \( f \in S \) be a polynomial that is nonzero and of degree \( d \). Then there exists a sequence \( \{n_i\}_{i=1}^s \) taking values in \( \{0, 1, \ldots, d^{s-1}\} \) such that

\[
f(x^{n_1}, \ldots, x^{n_s}) \neq 0.
\]

**Proof.** We prove this by complete 2-dimensional induction on \( s \) and \( d = \deg(f) \). The base cases where \( s = 1 \) or \( d = 0 \) are trivial. For the inductive step, let \( f \) be a degree \( d \) polynomial in \( R[x_1, \ldots, x_s] \) and write

\[
f(x_1, \ldots, x_s) = (h_0 + x_1 h_1)x_1^k,
\]

where \( h_0 \in R[x_2, \ldots, x_s] \) is nonzero, \( h_1 \in R[x_1, \ldots, x_s] \), and \( k \) a nonnegative integer. If \( k \neq 0 \), we are done by the inductive hypothesis applied to \( (h_0 + x_1 h_1) \), which has degree \( < d \). We assume, thusly, that \( k = 0 \). Since \( h_0 \) is nonzero and in \( R[x_2, \ldots, x_s] \) (note the variables start at \( x_2 \)), there exists, by the inductive hypothesis, \( n_2, \ldots, n_s \in \{0, 1, \ldots, d^{s-2}\} \) such that

\[
h_0(x^{n_2}, \ldots, x^{n_s}) \neq 0.
\]
We are done if \( h_1(x^{d_2}, x^{n_2}, \ldots, x^{n_s}) = 0 \) as then
\[
f(x^{d_2}, x^{n_2}, \ldots, x^{n_s}) = h_0(x^{n_2}, \ldots, x^{n_s}) \neq 0.
\]
Otherwise \( h_1(x^{d_2}, x^{n_2}, \ldots, x^{n_s}) \) is nonzero. In this case, we have
\[
\deg(h_0(x^{n_2}, \ldots, x^{n_s})) \leq d_2^{s-1} < d_2^s \leq \deg(x^{d_2} h_1(x^{d_2}, x^{n_2}, \ldots, x^{n_s})).
\]
Thus,
\[
f(x^{d_2}, x^{n_2}, \ldots, x^{n_s}) \neq 0
\]
as desired.

Now we handle the characteristic zero case.

**Lemma 2.2.** Let \( S = \mathbb{Z}[x_1, \ldots, x_s], f \in S \) with \( \deg(f) \leq d \), and assume that \( f \) is a nonzero function.
Set \( g \in \mathbb{Z}[x] \) to be a single variable polynomial obtained by Lemma 2.1 and \( \{a_i\} \) be given by
\[
g(x) = a_0 + a_1 x + \cdots + a_r x^r.
\]
Then for any \( \varepsilon > 0 \),
\[
D_S(f) \leq C \left( \log \left( \max \{|a_j|\} \right) + d^{(2s+1)+\varepsilon} \right),
\]
where \( C \) depends only on \( \mathbb{Z} \) and \( s \).

**Proof.** Let \( r = \deg(g) \) with \( r \leq d^{2s+1} \). \( g \) has at most \( r \) roots and so there exists \( \ell \in \mathbb{N} \) with \( \ell \leq r + 1 \) such that \( g(\ell) \neq 0 \). Setting \( g(\ell) = i \) and \( A = \max \{|a_j|\} \), note that \( i \in \mathbb{Z} \) and \( |i| \leq (r+1)\ell A \). Since \( F_{\mathbb{Z}}(i) \approx \log(i) \) (see [B10, Theorem 2.2]), we see that
\[
D_{\mathbb{Z}}(i) \leq C_0 \log((r+1)\ell A),
\]
where \( C_0 \) is a constant that only depends on \( \mathbb{Z} \). This inequality gives
\[
D_{\mathbb{Z}}(i) \leq C_0 \left( \log A + r \log \ell + \log(r+1) \right)
\]
\[
\leq C_0 \left( \log A + d^{2s+1} \log(d^{2s+1} + 1) + \log(d^{2s+1} + 1) \right)
\]
\[
\leq C_1 \left( \log A + d^{2s+1} \log d \right) < C(\log A + d^{(2s+1)+\varepsilon}),
\]
where \( C_1 \) and \( C \) only depends on \( \mathbb{Z} \) and \( s \). In total, we have the sequence of ring homomorphisms
\[
S \rightarrow \mathbb{Z}[x] \rightarrow \mathbb{Z} \rightarrow \mathbb{F}_p
\]
where
\[
f \mapsto g \mapsto i \mapsto \bar{i} \neq 0.
\]
In particular,
\[
D_S(f) \leq D_{\mathbb{Z}}(i) < C(\log A + d^{(2s+1)+\varepsilon}).
\]
\( \square \)
We next handle the positive characteristic case.

**Lemma 2.3.** Let $S = \mathbb{F}_p[x_1, \ldots, x_s]$, $f \in S$, $\deg(f) + 1 \leq d$, and assume that $f$ is nonzero. Then
\[ D_S(f) \leq d^{\log(p)}, \]
where $C$ depends only on $s$.

**Proof.** Set $g \in \mathbb{F}[x]$ to be a single variable polynomial obtained by Lemma 2.1. Then $g(x)$ is not the zero polynomial and $\deg(g) = r \leq d^2 + 1$. Let $I_\ell(p)$ be the number of monic irreducible polynomials in $\mathbb{F}_p[x]$ of degree equal to $\ell$. By a well-known result of Gauss (see for instance [Rom95, Corollary 9.2.3]), we have
\[ I_\ell(p) = \frac{1}{\ell} \sum_{d|\ell} \mu(d)p^{\ell/d}, \]
where
\[ \mu(d) = \begin{cases} 1, & d = 1 \\ (-1)^k, & d = p_1 \cdots p_k, \text{ } p_j \text{ are distinct primes}, \\ 0, & \text{otherwise}. \end{cases} \]

In particular, for large values of $\ell$, we have that
\[ \frac{1}{2\ell} p^\ell \leq I_\ell(p) \leq 2 \frac{1}{\ell} p^\ell. \]
Hence $I_\ell(p) \geq p^{\ell/2}$ for sufficiently large $\ell$. This inequality in tandem with
\[ \deg(g) \leq d^2 + 1 \]
gives that there exists some polynomial $h \in I_\ell^{\log(d)}(p)$ where $h$ does not divide $g$ and $C'$ only depends on $s$. The quotient $\mathbb{F}_p[x]/(h)$ has order less than or equal to $p^{C'\log(d)}$, and so we are done. \qed

## 3 Proof of Theorem 1.1

Before diving into the proof of Theorem 1.1, we give a brief sketch of the argument: for a finitely generated group, $\Gamma$, the field generated by the coefficients of the matrices over $\mathbb{Q}$ or $\mathbb{F}_p$ is finitely generated and so is a finite extension of a transcendental extension of some finite transcendence degree. Applying restriction of scalars (or corestriction), we can, at the cost of increasing the size of the matrices, assume the extension is purely transcendental. The coefficient ring generated over $\mathbb{Z}$ or $\mathbb{F}_p$ is then the ring $S$ from the previous section but with finitely many elements inverted. For a non-trivial element (which is represented by a matrix), we simply apply Lemma 2.2 or 2.3 to a non-trivial entry of that element after a scaling procedure. The map on matrices induced by the map of rings then provides us with a small finite quotient of $\Gamma$ that verifies the non-triviality of the given word. We then are able to write down bounds after relating the word length of the non-trivial word with the complexity of the non-trivial entry. With the sketch behind us, it is now time to dive.
For a given non-trivial word $S$ select a finite generating set $X$. For any ring homomorphism $T$, necessary, multiply this product by some fixed integer to ensure the coefficients of the resulting of the matrices in $\text{GL}(m,K)$. The first step in our proof follows that of Maltcev [M40]. Namely, we show that it suffices to restrict attention to a subring of $K$ that is more tenable. To that end, let $L$ be the field generated by the (finitely many) entries that appear in the elements of $X$. By construction, $L$ is finitely generated over $\mathbb{Q}$ or $\mathbb{F}_p$. Moreover, the field $L$ is a finite extension of $\mathbb{Q}(T)$ or $\mathbb{F}_p(T)$, where $T = \{x_1, \ldots, x_s\}$ is a transcendental basis (see, for instance, [Rom95, Corollary 3.3.3]). By choosing a finite basis for $L$ as a vector space over $\mathbb{Q}(T)$ or $\mathbb{F}_p(T)$, we can embed $L$ into $\text{Mat}(\mathbb{Q}(T), \mathbb{Q}(T))$ or $\text{Mat}(\mathbb{F}_p(T), \mathbb{F}_p(T))$. Applying this embedding on the coefficients of the matrices in $\text{GL}(m,L)$, we can view $\Gamma \leq \text{GL}(m,L) < \text{GL}(M,\mathbb{Q}(T))$ or $\text{GL}(M,\mathbb{F}_p(T))$, where $M = m[L : \mathbb{Q}(T)]$ or $m[L : \mathbb{F}_p(T)]$. For each generator $\gamma_i \in X$ and each matrix coefficient $(\gamma_i)_{jk}$, we have a finite number of elements in $\mathbb{Z}[T]$ or $\mathbb{F}_p[T]$ that are inverted; these are the elements in the denominators of the matrix coefficients of the generators. Ranging over all the generators and all of the matrix coefficients, we see that $\Gamma \leq \text{GL}(M,S')$, where $S'$ is obtained from $S = \mathbb{Z}[T]$ or $\mathbb{F}_p[T]$, with a finite number of inverted elements. Note that in the case of $\mathbb{Z}[T]$, we, if necessary, invert some coefficients of $\mathbb{Z}$ along with some polynomials in these extended coefficients and so the ring is of the form $\mathbb{Z}[1/p_1, \ldots, 1/p_a][T]$ with a finite number of inverted primes in the coefficients and a finite number of inverted polynomials. In either the case of $\mathbb{Z}$ or $\mathbb{F}_p$, there exists $\Phi(T) \in S$ such that for each generator $\gamma_i$, $\Phi(T)I_M \gamma_i \in \text{GL}(M,S)$. To obtain $\Phi(T)$, we can simply take the product of all of the denominators occurring in the coefficients $(\gamma_i)_{jk}$. In the case of $\mathbb{Z}$, we, if necessary, multiply this product by some fixed integer to ensure the coefficients of the resulting polynomials are integer valued and also ensure that all of the primes in $\mathbb{Z}$ that are inverted are also in the product; this last demand will be useful later. We will continue throughout to denote by $S'$, the above ring with $\Gamma \leq \text{GL}(M,S')$ and $\Phi(T) \in S$ such that $\Phi(T)I_M \gamma_i \in \text{GL}(M,S)$. We further note that every unit in $S'$ can be generated multiplicatively by the various factors of $\Phi(T)$.

Let $w$ be the word that gives $\gamma$ in terms of the generators $X$. We will instead consider $A = \gamma - I_M$. Since $X$ generates $\Gamma$ as a monoid and $\Phi(T)I_M$ is central, we have that

$$w(\Phi(T)X) = (\Phi(T))^{|\gamma|}w(X).$$

Hence, we can scale $A$ by $(\Phi(T))^{|\gamma|}I_M$ so that the resulting element is in $\text{Mat}(M,S)$. An off-diagonal coefficient of $(\Phi(T))^{|\gamma|}I_M A$ will be of the form

$$((\Phi(T))^{|\gamma|}I_M A)_{ij} = (\Phi(T))^{|\gamma|}\gamma_{ij}. $$

For any ring homomorphism $\phi : S' \to R$ where $R$ is a finite ring with identity and with

$$\phi((\Phi(T))^{|\gamma|}\gamma_{ij}) \neq 0,$$

we must have $\phi(\gamma_{ij}) \neq 0$ since $\Phi(T)$ is a unit in $S'$. The diagonal coefficients of $(\Phi(T))^{|\gamma|}I_M A$ have the form

$$((\Phi(T))^{|\gamma|}I_M A)_{ii} = (\Phi(T))^{|\gamma|}\gamma_{ii} - (\Phi(T))^{||}|\gamma_n|.$$

For any ring homomorphism $\phi : S' \to R$ where $R$ is a finite ring with identity and with

$$\phi((\Phi(T))^{|\gamma|}\gamma_{ii} - (\Phi(T))^{||}|\gamma_n|) \neq 0,$$
we must have
\[ \varphi(\gamma_i, -1) \neq 0 \]
since again \( \Phi(T) \) is a unit in \( S' \). In either case, the homomorphism
\[ \rho : \text{GL}(M, S') \to \text{GL}(M, R) \]
induced by \( \varphi : S' \to R \) will have \( \rho(\gamma) \neq 1 \). Therefore, it suffices to find a ring homomorphism \( \varphi: S' \to R \) that does not kill all of the coefficients of \( (\Phi(T))^{||\gamma||_X} I_{MA} \). For this task, since these coefficients are in \( S \), we can apply Lemma 2.2 or 2.3. Note that since those lemmas have target rings \( R \) that are finite fields and built into our assumptions, the image of \( \Phi(T) \) must be non-zero (hence a unit), these homomorphisms for \( S \to R \) extend to homomorphisms of \( S' \to R \); this is why we insisted that \( \Phi(T) \) involve enough units to generate the group of units of \( S' \).

Let \( A' \) be a non-zero coefficient of \( (\Phi(T))^{||\gamma||_X} I_{MA} \). In order to obtain quantified results, we must relate the word length of \( \gamma \) to the degree of the \( A' \). In the event \( S = \mathbb{Z}[T] \), we must relate the word length of \( \gamma \) to the maximum coefficients occurring in \( A' \) as well. For the maximum coefficient control, it is straightforward to see that there exists a constant \( \alpha \), depending on the generating set \( X \) such that
\[ \alpha_{i,j} < \alpha^{||\gamma||_X} \]
where \( \alpha_{i,j} \) is maximum of the absolute values of the coefficients of \( A' \); this fact was used previously in [B10]. For the required degree control, there exists a constant \( C_1 \) that depends only on the generating set \( X \) such that
\[ \text{deg}(A') < C_1 \||\gamma||_X \cdot \]

The reason is identical to the coefficient control except now degree is additive under multiplication, thus yielding linear control opposed to exponential control. Note that this control on degree holds over both \( \mathbb{Z} \) and \( \mathbb{F}_p \). With these relationships established, we press forward, separating into two cases again.

**Case 1.** \( A' \in \mathbb{Z}[T] \).

By Lemma 2.2 we can find a map of \( \mathbb{Z}[T] \) to a finite field \( R \) with \( |R| \leq C(\log(\alpha^{||\gamma||_X^2}) + ||\gamma||_X^{2s+2}) \). Note that in using Lemma 2.2 we need control on the coefficients of
\[ g(x) = A'(x^{n_1}, x^{n_2}, \ldots, x^{n_s}), \]
where \( n_i \leq \text{deg}(A') \). However, the maximum coefficient appearing in \( g(x) \) is certainly no bigger than \( \alpha^{||\gamma||_X^2} \). So regardless of \( A' \) being constant, we get an induced map of \( \text{GL}(M, S') \to \text{GL}(M, R) \) has order at most \( |R|^{M^2} \). Since the coefficient \( A' \) is not zero, the image of \( \gamma \) is not trivial and so
\[ \text{D}(\gamma) < C' ||\gamma||_X^{(2s+2)M^2}. \]

**Case 2.** \( A' \in \mathbb{F}_p[T] \).
The beginning of this case follows that of Case 1 with Lemma 2.3 playing the role of Lemma 2.2 (notice that the assumptions are slightly different). By increasing $C_1$ to a new constant $C_2$ (which depends only on $X$) we have

$$\deg(A') + 1 < C_2||\gamma||_X$$

and so we are in a situation where Lemma 2.3 applies. In either case, we obtain a field quotient of $S'$ to $R$ where $A'$ is not zero and $|R| < C'||\gamma||_X^{C_1 \log p}$ for a constant $C'$ depending only on $X$ and $|T|$. The induced map from $\text{GL}(M, S') \to \text{GL}(M, R)$ has order at most $|R|^{M^2} < (C')^{M^2} ||\gamma||_X^{CM^2 \log p}$. As $\gamma$ is nontrivial under this homomorphism, we see that

$$D_{\Gamma}(\gamma) < C ||\gamma||_X^{CM^2}$$

for some constant $C$ independent of $\gamma$. In particular, in each case, we have

$$D_{\Gamma}(\gamma) < C ||\gamma||_X^{d}$$

for constants $d, C$ independent of $\gamma$.

In both cases, we obtain the upper bound

$$F_{\Gamma,X}(n) \preceq n^d$$

for some constant $d$, as mandated by the theorem. \qed

4 Proof of Theorem 1.3

We proceed via contradiction and assume that $\Gamma$ is infinite. Specifically, fixing a generating set $X$ for $\Gamma$, we assume both that $\Gamma$ is infinite and the inequality

$$F_{\Gamma,X}(n) \preceq \log \log(n)$$

(1)

holds. With the aim of establishing a contradiction, we first note that

$$n \preceq w_{\Gamma,X}(n).$$

(2)

Second, we have the basic inequality

$$\log w_{\Gamma,X}(n) \preceq s_{\Gamma}(F_{\Gamma,X}(n)) \log F_{\Gamma,X}(n)$$

(3)

established in [BM10, Equation 1]. Note that this inequality holds for all generating sets $X$. Third, we have (see [LS03, Proposition 2.8])

$$\log s_{\Gamma}(n) \preceq (\log(n))^2.$$
In total, these inequalities yield the following string
\[
\log \log n \preceq \log \log w_{\Gamma,X}(n) \\
\preceq \log(s_{\Gamma}(F_{\Gamma,X}(n)) + \log \log F_{\Gamma,X}(n)) \\
\preceq (\log(F_{\Gamma,X}(n)))^2 + \log F_{\Gamma,X}(n) \\
\preceq (\log \log \log(n))^2,
\]
which is clearly impossible.

As mentioned in the introduction, if \( \Gamma \) contains an element of infinite order, according to [B10, Lemma 1.1, Theorem 2.2], we have \( \log(n) \preceq F_{\Gamma,X}(n) \). Thus, the question of whether or not the above bound is optimal concerns only infinite, residually finite, torsion groups.

**Question 4.1.** Does there exist an infinite, residually finite, torsion group \( \Gamma \) with strict asymptotic inequalities
\[
\log \log n \prec F_{\Gamma,X} \prec \log(n).
\]

One can certainly provide better lower bounds for \( F_{\Gamma,X}(n) \). If \( x = x(n) = \log F_{\Gamma,X}(n) \), we see from above that
\[
\log \log n \preceq x^2 + \log x.
\]
In particular, so long as
\[
\limsup_{n \to \infty} \frac{x^2}{\log \log n} = 0,
\]
we would derive a contradiction. Thus, we have:

**Scholium 4.2.** If
\[
\limsup_{n \to \infty} \frac{(\log F_{\Gamma,X}(n))^2}{\log \log n} = 0,
\]
then \( \Gamma \) is finite. In particular, \( e^{\log \log n} \preceq F_{\Gamma,X}(n) \) if \( \Gamma \) is infinite.

An example of a faster growing function that satisfies the condition of Scholium 4.2 is
\[
F(n) = (\log \log n)^{(\log \log \log n)^r},
\]
where \( r > 0 \) is a fixed constant. However, we do not know of any examples of infinite, residually finite groups with strict asymptotic inequality \( F_{\Gamma,X}(n) \prec \log n \) and so feel Question 4.1 is interesting regardless of the lower bound on growth.

## 5 Final remarks

There is geometric motivation for our work here and in [B10, B11, BM10, BM11]. For instance, let \( \Gamma \) be the fundamental group of a closed \( n \)-manifold \( M \) which admits a metric of negative
We have a bijection between conjugacy classes in $\Gamma$ with closed geodesics on $M$. Moreover, by the Švarc–Milnor Lemma, this bijection is bi-Lipschitz with respect to word and geodesic lengths. The function $D_{\Gamma}(\gamma)$ provides the degree of the smallest regular cover where the geodesic corresponding to $\gamma$ fails to lift. By Theorem \[1.1\] the existence of a faithful linear representation affords one control over how big this degree can be as a function of the length of the geodesic. In addition, lower bounds on the function $F_{\Gamma,X}$ give upper bounds on how quickly one can increase the systole of $M$ in finite regular covers. The growth threshold result, Theorem \[1.3\] gives a uniform lower bound on the degree of the regular covers where a geodesic fails to lift. Moreover, results like Gromov’s systolic inequality preclude one from growing the systole too quickly in finite covers, and the Girth inequality in \[BM11\] Equation 2] is analogous to a systolic inequality given the discussion here. It seems plausible that our work could be employed in systolic problems, though the fundamental group of the manifold would have more stringent restrictions than one might typically impose for these geometric problems. Consequently, the implementation of this ideology would likely only produce novel geometric results. We view this philosophical connection to be of greater interest.

**References**

[B10] K. Bou-Rabee, *Quantifying residual finiteness*, J. Algebra 323 (2010), 729–737.

[B11] K. Bou-Rabee, *Approximating a group by its solvable quotients*, New York J. Math. 17 (2011), 699–712.

[BK12] K. Bou-Rabee and T. Kaletha, *Quantifying residual finiteness of arithmetic groups*, Compos. Math. 148 (2012), 907–920.

[BM10] K. Bou-Rabee and D. B. McReynolds, *Bertrand’s postulate and subgroup growth*, J. of Algebra 324 (2010) 793–819.

[BM11] K. Bou-Rabee and D. B. McReynolds, *Asymptotic growth and least common multiples in groups*, Bull. Lond. Math. Soc. 43 (2011), 1059–1068.

[KM11] M. Kassabov and F. Matucci, *Bounding the residual finiteness of free groups* Proc. Amer. Math. Soc. 139 (2011), 2281–2286.

[LS03] A. Lubotzky and D. Segal, *Subgroup growth*, Birkhäuser 2003.

[M40] A. I. Mal’cev, *On the faithful representation of infinite groups by matrices*, Mat. SS. (N.S.) 50 (1940), 405–422.

[Rom95] S. Roman, *Field theory*, Springer–Verlag, 1995.