

Characterizing Linear Groups in Terms of Growth Properties

KHALID BOU-RABEE & D. B. MCREYNOLDS

ABSTRACT. Residual finiteness growth measures how well approximated a group is by its finite quotients. We prove that some related growth functions characterize linearity for a class of groups including all hyperbolic groups.

1. Introduction

Given a finitely generated, residually finite group Γ and a nontrivial $\gamma \in \Gamma$, we consider three functions that measure the difficulty of verifying that γ is non-trivial through homomorphisms to finite groups. The first function $D_\Gamma(\gamma)$ is the minimum $|Q|$, over all finite groups Q , such that there exists a homomorphism $\phi: \Gamma \rightarrow Q$ with $\phi(\gamma) \neq 1$. This function was introduced in [Bou10]. In this paper, we consider two variations of D_Γ obtained by restricting the class of groups Q . We define $L_\Gamma(\gamma)$ to be the minimum $|\text{GL}(n, \mathbf{F}_q)|$, over all $n \in \mathbf{N}$ and finite fields \mathbf{F}_q , such that there exists a homomorphism $\phi: \Gamma \rightarrow \text{GL}(n, \mathbf{F}_q)$ with $\phi(\gamma) \neq 1$. We define $S_\Gamma(\gamma)$ to be the minimal $|G|$, over all finite simple groups G , such that there exists a homomorphism $\phi: \Gamma \rightarrow G$ with $\phi(\gamma) \neq 1$. Note that we do not insist that any of the mentioned homomorphisms be surjective, though for D_Γ , the minimum $|Q|$ for an element γ always comes from a surjective homomorphism. Fixing a finite generating subset X for Γ , for each $m \in \mathbf{N}$, we define

$$\begin{aligned}
 F_\Gamma(m) &= \max_{\substack{\gamma \in \Gamma - \{1\}, \\ \|\gamma\|_X \leq m}} D_\Gamma(\gamma), \\
 F_{\Gamma, L}(m) &= \max_{\substack{\gamma \in \Gamma - \{1\}, \\ \|\gamma\|_X \leq m}} L_\Gamma(\gamma), \\
 F_{\Gamma, S}(m) &= \max_{\substack{\gamma \in \Gamma - \{1\}, \\ \|\gamma\|_X \leq m}} S_\Gamma(\gamma).
 \end{aligned}$$

For two functions $f, g: \mathbf{N} \rightarrow \mathbf{N}$, we write $f \preceq g$ if there exists a natural number C such that $f(m) \leq Cg(Cm)$ for all m and write $f \sim g$ when $f \preceq g$ and $g \preceq f$. The dependence of the above functions on the generating subset X is mild. Specifically, if Y is another generating subset, the associated functions for X, Y satisfy the equivalence relation \sim (see [Bou10, Lem 1.1]). In [BM15], we proved

Received May 11, 2015. Revision received November 21, 2015.

that if $\Gamma \leq \mathrm{GL}(n, \mathbf{K})$ for some $n \in \mathbf{N}$ and field \mathbf{K} , then $F_\Gamma(m) \leq m^D$ for $D \in \mathbf{N}$ depending only on n and \mathbf{K} . The main result of this article is the following characterization of linearity (Item (c)) for hyperbolic groups Γ in terms of the growth rates of $F_{\Gamma, L}, F_{\Gamma, S}$.

THEOREM 1.1. *Let Γ be a hyperbolic group. The following are equivalent:*

- (a) *There exists $D \in \mathbf{N}$ such that $F_{\Gamma, L}(m) \leq m^D$.*
- (b) *There exists $D' \in \mathbf{N}$ such that $F_{\Gamma, S}(m) \leq m^{D'}$.*
- (c) *There exist $n \in \mathbf{N}$, a field \mathbf{K} , and an injective homomorphism $\phi: \Gamma \rightarrow \mathrm{GL}(n, \mathbf{K})$.*

The first purely group theoretic characterization of (c), for fields \mathbf{K} with $\mathrm{char}(\mathbf{K}) = 0$, was established by Lubotzky [Lub88] and is based on the existence of uniformly powerful p -filtrations. Larsen [Lar01] proved that the abscissa of convergence of a certain subgroup ζ -function is the inverse of the minimal possible dimension of the Zariski closure over all finite-dimensional representations with infinite image. Though the representation that Larsen produces need not be faithful, his method is closely related to our approach, which is based on a well-known elementary characterization of (c); see Lemma 2.1 below.

2. Finite Groups

In this section, we record some results about finite groups that we will need for Theorem 1.1. Lemma 2.2 is the main technical result.

For a finite group G , set $m_1(G) = \max_{g \in G} |\langle g \rangle|$. For each prime $p \in \mathbf{N}$, set $r_p(G)$ to be the minimal positive integer n such that there exist $t \in \mathbf{N}$ and an injective homomorphism $\phi: G \rightarrow \mathrm{PGL}(n, \mathbf{F}_{p^t})$. We define $r(G) = \min_p \text{prime } r_p(G)$. We define $r_p^L(G), r^L(G)$ identically but with GL_n in place of PGL_n and note that if G is simple, then we have $r(G) \leq r^L(G)$. Further, since $\mathrm{PGL}_n(K) \leq \mathrm{GL}_{n^2}(K)$ for any field K , we have $r^L(G) \leq (r(G))^2$ for any group G .

Throughout, $\mathcal{F} = \{G_j\}_{j \in \mathbf{N}}$ will denote a set of finite groups. For our purposes, we will assume that the groups G_j are pairwise nonisomorphic. We say that \mathcal{F} has **bounded projective rank for some** $R \in \mathbf{N}$ if $r(G_j) \leq R$ for all $j \in \mathbf{N}$ and has **bounded rank for some** $R \in \mathbf{N}$ if $r^L(G_j) \leq R$ for all j . For any nonprincipal ultrafilter ω on \mathbf{N} , G_ω will denote the ultraproduct group $\prod_\omega G_j$ of \mathcal{F} relative to ω . The following is well known (see [Hal95] for instance).

LEMMA 2.1. *If $\mathcal{F} = \{G_j\}_{j \in \mathbf{N}}$ is a set of finite groups with either bounded rank or bounded projective rank for some $R \in \mathbf{N}$, then for any (nonprincipal) ultrafilter ω on \mathbf{N} , there is an injective homomorphism $\phi_\omega: G_\omega \rightarrow \mathrm{GL}(n, \mathbf{K})$ for some $n \in \mathbf{N}$ and field \mathbf{K} .*

The integer n can be taken to be R^2 in both cases since $r^L(G) \leq (r(G))^2$.

2.1. A Criterion for Bounded Rank

The following lemma was suggested to us by the referee.

LEMMA 2.2. Let $\mathcal{F} = \{G_j\}_{j \in \mathbb{N}}$ be a set of finite groups.

- (a) If $G_j = \text{GL}(n_j, \mathbf{F}_{q_j})$ for all j , then $\log |G_j| / \log(m_1(G_j))$ is unbounded if and only if $r^{\text{L}}(G_j)$ is unbounded.
- (b) If G_j is simple for all j , then $\log |G_j| / \log(m_1(G_j))$ is unbounded if and only if $r(G_j)$ is unbounded.

To prove this lemma, we have compiled the requisite information for certain families of finite groups. For a finite simple group of Lie type $G(\mathbf{F}_q)$ over \mathbf{F}_q with $q = p^f$, we refer the reader to [Che55; Car72; KL90], or [Wil12]. The orders of these groups are well known, and the bounds we provide are coarse; we will use these bounds in the sequel without specific mention. The monograph [KL90, Ch 5] contains a complete summary on bounds for $r(G)$ for both alternating groups and simple groups of Lie type; see Proposition 5.3.7, Table 5.4.C, and Corollary 5.4.14 in [KL90]. Lower bounds for $r_{p'}(G(\mathbf{F}_q))$ for primes $p' \neq p$ have been extensively studied; see [TZ96] and the references therein. The representation theory over fields with the defining characteristic p has also been extensively studied. In most cases, $r_p(G(\mathbf{F}_q)) = r(G(\mathbf{F}_q))$. The values for $r(G)$ given further are from Table 5.4.C and Corollary 5.4.14 in [KL90]. We write $f \approx g$ when $\lim_q \frac{f(q)}{g(q)} = C \in (0, \infty)$. For computational ease, with regard to the proof of Lemma 2.2, we have opted for simple, coarse inequalities over precise values/asymptotics in most situations. That is especially true for the values m_1 and $|G|$. Finally, our use of the classification of finite simple groups is at least that Lemma 2.2 holds for the sporadic groups. That is weaker than the assertion that there are only finitely many sporadic groups.

(1) **Alt(n) and $\text{GL}(n, \mathbf{F}_q)$.** For the alternating groups $\text{Alt}(n)$ for $n \geq 5$, we have:

$$\begin{aligned} |\text{Alt}(n)| &= n!/2, \\ \log(m_1(\text{Alt}(n))) &\approx \sqrt{n \log n}, \\ r(\text{Alt}(n)) &\leq n - 2, \quad r(\text{Alt}(n)) = n - 2 \quad \text{for } n \geq 9. \end{aligned}$$

The first estimate for m_1 is due to Landau [Lan03] (see (1) in [Mil87] for the above explicit asymptotics). We see that

$$C_1 \frac{\log(n!/2)}{\sqrt{n \log n}} \leq \frac{\log |\text{Alt}(n)|}{\log(m_1(\text{Alt}(n)))} < C_2 \frac{\log(n!/2)}{\sqrt{n \log n}} \tag{1}$$

for fixed constants $C_1, C_2 > 0$. For the groups $\text{GL}(n, \mathbf{F}_q)$ for $n \geq 1$ and $q = p^f$, we have

$$\begin{aligned} q^{n^2-1} &< |\text{GL}(n, \mathbf{F}_q)| < q^{n^2}, \\ q^{n-1} &< m_1(\text{GL}(n, \mathbf{F}_q)) < q^{n+1}, \\ n - 2 &\leq r^{\text{L}}(\text{GL}(n, \mathbf{F}_q)) \leq n. \end{aligned}$$

By Niven [Niv48] (see also [Dar05, Cor 2]), $m_1(\mathrm{GL}(n, \mathbf{F}_q)) = q^n - 1$. The lower bound for r^L is obtained by using derived/solvable lengths of solvable subgroups of $\mathrm{GL}(n, \mathbf{F}_q)$ (see Corollary on p. 152 of [Dix68]). We see that

$$n - 1 \leq \frac{\log |\mathrm{GL}(n, \mathbf{F}_q)|}{\log(m_1(\mathrm{GL}(n, \mathbf{F}_q)))} < \frac{n^2}{n - 1}. \quad (2)$$

(2) Type A_n . The groups of type $A_n(q)$ for $n \geq 1$ and $q = p^t$ are $\mathrm{PSL}(n + 1, q)$. We have

$$\begin{aligned} q^{n^2-3} &< |\mathrm{PSL}(n + 1, q)| < q^{n^2+2n+1}, \\ q^{n-2} &< m_1(\mathrm{PSL}(n + 1, q)) < q^{n+2}, \\ r(\mathrm{PSL}(n + 1, q)) &= r_p(\mathrm{PSL}(n + 1, q)) \\ &= n + 1 \quad (\text{for } (n, q) \neq (1, 4), (1, 5), (2, 2)). \end{aligned}$$

The numbers m_1 are explicitly calculated in [KS09, Table A.1]. We see that

$$\frac{(n^2 - 3)}{(n + 2)} < \frac{\log |\mathrm{PSL}(n + 1, q)|}{\log(m_1(\mathrm{PSL}(n + 1, q)))} < \frac{n^2 + 2n + 1}{(n - 2)}. \quad (3)$$

(3) Type 2A_n . The groups of type ${}^2A_n(q^2)$ for $n \geq 2$ and $q = p^t$ are $\mathrm{PSU}(n + 1, q)$. We have

$$\begin{aligned} q^{n^2+2n-1} &< |\mathrm{PSU}(n + 1, q)| < q^{n^2+2n+1}, \\ q^{n-4} &< m_1(\mathrm{PSU}(n + 1, q)) < q^{n+1}, \\ r(\mathrm{PSU}(n + 1, q)) &= r_p(\mathrm{PSU}(n + 1, q)) = n + 1 \quad (\text{for } (n, q) \neq (3, 2)). \end{aligned}$$

The numbers m_1 are explicitly calculated in [KS09, Table A.2]. We see that

$$\frac{n^2 + 2n - 1}{n + 1} < \frac{\log |\mathrm{PSU}(n + 1, q)|}{\log(m_1(\mathrm{PSU}(n + 1, q)))} < \frac{n^2 + 2n + 1}{n - 4}. \quad (4)$$

(4) Type B_n . The groups of type $B_n(q)$ for $n \geq 2$ and $q = p^t$ are given by $\mathrm{P}\Omega(2n + 1, q)$. We have

$$\begin{aligned} q^{2n^2+n-2} &< |\mathrm{P}\Omega(2n + 1, q)| < q^{2n^2+n+1}, \\ q^{n-2} &< m_1(\mathrm{P}\Omega(2n + 1, q)) < q^{n+2}, \\ r(\mathrm{P}\Omega(2n + 1, q)) &= r_p(\mathrm{P}\Omega(2n + 1, q)) = 2n + 1 \quad (\text{for odd } q \text{ and } n \neq 2), \\ r(\mathrm{P}\Omega(2n + 1, q)) &= r_p(\mathrm{P}\Omega(2n + 1, q)) = 2n \quad (\text{for } n = 2 \text{ or even } q). \end{aligned}$$

The numbers m_1 are explicitly calculated in [KS09, Table A.4] for odd q and [But13, Cor 4] when $q = 2^t$ (see also [Spi15] since $B_n(2^t) = C_n(2^t)$). We see that

$$\begin{aligned} \frac{2n^2 + n - 2}{n + 2} &< \frac{\log |\mathrm{P}\Omega(2n + 1, q)|}{\log(m_1(\mathrm{P}\Omega(2n + 1, q)))} \\ &< \frac{2n^2 + n + 1}{n - 2}. \end{aligned} \quad (5)$$

(5) Type C_n . The groups of type $C_n(q)$ for $n \geq 3$ and $q = p^t$ are given by $\text{PSp}(2n, q)$. We have

$$\begin{aligned} q^{2n^2+n-2} &< |\text{PSp}(2n, q)| < q^{2n^2+n+1}, \\ q^{n-2} &< m_1(\text{PSp}(2n, q)) < q^{n+2}, \\ r(\text{PSp}(2n, q)) &= r_p(\text{PSp}(2n, q)) = 2n. \end{aligned}$$

The numbers m_1 are explicitly calculated in [KS09, Table A.3] for q odd and [Spi15, Thm 1.1] (see also Lemma 2.3 in [Spi15]) when q is 2^t . We see that

$$\frac{2n^2 + n - 2}{n + 2} < \frac{\log |\text{PSp}(2n, q)|}{\log(m_1(\text{PSp}(2n, q)))} < \frac{2n^2 + n + 1}{n - 2}. \tag{6}$$

(6) Type D_n . The groups of type $D_n(q)$ for $n \geq 4$ and $q = p^t$ are given by $\text{P}\Omega^+(2n, q)$. We have

$$\begin{aligned} q^{2n^2-n-2} &< |\text{P}\Omega^+(2n, q)| < q^{2n^2-n+1}, \\ q^{n-2} &< m_1(\text{P}\Omega^+(2n, q)) < q^{n+2}, \\ r(\text{P}\Omega^+(2n, q)) &= r_p(\text{P}\Omega^+(2n, q)) = 2n \quad (\text{for } (n, q) \neq (4, 2)). \end{aligned}$$

The numbers m_1 are explicitly calculated in [KS09, Table A.5] for odd q and [But13, Cor 4] when $q = 2^t$. We see that

$$\frac{2n^2 - n - 2}{n + 2} < \frac{\log |\text{P}\Omega^+(2n, q)|}{\log(m_1(\text{P}\Omega^+(2n, q)))} < \frac{2n^2 - n + 1}{n - 2}. \tag{7}$$

(7) Type 2D_n . The groups of type ${}^2D_n(q^2)$ for $n \geq 4$ and $q = p^t$ are given by $\text{P}\Omega^-(2n, q)$. We have

$$\begin{aligned} q^{2n^2-n-2} &< |\text{P}\Omega^-(2n, q)| < q^{2n^2-n+1}, \\ q^{n-2} &< m_1(\text{P}\Omega^-(2n, q)) < q^{n+2}, \\ r(\text{P}\Omega^-(2n, q)) &= r_p(\text{P}\Omega^-(2n, q)) = 2n. \end{aligned}$$

The numbers m_1 are explicitly calculated in [KS09, Table A.6] for odd q and [But13, Cor 4] when $q = 2^t$. We see that

$$\frac{2n^2 - n - 2}{n + 2} < \frac{\log |\text{P}\Omega^-(2n, q)|}{\log(m_1(\text{P}\Omega^-(2n, q)))} < \frac{2n^2 - n + 1}{n - 2}. \tag{8}$$

Excluding alternating groups, in all the above simple families, $(\log |G(n, q)|) / (\log(m_1(G(n, q)))) \approx r(G(n, q))$ (in the parameter n).

(8) Exceptional groups Lie type. For the remaining exceptional finite simple groups of Lie type and cyclic groups of prime order, both $r(G)$ and $\log |G| / \log(m_1(G))$ are uniformly bounded above by 248; for the sporadic groups, 196,883 is an upper bound for both $r(G)$ and $\log |G| / \log(m_1(G))$. We have included a table summarizing the information for the exceptional and cyclic families. We refer the reader to Table 5.4.C and Corollary 5.4.14. in [KL90] for the values of r and to Table A.7 in [KS09] for the values of m_1 .

Table 1

Family	$ G \approx$	$m_1(G) \approx$	$r(G)$
$\mathbf{Z}/p\mathbf{Z}$, p prime	p	p	1
$E_6(q)$	q^{78}	q^6	27
$E_7(q)$	q^{133}	q^7	56
$E_8(q)$	q^{248}	q^8	248
$F_4(q)$	q^{52}	q^4	$25 \leq r(G) \leq 26$
$G_2(q)$	q^{14}	q^2	$6 \leq r(G) \leq 7$
${}^2E_6(q^2)$	q^{78}	q^6	27
${}^3D_4(q^3)$	q^{28}	q^4	8
${}^2B_2(2^{2j+1})$	q^5 , where $q = 2^{2j+1}$	q^2	4
${}^2G_2(3^{2j+1})$	q^2 , where $q = 3^{2j+1}$	q^2	7 (for $j \neq 1$)
${}^2F_4(2^{2j+1})$	q^{26} , where $q = 2^{2j+1}$	q^2	26 (for $j \neq 1$)

Proof of Lemma 2.2. In the case $G_j = \text{GL}(n_j, \mathbf{F}_{q_j})$, we see from (2) that $\log|G_j|/\log(m_1(G_j))$ is unbounded if and only if $r^L(G_j)$ is unbounded. In the case G_j is simple for all j , if either $r(G_j)$ or $\log|G_j|/\log(m_1(G_j))$ is unbounded, we know that there is a subsequence $\{G_{j_i}\}$ of $\{G_j\}$ where none of the terms are sporadic or in Table 1. Passing to another subsequence, we can assume that for all $i \in \mathbf{N}$, either $G_{j_i} = \text{Alt}(n_{j_i})$ or G_{j_i} is of Lie type and in precisely one of the families $A_{n_{j_i}}(q_{j_i}), {}^2A_{n_{j_i}}(q_{j_i}^2), B_{n_{j_i}}(q_{j_i}), C_{n_{j_i}}(q_{j_i}), D_{n_{j_i}}(q_{j_i}), {}^2D_{n_{j_i}}(q_{j_i}^2)$. In the alternating case, we see from (1) and the simple inequality $n! \geq (n/e)^n$ that $\log|G_{j_i}|/(m_1(G_{j_i}))$ is unbounded if and only if $r(G_{j_i})$ is unbounded. We see that the same holds for each of those families of Lie type by (3), (4), (5), (6), (7), (8), and the listed r -values. □

The following immediate consequence of Lemma 2.2 will be used later.

LEMMA 2.3. *For every $C > 0$, there exists $R(C) \in \mathbf{N}$ such that if $G = \text{GL}(n, \mathbf{F}_q)$ for some $n \in \mathbf{N}$ and finite field \mathbf{F}_q , and $\log|G|/\log(m_1(G)) \leq C$, then $r^L(G) \leq R$. Similarly, for every $C > 0$, there exists $R(C) \in \mathbf{N}$ such that if G is a finite simple group and $\log|G|/\log(m_1(G)) \leq C$, then $r(G) \leq R$.*

We require one additional result on finite simple groups.

LEMMA 2.4. *If $\mathcal{F} = \{G_j\}_{j \in \mathbf{N}}$ is a set of finite simple groups that has bounded projective rank for some $R \in \mathbf{N}$, then there is a $D(R) \in \mathbf{N}$ such that for each $j \in \mathbf{N}$, there are a finite field \mathbf{F}_{q_j} and an injective homomorphism $\psi_{G_j}: G_j \rightarrow \text{PSL}(R, \mathbf{F}_{q_j})$ with $|\text{PSL}(R, \mathbf{F}_{q_j})| \leq |G_j|^{D(R)}$.*

Proof. From (1) we see that only finitely many alternating groups can be in \mathcal{F} and set \mathcal{F}_0 to be the finite subset of sporadic and alternating groups in \mathcal{F} . There exists $D_1(\mathcal{F}_0) \in \mathbf{N}$ such that for each $G \in \mathcal{F}_0$, there exist a finite field \mathbf{F}_q and an injective

homomorphism $\psi_G : G \rightarrow \text{PSL}(R, \mathbf{F}_q)$ such that $|\text{PSL}(R, \mathbf{F}_q)| \leq |G|^{D_1}$. For any $G \in \mathcal{F} - \mathcal{F}_0$, either G is cyclic of prime order or of Lie type. If G is cyclic of prime order p , we have an injective homomorphism $\psi_G : G \rightarrow \text{PSL}(2, \mathbf{F}_p)$, and so $|\text{PSL}(2, \mathbf{F}_p)| < |G|^4$. If G is of Lie type with associated finite field \mathbf{F}_q , since $r(G) \leq R$, we see from the data in Subsection 2.1 that there exist $D_2(R) \in \mathbf{N}$ and an injective homomorphism $\psi_G : G \rightarrow \text{PSL}(R, \mathbf{F}_q)$ such that $|\text{PSL}(R, \mathbf{F}_q)| \leq |G|^{D_2}$; $D_2 = R^2$ works. Finally, set $D = \max\{D_1, D_2, 4\}$. \square

3. Infinite Groups

In this section, we establish the main technical result Proposition 3.6. From Proposition 3.6 we obtain Corollary 3.9, which we will use in the proof of Theorem 1.1. We also introduce malabelian and uniformly malabelian groups.

Given a group Γ and a set $\mathcal{F} = \{G_j\}_{j \in \mathbf{N}}$ of finite groups, we say that Γ is **residually** \mathcal{F} if for each nontrivial $\gamma \in \Gamma$, there exist $G \in \mathcal{F}$ and a homomorphism $\phi : \Gamma \rightarrow G$ such that $\phi(\gamma) \neq 1$. We say that Γ is **fully residually** \mathcal{F} if for each finite set $T \subset \Gamma - \{1\}$, there exist $G \in \mathcal{F}$ and a homomorphism $\phi : \Gamma \rightarrow G$ such that $\ker \phi \cap T = \emptyset$. If $\mathcal{F} = \{\text{GL}(n, \mathbf{F}_q)\}$ or $\{\text{PGL}(n, \mathbf{F}_q)\}$ for $n \in \mathbf{N}$ fixed and varying finite fields \mathbf{F}_q , we will simply say Γ is (fully) residually GL_n or PGL_n ; these families have bounded rank and bounded projective rank, respectively. The following result is also well known (see Theorem 3.11 in [Hal95] for instance).

LEMMA 3.1. *Let Γ be a countable group and $\mathcal{F} = \{G_j\}_{j \in \mathbf{N}}$ be a set of finite groups that has bounded rank or bounded projective rank. If Γ is fully residually \mathcal{F} , then there exist $n \in \mathbf{N}$, a field \mathbf{K} , and an injective homomorphism $\phi : \Gamma \rightarrow \text{GL}(n, \mathbf{K})$.*

Proof. We begin by enumerating $\Gamma = \{\gamma_0, \gamma_1, \dots\}$ with $\gamma_0 = 1$ and set $T_i = \{\gamma_k\}_{k=1}^i$. By assumption, for each $i \in \mathbf{N}$, there are a $j_i \in \mathbf{N}$ and a homomorphism $\phi_{j_i} : \Gamma \rightarrow G_{j_i}$ such that $\phi_{j_i}(\gamma) \neq 1$ for all $\gamma \in T_i$. Setting $\mathcal{F}_0 = \{G_{j_i}\}_{i \in \mathbf{N}}$, for any non-principal ultrafilter ω on \mathbf{N} , we have an injective homomorphism $\phi_\omega : \Gamma \rightarrow \prod_\omega G_{j_i}$. The proof is completed with an application of Lemma 2.1. \square

3.1. Malabelian Groups

Given a finite subset $T \subset \Gamma - \{1\}$, we have an associated normal subgroup $\Delta_T = \bigcap_{\gamma \in T} \overline{\langle \gamma \rangle}$, where $\overline{\langle \gamma \rangle}$ denotes the normal closure of the cyclic subgroup $\langle \gamma \rangle$. We call any nontrivial element in Δ_T a **common multiple** for T in Γ . The following lemma can be found in [BM11, Lemma 3.1].

LEMMA 3.2. *Let Γ be a group, $T \subset \Gamma - \{1\}$ a finite subset, and η a common multiple for T in Γ . If G is a group and $\phi : \Gamma \rightarrow G$ is a homomorphism with $\phi(\eta) \neq 1$, then $\phi(\gamma) \neq 1$ for all $\gamma \in T$.*

We say that a group Γ is **malabelian** if for any pair of (not necessarily distinct) nontrivial elements $\gamma, \eta \in \Gamma$, there exists $\mu \in \Gamma$ such that $[\mu^{-1}\gamma\mu, \eta] \neq 1$. In other words, every nontrivial conjugacy class in Γ has a trivial centralizer.

LEMMA 3.3. *If Γ is a malabelian group and $T \subset \Gamma - \{1\}$ a finite subset, then $\Delta_T \neq 1$, and T has a common multiple.*

Proof. Without loss of generality, we can assume that $|T| = 2^j$ for some integer j since we can enlarge T by adding nontrivial elements from Γ . We proceed via induction on j . Enumerating $T = \{\gamma_1, \dots, \gamma_{2^j}\}$, for each $1 \leq i \leq 2^{j-1}$, we select $\mu_i \in \Gamma$ such that $\gamma_{i,1} = [\mu_i^{-1} \gamma_{2i-1} \mu_i, \gamma_{2i}] \neq 1$. We obtain a new subset $T_1 = \{\gamma_{i,1}\}_{i=1}^{2^{j-1}}$. By induction, T_1 has a common multiple in Γ , and it follows from our selection of $\gamma_{i,1}$ that this common multiple is also a common multiple for T . \square

LEMMA 3.4. *If Γ is a countable, malabelian group that is residually \mathcal{F} for some set \mathcal{F} of finite groups, then Γ is fully residually \mathcal{F} .*

Proof. Given a finite subset $T \subset \Gamma - \{1\}$, since Γ is malabelian, by Lemma 3.3 there exists a common multiple γ_T for T in Γ . By assumption, there exist $G \in \mathcal{F}$ and a homomorphism $\phi_T: \Gamma \rightarrow G$ such that $\phi_T(\gamma_T) \neq 1$. By Lemma 3.2, $\phi_T(\gamma) \neq 1$ for all $\gamma \in T$, and thus Γ is fully residually \mathcal{F} . \square

3.2. Uniformly Malabelian Groups

For a finitely generated group Γ , a fixed finite generating subset X , and $K \in \mathbf{N}$, we say that Γ is **K -malabelian with respect to X** if for every pair of nontrivial $\gamma, \eta \in \Gamma$, there exists $\mu \in \Gamma$ with $\|\mu\|_X \leq K$ such that $[\mu^{-1} \gamma \mu, \eta] \neq 1$. If Γ is K -malabelian with respect to a finite generating subset X and Y is another finite generating subset for Γ , then Γ is K' -malabelian with respect to Y for some $K' \in \mathbf{N}$. We say that Γ is **uniformly malabelian** if Γ is K -malabelian with respect to X for some finite generating subset X and $K \in \mathbf{N}$. For a finite subset $T \subset \Gamma - \{1\}$, if T has a common multiple in Γ , we define the **least common multiple length** of T relative to X to be $\text{LCM}_X(T) = \min_{\eta \in \Delta_T - \{1\}} \|\eta\|_X$. We refer to any element $\eta \in \Delta_T$ with $\|\eta\|_X = \text{LCM}_X(T)$ as a **least common multiple** for the subset T .

LEMMA 3.5. *If Γ is a finitely generated, uniformly malabelian group and X a finite generating subset, then there exists $C(X) \in \mathbf{N}$ such that if $T \subset \Gamma - \{1\}$ with $|T| = t$ and $\|\gamma\|_X \leq d$ for all $\gamma \in T$, then $\text{LCM}_X(T) \leq Cdt^2$.*

As the proof of Lemma 3.5 is similar to the proof of Proposition 4.1 in [BM11], we have omitted it.

PROPOSITION 3.6. *Let Γ be a finitely generated, uniformly malabelian group with an element of infinite order.*

- (a) *If there exists $D \in \mathbf{N}$ such that $F_{\Gamma, L}(m) \leq m^D$, then there exists $n(D) \in \mathbf{N}$ such that Γ is residually GL_n .*

- (b) If there exists $D' \in \mathbf{N}$ such that $F_{\Gamma, S}(m) \leq m^{D'}$, then there exists $R(D') \in \mathbf{N}$ such that Γ is residually \mathcal{F} for a set of finite simple groups that has bounded projective rank for R .

Proof. Before proving (a) and (b), we require some common setup for both. We first fix an infinite-order element γ_0 and a finite generating subset X . Since Γ is uniformly malabelian, there exists $K \in \mathbf{N}$ such that Γ is K -malabelian with respect to X . Given a nontrivial $\gamma \in \Gamma$, there exists $\mu_0 \in \Gamma$ such that $[\mu_0^{-1}\gamma\mu_0, \gamma_0] \neq 1$ and $\|\mu_0\|_X \leq K$. Set $T_j = \{[\mu_0^{-1}\gamma\mu_0, \gamma_0], \gamma_0^2, \dots, \gamma_0^j\}$ and note that $|T_j| = j$. Moreover, there exists $j(\gamma) \in \mathbf{N}$ such that if $j \geq j(\gamma)$, then $\|\tau\|_X \leq j\|\gamma_0\|_X$ for all $\tau \in T_j$. By Lemma 3.5 there exists $C_1(X) \in \mathbf{N}$ such that if η_j is a least common multiple of T_j and $j \geq j(\gamma)$, then

$$\|\eta_j\|_X \leq C_1\|\gamma_0\|_X j^3 = C_2 j^3, \tag{9}$$

where $C_2 = C_1\|\gamma_0\|_X$.

Part (a). We must show that there exists $n \in \mathbf{N}$ such that for every nontrivial $\gamma \in \Gamma$, there exist a finite field \mathbf{F}_q and a homomorphism $\phi: \Gamma \rightarrow \text{GL}(n, \mathbf{F}_q)$ such that $\phi(\gamma) \neq 1$. By assumption, there exists $C_3 \in \mathbf{N}$ such that for each $j \in \mathbf{N}$, there exist $n_j \in \mathbf{N}$, a finite field \mathbf{F}_{q_j} , and a homomorphism $\phi_j: \Gamma \rightarrow \text{GL}(n_j, \mathbf{F}_{q_j})$ with $\phi_j(\eta_j) \neq 1$ and

$$|\text{GL}(n_j, \mathbf{F}_{q_j})| \leq C_3\|\eta_j\|_X^D. \tag{10}$$

Combining (9) and (10), for $C_4 = C_2^D C_3$ and $j \geq j(\gamma)$, we see that $|\text{GL}(n_j, \mathbf{F}_{q_j})| \leq C_4 j^{3D}$. By construction, $m_1(\text{GL}(n_j, \mathbf{F}_{q_j})) \geq j$, and so

$$\frac{\log |\text{GL}(n_j, \mathbf{F}_{q_j})|}{\log(m_1(\text{GL}(n_j, \mathbf{F}_{q_j})))} \leq 3D + \frac{\log(C_4)}{\log j}. \tag{11}$$

Since the right-hand side of (11) is uniformly bounded above, by Lemma 2.3 there exists $R(D, C_4) \in \mathbf{N}$ such that $r^L(\text{GL}(n_j, \mathbf{F}_{q_j})) \leq R$ for all $j \geq j(\gamma)$. Note that since the right-hand side of (11) is independent of Γ , the constant $R(D, C_4)$ is independent of Γ . Setting $n = R(D, C_4)$, we see that Γ is residually GL_n since $R(D, C_4)$ is independent of γ .

Part (b). By assumption, there exists $C_5 \in \mathbf{N}$ such that for each $j \in \mathbf{N}$, there exist a finite simple group G_j and homomorphism $\phi_j: \Gamma \rightarrow G_j$ with $\phi_j(\eta_j) \neq 1$ and

$$|G_j| \leq C_5\|\eta_j\|_X^D. \tag{12}$$

Combining (9) and (12), for $C_6 = C_2^D C_5$ and $j \geq j(\gamma)$, we have $|G_j| \leq C_6 j^{3D}$. As before, $m_1(G_j) \geq j$, and so

$$\frac{\log |G_j|}{\log(m_1(G_j))} \leq 3D + \frac{\log(C_6)}{\log j}. \tag{13}$$

Since the right-hand of (13) is uniformly bounded above, by Lemma 2.3 there exists $R(D, C_6) \in \mathbf{N}$ such that $r(G_j) \leq R$ for all $j \geq j(\gamma)$. Note that since the right-hand side of (13) is independent of Γ , the constant $R(D, C_6)$ is independent of Γ . Consequently, Γ is residually \mathcal{F} for some set of finite simple groups that has bounded projective rank. □

COROLLARY 3.7. *Let Γ be a finitely generated, uniformly malabelian group with an element of infinite order.*

- (a) *If there exists $D \in \mathbf{N}$ such that $F_{\Gamma, L}(m) \preceq m^D$, then there exist $n(D) \in \mathbf{N}$, a field \mathbf{K} , and an injective homomorphism $\phi: \Gamma \rightarrow \text{GL}(n, \mathbf{K})$. Moreover, $\phi(\Gamma) \cap (\mathbf{K}^\times \cdot I_n) = I_n$.*
- (b) *If there exists $D' \in \mathbf{N}$ such that $F_{\Gamma, S}(m) \preceq m^{D'}$, then there exist $n(D') \in \mathbf{N}$, a field \mathbf{K} , and an injective homomorphism $\phi: \Gamma \rightarrow \text{GL}(n, \mathbf{K})$. Moreover, $\phi(\Gamma) \cap (\mathbf{K}^\times \cdot I_n) = I_n$.*

Proof. The first parts of (a) and (b) follow from Lemma 3.1, Lemma 3.4, and Proposition 3.6. In either case, we have an injective homomorphism $\phi: \Gamma \rightarrow \text{GL}(n, \mathbf{K})$ for some $n \in \mathbf{N}$ and field \mathbf{K} . Moreover, it follows from the construction of ϕ that $\phi(\gamma) \notin \mathbf{K}^\times \cdot I_n$ for any nontrivial $\gamma \in \Gamma$ since $\phi_j(\gamma) \notin Z(\phi_j(\Gamma))$, where $Z(\phi_j(\Gamma))$ is the center of $\phi_j(\Gamma)$. □

The converse of Corollary 3.7 follows from the proof of Theorem 1.1 in [BM15] and does not require that Γ be malabelian. Since $\text{GL}(n, \mathbf{K}) < \text{SL}(n + 1, \mathbf{K})$, we will assume that $\Gamma < \text{SL}(n, \mathbf{K})$ in (b).

PROPOSITION 3.8. *Let Γ be a finitely generated group.*

- (a) *If $\Gamma \leq \text{GL}(n, \mathbf{K})$ for some $n \in \mathbf{N}$ and field \mathbf{K} , then there exists $D(n, \mathbf{K}) \in \mathbf{N}$ such that $F_{\Gamma, L}(m) \preceq m^D$.*
- (b) *If $\Gamma \leq \text{SL}(n, \mathbf{K})$ for some $n \in \mathbf{N}$ and field \mathbf{K} with $\Gamma \cap (\mathbf{K}^\times \cdot I_n) = I_n$, then there exists $D(n, \mathbf{K}) \in \mathbf{N}$ such that $F_{\Gamma, S}(m) \preceq m^D$.*

Proof. Part (a) follows immediately from the proof Theorem 1.1 of [BM15]. For (b), given a nontrivial element $\gamma \in \Gamma$, by [BM15] there exist $C_0, D_0 \in \mathbf{N}$ (independent of γ), a finite field \mathbf{F}_q with $q \leq C_0 \|\gamma\|_X^{D_0}$, and a homomorphism $\phi_q: \Gamma \rightarrow \text{SL}(n, \mathbf{F}_q)$ with $\phi_q(\gamma) \neq 1$. Moreover, since $\gamma \notin \mathbf{K}^\times \cdot I_n$, we can arrange for $\phi_q(\gamma) \notin \mathbf{F}_q^\times \cdot I_n$. Composing ϕ_q with the homomorphism $\text{SL}(n, \mathbf{F}_q) \rightarrow \text{PSL}(n, \mathbf{F}_q)$, we obtain $P\phi_q: \Gamma \rightarrow \text{PSL}(n, \mathbf{F}_q)$ with $P\phi_q(\gamma) \neq 1$. By selection of q we have $|\text{PSL}(n, \mathbf{F}_q)| \leq q^{n^2} \leq C_0^{n^2} \|\gamma\|_X^{D_0 n^2}$. Since γ was arbitrary, we have $F_{\Gamma, S}(m) \preceq m^{D_0 n^2}$. □

Combining Corollary 3.7 and Proposition 3.8, we obtain the following corollary.

COROLLARY 3.9. *If Γ is a finitely generated, uniformly malabelian group with an element of infinite order, then the following are equivalent:*

- (a) *There exists $D \in \mathbf{N}$ such that $F_{\Gamma, L}(m) \preceq m^D$.*
- (b) *There exists $D' \in \mathbf{N}$ such that $F_{\Gamma, S}(m) \preceq m^{D'}$.*
- (c) *There exist $n \in \mathbf{N}$, a field \mathbf{K} , and an injective homomorphism $\phi: \Gamma \rightarrow \text{GL}(n, \mathbf{K})$.*

We note that the equivalence of (a) and (c) is independent of the classification of finite simple groups whereas the equivalence of (b) and (c) is not.

4. Proof of Theorem 1.1

In the proof of Theorem 1.1, we will need to relate the functions $F_{\Gamma,L}$, $F_{\Gamma_0,L}$, and $F_{\Gamma,S}$, $F_{\Gamma_0,S}$ for a finitely generated group Γ and a finite index subgroup Γ_0 .

PROPOSITION 4.1. *Let Γ be a finitely generated group, and $\Gamma_0 \leq \Gamma$ a finite index subgroup.*

- (a) *There exists $D \in \mathbb{N}$ such that $F_{\Gamma,L}(m) \leq m^D$ if and only if there exists $D' \in \mathbb{N}$ such that $F_{\Gamma_0,L}(m) \leq m^{D'}$.*
- (b) *If Γ_0 is uniformly malabelian with an element of infinite order, then there exists $D \in \mathbb{N}$ such that $F_{\Gamma,S}(m) \leq m^D$ if and only if there exists $D' \in \mathbb{N}$ such that $F_{\Gamma_0,S}(m) \leq m^{D'}$.*

Proof. The direct implications for (a) and (b) are straightforward. For the reverse implications in (a) and (b), we assume that Γ_0 is normal since we can replace Γ_0 with a finite index subgroup $\Gamma_1 \leq \Gamma_0$ with $\Gamma_1 \triangleleft \Gamma$.

For (a), given a nontrivial $\gamma \in \Gamma$, we split into two cases. First, if $\gamma \in \Gamma - \Gamma_0$, then we have $\phi_0: \Gamma \rightarrow Q_0 = \Gamma/\Gamma_0$ with $\phi_0(\gamma) \neq 1$. Fixing $n_0 \in \mathbb{N}$ and a finite field \mathbf{F}_{q_0} with $Q_0 \leq \text{GL}(n_0, \mathbf{F}_{q_0})$, we see that $L_\Gamma(\gamma) \leq |\text{GL}(n_0, \mathbf{F}_{q_0})|$. If $\gamma \in \Gamma_0$, then by assumption there exist $n \in \mathbb{N}$, a finite field \mathbf{F}_q , and a homomorphism $\phi: \Gamma_0 \rightarrow \text{GL}(n, \mathbf{F}_q)$ with $\phi(\gamma) \neq 1$ and $|\text{GL}(n, \mathbf{F}_q)| \leq C_0 \|\gamma\|^{D'}$ for $C_0 \in \mathbb{N}$ that is independent of γ . Setting $\phi' = \text{Ind}_{\Gamma_0}^\Gamma(\phi)$, we have $\phi': \Gamma \rightarrow \text{GL}(n\ell_0, \mathbf{F}_q)$ with $\phi'(\gamma) \neq 1$, where $\ell_0 = [\Gamma : \Gamma_0]$. Since $|\text{GL}(n\ell_0, \mathbf{F}_q)| \leq q^{n^2\ell_0^2} \leq |\text{GL}(n, \mathbf{F}_q)|^{2\ell_0^2}$, we see that $L_\Gamma(\gamma) \leq C \|\gamma\|^{2\ell_0^2 D'}$ for some $C \in \mathbb{N}$ that is independent of γ .

For (b), if $\gamma \in \Gamma - \Gamma_0$, then we argue as in (a). When $\gamma \in \Gamma_0$, additional work is required. By Proposition 3.6 there exists a set of finite simple groups \mathcal{F} such that Γ_0 is residually \mathcal{F} and \mathcal{F} has bounded projective rank for some $R \in \mathbb{N}$. By Lemma 2.4 there exists $D''(R) \in \mathbb{N}$ such that for each $G \in \mathcal{F}$, there are a finite field \mathbf{F}_q and an injective homomorphism $\psi_G: G \rightarrow \text{PSL}(R, \mathbf{F}_q)$ with $|\text{PSL}(R, \mathbf{F}_q)| \leq |G|^{D''}$. For $\gamma \in \Gamma_0$, by assumption there exist a finite simple group $G \in \mathcal{F}$ and a homomorphism $\phi_1: \Gamma_0 \rightarrow G$ such that $\phi_1(\gamma) \neq 1$ and $|G| \leq C'' \|\gamma\|^{D'}$ for some $C'' \in \mathbb{N}$ that is independent of γ . Composing ϕ_1 and ψ_G , we have $\phi_2: \Gamma_0 \rightarrow \text{PSL}(R, \mathbf{F}_q)$ with $\phi_2(\gamma) \neq 1$. Setting $\phi = \text{Ind}_{\Gamma_0}^\Gamma(\phi_2)$, we obtain $\phi: \Gamma \rightarrow \text{PSL}(R\ell_0, \mathbf{F}_q)$. Since G is simple and $\phi_1(\gamma) \neq 1$, we see that $\phi(\gamma) \neq 1$. Since

$$\begin{aligned} |\text{PSL}(R\ell_0, \mathbf{F}_q)| &\leq q^{R^2\ell_0^2} \leq |\text{PSL}(R, \mathbf{F}_q)|^{R^2\ell_0^2} \\ &\leq |G|^{D''R^2\ell_0^2} \leq (C'')^{D''R^2\ell_0^2} \|\gamma\|^{D'D''R^2\ell_0^2}, \end{aligned}$$

we see that $S_\Gamma(\gamma) \leq C' \|\gamma\|^D$ for $D = D'D''R^2\ell_0^2$ and $C' = (C'')^{D/D'}$. □

The malabelian assumption in (b) seems like overkill but gives the needed control on $r(G)$ to use induction. We could instead take a wreath product with Γ/Γ_0 and G , but from that we still need to find a reasonably small finite simple group that contains it; the left regular representation is too large.

Proof of Theorem 1.1. The theorem is straightforward for elementary hyperbolic groups, and so we assume that Γ is nonelementary. If Γ is not residually finite, then by Mal'cev [Mal40], Γ does not satisfy (c). Moreover, both functions $F_{\Gamma,L}(m)$ and $F_{\Gamma,S}(m)$ are not defined for sufficiently large m .

If Γ is residually finite, then there exists a torsion-free, finite index subgroup $\Gamma_0 \leq \Gamma$, and it is straightforward to see that Γ_0 is uniformly malabelian (see [BH99, p. 459–462]). By Corollary 3.9 properties (a), (b), and (c) are equivalent for Γ_0 . By Proposition 4.1, Γ_0 satisfies (a) and (b) if and only if Γ satisfies (a) and (b). That Γ satisfies (c) if and only if Γ_0 satisfies (c) follows from induction/restriction. \square

ACKNOWLEDGMENTS. The authors are grateful to Noel Brady, Mikhail Ershov, Benson Farb, Daniel Groves, Richard Kent, Michael Larsen, Lars Louder, Denis Osin, Alan Reid, Ignat Sokoro, and Henry Wilton for conversations on this topic. The first author was partially supported by NSF RTG Grant DMS-0602191, NSF Grant DMS-1405609, and by Ventotene 2013. The second author was partially supported by NSF grants DMS-1105710 and DMS-1408458. Finally, a huge debt is owed to the referee for numerous helpful suggestions and corrections to an earlier draft of the paper.

References

- [Bou10] K. Bou-Rabee, *Quantifying residual finiteness*, J. Algebra 323 (2010), 729–737.
- [BM11] K. Bou-Rabee and D. B. McReynolds, *Asymptotic growth and least common multiples in groups*, Bull. Lond. Math. Soc. 43 (2011), 1059–1068.
- [BM15] ———, *Extremal behavior of divisibility functions*, Geom. Dedicata 175 (2015), 407–415.
- [BH99] M. R. Bridson and A. Haefliger, *Metric spaces of non-positive curvature*, Springer-Verlag, Berlin, 1999.
- [But13] A. A. Buturlakin, *Spectra of finite symplectic and orthogonal groups*, Siberian Adv. Math. 21 (2011), 176–210.
- [Car72] R. W. Carter, *Simple groups of Lie type*, Wiley and Son, New York, 1972.
- [Che55] C. Chevalley, *Sur certains groupes simples*, Tôhoku Math. J. (2) 7 (1955), 14–66.
- [Dar05] M. R. Darafsheh, *Order of elements in the groups related to the general linear group*, Finite Fields Appl. 11 (2005), 738–747.
- [Dix68] J. D. Dixon, *The solvable length of a solvable linear group*, Math. Z. 107 (1968), 151–158.
- [Hal95] J. I. Hall, *Locally finite simple groups of finitary linear transformations*, NATO Sci. Peace Secur. Ser. C Environ. Secur. 471 (1995), 147–188.
- [KS09] W. M. Kantor and A. Seress, *Large element orders and the characteristic of Lie-type simple groups*, J. Algebra 322 (2009), 802–832.
- [KL90] P. Kleidman and M. Liebeck, *The subgroup structure of the finite classical groups*, Cambridge University Press, Cambridge, 1990.
- [Lan03] E. Landau, *Über die Maximalordnung der Permutationen gegebenen Grades*, Arch. Math. Phys. Ser. (3) 5 (1903), 92–103.
- [Lar01] M. Larsen, *How often is $84(g-1)$ achieved?*, Israel J. Math. 126 (2001), 1–16.

- [Lub88] A. Lubotzky, *A group theoretic characterization of linear groups*, J. Algebra 113 (1988), 207–214.
- [Mal40] A. I. Mal'cev, *On the faithful representation of infinite groups by matrices*, Mat. SS. (N. S.) 8(50) (1940), 405–422.
- [Mil87] W. Miller, *The maximum order of an element of a finite symmetric group*, Amer. Math. Monthly 94 (1987), 497–506.
- [Niv48] I. Niven, *Fermat's theorem for matrices*, Duke Math. J. 15 (1948), 823–826.
- [Spi15] P. Spiga, *The maximum order of the elements of a finite symplectic group of even characteristic*, Comm. Algebra 43 (2015), 1417–1434.
- [TZ96] P. H. Tiepa and A. E. Zalesskii, *Minimal characters of the finite classical groups*, Comm. Algebra 24 (1996), 2093–2167.
- [Wil12] R. A. Wilson, *The finite simple groups*, Springer-Verlag, London, 2009.

K. Bou-Rabee
The City College of New York
New York, NY
USA

D. B. McReynolds
Purdue University
West Lafayette, IN
USA

khalid.math@gmail.com

dmcreyno@purdue.edu