Received: 13 September 2023 | Revised: 13 February 2024 | Accepted: 13 March 2024

DOI: 10.1112/blms.13058

RESEARCH ARTICLE

Bulletin of the London Mathematical Society

On the length of nonsolutions to equations with constants in some linear groups

Henry Bradford[1] | **Jakob Schneider**[2] | **Andreas Thom**[2]

[1]Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, Centre for Mathematical Sciences, Cambridge, UK

[2]Institut für Geometrie, TU Dresden, Faculty of Mathematics, Dresden, Germany

Correspondence
Henry Bradford, Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, Centre for Mathematical Sciences, Wilberforce Road, Cambridge, CB3 0WB, UK.
Email: hb470@cam.ac.uk

Abstract

We show that for any finite-rank–free group Γ, any word-equation in one variable of length n with constants in Γ fails to be satisfied by some element of Γ of word-length $O(\log(n))$. By a result of the first author, this logarithmic bound cannot be improved upon for any finitely generated group Γ. Beyond free groups, our method (and the logarithmic bound) applies to a class of groups including $\mathrm{PSL}_d(\mathbb{Z})$ for all $d \geqslant 2$, and the fundamental groups of all closed hyperbolic surfaces and 3-manifolds. Finally, using a construction of Nekrashevych, we exhibit a finitely generated group Γ and a sequence of word-equations with constants in Γ for which every nonsolution in Γ is of word-length strictly greater than logarithmic.

MSC 2020
20F69, 20F70 (primary), 20F65, 20F67 (secondary)

1 | INTRODUCTION

For Γ any group and any $g \in \Gamma$, there is a unique homomorphism $\pi_g : \Gamma * \mathbb{Z} \to \Gamma$ restricting to the identity on Γ and sending a specified generator x of $\mathbb{Z}$ to g. We call w a *mixed identity* (or an *identity with constants*) for Γ if w is nontrivial but $\pi_g(w) = e_\Gamma$ for all $g \in \Gamma$. Equivalently, we may define a *word-map* $w : \Gamma \to \Gamma$ by $w(g) = \pi_g(w)$; w is then a mixed identity for Γ if and only if $w^{-1}(e_\Gamma) = \Gamma$.

We describe Γ as *MIF* (mixed identity-free) if there are no mixed identities for Γ in $\Gamma * \mathbb{Z}$. Nonabelian free groups are MIF (a fact due to Baumslag [4]), as more generally are all torsion-free nonelementary Gromov hyperbolic groups (see [1] and the references therein). Being MIF imposes significant structural restrictions on Γ: An MIF group has no nontrivial finite conjugacy classes, and admits no nontrivial decomposition as a direct product. Moreover, MIF is inherited by nontrivial normal subgroups.

Given a finite generating set S for Γ, if Γ is MIF, then for any $w \in \Gamma * \mathbb{Z}$, there exists $g \in \Gamma$ of minimal word-length $|g|_S$ satisfying $w(g) \neq e$. Intuitively, the greater this minimal word-length should be, the harder it is to verify that w is not a mixed identity for Γ. The goal of this paper is to study how $|g|_S$ can depend on the length of w. Following [5], we formalize this as follows. The *complexity* of $w \in \Gamma * \mathbb{Z}$ (with respect to S) is given by:

$$\chi_\Gamma^S(w) = \min\{|g|_S : g \in \Gamma, w(g) \neq e_\Gamma\}$$

(with the convention that $\chi_\Gamma^S(w) = +\infty$ if w is a mixed identity for Γ). Here, $|g|_S$ denotes the *word-length* of g with respect to the generating set S. The *MIF growth function* $\mathcal{M}_\Gamma^S : \mathbb{N} \to \mathbb{N} \cup \{+\infty\}$ of Γ (with respect to S) is then given by:

$$\mathcal{M}_\Gamma^S(n) = \max\left\{\chi_\Gamma^S(w) : w \in \Gamma * \mathbb{Z}, |w|_{S\cup\{x\}} \leqslant n\right\}.$$

Intuitively, a group of slow MIF growth is "strongly MIF": It is easy to verify that a given w is not a mixed identity for Γ, because there exists a witness of short word-length. As the dependence of $\mathcal{M}_\Gamma^S$ on S is slight, we suppress it from our notation for the remainder of the Introduction (with the understanding that all implied constants may depend on S).

Since MIF places such powerful structural restrictions on a group, it is no surprise that groups of slow MIF growth are difficult to identify, and indeed, there are no groups of bounded MIF growth.

Theorem 1.1 [5] Theorem 1.9. *For any finitely generated group Γ, $\mathcal{M}_\Gamma(n) \gg \log(n)$.*

In light of Theorem 1.1, we shall refer to a finitely generated group Γ as *sharply MIF* if its MIF growth function $\mathcal{M}_\Gamma$ satisfies $\mathcal{M}_\Gamma(n) \ll \log(n)$. Prior to this paper, we did not have any examples of sharply MIF groups. In fact the only previously existing explicit upper bound on MIF growth was as follows: If Γ is a finite-rank nonabelian free group, then $\mathcal{M}_\Gamma(n) \ll n\log(n)$ [5, Theorem 1.10]. Employing different methods from those of [5], we improve this result for free groups, and extend it to many other groups besides.

Theorem 1.2 (Theorem 3.2). *Let Γ be a finitely generated torsion-free nonelementary Kleinian group. Then, Γ is sharply MIF.*

Since free groups are Kleinian, we can consequently improve upon the result from [5].

Corollary 1.3 (Theorem 3.4). *Let Γ be a free group of finite rank at least 2. Then Γ is sharply MIF.*

More generally, Theorem 1.2 implies the following.

Corollary 1.4. *Let M be either (i) a closed orientable surface of genus at least 2 or (ii) a closed orientable hyperbolic 3-manifold. Then, $\pi_1(\Gamma)$ is sharply MIF.*

As these two corollaries illustrate, there are large families of torsion-free Gromov hyperbolic groups with logarithmic MIF growth. One may ask whether these are instances of a more general phenomenon.

Question 1.5. Let Γ be a torsion-free nonelementary Gromov hyperbolic group. Must Γ be sharply MIF?

Of necessity, any proof of an affirmative answer to Question 1.5 would require radically different methods from ours, since we make essential use of the abundant supply of finite quotients of Kleinian groups. As such, there is no obvious way to apply our proof-strategy to groups, which are not known to be residually finite.

More generally still, if $\mathbb{K}$ is an algebraically closed field, and $\mathbb{G}$ is an algebraic group defined over $\mathbb{K}$, then for any $w \in \mathbb{G} * \mathbb{Z}$, the associated word-map $w : \mathbb{G} \to \mathbb{G}$ is a morphism of algebraic varieties, so that $w^{-1}(e_{\mathbb{G}}) \subseteq \mathbb{G}$ is Zariski-closed. Therefore, if $\mathbb{G}$ is MIF, then so is any Zariski-dense subgroup $\Gamma \leqslant \mathbb{G}$. Here, we focus on the case $\mathbb{G} = \mathrm{PGL}_d(\mathbb{C})$: By Theorem 5 of [17], $\mathrm{PGL}_d(\mathbb{C})$ is MIF. Our most general result gives sharp bounds on the MIF growth of certain finitely generated Zariski-dense subgroups of $\mathrm{PGL}_d(\mathbb{C})$ (see Theorem 2.2 below).

Theorem 1.6. *Let $d \geqslant 2$ and let K be a number field. Let $\Gamma \leqslant \mathrm{PSL}_d(K)$ be finitely generated and Zariski-dense in $\mathrm{PGL}_d(\mathbb{C})$. If $d \geqslant 3$, suppose*

$$K = \mathbb{Q}(\{\mathrm{tr}(\mathrm{Ad}(g)) : g \in \Gamma\}). \tag{1}$$

Then Γ is sharply MIF.

Here, Ad denotes the adjoint representation of $\mathbb{G}$ on the associated Lie algebra. It is well known that every nonelementary Kleinian group satisfies the conclusion of Theorem 1.6 with $d = 2$, so Theorem 1.2 follows immediately. Other examples, which clearly satisfy the conditions of Theorem 1.6, are the following (see Section 3 below).

Example 1.7. For every $d \geqslant 2$, $\mathrm{PSL}_d(\mathbb{Z})$ is sharply MIF; so too is every finitely generated subgroup Γ of $\mathrm{PSL}_d(\mathbb{Z})$, which is Zariski-dense in $\mathrm{PGL}_d(\mathbb{C})$.

There has been much interest in recent years in so-called *thin* groups, that is, subgroups of an arithmetic group that have infinite index but are nevertheless Zariski-dense in the ambient algebraic group. Specifically, there are many interesting open questions asking which group-theoretic properties a thin group must satisfy [8]. Theorem 1.6 shows that, beside $\mathrm{PSL}_d(\mathbb{Z})$ itself, any finitely generated thin subgroup of $\mathrm{PSL}_d(\mathbb{Z})$ must be sharply MIF.

Remark 1.8. One could also define MIF growth in terms of words with constants in k variables, for any $k \in \mathbb{N}$, by considering the complexity in Γ of elements of $\Gamma * \mathbb{F}_k$, where $\mathbb{F}_k$ is a free group of rank k (with the complexity of $w \in \Gamma * \mathbb{F}_k$ being defined in terms of an appropriate metric on Γ^k). However, whether or not the the group is MIF, and the asymptotic behavior of the MIF growth function will be the same, irrespective of which (fixed) value of k we use to define it, see [6, Lemma 2.2]; for instance, whether or not Γ is sharply MIF does not depend on the value of k. For simplicity, we therefore restrict to the one-variable case.

All of our upper bounds on MIF growth are based on the existence of a rich supply of finite quotients of Γ, which have no short mixed identities, and with good expansion properties. The lengths of mixed identities for finite groups were studied by the authors in [6], where the following result was proved (see [6, Theorem 3], of which the following is a special case).

Theorem 1.9. *There exists $c > 0$ such that for all primes p and all $d \geqslant 2$, $\mathrm{PSL}_d(p)$ has no mixed identity of length $\leqslant cp$.*

The basic proof-strategy of all our upper bounds on $\mathcal{M}_\Gamma$ in this paper is the same. To ease the understanding of the general proof to follow, let us sketch the argument in the special case of Γ a nonabelian free group, with finite free basis S. First, we faithfully represent Γ as a subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Let $w(x) = x^{a_0}c_1x^{a_1}\cdots c_kx^{a_k}$ be a nontrivial reduced word in $\Gamma * \mathbb{Z}$ so that all $c_i \in \mathrm{SL}_2(\mathbb{Z})$ are nontrivial (indeed noncentral). For p a prime number, let $\pi_p : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(p)$ be reduction modulo p. By the Prime Number Theorem, there exists p of moderate size such that all $\pi_p(c_i) \in \mathrm{SL}_2(p)$ are still noncentral. By Theorem 1.9, there exists $\overline{g} \in \mathrm{SL}_2(p)$ for which $\overline{w}(\overline{g})$ is noncentral in $\mathrm{SL}_2(p)$, where $\overline{w}(x) = x^{a_0}\pi_p(c_1)x^{a_1}\cdots\pi_p(c_k)x^{a_k} \in \mathrm{SL}_2(p) * \mathbb{Z}$. We would like to lift $\overline{g}$ to $g \in \Gamma$, so that $w(g) \neq e$. By deep results on the expansion properties of $\mathrm{SL}_2(p)$, not only is the restriction of π_p to Γ surjective (so that such a lift g exists), but the Cayley graph of $\mathrm{SL}_2(p)$ with respect to generating set $\pi_p(S)$ has small diameter, so that we can choose that lift g to have small word-length with respect to S.

In the setting of Theorem 1.6, we will be working over a number field K, so instead of reductions modulo a rational prime, we shall be considering reductions $\pi_\mathcal{P}$ modulo a prime element $\mathcal{P}$ in the ring of integers of K. If $d \geqslant 3$, the surjectivity of $\pi_\mathcal{P}$ is not such a straightforward matter as it is for $d = 2$; the technical hypothesis (1) is assumed in Theorem 1.6, so that surjectivity is guaranteed, by an appropriate "Strong Approximation" Theorem.

In light of our results as described above, one might wonder whether in fact *every* finitely generated MIF group is sharply MIF. It transpires that this is not the case. It was noted already in [5] (Remark 9.3) that to find a counterexample, it would be sufficient to find a finitely generated MIF group of subexponential word growth. Following circulation of an earlier version of our results, N. Matte Bon kindly pointed out to us that a construction of Nekrashevych, based on ideas from topological dynamics, provides such a group. As such we have the following.

Theorem 1.10. *There exists a finitely generated MIF group, which is not sharply MIF.*

2 | LINEAR GROUPS OVER NUMBER FIELDS

Let K be a number field, with $|K : \mathbb{Q}| = D$. Let $C_0 > 0$ (to be chosen). Let P_n be the set of rational primes p satisfying $C_0 n < p \leqslant C_0 n^2$, and let $Q_n \subseteq P_n$ be the subset of those primes, which split completely over K.

Lemma 2.1. *For all $c > 0$, if C_0 is chosen sufficiently large (depending on c and D), then for all $n \gg_D 1$,*

$$\prod_{p \in Q_n} p \geqslant \exp(cn^2).$$

Proof. By the Prime Number Theorem, the product $p(x)$ of all rational primes at most x satisfies:

$$\lim_{x\to\infty} \log(p(x))/x = 1.$$

By Chebotarev's Density Theorem, the proportion of rational primes at most Cn^2, which split completely over K is at least $1/2D$ (for all n larger than a constant depending only on K), hence the product of all such primes is at least $p(C_0 n^2/2D)$. Thus:

$$\prod_{p\in Q_n} p \geqslant p(C_0 n^2/2D)/p(C_0 n)$$

and the conclusion follows. □

Let $\mathcal{O}_K$ be the ring of integers of K. Let $\sigma_1, \dots, \sigma_D : K \hookrightarrow \mathbb{C}$ be the distinct field embeddings of K into $\mathbb{C}$. Recall that the *norm* of an element $x \in K$ is given by:

$$N_{K/\mathbb{Q}}(x) = \prod_{i=1}^{D} \sigma_i(x).$$

For $\alpha \in \mathcal{O}_K$ define:

$$\mu(\alpha) = \max_{1\leqslant i\leqslant D} |\sigma_i(\alpha)|$$

Then, for all $\alpha, \beta \in \mathcal{O}_K$:

(i) $\mu(\alpha+\beta) \leqslant \mu(\alpha) + \mu(\beta)$;
(ii) $\mu(\alpha\beta) \leqslant \mu(\alpha)\mu(\beta)$;
(iii) if $\alpha \neq 0$ then $\mu(\alpha) \geqslant 1$;
(iv) $\mu(\alpha)^D \geqslant N_{K/\mathbb{Q}}(\alpha)$.

Thus, for p a rational prime and $\mathcal{P} \in \mathcal{O}_K$ a K-prime dividing p, p divides $N_{K/\mathbb{Q}}(\mathcal{P})$, hence $\mu(\mathcal{P}) \geqslant p^{1/D}$.

Let $\Gamma \leqslant \mathrm{SL}_d(K)$ be generated by the finite set S, which we may assume to be symmetric and to contain I_d. Let $\mathbb{Z} = \langle x \rangle$, so that $S \cup \{x\}$ generates $\Gamma * \mathbb{Z}$. Our main technical result is as follows.

Theorem 2.2. *Suppose $\Gamma \leqslant \mathrm{SL}_d(K)$ is Zariski-dense in $\mathrm{SL}_d(\mathbb{C})$. If $d \geqslant 3$, suppose that K and Γ satisfy condition (1). There exists $C = C(S) > 0$ such that the following holds. Let:*

$$w(x) = x^{a_0} c_1 x^{a_1} \cdots c_k x^{a_k} \in \Gamma * \mathbb{Z} \tag{2}$$

for some $c_i \in \Gamma \setminus Z(\Gamma)$ and integers a_i with $a_i \neq 0$ for $1 \leqslant i \leqslant k-1$. Suppose $|w|_{S\cup\{x\}} = n$. Then there exists $g \in \Gamma$ such that $|g|_S \leqslant C\log(n)$ and $w(g) \notin Z(\Gamma)$.

The rest of this section is devoted to the proof of Theorem 2.2, and the deduction of Theorem 1.6 from it. In what follows, we continue to assume that the hypotheses of Theorem 2.2 hold. Note that since $|w|_{S\cup\{x\}} = n$, we have $|c_i|_S \leqslant n$ for $1 \leqslant i \leqslant k$. We may take n to be larger than a quantity depending only on K and d, which will be chosen in the course of the proof.

For each $s \in S$, we may choose $s^* \in \mathbb{M}_d(\mathcal{O}_K)$ and $\delta(s) \in \mathcal{O}_K$ such that $s = (1/\delta(s))s^*$ in $\mathbb{M}_d(K)$. We can then extend to the whole of Γ, by choosing, for each $g \in \Gamma$, a representative $g = s_1 \cdots s_{|g|_S}$ of g as a word in S of minimal length, and setting:

$$g^* = s_1^* \cdots s_{|g|_S}^* \text{ and } \delta(g) = \delta(s_1) \cdots \delta(s_{|g|_S}) \tag{3}$$

so that for all $g \in \Gamma$, $g = (1/\delta(g))g^*$. Let M be the maximal value of μ over the nonzero elements of $\{s^*_{i,j} : s \in S, 1 \leqslant i,j \leqslant d\} \cup \{\delta(s) : s \in S\}$.

Lemma 2.3. *For any $g \in \Gamma$, every entry $g^*_{i,j}$ of g^* satisfies $\mu(g^*_{i,j}) \leqslant (dM)^{|g|_S}$, and $\mu(\delta(g)) \leqslant M^{|g|_S}$.*

Proof. We show that μ takes value at most $(dM)^r$ on all entries of products of the form $X = s_1^* \cdots s_r^*$. Writing $Y = s_2^* \cdots s_r^*$, so that $X = s_1^* Y$, we have:

$$\mu(X_{i,j}) = \sum_{l=1}^{d} \mu(s^*_{i,k})\mu(Y_{k,j}) \leqslant M \sum_{l=1}^{d} \mu(Y_{k,j}) \leqslant M \sum_{l=1}^{d} (dM)^{r-1} = (dM)^r$$

(by induction on r). The second claim holds by submultiplicativity of μ. □

If p splits completely over K, then for any K-prime $\mathcal{P} \in \mathcal{O}_K$ dividing p, reduction modulo $\mathcal{P}$ induces a surjective ring homomorphism $\pi_{\mathcal{P}} : \mathcal{O}_K \to \mathbb{F}_p$. If moreover $\mathcal{P}$ does not divide any element of $\{\delta(s) : s \in S\}$, then every nonzero entry of every element of Γ is invertible modulo $\mathcal{P}$, and $\pi_{\mathcal{P}}$ induces a group homomorphism $\Gamma \to \mathrm{SL}_d(p)$, which we also denote by $\pi_{\mathcal{P}}$.

For G a group, $T \subseteq G$ a generating set, and $r \geqslant 0$, let:

$$B_T(r) = \{g \in G : |g|_T \leqslant r\}$$

denote the closed ball of radius r about the identity in the word-metric induced by T on G.

Lemma 2.4. *There exists $\tilde{c} = \tilde{c}(S) > 0$ such that the following holds. Let $p \in Q_n$ and let $\mathcal{P} \in \mathcal{O}_K$ be a K-prime dividing p. Suppose $\mathcal{P}$ does not divide any element of $\{\delta(s) : s \in S\}$. Then, the restriction of $\pi_{\mathcal{P}}$ to $B_S(c \log(p))$ is injective.*

Proof. Note that if $h, k \in \Gamma$ satisfy $\pi_{\mathcal{P}}(h) = \pi_{\mathcal{P}}(k)$, then $g = hk^{-1} \in \ker(\pi_{\mathcal{P}})$ and $|g|_S \leqslant |h|_S + |k|_S$. Hence suppose $I_d \neq g \in \ker(\pi_{\mathcal{P}})$. Then, $0 \neq X = g^* - \delta(g)I_d \in \mathbb{M}_d(\mathcal{O}_K)$ has all entries divisible by $\mathcal{P}$. Letting $x \in \mathcal{O}_K$ be a nonzero entry of X, we therefore have $\mu(x) \geqslant p^{1/D}$. On the other hand, by Lemma 2.3, $\mu(x) \leqslant (dM)^{|g|_S} + M^{|g|_S} \leqslant ((d+1)M)^{|g|_S}$, and the conclusion follows. □

Proposition 2.5. *Let Q_n be as in Lemma 2.1. There exists $p \in Q_n$ and a K-prime $\mathcal{P} \in \mathcal{O}_K$ dividing p, such that:*

(i) *$\mathcal{P}$ does not divide any element of $\{\delta(s) : s \in S\}$;*
(ii) *$\pi_{\mathcal{P}} : \Gamma \to \mathrm{SL}_d(p)$ is surjective;*
(iii) *for all $1 \leqslant i \leqslant k$, $\pi_{\mathcal{P}}(c_i) \in \mathrm{SL}_d(p)$ is noncentral.*

For the proof, we require the following well-known auxiliary fact.

Lemma 2.6. *For every prime p and every proper subgroup $H < \mathrm{SL}_2(p)$, either H is metabelian or $|H| \mid 240$.*

Proof of Proposition 2.5. Since S is finite, there are only finitely many K-primes $\mathcal{P} \in \mathcal{O}_K$ for which (i) fails. We claim that there are only finitely many $\mathcal{P}$ satisfying (i) but not (ii). For $d \geqslant 3$, [18, Theorem 10.5] applies (by (1)). The case $d = 2$ is described in [12, section 3]; we outline the argument here for the reader's convenience. By the Tits alternative, there exist $a, b \in \Gamma$ freely generating a nonabelian free subgroup of Γ. Set $g = [[a, b], [b^{-1}, a]]^{240} \in \Gamma$ (so that g is nontrivial). If $\pi_{\mathcal{P}}$ is not surjective, then by Lemma 2.6, $\pi_{\mathcal{P}}(g) = I_2$. This contradicts Lemma 2.4 for n sufficiently large (in terms of S).

Let B be the set of all K-primes for which either (i) or (ii) fails, so that $|B|$ is bounded in terms of S alone. Suppose for a contradiction that for all $p \in Q_n \setminus B$ and all K-primes $\mathcal{P} \in \mathcal{O}_K$ dividing p, there exists $1 \leqslant i \leqslant k$ such that $\pi_{\mathcal{P}}(c_i) \in Z(\mathrm{SL}_d(p))$. Thus, for all $s \in S$,

$$\pi_{\mathcal{P}}(s)\pi_{\mathcal{P}}(c_i) - \pi_{\mathcal{P}}(c_i)\pi_{\mathcal{P}}(s) = 0 \mathrm{in} \mathbb{M}_{\mathrm{d}}(\mathrm{p}).$$

By contrast, since all the c_i are noncentral in Γ and S generates Γ, we have for all $1 \leqslant i \leqslant k$ that there exists $s \in S$ such that $0 \neq sc_i - c_i s \in \mathbb{M}_d(K)$. Multiplying through by $\delta(c_i)\delta(s)$, we have $0 \neq s^* c_i^* - c_i^* s^* \in \mathbb{M}_d(\mathcal{O}_K)$, but all entries of $s^* c_i^* - c_i^* s^*$ are divisible by $\mathcal{P}$.

Thus, taking the product of all nonzero entries of all matrices $s^* c_i^* - c_i^* s^*$, we obtain an element $z \in \mathcal{O}_K$, which is divisible by all of the $\mathcal{P}$. Thus, as observed above $p | N_{K/\mathbb{Q}}(\mathcal{P}) | N_{K/\mathbb{Q}}(z)$ for each $p \in Q_n \setminus B$, so that:

$$\frac{1}{C_0^{|B|}} \exp\left(cn^2 - 2|B|\log(n)\right) = \exp(cn^2)/(C_0 n^2)^{|B|} \leqslant \prod_{Q_n \setminus B} p \leqslant N_{K/\mathbb{Q}}(z) \leqslant \mu(z)^D \tag{4}$$

by Lemma 2.1. By contrast, by Lemma 2.3, μ takes value at most $2(dM)^{n+1}$ on the entries of $s^* c_i^* - c_i^* s^*$. Since $k \leqslant n$, there are at most $d^2 n$ nonzero elements of $\mathcal{O}_K$, which are entries of one of the $s^* c_i^* - c_i^* s^*$, and as such:

$$\mu(z) \leqslant 2^{d^2 n}(dM)^{d^2 n(n+1)} \leqslant \exp\left(d^2(2\log(dM) + \log(2)/n)n^2\right). \tag{5}$$

Taking c sufficiently large in Lemma 2.1 (which in turn requires C_0 to be chosen sufficiently large), this contradicts (4) for n sufficiently large (in terms of S). □

If G is a finite group, recall that the *diameter* of G with respect to T is:

$$\mathrm{diam}(G, T) = \min\{r \geqslant 0 \,:\, B_T(r) = G\}.$$

Proposition 2.7. *There exists $C = C(S) > 0$ such that for all but finitely many rational primes p, which completely split in K, for all primes $\mathcal{P}$ of $\mathcal{O}_K$, which divide p, $\pi_{\mathcal{P}}(S)$ generates $\mathrm{SL}_d(p)$ and $\mathrm{diam}(\mathrm{SL}_d(p), \pi_{\mathcal{P}}(S)) \leqslant C\log(p)$.*

The proof rests on the following deep result, due to Helfgott [10], Breuillard-Green-Tao [7], and Pyber-Szabó [14].

Theorem 2.8. *There exists $\epsilon = \epsilon(d) > 0$ such that for any prime p and any generating set $A \subseteq \mathrm{SL}_d(p)$, either (a) $AAA = \mathrm{PSL}_d(p)$ or (b) $|AAA| \geqslant |A|^{1+\epsilon}$.*

Here, $AAA = \{abc : a, b, c \in A\}$. We also require a lemma, the proof of which is similar to that of Proposition 2.7.

Proof of Proposition 2.7. First, as in Proposition 2.5, we may assume that $\mathcal{P}$ does not divide any element of $\{\delta(s) : s \in S\}$ and that $\pi_{\mathcal{P}}(S)$ generates $\mathrm{SL}_2(p)$. Next, Γ has exponential word growth, that is, there exists $\delta = \delta(S) > 0$ such that for all $r > 0$, $|B_S(r)| \geqslant (1+\delta)^r$ (this follows, for instance, from the Tits alternative, since Γ has a nonabelian free subgroup). Let $\tilde{c}$ be as in Lemma 2.4 and let:

$$A_0 = \pi_{\mathcal{P}}(B_S(\tilde{c}\log(p))) = B_{\pi_{\mathcal{P}}(S)}(\tilde{c}\log(p)), A_{m+1} = A_m A_m A_m,$$

so that for all m, $A_m \subseteq B_{\pi_{\mathcal{P}}(S)}(3^m \tilde{c}\log(p))$. Then by Lemma 2.4, $|A_0| \geqslant p^c$ for some $c = c(S) > 0$. If none of $A_0, A_1, \dots, A_m$ satisfy conclusion (a) of Theorem 2.8, then $|A_m| \geqslant p^{c(1+\epsilon)^m}$. This is impossible for $m \geqslant \tilde{C} = (2\log(d) - \log(c))/\log(1+\epsilon)$, since $|\mathrm{SL}_d(p)| \leqslant p^{d^2}$. Thus, for some $m \leqslant \tilde{C}$, $\mathrm{SL}_d(p) \subseteq A_{m+1} \subseteq B_{\pi_{\mathcal{P}}(S)}(3^{\tilde{C}}\tilde{c}\log(p))$. Thus, we have the desired bound, with $C = 3^{\tilde{C}}\tilde{c}$. ☐

Proof of Theorem 2.2. Let $p \in Q_n$ and $\mathcal{P}$ be as in Proposition 2.5. Let $w(x) \in \Gamma * \mathbb{Z}$ be as in (2). For $1 \leqslant i \leqslant k$, let $\overline{c}_i \in \mathrm{PSL}_d(p)$ be the image in $\mathrm{PSL}_d(p)$ of $\pi_{\mathcal{P}}(c_i) \in \mathrm{SL}_d(p)$. By Proposition 2.5, all $\overline{c}_i$ are nontrivial, so that:

$$\overline{w}(x) = x^{a_0}\overline{c}_1 x^{a_1} \cdots \overline{c}_k x^{a_k} \in \mathrm{PSL}_d(p) * \mathbb{Z}$$

is nontrivial. Choosing C_0 sufficiently large in the definition of Q_n, as we may, Theorem 1.9 applies to $\overline{w}(x)$, so there exists $\overline{g} \in \mathrm{PSL}_d(p)$ such that $\overline{w}(\overline{g}) \neq e$. Let $g \in \mathrm{SL}_d(p)$ be a lift of $\overline{g}$. Then noting that $\pi_{\mathcal{P}}(B_S(r)) = B_{\pi_{\mathcal{P}}(S)}(r)$, and applying Proposition 2.7, there exists $\tilde{g} \in B_S(C\log(p))$ such that $\pi_{\mathcal{P}}(\tilde{g}) = g$. Since $\pi_{\mathcal{P}}$ is surjective and $\pi_{\mathcal{P}}(w(\tilde{g}))$ is not central in $\mathrm{SL}_d(p)$, $w(\tilde{g})$ is not central in Γ. Finally, since $p \in Q_n$, $\log(p) = O(\log(n))$, as desired. ☐

Proof of Theorem 1.6. Let Γ be as in the statement of the theorem, and let S be a finite generating set for Γ. Let $\iota : \mathrm{SL}_d(\mathbb{C}) \to \mathrm{PGL}_d(\mathbb{C})$ be the standard isogeny. Let $\hat{\Gamma} = \iota^{-1}(\Gamma)$ and $\hat{S} = \iota^{-1}(S)$. We note first that $\hat{\Gamma}$ is Zariski-dense in $\mathrm{SL}_d(\mathbb{C})$. Let $\mathbb{G} \leqslant \mathrm{SL}_d(\mathbb{C})$ be the Zariski closure of $\hat{\Gamma}$ in $\mathrm{SL}_d(\mathbb{C})$. Since ι is a morphism of algebraic groups, $\iota(\mathbb{G})$ is a closed subgroup of $\mathrm{PGL}_d(\mathbb{C})$ containing Γ, hence equals $\mathrm{PGL}_d(\mathbb{C})$. Thus, $\dim(\mathbb{G}) \geqslant \dim(\iota(\mathbb{G})) = d^2 - 1$, and since $\mathrm{SL}_d(\mathbb{C})$ is a connected group of dimension $d^2 - 1$, we have $\mathbb{G} = \mathrm{SL}_d(\mathbb{C})$, as desired.

Second, the adjoint representation of $\mathrm{SL}_d(\mathbb{C})$ factors through ι. Thus, by condition (1), $\hat{\Gamma}$ satisfies the hypotheses of Theorem 2.2. Let:

$$w(x) = x^{a_0} c_1 x^{a_1} \cdots c_k x^{a_k} \in \Gamma * \mathbb{Z}$$

with $|w|_{S\cup\{x\}} = n$ and $a_i \neq 0$ for $1 \leqslant i \leqslant k-1$. We can lift $w(x)$ to $\hat{w}(x) \in \hat{\Gamma} * \mathbb{Z}$ by replacing each c_i by $\hat{c}_i \in \hat{\Gamma}$ satisfying $\iota(\hat{c}_i) = c_i$ and $|\hat{c}_i|_{\hat{S}} = |c_i|_S$. Then, all $\hat{c}_i$ lie in $\hat{\Gamma} \setminus Z(\hat{\Gamma})$ and $|\hat{w}(x)|_{\hat{S}\cup\{x\}} = n$. Applying Theorem 2.2 (with $\hat{\Gamma}$; $\hat{S}$ and $\hat{w}(x)$ playing the rôles of Γ; S and $w(x)$), we obtain $\hat{g} \in \hat{\Gamma}$ satisfying $|\hat{g}|_{\hat{S}} \leqslant C\log(n)$ and $\hat{w}(\hat{g}) \notin Z(\hat{\Gamma})$. Then, $g = \iota(\hat{g}) \in \Gamma$ satisfies $w(\iota(\hat{g})) = \iota(\hat{w}(\hat{g})) \neq e$ and

$|g|_S \leqslant |\hat{g}|_{\hat{S}}$, so g witnesses that $\chi_\Gamma^S(w) \leqslant C\log(n)$. Since this holds for all such w, we conclude $\mathcal{M}_\Gamma^S(n) \leqslant C\log(n)$, as desired. □

3 | APPLICATIONS

As a first application of Theorem 1.6, we return to Example 1.7, and prove that $\mathrm{PSL}_d(\mathbb{Z})$ is sharply MIF. We shall be applying Theorem 1.6 with $K = \mathbb{Q}$, so that hypothesis (1) holds automatically. Finite generation of $\mathrm{PSL}_d(\mathbb{Z})$ is classical. Finally, since $\mathrm{PSL}_d(\mathbb{Z})$ is a lattice in $\mathrm{PSL}_d(\mathbb{R})$, it is Zariski-dense by the Borel Density Theorem.

Remark 3.1. Of course, the preceding argument extends to any finitely generated subgroup of $\mathrm{PSL}_d(\mathbb{Z})$, which is Zariski-dense in $\mathrm{PSL}_d(\mathbb{R})$. In particular, any finite-index subgroup of $\mathrm{PSL}_d(\mathbb{Z})$ is sharply MIF.

In the remainder of this section, we deduce Theorem 1.2 and Corollaries 1.3 and 1.4 from Theorem 1.6.

3.1 | Kleinian groups

We refer to [16] for general background on Kleinian group. Our exposition in this subsection is closely inspired by the proof of Theorem 1.2 from [12].

Theorem 3.2. *Let Γ be a finitely generated torsion-free nonelementary Kleinian group. Then Γ is sharply MIF.*

As noted in [16], examples of torsion-free nonelementary Kleinian group include all fundamental groups of closed orientable hyperbolic 2- and 3-manifolds. As such, Corollary 1.4 follows immediately from Theorem 3.2.

In proving Theorem 3.2, it is helpful to recall the following well-known characterization of Zariski-density in the case of SL_2.

Theorem 3.3. *For $\Gamma \leqslant \mathrm{SL}_2(\mathbb{C})$, the following are equivalent.*

(i) *Γ is Zariski-dense in $\mathrm{SL}_2(\mathbb{C})$;*
(ii) *Γ has a nonabelian free subgroup;*
(iii) *Γ is not virtually soluble.*

Proof of Theorem 3.2. Suppose first that Γ has finite covolume. Let $\tilde{\Gamma}$ be the preimage of Γ in $\mathrm{SL}_2(\mathbb{C})$. By Mostow–Prasad rigidity, up to conjugacy, we can assume $\tilde{\Gamma} \leqslant \mathrm{SL}_2(K)$ for some number field K. Moreover $\tilde{\Gamma}$ is not virtually soluble, so is Zariski-dense in $\mathrm{SL}_2(\mathbb{C})$. Thus, Theorem 2.2 applies to $\tilde{\Gamma}$, and the conclusion for Γ follows immediately.

If Γ has infinite covolume but is geometrically finite, then there exists a finite-covolume Kleinian group Γ' such that Γ is isomorphic to a subgroup of Γ', by [9]. Then the faithful representation of $\tilde{\Gamma}'$ into $\mathrm{SL}_2(K)$ described in the previous paragraph restricts to $\tilde{\Gamma}$. Once again $\tilde{\Gamma}$ is not virtually soluble, so is Zariski dense in $\mathrm{SL}_2(K)$, and Theorem 2.2 applies.

Finally if Γ is geometrically infinite, then it is isomorphic to a geometrically finite Kleinian group (see [2]). $\square$

3.2 | Free groups

Theorem 3.4. *Every free group of finite rank $r \geqslant 2$ is sharply MIF.*

By Theorem 3.2, it suffices to note that every finite-rank nonabelian free group is torsion-free nonelementary Kleinian. Alternatively, we can deduce Theorem 3.4 using Remark 3.1 and the following well-known result of Sanov [15].

Theorem 3.5. *Let:*

$$a = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, b = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Then $\langle a, b \rangle$ is a free group of rank 2, of finite index in $\mathrm{SL}_2(\mathbb{Z})$.

Proof of Theorem 3.4. By Theorem 3.5, and the fact that the rank-r free group F_r embeds as a finite-index subgroup of F_2 for all $r \geqslant 2$, we can assume that F_r is faithfully represented as a finite-index subgroup of $\mathrm{SL}_2(\mathbb{Z})$. The restriction of the natural quotient $\mathrm{SL}_2(\mathbb{Z}) \twoheadrightarrow \mathrm{PSL}_2(\mathbb{Z})$ to F_r is injective, since F_r is torsion-free and $Z(\mathrm{SL}_2(\mathbb{Z}))$ is finite, hence F_r is also faithfully represented as a finite-index subgroup of $\mathrm{PSL}_2(\mathbb{Z})$. The result follows as in Remark 3.1. $\square$

4 | TOPOLOGICAL FULL GROUPS

In this section, we prove Theorem 1.10, which asserts that not every finitely generated MIF group is sharply MIF. Let X denote the Cantor space.

Definition 4.1. Let G be a group and let $\alpha : G \to \mathrm{Homeo}(X)$ be a continuous action on X. The *topological full group* $T(\alpha)$ of the action is the group consisting of all homeomorphisms ϕ of X for which there exists a finite partition $X = C_1 \sqcup \cdots \sqcup C_p$ of X consisting of nonempty clopen sets C_i, and elements $g_1, \ldots g_p \in G$ such that $\phi|_{C_i} = \alpha(g_i)|_{C_i}$ for $1 \leqslant i \leqslant p$.

Recall that an action of a group G on a set Ω is *highly transitive* if, for every positive integer n, and every two n-tuples $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ of distinct points of Ω, there exists $g \in G$ such that $g(x_i) = y_i$ for $1 \leqslant i \leqslant n$. It is easy to see that if the action of G on Ω is highly transitive, then so is the restriction of that action to any finite-index subgroup of G.

Proposition 4.2. *Let G and α be as in Definition 4.1. Let $x \in X$ and suppose the orbit* $\mathrm{Orb}(x)$ *of x in X is infinite. Then, the action of $T(\alpha)$ on* $\mathrm{Orb}(x)$ *is highly transitive.*

Proof. It suffices to prove that for any nonempty finite subset $\Sigma \subseteq \mathrm{Orb}(x)$, there is a subgroup $H(\Sigma)$ of $T(\alpha)$ preserving Σ and acting on Σ as $\mathrm{Sym}(\Sigma)$. Let $y, z \in \Sigma$ be distinct points, and let $g \in G$ with $\alpha(g)(y) = z$. There exists a clopen neighborhood C of y such that $C \cap \alpha(g)(C) = \emptyset$, $C \cap \Sigma = \{y\}$, and $\alpha(g)(C) \cap \Sigma = \{z\}$. Let $\tau_{y,z} \in T(\alpha)$ fix $X \setminus (C \cup \alpha(g)(C))$, act on C as $\alpha(g)$, and act on $\alpha(g)(C)$ as $\alpha(g)^{-1}$. Then, $\tau_{y,z}$ preserves Σ and acts upon it as the transposition $(y\ z)$. The desired result follows. □

An action of a group on X is *minimal* if every orbit of the action is dense in X.

Theorem 4.3 [13, Theorem 8.1]. *There exists a finitely generated infinite group F of subexponential word growth with a faithful continuous minimal action $\alpha : F \to \mathrm{Homeo}(X)$, such that $T(\alpha) \cong F$. Moreover the derived subgroup $[F, F]$ of F is simple, and has finite index in F.*

Proof of Theorem 1.10. Let F be as in Theorem 4.3. Our example shall be $\Gamma = [F, F]$. Being of finite index in F, Γ is also a finitely generated group of subexponential growth. As noted in [5, Remark 9.3], no group of subexponential growth can be sharply MIF. It therefore suffices to verify that Γ is MIF.

Let $x \in X$ and set $\Omega = \mathrm{Orb}(x)$, a countably infinite set. Then, by Proposition 4.2 and $F \cong T(\alpha)$, F admits a highly transitive action on Ω, hence so does Γ. Moreover, since Ω is dense in X, under this action no nontrivial element of Γ has finite support on Ω. Finally, we apply Theorem 5.9 of [11]: If Γ is not MIF, then Γ contains a normal subgroup isomorphic to the group A of all finitely supported even permutations of $\mathbb{N}$. Since Γ is simple, we have $\Gamma \cong A$. This is a contradiction, as Γ is finitely generated and A is not. □

Remark 4.4. As noted in the Introduction to [13], the construction given therein yields an upper bound on the word-growth of Γ of the form $C_1 \exp\left(n/\exp(C_2\sqrt{\log n})\right)$. This is improved in [3] to $f(n) = C_1 \exp(C_2 n^{\alpha})$ for some constant $\alpha \in (0,1)$. By the argument of [5, Remark 9.3], we obtain a lower bound for $\mathcal{M}_{\Gamma}$, which is approximately an inverse function to $n^2 f(n)$. The lower bound thus obtained is of the form $\log(n)^C$, for some $C > 1$. Presumably this lower bound is far from sharp; MIF growth for topological full groups should be investigated elsewhere.

ACKNOWLEDGMENTS

We are grateful to Nicolás Matte Bon for drawing our attention to the relevance of Nekrashevych's construction to proving Theorem 1.10.

JOURNAL INFORMATION

The *Bulletin of the London Mathematical Society* is wholly owned and managed by the London Mathematical Society, a not-for-profit Charity registered with the UK Charity Commission. All surplus income from its publishing programme is used to support mathematicians and mathematics research in the form of research grants, conference grants, prizes, initiatives for early career researchers and the promotion of mathematics.

ORCID

Henry Bradford https://orcid.org/0000-0003-2949-8095

REFERENCES

1. M. G. Amaglobeli and V. N. Remeslennikov, *G-identities and G-varieties*, Algebra Logic **39** (2000), no. 3.
2. J. W. Anderson, *A brief survey of the deformation theory of Kleinian groups*, The Epstein Birthday Schrift, Geom. Topol. Monogr. **1** (1998), 23–49.

3. L. Bartholdi, V. Nekrashevych, and T. Zheng, *Growth of groups with linear Schreier graphs*, arXiv:2205.01792 [math.GR]
4. G. Baumslag, *On generalised free products*, Math. Zeitschr. **78** (1962), 423–438.
5. H. Bradford, *Quantifying lawlessness in finitely generated groups*, J. Group Theory **27** (2024), no. 1, 31–59.
6. H. Bradford, J. Schneider, and A. Thom, *The length of mixed identities for finite groups*, arXiv:2306.14532 [math.GR]
7. E. Breuillard, B. Green, and T. Tao, *Approximate subgroups of linear groups*, Geom. Funct. Anal. **21** (2011), 774–819.
8. E. Breuillard and H. Oh, eds., *Thin groups and superstrong approximation*, vol. 61, Cambridge University Press, Cambridge, 2014.
9. R. Brooks, *Circle packings and co-compact extensions of Kleinian groups*, Invent. Math. **86** (1986), 461–469.
10. H. A. Helfgott, *Growth and generation in* $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, Ann. Math. **167** (2008), 601–623.
11. M. Hull and D. Osin, *Transitivity degrees of countable groups and acylindrical hyperbolicity*, Israel J. Math. **216** (2016), 307–353.
12. D. D. Long, A. Lubotzky, and A. W. Reid, *Heegaard genus and property τ for hyperbolic 3-manifolds*, J. Topol. **1**, no. 1, 152–158.
13. V. Nekrashevych, *Palindromic subshifts and simple periodic groups of intermediate growth*, Ann. Math. **187** (2018), no. 3, 667–719.
14. L. Pyber and E. Szabó, *Growth in finite simple groups of Lie type*, J. Amer. Math. Soc. **29** (2016), no. 1, 95–146.
15. I. N. Sanov, *A property of a representation of a free group*, Dokl. Akad. Nauk **57** (1947), 657–659.
16. C. Series, *A crash course on Kleinian groups*, Rend. Istit. Mat. Univ. Trieste **XXXVII** (2005), 1–38.
17. G. M. Tomanov, *Generalized group identities in linear groups*, Math. USSR-Sbornik **51** (1985), no. 1, 33.
18. B. Weisfeiler, *Strong approximation for Zariski-dense subgroups of semi-simple algebraic groups*, Ann. Math. **120** (1984), no. 2, 271–315.