INTERSECTION GROWTH IN GROUPS

IAN BIRINGER, KHALID BOU-RABEE, MARTIN KASSABOV, AND FRANCESCO MATUCCI

ABSTRACT. The intersection growth of a group G is the asymptotic behavior of the index of the intersection of all subgroups of G with index at most n, and measures the Hausdorff dimension of G in profinite metrics. We study intersection growth in free groups and special linear groups and relate intersection growth to quantifying residual finiteness.

1. INTRODUCTION

A group G is called *residually finite* if for every nontrivial element $g \in G$ there is a homomorphism $\varphi : G \to F$ onto a finite group with $\varphi(g) \neq 1$. A subtle related problem is to determine how many elements of G can be detected as nontrivial in *small* finite quotients F, i.e. those with cardinality at most some n. This problem is known as *quantifying residual finiteness*, and has been studied in [Bou10, Bus09, BM11, BM10, KM11, KT15]. In these papers, the idea is to fix a generating set S for G and to determine the size $F_G^S(r)$ of the largest finite quotient needed to detect as nontrivial an element of G that can be written as an S-word with length at most r. Fine asymptotic bounds for this *residual finiteness growth function* $F_G^S(r)$ are given for a number of groups, in particular free groups, and a closely related function is shown to characterize virtual nilpotence in [BM11].

In this article, we study instead the *percentage* of elements of G that can be detected as nontrivial in a quotient of size n. Specifically, the (normal) *intersection growth function* $i_G^{\lhd}(n)$ of G is the index of the intersection of all normal subgroups of G with index at most n. In addition to its relation to the program above, this function has geometric motivation: we show in Section 4 that intersection growth is a profinite invariant and that its asymptotics control the Hausdorff dimension of the profinite completion of G.

The majority of this paper concerns bounds for variants of $i_G^{\lhd}(n)$ in special linear groups and free groups, which we will state precisely in the next section. However, in Section 8, we also explain how intersection growths can be used to extract information about the residual finiteness growth function and identities in groups. Moreover, in an upcoming work by the authors, a fine analysis of $i_G^{\lhd}(n)$ will be given for nilpotent groups, mirroring the work of Grunewald, Lubotzky, Segal, and Smith [LS03] on *subgroup growth*, which counts the number of subgroups of index at most n in a group. In this case the numbers $i_G^{\lhd}(n)$ can be combined into a zeta function which has an Euler product decomposition and whose local factors are rational.

2. DEFINITIONS AND STATEMENTS OF MAIN RESULTS

Let $\mathscr{G}$ be a class of subgroups of a group Γ. We define the $\mathscr{G}$*-intersection growth function* of Γ by letting $i_\Gamma^{\mathscr{G}}(n)$ be the index of the intersection of all $\mathscr{G}$-subgroups of Γ with

---

2010 *Mathematics Subject Classification.* Primary 20F69; Secondary 20E05, 20E07, 20E26, 20E28.

Key words and phrases. Residually finite groups; growth in groups; intersection growth; residual finiteness growth.

index at most n. In symbols,

$$i_\Gamma^{\mathscr{G}}(n) := [\Gamma : \Lambda_\Gamma^{\mathscr{G}}(n)], \quad \text{where } \Lambda_\Gamma^{\mathscr{G}}(n) := \bigcap_{[\Gamma:\Delta]\leq n, \Delta\in\mathscr{G}} \Delta.$$

Here, $\mathscr{G}$ will always be either the class $<$ of all subgroups, the class $\lhd$ of normal subgroups, the class c of all characteristic subgroups, the class max of maximal subgroups or the class max$\lhd$ of maximal normal subgroups of Γ, i.e. those subgroups that are maximal among normal subgroups. The corresponding intersection growth functions will then be written $i_\Gamma^<(n)$, $i_\Gamma^\lhd(n)$, $i_\Gamma^c(n)$, $i_\Gamma^{\max}(n)$, and $i_\Gamma^{\max\lhd}(n)$.

Our main theorem is a precise asymptotic calculation of the maximal normal intersection growth and the maximal intersection growth of free groups.

Theorem 7.1. *Let $\mathscr{F}^k$ be the rank k free group, $k \geq 2$. Then we have*

$$i_{\mathscr{F}^k}^{\max\lhd}(n) \dot{\sim} e^{n^{k-\frac{2}{3}}} \quad \textit{and} \quad i_{\mathscr{F}^k}^{\max}(n) \dot{\sim} i_{\mathscr{F}^k}^<(n) \dot{\sim} e^{n^n}.$$

Here we write $f(n) \dot{\sim} g(n)$ if there exist suitable constants $A,B,C,D > 0$ such that $f(n) \leq Ag(Bn)$ and $g(n) \leq Cf(Dn)$ for all positive integers n. In the proof, we use the classification theorem for finite simple groups to show that the maximal normal intersection growth of $\mathscr{F}^k$ is controlled by subgroups with quotient isomorphic to $\mathrm{PSL}_2(p)$, whereas the maximal intersection growth comes from alternating groups. Note that Theorem 7.1 clearly gives a lower bound for the normal intersection growth of $\mathscr{F}^k$.

We can also calculate the intersection growth of special linear groups.

Theorem 6.1. *For the special linear groups $\mathrm{SL}_k(\mathbb{Z})$, where $k \geq 3$, we have*

$$i_{\mathrm{SL}_k(\mathbb{Z})}^c(n) \dot{\sim} i_{\mathrm{SL}_k(\mathbb{Z})}^\lhd(n) \dot{\sim} i_{\mathrm{SL}_k(\mathbb{Z})}^{\max\lhd}(n) \dot{\sim} e^{n^{1/(k^2-1)}}, \ \textit{but} \ i_{\mathrm{SL}_k(\mathbb{Z})}^<(n) \dot{\sim} i_{\mathrm{SL}_k(\mathbb{Z})}^{\max}(n) \dot{\sim} e^{n^{1/(k-1)}}.$$

Variants of Theorem 6.1 hold in a more general context for example when SL_k is replaced with another high rank absolutely simple group scheme and $\mathbb{Z}$ with ring of integers in a number field), additionally under a mild additional assumptions it holds for most high rank arithmetic groups and even Zariski dense subgroups inside such groups. With the goal of making the main body of this article more widely accessible, we placed these more general statements, and their proofs, in Appendix B.

Note that the group $\mathrm{SL}_2(\mathbb{Z})$ is virtually free and therefore the asymptotics in the $k = 2$ case are wildly different from those in Theorem 6.1.

2.1. **Acknowledgements.** The first author was partially supported by NSF Postdoctoral Fellowship DMS-0902991. The second author was partially supported by NSF RTG grant DMS-0602191 and the Ventotene 2013 conference. The third author was partially supported by NSF grants DMS-0900932 and DMS-1303117 and Simons Foundation grant 305181. The fourth author gratefully acknowledges the Fondation Mathématique Jacques Hadamard (ANR-10-CAMP-0151-02 - FMJH - Investissement d'Avenir) for the support received during the development of this work. Finally, we are grateful to Benson Farb, Alex Lubotzky, Ben McReynolds, Peter Neumann, Juan Souto, and Christopher Voll for helpful mathematical conversations and references. We also would like to thank an anoymous referee for comments which greatly improved the paper.

3. NOTATION AND BASIC PROPERTIES OF INTERSECTION GROWTH

We introduce here some asymptotic notation and study the relationship between the intersection growth of a group and of its subgroups. We say

$$a(n) \dot{\preceq} b(n) \quad \text{if} \quad \exists C, D > 0 \text{ such that } \forall n,\ a(n) \le C\, b(Dn).$$

Similarly, $a(n) \dot{\sim} b(n)$ means that both $a(n) \dot{\preceq} b(n)$ and $b(n) \dot{\preceq} a(n)$. Sometimes we will have sharper asymptotic control, in which case we write

$$a(n) \preceq b(n) \quad \text{if} \quad \limsup_{n\to\infty} \frac{a(n)}{b(n)} \le 1.$$

Then, as before, $a(n) \sim b(n)$ means that both $a(n) \preceq b(n)$ and $b(n) \succeq a(n)$.

Lemma 3.1. *Let k be a natural number and Δ an index k subgroup of Γ. Then*

- $i_\Gamma^{\le}(n) \le k \cdot i_\Delta^{\le}(n) \le i_\Gamma^{\le}(kn)$*, so we have*
$$i_\Delta^{\le}(n) \dot{\sim} i_\Gamma^{\le}(n);$$
- $i_\Gamma^{\lhd}(n) \le k \cdot i_\Delta^{\lhd}(n) \le i_\Gamma^{\lhd}((kn)^k)$*, so we have*
$$i_\Gamma^{\lhd}(n) \dot{\preceq} i_\Delta^{\lhd}(n) \dot{\preceq} i_\Gamma^{\lhd}(n^k);$$
- *If Δ is a normal subgroup of Γ then $k \cdot i_\Delta^{c}(n) \le i_\Gamma^{\lhd}(kn)$, so we have*
$$i_\Delta^{c}(n) \dot{\preceq} i_\Gamma^{\lhd}(n).$$

Proof. For the first part, note that an index n subgroup of Δ is an index kn subgroup of Γ. This shows that $\Lambda_\Delta^{\le}(n) \ge \Lambda_\Gamma^{\le}(kn)$. Moreover, if $H \le \Gamma$ then $[\Gamma : H] \ge [\Delta : \Delta \cap H]$. From this we obtain that

$$\Lambda_\Gamma^{\le}(n) \;=\; \bigcap_{H \le \Gamma,\, [\Gamma:H]\le n} H \;\ge\; \bigcap_{H \le \Gamma,\, [\Delta:\Delta\cap H]\le n} \Delta \cap H \ge\; \Lambda_\Delta^{\le}(n).$$

The first item of the lemma then follows since

$$\Lambda_\Gamma^{\le}(kn) \le \Lambda_\Delta^{\le}(n) \le \Lambda_\Gamma^{\le}(n).$$

The first inequality of the second item follows exactly as above, since intersecting an index n normal subgroup of Γ with Δ gives an index at most n normal subgroup of Γ. The second inequality, however, is different since normal subgroups of Δ are not necessarily normal in Γ.

For the second inequality, suppose that Δ has coset representatives $g_1, \ldots, g_k$. For any normal subgroup N of Δ, we have

$$\bigcap_{i=1}^{k} g_i N g_i^{-1}$$

is normal in Γ and has index at most $([\Gamma : N])^k$. Hence, $\Lambda_\Delta^{\lhd}(n) \ge \Lambda_\Gamma^{\lhd}((kn)^k)$. Further,

$$[\Gamma : \Lambda_\Gamma^{\lhd}((kn)^k)] \ge [\Gamma : \Lambda_\Delta^{\lhd}(n)] = k[\Delta : \Lambda_\Delta^{\lhd}(n)].$$

It follows that $i_\Gamma(kn^k) \ge k i_\Delta(n)$, as desired.

The last inequality follows from the the observation that any characteristic subgroup of Δ is normal subgroup of Γ, provided that $\Delta \lhd \Gamma$. $\square$

We will soon see in Proposition 5.1 and Theorems 6.1 and 7.1 that

$$i^{\lhd}_{\mathbb{Z}}(n) \stackrel{\cdot}{\sim} e^n, \;\; i^{\lhd}_{\mathscr{F}^2}(n) \stackrel{\cdot}{\succeq} e^{n^{\frac{4}{3}}}, \text{ and } \;\; i^{\lhd}_{\mathrm{SL}_3(\mathbb{Z})}(n) \stackrel{\cdot}{\sim} e^{n^{\frac{1}{8}}}.$$

Since there are inclusions $\mathbb{Z} \leq \mathscr{F}^2 \leq \mathrm{SL}_3(\mathbb{Z})$, for infinite index subgroups there is no general relationship between containment and intersection growth.

Here is an example showing the necessity of a power n^k in the second half of Lemma 3.1. We do not know if the exponent k is the best possible; however, this example can be extended to show that it must grow with index.

Example 3.2. Let $Q < \mathrm{GL}_2(\mathbb{Z})$ be the order 8 subgroup generated by

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

One can compute that $\Gamma := \mathbb{Z}^2 \rtimes Q$ has $i^{\lhd}_{\Gamma}(n) \stackrel{\cdot}{\sim} e^{\sqrt{n}}$. Since $i^{\lhd}_{\mathbb{Z}^2}(n) \stackrel{\cdot}{\sim} e^n$, this shows that the *normal* intersection growth may indeed increase upon passing to a finite index subgroup, as is allowed by Lemma 3.1. The difference comes from the fact that Q acts irreducibly on $(\mathbb{Z}/p\mathbb{Z})^2$ for $p \geq 2$.

In fact, one can also prove that $\log i_{\Gamma}(n) \preceq n$ while $\log i_{\mathbb{Z}^2}(n) \sim 2n$, which shows the necessity of a factor like k in $i_{\Gamma}(kn)$ in the first part of the lemma. The point is that the subgroups $i\mathbb{Z} \times \mathbb{Z}$ and $\mathbb{Z} \times i\mathbb{Z}$, $i \leq n$, of $\mathbb{Z}^2$ that one intersects to realize $i_{\mathbb{Z}^2}(n)$ cannot themselves be realized as intersections $\Delta \cap \mathbb{Z}^2$ of subgroups $\Delta < \Gamma$ with $[\Gamma : \Delta] = i$. This contrasts with the case of the product $\mathbb{Z}^2 \times Q$, wherein any subgroup $\Delta < \mathbb{Z}^2$ is the intersection with $\mathbb{Z}^2$ of $\Delta \times Q$, a subgroup of the product with the same index as Δ had in $\mathbb{Z}^2$.

Intersection growth behaves well with respect to direct products:

Proposition 3.3. *Suppose that* $\bullet \in \{<, \max, \lhd, \max \lhd\}$.

(1) *If* $\Gamma = \Delta_1 \times \Delta_2$, *then* $i^{\bullet}_{\Gamma}(n) = i^{\bullet}_{\Delta_1}(n) \cdot i^{\bullet}_{\Delta_2}(n)$.
(2) *If* $\Gamma = \prod_{s=1}^{\infty} \Delta_s$, *then* $i^{\bullet}_{\Gamma}(n) = \prod_s i^{\bullet}_{\Delta_s}(n)$ *provided that* $i^{\bullet}_{\Delta_s}(n) = 1$ *for almost all s.*
(3) *If each* Δ_i *is a characteristic subgroup of* Γ, *then the previous two parts also hold for the class of characteristic subgroups.*

Proof. Part (2) is an immediate corollary of part (1). We show (1) for $\bullet$ being $<$, the other cases being similar.

First, note that if H has index $\leq n$ in Γ, we have

$$[\Delta_i : \Delta_i \cap H] \leq [\Delta \times \Delta : H] \leq n,$$

while if K has index $\leq n$ in Δ_2, then $\Delta_1 K$ has the same index in Γ. Keeping this in mind, we compute the following string of containments:

$$\begin{aligned} \Delta_1 \Lambda_{\Delta_2}(n) = \left(\bigcap_{\substack{K \leq \Delta_2 \\ [\Delta_2 : K] \leq n}} \Delta_1 K \right) &\geq \Lambda_{\Delta_1 \times \Delta_2}(n) = \left(\bigcap_{\substack{H \leq \Delta_1 \times \Delta_2 \\ [\Delta_1 \times \Delta_2 : H] \leq n}} H \right) \\ &\geq \left(\Delta_1 \bigcap_{\substack{H \leq \Delta_1 \times \Delta_2 \\ [\Delta_1 \times \Delta_2 : H] \leq n}} H \cap \Delta_2 \right) \geq \left(\bigcap_{\substack{S \leq \Delta_2 \\ [\Delta_2 : S] \leq n}} S \right) = \Delta_1 \Lambda_{\Delta_2}(n). \end{aligned}$$

Similarly one has that $\Lambda_{\Delta_1}(n)\Delta_2 \geq \Lambda_{\Delta_1 \times \Delta_2}(n) \geq \Lambda_{\Delta_1}(n)$. Thus one has that

$$\Lambda_{\Delta_1}(n)\Lambda_{\Delta_2}(n) = \Lambda_{\Delta_1}(n)\Delta_2 \cap \Delta_1 \Lambda_{\Delta_2}(n) \geq \Lambda_{\Delta_1 \times \Delta_2}(n) \geq \Lambda_{\Delta_1}(n)\Lambda_{\Delta_2}(n)$$

and the result follows.

For part (3) it is enough to notice that the characteristic subgroups of Δ_i can be pulled back to characteristic subgroups of Γ. □

For quotients, the correspondence theorem always yields a lower bound.

Observation 3.4. *Let $N \lhd \Gamma$. Then if $\bullet \in \{<, \max, \lhd, \max\lhd\}$,*

$$i^{\bullet}_{\Gamma/N}(n) \leq i^{\bullet}_{\Gamma}(n).$$

For extensions, one still has upper bounds.

Proposition 3.5. *Suppose that $1 \longrightarrow N \longrightarrow \Gamma \longrightarrow Q \longrightarrow 1$ is exact. Then*

$$i^{\bullet}_{\Gamma}(n) \leq i^{\bullet}_{N}(n) \cdot i^{\bullet}_{Q}(n),$$

where $\bullet$ is $\lhd$ or $<$. The same bound holds for max *and* $\max\lhd$ *when the extension is split.*

Proof. This follows from the fact that if $\Delta \subset \Gamma$ is a subgroup and Δ_N, Δ_Q are its intersection with N and projection to Q, then we have

$$\max([\Delta : \Delta_N], [Q : \Delta_Q]) \ \leq\ [\Gamma : \Delta] \ \leq\ [\Delta : \Delta_N] \cdot [Q : \Delta_Q].$$

The split assumption is used in the latter two cases to show that if Δ is maximal or maximal normal in Γ, then so are $\Delta_N < N$ and $\Delta_Q < Q$. □

4. The profinite perspective

If Γ is a finitely generated group, its *profinite completion* $\widehat{\Gamma}$ is the inverse limit of the system of finite quotients of Γ, taken in the category of topological groups. In fact, intersection growth is really a profinite invariant, in that it only depends on the profinite completion of the group Γ.

Lemma 4.1. *Let Γ be a finitely generated group and let $\widehat{\Gamma}$ be its profinite completion. Then $i^{\bullet}_{\Gamma}(n) = i^{\bullet}_{\widehat{\Gamma}}(n)$ for every positive integer n, where $\bullet$ is one of $<, \max, \lhd, c, \max\lhd$.*

Proof. This follows from the observation that there is a bijection between finite index subgroups of Γ and finite index closed subgroups of $\widehat{\Gamma}$ that preserves intersections. In the definition of $i^{\bullet}_{\widehat{\Gamma}}$ we can either take all finite index subgroups or all closed finite index subgroups, as by a result of Nikolov and Segal [NS07] all finite index subgroups in a topologically finitely generated profinite groups are closed, so there is no difference in either case. □

The profinite completion of Γ can also be considered as a metric completion. Namely, a *profinite metric* on Γ is defined by fixing a decreasing function $\rho : [0,\infty) \to [0,\infty)$ with $\lim_{x\to\infty} \rho(x) = 0$ and letting

$$d_\rho(g,h) := \rho\left(\min\{[\Gamma : \Delta] : \Delta \lhd \Gamma, gh^{-1} \notin \Delta\}\right).$$

When Γ is residually finite, d_ρ is a metric on Γ, while in general it defines a metric on the quotient of Γ by the intersection of its finite index subgroups. In any case, the metric completion of this space is homeomorphic to $\widehat{\Gamma}$.

Now let X be a metric space and consider a subset $S \subset X$. Recall that the *d-dimensional Hausdorff content* of S is defined by

$$C^d_H(S) := \inf\left\{\sum_i r_i^d : \text{ there is a cover of } S \text{ by balls of radii } r_i > 0\right\},$$

and the *Hausdorff dimension* of X is $\dim_H(X) := \inf\{d \geq 0 : C_H^d(X) = 0\}$.

We then have the following Proposition.

Proposition 4.2. *If Γ is a group,* $\dim_H(\widehat{\Gamma}) = -\liminf_{n\to\infty} \frac{\log i_\Gamma^{\triangleleft}(n)}{\log \rho(n)}$.

For instance, if $\rho(n) = e^{-n}$ then the Hausdorff dimension is the coefficient c in exponential intersection growth e^{cn}. If $\rho(n) = \frac{1}{n}$, then $\dim_H(\widehat{\Gamma})$ is the degree of polynomial intersection growth.

There is actually no difference in Hausdorff dimension between the profinite completion $\widehat{\Gamma}$ and the group Γ, considered with the (pseudo)-metric d_ρ. A priori, the Hausdorff dimension of Γ could be less, but the second half of the proof below works just as well for Γ as for $\widehat{\Gamma}$.

For simplicity, we stated this proposition for normal intersection growth. However, after changing the definition of d_ρ by considering only subgroups Δ in a class $\bullet$, an analogous result follows for $\bullet$-intersection growth.

Proof. The main point here is that $B_{d_\rho}(e, \rho(n)) = \overline{\Lambda_\Gamma^{\triangleleft}(n)}$, where the set on the left is the ball of radius $\rho(n)$ around the origin in $\widehat{\Gamma}$ and the set on the right is the profinite closure. To prove that

$$\dim_H(\widehat{\Gamma}) \geq -\liminf_{n\to\infty} \frac{\log i_\Gamma^{\triangleleft}(n)}{\log \rho(n)},$$

we just note that if d is greater than the right-hand side then there are arbitrarily large n such that

$$d \geq -\frac{\log i_\Gamma^{\triangleleft}(n)}{\log \rho(n)}.$$

However this implies that $i_\Gamma^{\triangleleft}(n) \leq \rho(n)^{-d}$, so using cosets of $\overline{\Lambda_\Gamma^{\triangleleft}(n)}$ we can cover $\widehat{\Gamma}$ with at most $\rho(n)^{-d}$ balls of radius $\rho(n)$. Therefore, we have that the d-dimensional Hausdorff content of $\widehat{\Gamma}$ is at most 1. This proves the first half of the proposition.

We must now show that

$$\dim_H(\widehat{\Gamma}) \leq -\liminf_{n\to\infty} \frac{\log i_\Gamma^{\triangleleft}(n)}{\log \rho(n)}.$$

That is, if d is less than the right-hand side then we need to show that the d-dimensional Hausdorff content of $\widehat{\Gamma}$ is greater than zero. Suppose that $\{B_i\}$ are balls with radii $\rho(n_i)$ that cover $\widehat{\Gamma}$. Choosing the radii to be small, we may assume that all n_i are large enough that $d < -\frac{\log i_\Gamma^{\triangleleft}(n)}{\log \rho(n)}$. If μ is the Haar (probability) measure on $\widehat{\Gamma}$, then

$$1 \leq \sum_i \mu(B_i) = \sum_i \frac{1}{i_\Gamma^{\triangleleft}(n_i)} \leq \sum_i \rho(n_i)^d,$$

which shows that the d-dimensional Hausdorff content of $\widehat{\Gamma}$ is at least 1. $\square$

5. Intersection growth of polycyclic groups

We begin this section with determining intersection growths of finitely generated abelian groups.

Proposition 5.1. *For the group $\mathbb{Z}^k$, we have $i_{\mathbb{Z}^k}(n) = \operatorname{lcm}\{1,\ldots,n\}^k$, and $i_{\mathbb{Z}^k}^{\max}(n) = \operatorname{lcm}\{p \mid p < n, p\text{-prime}\}^k$.*

Proof. Using Proposition 3.3, it is enough to verify the statement for $k=1$. Since $\mathbb{Z}$ has a unique (automatically normal) subgroup of index l for each l,

$$\Lambda_{\mathbb{Z}}^{<}(n) = \bigcap_{l\leq n} l\mathbb{Z} = \operatorname{lcm}\{1,\dots,n\}\mathbb{Z}.$$

Now Corollary A.3 yields that $i_{\mathbb{Z}}^{<}(n) = \operatorname{lcm}(1,\dots,n) \dot{\sim} e^n$.

The situation with maximal subgroups is similar – the subgroup $l\mathbb{Z}$ is maximal in $\mathbb{Z}$ only when l is prime, so

$$\Lambda_{\mathbb{Z}}^{\max}(n) = \bigcap_{p\leq n} p\mathbb{Z} = \left(\prod_{p\leq n} p\right)\mathbb{Z},$$

and $i_{\mathbb{Z}}^{\max}(n) = \left(\prod_{p\leq n} p\right) \dot{\sim} e^n$.

One can also give a profinite version of this argument, as $i_{\mathbb{Z}}^{\bullet} = i_{\widehat{\mathbb{Z}}}^{\bullet}$ by Lemma 4.1. The Chinese reminder theorem gives that $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$, so one only needs to compute the functions $i_{\mathbb{Z}_p}^{\bullet}$ and apply Proposition 3.3. $\square$

Combined with Proposition 3.3 and the prime number theorem (see Corollary A.3), Proposition 5.1 gives

Corollary 5.2. *If Γ is a finitely generated abelian group, then*

$$i_\Gamma^{\bullet}(n) \dot{\sim} e^n,$$

where $\bullet \in \{<, \max, \lhd, \max\lhd\}$. Moreover, if Γ has rank k, then

$$\log i_\Gamma^{\bullet}(n) \sim kn.$$

As in Section 3, $f \preceq g$ means that the $\limsup_{n\to\infty} f(n)/g(n) \leq 1$. Most of our calculations of $\log i_\Gamma^{\bullet}(n)$ only work up to multiplicative error, but in the beginning of this section some finer calculations are possible.

Recall that a *polycyclic group* Γ is a group that admits a subnormal series

$$\Gamma = \Gamma_1 \rhd \Gamma_2 \rhd \cdots \rhd \Gamma_k = \{e\}$$

in which all the quotients Γ_i/Γ_{i+1} are cyclic. Examples include finitely generated nilpotent groups and extensions of such groups by finitely generated abelian groups. The number of infinite factors Γ_i/Γ_{i+1} in such a subnormal series is called the *Hirsch length* of Γ.

Proposition 5.3. *Any infinite polycyclic group Γ has $i_\Gamma^{<}(n) \dot{\sim} e^n$. Specifically, we have that $\frac{n}{c} \preceq \log i_\Gamma^{<}(n) \preceq kn$, where c is the smallest index of a subgroup of Γ with infinite abelianization and k is the Hirsch length of Γ.*

Proof. Suppose that Δ is an index c subgroup of Γ with infinite abelianization. Then by Lemma 3.1, $i_\Gamma^{<}(n) \leq c \cdot i_\Delta^{<}(n) \leq i_\Gamma^{<}(cn)$. Observation 3.4 now yields the lower bound, since $\log i_\Delta^{<}(n) \geq \log i_{\Delta^{ab}}^{<}(n) \succeq n$. For the upper bound, let $N < \Delta$ be a subgroup with Δ/N infinite cyclic. Then as N has Hirsch length $k-1$, we have by induction, Proposition 3.5, and Corollary 5.2 that

$$\log i_\Gamma^{<}(n) \preceq \log i_\Delta^{<}(n) \preceq n + (k-1)n = kn. \quad \square$$

Proposition 5.3 certainly gives upper bounds for the normal, maximal normal, and maximal intersection growth of polycyclic groups. However, we remind the reader that as in Example 3.2 these upper bounds may not be sharp. In fact, the same example illustrates how the lower bound for $i_\Gamma(n)$ may be affected by the index of a subgroup with infinite abelianization.

6. INTERSECTION GROWTH OF $\mathrm{SL}_k(\mathbb{Z})$

Here is a first calculation of intersection growth in a non-polycyclic group.

Theorem 6.1. *For the special linear groups* $\mathrm{SL}_k(\mathbb{Z})$*, where* $k \geq 3$*, we have*

$$i^{c}_{\mathrm{SL}_k(\mathbb{Z})}(n) \precsim i^{\triangleleft}_{\mathrm{SL}_k(\mathbb{Z})}(n) \sim i^{\max\triangleleft}_{\mathrm{SL}_k(\mathbb{Z})}(n) \precsim e^{n^{1/(k^2-1)}}, \quad \textit{but} \quad i^{<}_{\mathrm{SL}_k(\mathbb{Z})}(n) \sim i^{\max}_{\mathrm{SL}_k(\mathbb{Z})}(n) \precsim e^{n^{1/(k-1)}}.$$

As mentioned in the introduction this result extends many high rank -arithmetic groups, where the roles of k^2-1 and $k-1$ are played by the dimension of the group and the dimension of the smallest projective variety on which the group acts faithfully, see Appendix B for details.

Proof of Theorem 6.1. One of the main ingredients in the proof is the congruence subgroup property. One way to state this is that the map

$$\pi : \widehat{\mathrm{SL}_k(\mathbb{Z})} \to \mathrm{SL}_k(\widehat{\mathbb{Z}})$$

is an isomorphism. Here $\widehat{\mathrm{SL}_k(\mathbb{Z})}$ denotes the profinite completion of the group $\mathrm{SL}_k(\mathbb{Z})$ and $\widehat{\mathbb{Z}}$ is the profinite completion of the ring $\mathbb{Z}$. Since $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$, we have a product decomposition

$$\widehat{\mathrm{SL}_k(\mathbb{Z})} \simeq \prod_p \mathrm{SL}_k(\mathbb{Z}_p). \tag{1}$$

So, Proposition 3.3 reduces the computation of $i^{\bullet}_{\mathrm{SL}_k(\mathbb{Z})}$ to that of $i^{\bullet}_{\mathrm{SL}_k(\mathbb{Z}_p)}$.

We recall a classical fact from the theory of Moy-Prasad filtrations [MP94], that we will use in our proofs. For this, we set

$$\mathrm{SL}^s_k(\mathbb{Z}_p) = \ker\left(\mathrm{SL}_k(\mathbb{Z}_p) \to \mathrm{SL}_k(\mathbb{Z}_p/p^s\mathbb{Z}_p)\right).$$

The following holds in much greater generality, but we state it only for SL_k. In this case, it can be proved using only elementary methods.

Lemma 6.2. (Moy-Prasad)

(i) $[\mathrm{SL}^i_k(\mathbb{Z}_p), \mathrm{SL}^j_k(\mathbb{Z}_p)] \subset \mathrm{SL}^{i+j}_k(\mathbb{Z}_p)$.

(ii) *For* $1 \leq i \leq k-1$ *the map*

$$\mathrm{SL}^i_k(\mathbb{Z}_p)/\mathrm{SL}^{i+1}_k(\mathbb{Z}_p) \to \mathfrak{sl}(\mathbb{F}_p), \;\; 1 + p^i x \mapsto x \mod p$$

induces an isomorphism of groups, which is equivariant with respect to the action of $\mathrm{SL}(\mathbb{F}_p)$ *on both sides by conjugation.*

Lemma 6.3. *For all but finitely many p, the Lie-algebra* $\mathfrak{sl}(\mathbb{F}_p)$ *has no center, and the adjoint action of* $\mathrm{SL}_k(\mathbb{F}_p)/Z(\mathrm{SL}_k(\mathbb{F}_p))$ *on* $\mathfrak{sl}(\mathbb{F}_p)$ *is faithful and irreducible.*

Proof. As is stated in [BK12, Lemma 3.9], this is a well-known classical result. See there for references. □

Recall that the *Frattini subgroup* of a group G is the intersection of all maximal subgroups of G, and is denoted by $\Phi(G)$. Alternatively, the Frattini subgroup consists of all elements of G that are always redundant in generating sets for G:

$$\Phi(G) = \left\{ g \in G \;\middle|\; \langle \{g\} \cup X \rangle = G \iff \langle X \rangle = G \text{ for every } X \subset G \right\}. \tag{2}$$

Lemma 6.4. *Fixing k, the following is true for all but finitely many primes p. Let* $G = \mathrm{SL}_k(\mathbb{Z}/p^i\mathbb{Z})$ *and let* $\eta : G \longrightarrow \mathrm{SL}_k(\mathbb{Z}/pZ)$ *be the reduction map. Then*

$$\Phi(G) = Z(G)\ker\eta.$$

This result is well-known, and the standard reference is [LS03, Lemma 16.4.5]. However, the proof given there is only a sketch and does not apply to the case $G = \mathrm{SL}_k$ since SL_k is not a simple algebraic group. So for completeness, we include an elementary proof here.

Proof. We'll prove the cases $i = 1, 2$ directly, and then proceed by induction on i. We'll assume always that $p > 3$, adding additional assumptions when necessary. Then for all i,

$$Z(G) \subseteq \Phi(G) \subseteq Z(G) \ker \eta. \tag{3}$$

The first inclusion is because G is perfect. The second inclusion follows from the fact that the Frattini subgroup of $\mathrm{PSL}_k(\mathbb{Z}/p\mathbb{Z})$ is trivial (intersect all line stabilizers).

So, it suffices to show that $\ker \eta \leq \Phi(G)$.

The case $i = 1$: Here, $\ker \eta = \{1\}$, so the lemma follows.

The case $i = 2$: Let $h \in \ker \eta$. With (2) in mind, suppose $\langle X, h \rangle = G$ and $\langle X \rangle \neq G$. By Lemma 6.2 and Lemma 6.3, $\langle X, h \rangle = G$ acts irreducibly on $\ker \eta$ by conjugation. But h acts trivially, so $\langle X \rangle$ acts irreducibly as well. Hence, $\langle X \rangle \cap \ker \eta = \{1\}$. But we also have $\langle X \rangle \ker \eta = G$, so $\langle X \rangle$ is the image of a section for η:

$$\langle X \rangle = \mathrm{Im}(\nu), \ \text{ where } \ \nu : \mathrm{SL}_k(\mathbb{Z}/p\mathbb{Z}) \longrightarrow G, \ \ \eta \circ \nu = id.$$

We claim this is impossible. Recall that the p-Sylow subgroups of $\mathrm{SL}_k(\mathbb{Z}/p\mathbb{Z})$ are the conjugates of N, subgroup of upper triangular matrices with 1's along the diagonal. Because $\ker \eta$ is a p-group, the p-Sylow subgroups of G are the conjugates of

$$\eta^{-1}(N) = \nu(N) \ker \eta.$$

Note that N is generated by elements of order p, e.g. by the elementary matrices, and every element of $\ker \eta$ has order p. Any p-group of order at most p^p is regular, and in a regular p-group the set of elements of order p is a group [Hall59, Ch. 12.4]. So, as long as $|\eta^{-1}(N)| \leq p^p$, which is the case for large p, $\eta^{-1}(N)$ has exponent p. This is impossible, since it is a p-Sylow subgroup of G, but any elementary matrix in G has order p^2.

The case $i > 2$: Proceeding by induction, let

$$G^{i-1} = \ker \big(\mathrm{SL}_k(\mathbb{Z}/p^i\mathbb{Z}) \longrightarrow \mathrm{SL}_k(\mathbb{Z}/p^{i-1}\mathbb{Z}) \big).$$

It suffices to show that the Frattini subgroup of G contains G^{i-1}, since then the induction hypothesis will imply that it contains $\ker \eta$.

So, let $h \in G^{i-1}$ and suppose that $\langle X, h \rangle = G$. To show that the generator h is redundant, we will prove that $\langle X \rangle$ contains the entire subgroup G^{i-1}. Now G^{i-1} is generated by elementary matrices of the form $E_{ij}^{p^{i-1}}$, where E_{ij} has ones along the diagonal and in the (ij)-entry and is zero elsewhere. So, we claim that these generators lie in $\langle X \rangle$.

As $E_{ij}^{p^{i-2}} \in G = \langle X \rangle G^{i-1}$, we can write it as

$$E_{ij}^{p^{i-2}} = xy, \ \ x \in \langle X \rangle, \ y \in G^{i-1}.$$

By Lemma 6.2, the elements $E_{ij}^{p^{i-2}}$ and y commute, so

$$X \ni x^p = (E_{ij}^{p^{i-2}} y^{-1})^p = \big(E_{ij}^{p^{i-2}}\big)^p y^{-p} = E_{ij}^{p^{i-1}},$$

as all $y \in G^{i-1}$ have order p. It follows that $\langle X \rangle$ contains all of G^{i-1}. □

Fix $k \geq 3$ and a prime p. If H is a subgroup of finite index in $\mathrm{SL}_k(\mathbb{Z}_p)$, then by the congruence subgroup property, there is a minimal non-negative integer s, called the *level* of H, such that H contains the congruence subgroup $\mathrm{SL}_k^s(\mathbb{Z}_p)$. By row reduction, $\mathrm{SL}_k^s(\mathbb{Z}_p)$ is generated by the p^s-powers of the elementary matrices $\{E_{ij}\}$, where E_{ij} has ones on the diagonal and in the ij^{th} entry, and is zero elsewhere.

We remark that in the following lemma, one can take $c = 1$ if one removes finitely many primes p.

Lemma 6.5. *Fixing k, there is some $c > 0$ with the following property. If H is a subgroup of $\mathrm{SL}_k(\mathbb{Z}_p)$ of level s, then $[\mathrm{SL}_k(\mathbb{Z}_p) : H] \geq cp^s$.*

Proof. When $s = 1$, the minimal index of a finite-index subgroup of $\mathrm{PSL}(n,p)$ is $(p^n - 1)/(p-1)$ for all primes $p > 4$, (see, for instance, [C78], the statement is also true for all prime powers greater than 4). So, taking c sufficiently small gives the desired inequality.

For the general case, we will show that if H is a subgroup of level $s \geq 2$ then $H \cdot \mathrm{SL}_k^{s-1}(\mathbb{Z}_p)$ is a subgroup of level $s-1$. From this, the index bound will follow by induction, since as $\mathrm{SL}_k^{s-1}(\mathbb{Z}_p)$ is a p-group the index of $H \cdot \mathrm{SL}_k^{s-1}(\mathbb{Z}_p)$ in $\mathrm{SL}_k^{s-1}(\mathbb{Z}_p)$ is at least p. We split the remaining cases into two parts depending on s.

The case $s = 2$: Let B be the finite set of primes where Lemma 6.4 fails. For every $p \in B$, there are only finitely many finite-index subgroups of $\mathrm{SL}_k(\mathbb{Z}_p)$ of level 2. Hence as B is a finite set, by selecting c to be sufficiently small we can handle all such primes. Thus, we continue assuming that Lemma 6.4 holds. Since H is a proper subgroup of $\mathrm{SL}_k(\mathbb{Z}_p)$ it follows that $H \cdot \mathrm{SL}_k^1(\mathbb{Z}_p)$ is a proper subgroup, as $\Phi(\mathrm{SL}_k(\mathbb{Z}_p)) = SL_k^1(\mathbb{Z}_p)$ by Lemma 6.4. Hence, $H \cdot \mathrm{SL}_k^1(\mathbb{Z}_p)$ has level 1, as desired.

The case $s > 2$: If $H \cdot \mathrm{SL}_k^{s-1}(\mathbb{Z}_p)$ does not have level $s-1$, it contains $\mathrm{SL}_k^{s-2}(\mathbb{Z}_p)$. So, every element of $\mathrm{SL}_k^{s-2}(\mathbb{Z}_p)$ is congruent mod p^{s-1} to an element of H. In particular, for every i, j,

$$E_{ij}^{p^{s-2}} y \in H, \text{ for some } y \in \mathrm{SL}_k^{s-1}(\mathbb{Z}_p).$$

Lemma 6.2 implies that $E_{ij}^{p^{s-2}}$ and y commute modulo $\mathrm{SL}_k^s(\mathbb{Z}_p)$. So as

$$\left(E_{ij}^{p^{s-2}} y\right)^p \in H,$$

we have $E_{ij}^{p^{s-1}} y^p \in H$ as well. But $y^p \in \mathrm{SL}_k^s(\mathbb{Z}_p) \subset H$, so $E_{ij}^{p^{s-1}} \in H$. As i and j were arbitrary, $\mathrm{SL}_k^{s-1}(\mathbb{Z}_p) \subset H$, contradicting that the level of H is s. □

Corollary 6.6. *There exists $C \geq 1$ such that for every $n \in \mathbb{N}$, we have*

$$i^{<}_{\mathrm{SL}_k(\mathbb{Z}_p)}(n) \leq Cn^{k^2-1}.$$

For all but finitely many primes, we may take $C = 1$.

Proof. From Lemma 6.5, there is $c > 0$ such that every subgroup of $\mathrm{SL}_k(\mathbb{Z}_p)$ with index at most cn has level at most $\lfloor \log_p(n) \rfloor$. So, the intersection of all such subgroups contains $\mathrm{SL}_k^{\lfloor \log_p n \rfloor}(\mathbb{Z}_p)$. As $[\mathrm{SL}_k(\mathbb{Z}_p) : \mathrm{SL}_k^{\lfloor \log_p n \rfloor}(\mathbb{Z}_p)] \leq n^{k^2-1}$, we can take $C = \left(\frac{1}{c}\right)^{k^2-1}$. □

The careful reader may recall that there was also a $k^2 - 1$ in the statement of Theorem 6.1, and may then be confused by the fact that it only appears in the part about $i^{\triangleleft}_{\mathrm{SL}_k(\mathbb{Z}_p)}(n)$, while Corollary 6.6 refers to $i^{<}_{\mathrm{SL}_k(\mathbb{Z}_p)}(n)$. However, all we will ever use about Corollary 6.6 is that it gives a polynomial upper bound. The constants appearing in Theorem 6.1 actually come instead from the following well known lemma.

Lemma 6.7 (Maximal subgroups of $\mathrm{SL}_k(\mathbb{Z}_p)$)**.** *For all but finitely many primes p,*

(1) *There is a unique maximal normal subgroup N of* $\mathrm{SL}_k(\mathbb{Z}_p)$*, the kernel of the map* $\mathrm{SL}_k(\mathbb{Z}_p) \longrightarrow \mathrm{PSL}_k(\mathbb{F}_p)$*, which has index* $|\mathrm{PSL}_k(\mathbb{F}_p)|$*, and*

$$(p/2)^{k^2-1} \leq |\mathrm{PSL}_k(\mathbb{F}_p)| \leq p^{k^2-1}.$$

(2) *The subgroups of* $\mathrm{SL}_k(\mathbb{Z}_p)$ *with smallest index have index* $\frac{p^k-1}{p-1}$*, and the intersection of all such subgroups is the normal subgroup N in (1). Here, note that*

$$(p/2)^{k-1} \leq \frac{p^k-1}{p-1} \leq 2p^{k-1}.$$

Proof. If N is a maximal normal subgroup of $\mathrm{SL}_k(\mathbb{Z}_p)$, then the maximal subgroup (amongst all subgroups) containing N must be proper. This maximal subgroup, by definition of the Frattini subgroup, contains $\Phi(\mathrm{SL}_k(\mathbb{Z}_p))$. Thus the group, $N\Phi(\mathrm{SL}_k(\mathbb{Z}_p))$, is proper. Since Frattini subgroups are always normal, it follows from maximality (over all normal subgroups) of N that $\Phi(\mathrm{SL}_k(\mathbb{Z}_p)) \leq N$. Hence, Statement (1) follows from Lemma 6.4 and the fact that $\mathrm{PSL}_k(\mathbb{F}_p)$ is a finite simple group.

For (2), Lemma 6.4 implies that any minimal index subgroup $\mathrm{SL}_k(\mathbb{Z}_p)$ contains N, so is the preimage of a minimal index subgroup of $\mathrm{PSL}_k(\mathbb{F}_p)$. By [C78, Table 1], then, this minimal index is $(p^k-1)/(p-1)$ for all primes $p > 4$. As line stabilizers in $\mathrm{PSL}_k(\mathbb{F}_p)$ have this index and intersect trivially, the intersection of all minimal index subgroups of $\mathrm{SL}_k(\mathbb{Z}_p)$ is the kernel N. $\square$

Now we are ready to estimate the intersection group functions of $\mathrm{SL}_k(\mathbb{Z})$. We'll discuss normal intersection growth first, although all the computations are similar. Partition the set of all primes Π into two sets A and B, where B consists of the finitely many primes where the above results fail. By (7),

$$i^{\lhd}_{\mathrm{SL}_k(\mathbb{Z})}(n) \;=\; \prod_{p\in\Pi} i^{\lhd}_{\mathrm{SL}_k(\mathbb{Z}_p)}(n).$$

Note that Lemma 6.7 implies that $i^{\lhd}_{\mathrm{SL}_k(\mathbb{Z}_p)}(n) = 1$ when $p > 2\sqrt[k^2-1]{n}$ and $p \in B$. Thus,

$$i^{\lhd}_{\mathrm{SL}_k(\mathbb{Z})}(n) \;=\; \prod_{p\leq 2\sqrt[k^2-1]{n}} i^{\lhd}_{\mathrm{SL}_k(\mathbb{Z}_p)}(n) \prod_{p\in B} i^{\lhd}_{\mathrm{SL}_k(\mathbb{Z}_p)}(n).$$

Thus, as B is a finite set, applying Corollary 6.6,

$$i^{\lhd}_{\mathrm{SL}_k(\mathbb{Z})}(n) \;\leq \prod_{p\in B} i^{\lhd}_{\mathrm{SL}_k(\mathbb{Z}_p)}(n) \prod_{p\leq 2\sqrt[k^2-1]{n}} Cn^{k^2-1} \;\dot{\precsim}\; n^{|A|(k^2-1)}\left(n^{k^2-1}\right)^{\frac{2\sqrt[k^2-1]{n}}{\log(2\sqrt[k^2-1]{n})}} \;\dot{\sim}\; e^{\sqrt[k^2-1]{n}},$$

where we estimate the number of p in the product using the prime number theorem. Only the exponent $\sqrt[k^2-1]{n}$ matters in the result, essentially because $e^{an} \,\dot{\sim}\, e^n$ for all a. Next, as A is finite, we have $d > 0$ such that

$$\begin{aligned} i^{\max\lhd}_{\mathrm{SL}_k(\mathbb{Z})}(n) \;&=\; \prod_{p} i^{\max\lhd}_{\mathrm{SL}_k(\mathbb{Z}_p)}(n) \geq \prod_{p\leq \sqrt[k^2-1]{n},\, p\in A} i^{\max\lhd}_{\mathrm{SL}_k(\mathbb{Z}_p)}(n) \\ &\geq d \prod_{p\leq \sqrt[k^2-1]{n}} (p/2)^{k^2-1} \;\dot{\succeq}\; e^{\sqrt[k^2-1]{n}}, \end{aligned}$$

where the first and second inequalities follow from Lemma 6.7, and the last is Lemma A.2. Combining the upper and lower bounds, we have

$$e^{\sqrt[k^2-1]{n}} \succeq i^{\triangleleft}_{\mathrm{SL}_k(\mathbb{Z})}(n) \succeq i^{c}_{\mathrm{SL}_k(\mathbb{Z})}(n) \succeq i^{\max\triangleleft}_{\mathrm{SL}_k(\mathbb{Z})}(n) \succeq e^{\sqrt[k^2-1]{n}},$$

using that all maximal normal subgroups of $\mathrm{SL}_k(\mathbb{Z})$ are characteristic.

The computations for $i^{<}_{\mathrm{SL}_k(\mathbb{Z})}$ and $i^{\max}_{\mathrm{SL}_k(\mathbb{Z})}$ are essentially the same, but the products are only over $p \leq \sqrt[k-1]{2n}$. This ends the proof of Theorem 6.1. □

7. Intersection growth of nonabelian free groups

By Observation 3.4, the free group of rank k has the fastest-growing intersection growth functions among groups generated by k elements. Here are their asymptotics:

Theorem 7.1. *Let $\mathscr{F}^k$ be the rank k free group, $k \geq 2$. Then*

$$i^{\max\triangleleft}_{\mathscr{F}^k}(n) \mathrel{\dot\sim} e^{\left(n^{k-2/3}\right)} \quad \text{and} \quad i^{\max}_{\mathscr{F}^k}(n) \mathrel{\dot\sim} i^{<}_{\mathscr{F}^k}(n) \mathrel{\dot\sim} e^{(n^n)}.$$

The proof for $i^{\max\triangleleft}_{\mathscr{F}^k}(n)$ uses the classification theorem for finite simple groups: we calculate separately the index of the intersection of subgroups with quotient a fixed finite simple group and then combine these estimates to give the asymptotics above. In fact, we will show that the growth rate of $i^{\max\triangleleft}_{\mathscr{F}^k}(n)$ is dictated by subgroups with quotient $\mathrm{PSL}_2(p)$. The contributions of other families of finite simple groups are comparatively negligible.

The lower bound for $i^{\max}_{\mathscr{F}^k}(n)$ and $i^{<}_{\mathscr{F}^k}(n)$ comes from the alternating group $A(n)$. Since the (maximal) index n subgroups of $A(n)$ intersect trivially, one automatically gets a factorial lower bound for intersection growth from any surjection $\mathscr{F}^k \longrightarrow A(n)$. We will see that multiplying the estimates that one gets from all possible surjections gives the lower bound of e^{n^n}. As this requires some of the same machinery as does the calculation of $i^{\max\triangleleft}_{\mathscr{F}^k}(n)$, we will finish this argument at the end of the section.

However, the proof of the upper bound of $e^{(n^n)}$ is completely general:

Proposition 7.2. *If Γ is a finitely generated group, then $i^{<}_{\Gamma}(n) \mathrel{\dot\preceq} e^{n^n}$.*

Proof. If $H \leq \Gamma$ is a subgroup with index i, then H contains the kernel of the map $\Gamma \longrightarrow S_i$ determined by the action of Γ on the cosets of H. Thus,

$$\bigcap_{H \leq \Gamma, [\Gamma:H]=i} H \;\supseteq\; \bigcap_{f:\Gamma\to S_i} \ker f.$$

Each such kernel has index at most $i!$, and if Γ is k-generated, there are at most $(i!)^k$ homomorphisms from Γ to S^i. So, this implies that

$$i^{<}_{\Gamma}(n) \leq \prod_{i=1}^{n} (i!)^{(i!)^k} \mathrel{\dot\sim} \prod_{i=1}^{n} (i^i)^{(i^i)} \mathrel{\dot\sim} \prod_{i=1}^{n} (i^{i^i}) \mathrel{\dot\sim} \prod_{i=1}^{n} (e^{i^i}) \mathrel{\dot\sim} e^{n^n}. \quad \square$$

We now start on the calculation of the asymptotics of $i^{\max\triangleleft}_{\mathscr{F}^k}(n)$. The key is to consider first the index of the intersection of subgroups with a specific quotient and then to analyze how these estimates combine. As abelian quotients are easy to handle, we focus mostly on the non-abelian case.

Fix a finite simple group S and let $i_{\mathscr{F}^k}(S)$ be the index of the subgroup

$$\Lambda_{\mathscr{F}^k}(S) = \bigcap_{\substack{\Delta \triangleleft \mathscr{F}^k \\ \mathscr{F}^k/\Delta \cong S}} \Delta \;\leq\; \mathscr{F}^k.$$

Proposition 7.3. *If S is a non-abelian finite simple group, then $\mathscr{F}^k/\Lambda_{\mathscr{F}^k}(S) \cong S^{d(k,s)}$, where $d(k,S)$ is the number of $\Delta \lhd \mathscr{F}^k$ with $\mathscr{F}^k/\Delta \cong S$.*

Proof. If $\Delta_1, \ldots, \Delta_i \trianglelefteq \mathscr{F}^k$ are distinct normal subgroups with $\mathscr{F}^k/\Delta_i \cong S$, then

$$\begin{array}{rccc} \varphi: & \mathscr{F}^k/(\Delta_1 \cap \ldots \cap \Delta_i) & \hookrightarrow & \mathscr{F}^k/\Delta_1 \times \cdots \times \mathscr{F}^k/\Delta_i, \\ & g(\Delta_1 \cap \ldots \cap \Delta_i) & \mapsto & (g\Delta_1, \ldots, g\Delta_i). \end{array}$$

is the required isomorphism. □

The advantage of Proposition 7.3 is that $d(k,S)$ is easily computed: namely, observe that $d(k,S)$ measures exactly the number of generating k-tuples in S, modulo the action of the automorphism group $\mathrm{Aut}(S)$. In other words, we have the following

Lemma 7.4. *If S is a non-abelian finite simple group, then*

$$d(k,S) = p(k,S)\frac{|S|^k}{|\mathrm{Aut}(S)|} \sim \frac{|S|^{k-1}}{|\mathrm{Out}(S)|},$$

where $p(k,S)$ is the probability that a k-tuple of elements in S generates.

Proof. For the first equality, note that under the action of $\mathrm{Aut}(S)$ on S^k each generating tuple has orbit of size $|\mathrm{Aut}(S)|$. Since S is non-abelian and simple, the conjugation action of S is faithful, so $|\mathrm{Aut}(S)| = |S||\mathrm{Out}(S)|$. Finally, Liebeck-Shalev [LS95] and Kantor-Lubotzky [KL90] have shown that for any fixed k the probability $p(k,s)$ tends to 1 as $|S| \to \infty$, which gives the asymptotic estimate. □

We mention that recently Menezes, Quick and Roney-Dougal [MQR13, Theorem 1.3] have given an explicit lower bound for $d(k,S)$ and show when it can be attained.

Corollary 7.5. *There is some fixed $\varepsilon > 0$ such that if S is a finite non-abelian simple group, then we have the estimate*

$$|S|^{\varepsilon \cdot \frac{|S|^{k-1}}{|\mathrm{Out}(S)|}} \leq i_{\mathscr{F}^k}(S) \leq |S|^{\frac{|S|^{k-1}}{|\mathrm{Out}(S)|}}.$$

To calculate $i^{\max \lhd}_{\mathscr{F}^k}(n)$, we now analyze the intersections of subgroups of $\mathscr{F}^k$ with quotients lying in a given infinite family of finite simple groups. Table 1 gives the classification of infinite families; the list includes all finite simple groups other than the finitely many 'sporadic' groups.

Let $i^{\mathscr{G}}_{\mathscr{F}^k}(n)$ be the index of the intersection of all normal subgroups of $\mathscr{F}^k$ with index at most n and quotient lying in a family $\mathscr{G}$ of finite simple groups. It will be convenient to split the rows in Table 1 into *single parameter* families: if a row has two indices, we fix m while varying q. Examples of single parameter $\mathscr{G}$ include A, ${}^2E_6$, PSL_2, PSL_3, etc.

Proposition 7.6. *There is a product formula*

$$i^{\max \lhd}_{\mathscr{F}_k}(n) \ \dot{\sim} \prod_{\substack{\textit{single parameter} \\ \textit{families } \mathscr{G}}} i^{\mathscr{G}}_{\mathscr{F}_k}(n) \ = \ \prod_{\mathscr{G}} \prod_{\substack{S \in \mathscr{G} \\ |S| \leq n}} i_{\mathscr{F}^k}(S).$$

The multiplicative discrepancy is due to the absence of the sporadic groups in the product: since there are only finitely many of them they contribute at most a multiplicative constant to $i_{\mathscr{F}^k}$. Also, although the product is infinite, for each n there are at most Cn non-unit factors for some universal C.

Family	Approximate Order	Approximate $\lvert\mathrm{Out}\rvert$
$\mathbb{Z}/p\mathbb{Z}$, p prime	p	$p-1$
$A(m), m \geq 5$	$\frac{m!}{2}$	2, unless $m=6$
$\mathrm{PSL}_m(q), m \geq 2$	$\frac{1}{(m,q-1)}q^{m^2-1}$	$(m,q-1)\cdot s$
$B_m(q), m \geq 2$	$\frac{1}{(2,q-1)}q^{2m^2+m}$	s
$C_m(q), m \geq 3$	$\frac{1}{(2,q-1)}q^{2m^2+m}$	s
$D_m(q), m \geq 4$	$\frac{1}{(4,qm-1)}q^{2m^2-m}$	s
${}^2A_m(q^2), m \geq 2$	$\frac{1}{(m+1,q-1)}q^{m^2+2m+1}$	$(m+1,q+1)\cdot s$
${}^2D_m(q^2), m \geq 4$	$\frac{1}{(4,q^m+1)}q^{2m^2-m}$	s
$E_6(q)$	$\frac{1}{(3,q-1)}q^{78}$	s
$E_7(q)$	$\frac{1}{(2,q-1)}q^{133}$	s
$E_8(q)$	q^{248}	s
$F_4(q)$	q^{52}	s
$G_2(q)$	q^{14}	s
${}^2E_6(q^2)$	$\frac{1}{(3,q+1)}q^{78}$	s
${}^3D_4(q^3)$	q^{28}	s
${}^2B_2(2^{2j+1})$	q^5, where $q=2^{2j+1}$	$2j+1$
${}^2G_2(3^{2j+1})$	q^7, where $q=3^{2j+1}$	$2j+1$
${}^2F_4(2^{2j+1})$	q^{26}, where $q=2^{2j+1}$	$2j+1$

TABLE 1. Infinite families of finite simple groups, their sizes and the sizes of their outer automorphism groups. We assume $m,j \in \mathbb{N}$ and that $q=p^s$ is a prime power. The approximations given are true up to a universal multiplicative error (see [CCNPW85] for a reference of the table).

Proof of Proposition 7.6. This follows inductively from the fact that if Δ_1,Δ_2 are normal subgroups of $\mathscr{F}^k$ such that G/Δ_1 and G/Δ_2 have no nontrivial isomorphic quotients, then $\mathscr{F}^k/(\Delta_1 \cap \Delta_2) \cong \mathscr{F}^k/\Delta_1 \times \mathscr{F}^k/\Delta_2$. □

Proposition 7.7. *For a single parameter family $\mathscr{G}$ of finite simple groups,*

1. $\log i^{\mathscr{G}}_{\mathscr{F}^k}(n) \approx n$, *if $\mathscr{G}$ is the family of cyclic groups.*
2. $\log i^{\mathscr{G}}_{\mathscr{F}^k}(n) \approx n^{k-1}$, *if $\mathscr{G} = {}^2B_2, {}^2G_2$, or ${}^2F_4$.*
3. $\log i^{\mathscr{G}}_{\mathscr{F}^k}(n) \precsim n^{k-1}\log(n)$, *if $\mathscr{G} = A$.*
4. $\log i^{\mathscr{G}}_{\mathscr{F}^k}(n) \approx n^{(k-1)+\frac{1}{d}}$, *if $\mathscr{G}$ is one of the remaining families of Lie type and d is the dimension of the corresponding Lie group, which appears in Table 1 as the exponent of q. More specifically, there is some universal C such that* $\log i^{\mathscr{G}}_{\mathscr{F}^k}(n) \leq C \cdot d^{k+\frac{1}{d}} \cdot n^{(k-1)+\frac{1}{d}}$.

As the dimension d is uniquely minimized when $\mathscr{G} = \mathrm{PSL}_2$, this implies that the family PSL_2 has the fastest intersection growth. The point of Theorem 7.1 is that this is faster than the growth of all other families combined.

Proof. The cyclic case is essentially Corollary 5.2. For all the others, we will combine Corollary 7.5 with the product formula in Proposition 7.6.

When $\mathscr{G} = {}^2B_2$, we have that

$$\begin{aligned}
\log i^{\mathscr{G}}_{\mathscr{F}^k}(n) &= \sum_{q \le n} \log\left(|{}^2B_2(q)|^{\frac{|{}^2B_2(q)|^{k-1}}{|\mathrm{Out}|}} \right) \\
&= \sum_{2^{10j+5} \le n} \frac{(2^{10j+5})^{k-1}}{2j+1} \log\left(2^{10j+5}\right) \\
&\dot{\sim}\ n^{k-1},
\end{aligned}$$

where the last step comes from the fact that a sum of exponentially increasing terms is proportional to the last term. The Ree groups ${}^2G_2$ and ${}^2F_4$ admit similar computations. For the alternating group,

$$\log i^{A}_{\mathscr{F}^k}(n) \ \dot{\sim} \sum_{m!/2 \le n} \frac{(m!/2)^{k-1}}{2} \log(m!/2) \ \dot{\preceq}\ n^{k-1} \log(n).$$

Again the sum is proportional to its last term, but if $n = \frac{m!}{2} - 1$, this last term is much smaller than $n^{k-1}\log(n)$, and we stop with the upper bound. The difference between this and the computation for Suzuki and Ree groups is that the gaps between successive factorials are large enough to make an asymptotic estimate that works for all n unwieldy.

For the last case, we use the notation $\le_c, \ge_c, =_c$ for comparisons that are true up to a *universal* multiplicative error, in contrast to those in the statement of the proposition, where the error may depend on the family $\mathscr{G}$.

First, note that from Table 1, for any of the groups $\mathscr{G}(q)$ in (4) we have

$$\frac{1}{d} q^d \le_c \ |\mathscr{G}(q)| \le_c \ q^d,$$

where the $\frac{1}{d}$ is to account for the gcds in $|\mathrm{PSL}_m(q)|$ and $|{}^2A_m(q^2)|$. So for *fixed* $\mathscr{G}$ we have $|\mathscr{G}(q)| \ \dot{\sim}\ q^d$. By Corollary 7.5,

$$\begin{aligned}
\log i_{\mathscr{F}^k}(\mathscr{G}(q)) &\le \log\left(|\mathscr{G}(q)|^{|\mathscr{G}(q)|^{k-1}} \right) \\
&= |\mathscr{G}(q)|^{k-1} \log |\mathscr{G}(q)| \\
&=_c\ d \cdot q^{(k-1)d} \log q.
\end{aligned}$$

Next, we compute

$$\begin{aligned}
\log i^{\mathscr{G}}_{\mathscr{F}^k}(n) &= \sum_{\substack{\text{prime powers } q \\ \text{with } |\mathscr{G}(q)| \le n}} \log i_{\mathscr{F}^k}(\mathscr{G}(q)) \\
&=_c\ d \cdot \sum_{\substack{\text{prime powers } q \\ \text{with } \frac{1}{d \cdot C} q^d \le n}} q^{(k-1)d} \log q \\
&=_c\ d \cdot \left((d \cdot Cn)^{\frac{1}{d}} \right)^{(k-1)d+1} \quad \text{(by Lemma A.2)} \\
&=_c\ d^{k+\frac{1}{d}} \cdot n^{(k-1)+\frac{1}{d}},
\end{aligned}$$

This is the explicit upper bound promised. If now $\mathscr{G}$ is fixed, then d is a constant, so this bound becomes $\dot{\preceq}\ n^{(k-1)+\frac{1}{d}}$.

For the lower bound, it suffices to only consider $\mathscr{G}(p)$ where p is prime. From Table 1, we see that $|\mathrm{Out}(\mathscr{G}(p))|$ is bounded for prime p. Therefore,

$$\log i_{\mathscr{F}^k}(\mathscr{G}(p)) \stackrel{\cdot}{\succeq} \log\left(|\mathscr{G}(p)|^{\frac{|\mathscr{G}(p)|^{k-1}}{|\mathrm{Out}(\mathscr{G}(p))|}}\right) \stackrel{\cdot}{\succeq} d \cdot p^{(k-1)d} \log p.$$

The lower bound then proceeds exactly as above, except that the sums are now over primes rather than prime powers. But as this does not affect the output of Lemma A.2, we see that $\log i^{\mathscr{G}}_{\mathscr{F}^k}(n) \stackrel{\cdot}{\succeq} n^{(k-1)+\frac{1}{d}}$. □

We are now ready to prove the main theorem.

Theorem 7.1. *Let $\mathscr{F}^k$ be the rank k free group, $k \geq 2$. Then*

$$i^{\max\triangleleft}_{\mathscr{F}^k}(n) \stackrel{\cdot}{\sim} e^{\left(n^{k-2/3}\right)}, \quad i^{\max}_{\mathscr{F}^k}(n) \stackrel{\cdot}{\sim} i^{<}_{\mathscr{F}^k}(n) \stackrel{\cdot}{\sim} e^{(n^n)}.$$

Proof. For $i^{\max}_{\mathscr{F}^k}(n)$ and $i^{<}_{\mathscr{F}^k}(n)$, it suffices by Proposition 7.2 to prove that $i^{\max}_{\mathscr{F}^k}(n) \stackrel{\cdot}{\succeq} e^{(n^n)}$. Since the kernel of any surjection $\mathscr{F}^k \longrightarrow A(n)$ is the intersection of (maximal) index n subgroups corresponding to the conjugates of $A(n-1) \subset A(n)$, we have by Corollary 7.5 that

$$i^{\max}_{\mathscr{F}^k}(n) \geq i_{\mathscr{F}^k}(A(n)) \geq (n!/2)^{\varepsilon \cdot \frac{(\frac{n!}{2})^{k-1}}{2}} \stackrel{\cdot}{\sim} e^{n^n}.$$

We next show that $i^{\max\triangleleft}_{\mathscr{F}^k}(n) \stackrel{\cdot}{\sim} e^{\left(n^{k-2/3}\right)}$. By Propositions 7.6 and 7.7,

$$\log i^{\max\triangleleft}_{\mathscr{F}^k}(n) \stackrel{\cdot}{\sim} \sum_{\mathscr{G}} \log i^{\mathscr{G}}_{\mathscr{F}^k}(n) \geq \log i^{\mathrm{PSL}_2}_{\mathscr{F}^k}(n) \stackrel{\cdot}{\sim} n^{k-\frac{2}{3}},$$

which gives the lower bound. For the upper bound, first observe that as the five families of types $(1)-(3)$ in Proposition 7.7 have slower intersection growth than PSL_2, removing them from the sum does not change its asymptotics. Moreover, we only need to sum over type (4) families $\mathscr{G}$ such that $|\mathscr{G}(2)| \leq n$, which implies that the dimension $d \leq C \log n$ for some universal C. So by the explicit estimate in the last part of Proposition 7.7,

$$\begin{aligned}
\sum_{\mathscr{G} \text{ with } d \leq C\log n} \log i^{\mathscr{G}}_{\mathscr{F}^k}(n) &\stackrel{\cdot}{\preceq} \log i^{\mathrm{PSL}_2}_{\mathscr{F}^k}(n) + \sum_{\substack{\text{Type (4) } \mathscr{G} \neq PSL_2 \\ \text{with } d \leq C\log n}} C \cdot d^{k+\frac{1}{d}} \cdot n^{(k-1)+\frac{1}{d}} \\
&\stackrel{\cdot}{\preceq} n^{k-\frac{2}{3}} + \log n \cdot (\log n)^{k+1} \cdot n^{(k-1)+\frac{1}{8}} \\
&\stackrel{\cdot}{\sim} n^{k-\frac{2}{3}}.
\end{aligned}$$

For the second inequality, a consultation of Table 1 shows that in the summation we actually have $8 \leq d \leq C \log n$. Moreover, the number of terms in the sum is at most some constant multiple of $\log n$, which contributes the additional logarithm. □

8. IDENTITIES IN FINITE SIMPLE GROUPS AND RESIDUAL FINITENESS GROWTH

In this section, we discuss relations between the intersection growth function, the residual finiteness growth function, and identities in groups.

Definition. An *identity* or *law* on k letters in a group Γ is a word $w(x_1, \ldots, x_k)$ in the free group $\mathscr{F}^k$ such that $w(g_1, \ldots, g_k) = 1$ for all $g_1, \ldots, g_k \in \Gamma$.

Much work has been devoted to study laws in finite groups. We only mention a few of them. Oates and Powell [OP64] and Kovács and Newman [KN66] find the smallest set of laws which generate every other law in a finite group. Hadad [Had11] and, more recently, Thom and Kozma [KT15], find estimates on the shortest law in a finite simple group. Laws can also be used to characterize classes of groups defined by a set of laws (see the survey by Grunewald, Kunyavskii and Plotkin [GKP12] for the case of solvable groups). A question by Hanna Neumann [Neu67, p. 166] asks if there is a law which is satisfied in an infinite number of non-isomorphic non-abelian finite simple groups. This question has been answered negatively by Jones [Jon74].

Our next result can be seen as an answer to the finite version of Hanna Neumann's question and follows the same line of arguments used in [BM11, KM11], where one finds a law for all finite groups of order at most a given size. We apply our result on maximal intersection growth of $\mathscr{F}^k$ to find identities in all finite simple groups of at most a given size.

Theorem 8.1. *For every positive integer n, there exists a reduced word $w_n \in \mathscr{F}^2$ of length $|w_n| \dot{\preceq} n^{\frac{4}{3}}$ which is an identity on 2 letters for all finite simple groups of size $\leq n$.*

Proof. The proof is essentially an adaptation of the one of Lemma 5 in [KM11] and we mention it here for the reader's convenience.

If $B_2(t)$ denotes the size of the ball of radius t within $\mathscr{F}^2$, we let t grow until the size of $B_k(t)$ is bigger than $[\mathscr{F}^2 : \Lambda_\Gamma^{\max \triangleleft}(n)]$. This counting argument shows that one can find a non-trivial word $w_n \in \Lambda_\Gamma^{\max \triangleleft}(n)$ of length at most $\log[\mathscr{F}^2 : \Lambda_\Gamma^{\max \triangleleft}(n)] = \log i_{\mathscr{F}^2}^{\max \triangleleft}(n) \mathrel{\dot{\sim}} n^{2-\frac{2}{3}}$.

By construction, the word w_n vanishes for any homomorphism of $\mathscr{F}^k$ to a finite simple group Γ of size $\leq n$ and it is thus an identity on Γ. □

Remark 8.2. It seems that the result above can be improved following the methods in [BM11] and [KM11] to build identities as "long commutators". In order to do so, one should use the classification theorem for finite simple groups to verify that, in any finite simple group of size $\leq n$, the order of an element is essentially not bigger that $\sqrt[3]{n}$. From this, one should use the methods in Theorem 1.2 in [BM11] or of Corollary 11 in [KM11] to show that there exists an identity of length $\mathrel{\dot{\sim}} n$ on k letters which holds for every finite group of size $\leq n$. We also refer the reader to the discussion in Remark 15 in [KM11].

Given a finitely generated, residually finite group $\Gamma = \langle S \rangle$ and $g \in \Gamma$, let

$$k_\Gamma(g) = \min\{[\Gamma : N] : g \notin N, N \trianglelefteq \Gamma\}.$$

The *residual finiteness growth function* (also called the *depth function* in [KMS12]) is the function

$$F_\Gamma^S(n) = \max_{g \in B_\Gamma^S(n)} k_\Gamma(g),$$

where $B_\Gamma^S(n)$ denotes the ball of radius n with respect to the generating set S. The growth rate of $F_\Gamma^S(n)$ is independent of the generating set S (see [Bou10]). The function was first introduced by Bou-Rabee in [Bou10] and subsequently it has been computed in several groups [Bou10, Bou11, BM11, BM12, BK12, KM11, KMS12].

As hinted at in the proof of Theorem 8.1, bounds for $i_\Gamma^{\triangleleft}(n)$ easily translate to lower bounds for F_Γ^S using the word growth of Γ. Namely,

Observation 8.3. *If $\Gamma = \langle S \rangle$ is a finitely generated, residually finite group,*

$$|B_\Gamma^S(k)| > i_\Gamma^{\triangleleft}(n) \implies F_\Gamma^S(2k) \geq n.$$

Proof. If $|B_\Gamma^S(k)| > i_\Gamma^{\triangleleft}(n)$ then there is some $w \in B_\Gamma^S(2k)$ that is in every subgroup of Γ with index at most n. □

This observation and Theorem 8.1 lead us to ask the following question:

Question 8.4. *Is it true that* $i^{\triangleleft}_{\mathscr{F}^k}(n) \dot{\sim} i^{\max\triangleleft}_{\mathscr{F}^k}(n)$*? If it is indeed true, then we have the following two consequences:*

(1) *The statement of Theorem 8.1 can be replaced with one which is true for all finite groups of order* $\leq n$ *(and not only simple ones).*
(2) *The residual finiteness growth function satisfies* $F_{\mathscr{F}^2}(n) \dot{\succeq} n^{3/4}$ *(which would improve the current result* $F_{\mathscr{F}^2}(n) \dot{\succeq} n^{2/3}$ *proven in* [KM11]*).*

Appendix A. Number theoretic facts

The prime number theorem states that $\pi(n) \sim n/\log(n)$, where $\pi(n)$ is the number of primes less than or equal to n. We record here some consequences of the prime number theorem used in our asymptotic estimates.

Fact A.1. *If* p_n *is the* n^{th} *prime and* q_n *is the* n^{th} *prime power, then we have*

$$p_n \sim q_n \sim n \log n.$$

Lemma A.2. *Suppose* $n, l \in \mathbb{N}$*. Then*

$$\sum_{\substack{\text{prime powers} \\ q \leq n}} q^l \log(q) \ \dot{\sim} \sum_{\substack{\text{primes} \\ p \leq n}} p^l \log(p) \ \dot{\sim}\ n^{l+1}.$$

Proof. The first asymptotic equality is just the fact that the i^{th} prime is asymptotic to the i^{th} prime power. For the asymptotics, first note that

$$\sum_{\substack{\text{primes} \\ p \leq n}} p^l \log(p) \dot{\sim} \sum_{i \leq \frac{n}{\log(n)}} (i \log i)^l \log(i \log i) \dot{\sim} \sum_{i \leq \frac{n}{\log(n)}} i^l (\log i)^{l+1}$$

So, using integration by parts this is

$$\dot{\sim} \left(\frac{n}{\log n}\right)^{l+1} \left(\log\left(\frac{n}{\log n}\right)\right)^{l+1} - \sum_{i \leq \frac{n}{\log(n)}} i^{l+1} \cdot \frac{1}{i} \log(i)^l$$

However, this latter sum grows slower than $\sum_{i \leq \frac{n}{\log(n)}} i^l (\log i)^{l+1}$, so

$$\sum_{i \leq \frac{n}{\log(n)}} i^l (\log i)^{l+1} \dot{\sim} \left(\frac{n}{\log n}\right)^{l+1} \log^{l+1}(n)$$
$$= n^{l+1}.$$

□

Corollary A.3. $\lim_{n\to\infty} \frac{\log \operatorname{lcm}(1,\ldots,n)}{n} = 1$*, so* $\operatorname{lcm}(1,\ldots,n) \dot{\sim} e^n$*.*

Appendix B. Intersection Growth in Arithmetic Groups

Here, we show that the conclusion of Theorem 6.1 holds for some arithmetic groups having the generalized congruence subgroup property. We assume familiarity with arithmetic groups and group schemes (for this theory, please see [PR95]).

Let G be a connected absolutely almost simple, simply connected group scheme, defined over a finite extension L of $\mathbb{Q}$, and $\mathfrak{g}$ be the corresponding Lie algebra. Let $K \supset L$ be a number field with ring of integers $\mathscr{O}$, let S be a finite set of non-archimedean places (maximal ideals in $\mathscr{O}$) and $\mathscr{O}_S$ be the ring of S-integers. Our goal is to compute the intersection growth of finitely generated groups Γ that are commensurable to the group $G(\mathscr{O}_S)$.

The bulk of the proof involves estimating the intersection growth of (finite index subgroups of) $G(\widehat{\mathscr{O}_S})$, where $\widehat{\mathscr{O}_S}$ is the profinite completion of $\mathscr{O}_S$. By the Chinese Remainder

Theorem, $\widehat{\mathscr{O}_S}$ is ring isomorphic to the product $\prod_{\mathfrak{p}\notin S}\mathscr{O}_{\mathfrak{p}}$, where $\mathscr{O}_{\mathfrak{p}}$ is the localization of $\mathscr{O}$ (equivalently, of $\mathscr{O}_S$) at the prime $\mathfrak{p}$. It follows that

$$G(\widehat{\mathscr{O}_S}) \cong \prod_{\mathfrak{p}\notin S} G(\mathscr{O}_{\mathfrak{p}}).$$

Our first step is to compute the intersection growth of the local factors $G(\mathscr{O}_{\mathfrak{p}})$.

Lemmas 6.2, 6.3, 6.4, and 6.5 all hold with SL_k replaced with G with some modifications (6.5 may not hold if the prime is ramified). To state these generalizations, we need to fix some notation. By the above work, it makes sense to focus attention on the powers of a single prime $\mathfrak{p}$. By p we will denote the unique prime number which is in $\mathfrak{p}$, and we let $d_{\mathfrak{p}}$ denote the ramification index, i.e., $p \in \mathfrak{p}^{d_{\mathfrak{p}}}$ but $p \notin \mathfrak{p}^{d_{\mathfrak{p}}+1}$. It is well known that in the ring $\mathscr{O}_S$ there are only finitely many ideals $\mathfrak{p}$ with $d_{\mathfrak{p}} > 1$. Let $G_{\mathfrak{p}}$ denote the algebraic group over the completion of $\mathscr{O}_S$ at $\mathfrak{p}$, i.e., $G_{\mathfrak{p}} = G(\mathscr{O}_{\mathfrak{p}})$. For $i \geq 0$, let $G_{\mathfrak{p}}^i := \ker(G_{\mathfrak{p}} \to G(\mathscr{O}/\mathfrak{p}^i))$. This provides a descending filtration

$$G_{\mathfrak{p}} = G_{\mathfrak{p}}^0 \geq G_{\mathfrak{p}}^1 \geq \cdots \geq G_{\mathfrak{p}}^i \geq \ldots.$$

The following results are well-known.

Lemma B.1 (Moy-Prasad)**.**

(1) $[G_{\mathfrak{p}}^i, G_{\mathfrak{p}}^j] \subset G_{\mathfrak{p}}^{i+j}$.
(2) *For $i \geq 1$ we have an isomorphism*

$$G_{\mathfrak{p}}^i/G_{\mathfrak{p}}^{i+1} \to \mathfrak{g}(\mathscr{O}/\mathfrak{p}),$$

which is equivariant with respect to the action of $G(\mathscr{O}/\mathfrak{p})$ on both sides by conjugation.

Lemma B.2. *For $i \geq d_{\mathfrak{p}}+1$ the map $g \to g^p$ induces a set theoretic map $G_{\mathfrak{p}}^i \to G_{\mathfrak{p}}^{i+d_{\mathfrak{p}}}$. This map induces an isomorphism $G_{\mathfrak{p}}^i/G_{\mathfrak{p}}^{i+1} \to G_{\mathfrak{p}}^{i+d_{\mathfrak{p}}}/G_{\mathfrak{p}}^{i+d_{\mathfrak{p}}+1}$.*

Proof. $G_{\mathfrak{p}} = G(\mathscr{O}_{\mathfrak{p}})$ is isomorphic to a subgroup of $\mathrm{GL}_N(\mathscr{O}_{\mathfrak{p}})$ for some N. The image of $G_{\mathfrak{p}}^i$ under this embedding consist of all matrices in the image which are congruent to the identity modulo $\mathfrak{p}^i$. Let $g \in G_{\mathfrak{p}}^i$, then $g = I + x \in \mathrm{GL}_N(\mathscr{O}_{\mathfrak{p}})$, where I is the identity matrix and x is a $N \times N$ matrix with entries in $\mathfrak{p}^i$. By the Binomial Theorem, we have that $g^p = I + px \mod (p\mathfrak{p}^{2i} + \mathfrak{p}^{pi})$. By the definition of $d_{\mathfrak{p}}$ it is clear that $p\mathfrak{p}^i \subset \mathfrak{p}^{i+d_{\mathfrak{p}}}$ in $\mathscr{O}_{\mathfrak{p}}$, also if $i \geq d_{\mathfrak{p}}+1$, we have $\mathfrak{p}^{pi} \subset \mathfrak{p}^{2i} \subset \mathfrak{p}^{i+d_{\mathfrak{p}}}$, i.e., $g^p = I + px \mod p\mathfrak{p}^{i+d_{\mathfrak{p}}}$ is an element in $G_{\mathfrak{p}}^{i+d_{\mathfrak{p}}}$. Thus $g \to g^p$ induces a set map between $G_{\mathfrak{p}}^i$ and $G_{\mathfrak{p}}^{i+d_{\mathfrak{p}}}$. The condition $i \geq d_{\mathfrak{p}}+1$, gives $p\mathfrak{p}^{2i} + \mathfrak{p}^{pi} \subset \mathfrak{p}^{i+d_{\mathfrak{p}}+1}$. Hence, this map induces an isomorphism $G_{\mathfrak{p}}^i/G_{\mathfrak{p}}^{i+1} \to G_{\mathfrak{p}}^{i+d_{\mathfrak{p}}}/G_{\mathfrak{p}}^{i+d_{\mathfrak{p}}+1}$ because multiplication by p induces an isomorphism between $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ and $\mathfrak{p}^{i+d}/\mathfrak{p}^{i+d+1}$ in the local ring $\mathscr{O}_{\mathfrak{p}}$.

□

Lemma B.3. *For all but finitely many $\mathfrak{p}$, the Lie-algebra $\mathfrak{g}(\mathscr{O}/\mathfrak{p})$ has no center, and the adjoint action of $G(\mathscr{O}/\mathfrak{p})/Z(G(\mathscr{O}/\mathfrak{p}))$ on $\mathfrak{g}(\mathscr{O}/\mathfrak{p})$ is faithful and irreducible.*

As in the main body, we prove a slight generalization of [LS03, Lemma 16.4.5].

Lemma B.4. *Let $\pi_{\mathfrak{p}} : G(\mathscr{O}_{\mathfrak{p}}) \to G(\mathscr{O}/\mathfrak{p})$ be the mod $\mathfrak{p}$ reduction map. For all but finitely many primes $\mathfrak{p}$, we have*

$$\Phi(G(\mathscr{O}_{\mathfrak{p}})) = Z(G(\mathscr{O}/\mathfrak{p}))\ker(\pi_{\mathfrak{p}} : G(\mathscr{O}_{\mathfrak{p}}) \to G(\mathscr{O}/\mathfrak{p})).$$

Proof. Applying [LS03, Lemma 16.4.5], we see that the Frattini subgroup contains $\ker(\pi_p)$. Since $G(\mathcal{O}/\mathfrak{p})$ is semi-simple and thus perfect for all but finitely many primes, $\mathfrak{p}$, we have that the Frattini subgroup also contains $Z(G(\mathcal{O}/\mathfrak{p}))$. We are done since $G(\mathcal{O}/\mathfrak{p})/Z(G(\mathcal{O}/\mathfrak{p}))$ is a classical finite simple group. □

Let $H \leq G(\mathcal{O}_\mathfrak{p})$. Then, as in the SL_k case, we say the *level* of H with respect to the prime $\mathfrak{p}$ is the minimal non-negative integer s such that H is contains the principal congruence subgroup $G^{\mathfrak{p}^s}(\mathcal{O}_S)$. The first result we prove is a generalization of Proposition 6.1.2 in [LS03].

Lemma B.5. *Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_S$. There is some $c > 0$, depending only on G and $\mathcal{O}_S$, with the following property. If H is a subgroup of $G(\mathcal{O}_\mathfrak{p})$ of level s with respect to the prime $\mathfrak{p}$, then $[G(\mathcal{O}_\mathfrak{p}) : H] \geq c p^{\lfloor s/d_\mathfrak{p} \rfloor}$.*

Proof. We will prove this by induction on the level, s. The conclusion of the lemmas is clearly satisfied if $< d_\mathfrak{p}$. The case $s \leq 2d_\mathfrak{p}$ follows easily from Lemma B.3 and B.2 – for all but finitely many primes the group $G(\mathcal{O}/\mathfrak{p})$ is a finite almost simple group over an extension of $\mathbb{F}_p$ and therefore the smallest index of a maximal subgroup is bounded below by p (usually it is much more).

The induction is an easy consequence of Lemma B.2: it is enough to notice that that if H is a subgroup of level s, then $\bar{H} = H.G_\mathfrak{p}^{s-d_\mathfrak{p}}$ is a subgroup of level $s - d_\mathfrak{p}$ and the index of H in $\bar{H}$ is atleast p since $\bar{H}$ is a pro-p group. □

Remark B.6. Even though lemmas B.2 and B.3 do not hold in the case of positive characteristic, i.e., if we replace $\mathcal{O}$ with $\mathbb{F}_p[t]$, Lemma B.5 is valid in the case of positive characteristic. In fact, the lemma can be strengthened by removing the dependence on $d_\mathfrak{p}$.

We will also need the following analogue of Lemma 6.7.

Lemma B.7 (Maximal subgroups of $G(\mathcal{O}_\mathfrak{p})$)**.** *For all but finitely many prime ideals $\mathfrak{p}$:*

(1) *There is a unique maximal normal subgroup $N < G(\mathcal{O}_\mathfrak{p})$, the preimage of the center $Z(G(\mathcal{O}/\mathfrak{p}))$, which has index between $(|\mathfrak{p}|/2)^d$ and $|\mathfrak{p}|^d$.*
(2) *The smallest index of a subgroup of $G(\mathcal{O}_\mathfrak{p})$ is equal to the index of the preimage of a maximal parabolic subgroup of $G(\mathcal{O}/\mathfrak{p})/Z(G(\mathcal{O}/\mathfrak{p}))$. If P is any such subgroup, we have*

$$(|\mathcal{O}/\mathfrak{p}|/2)^a \leq [G(\mathcal{O}_\mathfrak{p}) : P] \leq 2|\mathcal{O}/\mathfrak{p}|^a,$$

where a is the largest codimension of a parabolic subgroup in G. The intersection of all such P is the normal subgroup N in (1).

Proof. The proof of (1) follows that of Lemma 6.7, using Lemma B.4. We need only note that $G(\mathcal{O}/\mathfrak{p})/Z(G(\mathcal{O}/\mathfrak{p}))$ is a classical finite simple group.

The proof of (2) also follows that of Lemma 6.7. This requires checking the table values in [C78, Table 1]. □

With the above tools, it is straightforward to modify the proof of Lemma 6.6 to a more general setting:

Lemma B.8 (Polynomial upper bounds)**.** *There is a constant C, depending only on the group scheme G, such that for every prime $\mathfrak{p}$, we have*

$$i^{<}_{G(\mathcal{O}_\mathfrak{p})}(n) < C|\mathfrak{p}|^C (n)^{d.d_\mathfrak{p}},$$

where d is the dimension of G.

Proof. This follows from Lemma B.5, which gives a logarithmic upper bound for the index s of a subgroup of index n. This combined with a trivial estimate for the index of the principal congruence subgroups lead to the desired bound. $\square$

Note that the intersection growth over all subgroups dominates the growths for other classes, so the same upper bound applies to $i^{\bullet}_{G(\mathscr{O}_\mathfrak{p})}$ when $\bullet$ is any of $\lhd$, c, max.

As in §6, combining our estimates for individual primes $\mathfrak{p}$, following the proof of Theorem 6.1, we can now compute the intersection growth of finite index subgroups of $G(\widehat{\mathscr{O}_S})$.

Theorem B.9. *Let Δ be a finite index subgroup of $G(\widehat{\mathscr{O}_S})$. Then*

(1) $i^{\lhd}_{\Delta}(n) \dot{\sim} i^{\max\lhd}_{\Delta}(n) \dot{\sim} e^{n^{1/d}}$,
(2) $i^{<}_{\Delta}(n) \dot{\sim} i^{\max}_{\Delta}(n) \dot{\sim} e^{n^{1/a}}$,
(3) *if $K=\mathbb{Q}$ then* $i^{c}_{\Delta}(n) \dot{\sim} e^{n^{1/d}}$,

where $d=\dim G$ and a is the smallest codimension of a parabolic subgroup of G.

Proof. The proof is essentially the same as that of Theorem 6.1. We start by rewriting

$$i^{\bullet}_{\Delta}(n) = \prod_{\mathfrak{p}\notin S} i^{\bullet}_{\Delta_\mathfrak{p}}(n),$$

where $\Delta_\mathfrak{p}$ denotes the projection of Δ into $G(\mathscr{O}_\mathfrak{p})$. This equation follows from Proposition 3.3, and holds when $\bullet$ is any of the classes of subgroups indicated in the statement of the theorem, except that when $\bullet = c$, we need that the local factors $G(\mathscr{O}_\mathfrak{p})$ are characteristic. This is the case if $K=\mathbb{Q}$, because G is semi-simple and simply connected, $G^p(\mathbb{Z}_p)$ is the unique maximal normal pro-p subgroup of $G(\widehat{\mathbb{Z}})$, see [PR95, Theorem 3.10]. (However, if there are automorphisms of K that fix the field of definition of G, the groups $G(\mathscr{O}_\mathfrak{p})$ are not characteristic.) Note that as Δ has finite index in $G(\widehat{\mathscr{O}_S})$, each $\Delta_\mathfrak{p}$ has finite index in $G(\mathscr{O}_\mathfrak{p})$, and $\Delta_\mathfrak{p} = G(\mathscr{O}_\mathfrak{p})$ for all but finitely many $\mathfrak{p}$.

Each $i^{\bullet}_{\Delta_\mathfrak{p}}(n)$ has at most polynomial growth, since we can use Lemma 3.1 to transfer Lemma B.8 to $\Delta_\mathfrak{p}$. So, if we promise to provide exponential estimates for the intersection growth functions $i^{\bullet}_{\Delta}(n)$, the growth type will be unaffected if we ignore finitely many $\mathfrak{p}$. So, assume from now on that for all p, all the preceding lemmas in this section hold and $\Delta_\mathfrak{p} = G(\mathscr{O}_\mathfrak{p})$.

By Lemma B.8 and Lemma B.7, we then compute:

$$i^{\bullet}_{\Delta}(n) \dot{\sim} \prod_{\mathfrak{p}\notin S} i^{\bullet}_{G(\mathscr{O}_\mathfrak{p})}(n) \ \dot{\preceq} \prod_{\text{primes } |\mathfrak{p}|<2n^{1/b}} C|\mathfrak{p}|^C n^{d.d_\mathfrak{p}}$$

where $b=d$ if $\bullet=\lhd$, and $b=a$ when $\bullet = <, \max$. There are approximately $N/\log N$ primes in $\mathscr{O}$ with norm less than N, so after replacing $|\mathfrak{p}|$ above by the upper bound $2n^{1/b}$ and noticing that $d_\mathfrak{p}$ is bounded by a constant D

$$i^{\bullet}_{\Delta}(n) \ \dot{\preceq} \ \left(C(2n^{1/b})^C \cdot n^{Dd}\right)^{\frac{2n^{1/b}}{\log(2n^{1/b})}} \dot{\sim} e^{n^{1/b}}.$$

In the last asymptotic equality, we use that $n^{n/\log n} \dot{\sim} e^n$, and $e^{kn} \dot{\sim} e^n$ for any k.

The lower bound is obtained in the same way, using that

$$i^{\bullet}_{G(\mathscr{O}_\mathfrak{p})}(n) > |G(\mathscr{O}/\mathfrak{p})| > (|\mathfrak{p}|/2)^d, \quad \text{for } n > (|\mathfrak{p}|/2)^b. \quad \square$$

For any arithmetic group $G(R)$ there is a map

$$\iota : \widehat{G(R)} \longrightarrow G(\widehat{R}),$$

where $\widehat{\cdot}$ denotes profinite completion. Let $G(\mathscr{O}_S)$ be infinite, and hence not compact. Since G is absolutely simple, the only L-simple component of G is itself. It follows that G does not contain any L-simple component G^i with $G^i(\mathscr{O}_S)$ compact. Moreover, since G is connected, [PR95, Theorem 7.12] gives the *strong approximation property*: $G(\mathscr{O}_S)$ is dense in $G(\widehat{\mathscr{O}_S})$. This property is equivalent to ι having finite co-kernel when $R = \mathscr{O}_S$. Recall that $G(R)$ is said to satisfy the *generalized congruence subgroup property* if ι has a finite kernel that is central. Informally, all finite index subgroups of $G(R)$ are "close" to a congruence subgroup.

Theorem B.10. *Suppose the group $G(\mathscr{O}_S)$ is infinite and satisfies the generalized congruence subgroup property, and let Γ be a f.g. group commensurable to $G(\mathscr{O}_S)$. Let d be the dimension of G and a the smallest codimension of a parabolic subgroup of G. Then*

$$i_\Gamma^{<}(n) \simeq e^{n^{1/a}}.$$

Moreover, if either Γ is a subgroup of $G(\mathscr{O}_S)$ or $K = \mathbb{Q}$ then

$$i_\Gamma^{\lhd}(n) \simeq e^{n^{1/d}}.$$

Proof. Let Δ be a finite index subgroup of $G(\mathscr{O}_S)$ that is isomorphic to a finite index normal subgroup of Γ. The intersection growth of Δ is the same as that of $\iota(\Delta)$, which, by the discussion preceding the theorem, is a finite index subgroup of $G(\widehat{\mathscr{O}_S})$, so by Theorem B.9 the intersection growth of Δ is $e^{n^{1/a}}$. Since Δ is a finite index subgroup of Γ, the intersection growth of Γ is the same.

Next, Theorem B.9 gives that the normal intersection growth of Δ is $e^{n^{1/d}}$. This proves the second part of the theorem when $\Gamma = \Delta$ is a subgroup of $G(\mathscr{O}_S)$. Alternatively, if $K = \mathbb{Q}$, Theorem B.9 says that the normal intersection growth of Δ is the same as its characteristic intersection growth. Therefore, one can use Lemma 3.1 to show that the normal intersection growths of Γ and Δ agree. $\square$

Remark B.11. The above result is not valid for arbitrary arithmetic groups. For example, the group $\Gamma_1 = \mathrm{SL}_3(\mathbb{Z}[i])$ satisfies $i_{\Gamma_1}^{\lhd}(n) \simeq e^{n^{1/8}}$. However, for $\Gamma_2 = (\mathbb{Z}/2\mathbb{Z}) \ltimes \Gamma_1$, where the action is via the Galois automorphism, one has $i_{\Gamma_2}^{\lhd}(n) \simeq e^{n^{1/16}}$.

Remark B.12. We do not know if Theorem B.10 holds when K is replaced with a function field. One of the main problems is that Lemma B.8 does not hold in this case – in fact the the congruence subgroups $G^s(\mathscr{O}_\mathfrak{p})$ have a huge mod p abelianization, thus the intersection of the subgroups of index p is much smaller than it needs to be.

We finish by remarking that the proof of Theorem B.10 also gives

Theorem B.13. *Let Γ be a f.g. subgroup of $G(\mathscr{O}_S)$ that is Zariski dense inside $G(\mathscr{O}_S)$. Let d be the dimension of G and a the smallest codimension of a parabolic subgroup of G. Then*

$$i_\Gamma^{\lhd,\mathrm{cong}}(n) \simeq e^{n^{1/d}} \quad \textit{and} \quad i_\Gamma^{<,\mathrm{cong}}(n) \simeq e^{n^{1/a}},$$

where the superscript cong *denotes that we are only considering subgroups H of Γ that contain $\Gamma \cap G(\mathscr{O}_S)^I$ for some ideal $I \lhd \mathscr{O}_S$.*

Proof. The congruence completion $\widehat{\Gamma}^{\text{cong}}$ of Γ is a subgroup of $\widehat{G(\mathscr{O}_S)}^{\text{cong}} < G(\widehat{\mathscr{O}_S})$. The strong approximation theorem gives that $\widehat{\Gamma}^{\text{cong}}$ is a finite index subgroup of $G(\widehat{\mathscr{O}_S})$, which allows us to apply Theorem B.9 to compute the intersection growth of $\widehat{\Gamma}^{\text{cong}}$. □

REFERENCES

BMS67. H. Bass, J. Milnor and J.-P. Serre. Solution of the congruence subgroup problem for SL_n $(n \geq 3)$ and Sp_{2n} $(n \geq 2)$, *Inst. Hautes Études Sci. Publ. Math.*, 33:59–137, 1967.

Bou10. K. Bou-Rabee. Quantifying residual finiteness. *J. Algebra*, 323(3):729–737, 2010.

Bou11. K. Bou-Rabee. Quantifying residual finiteness of solvable groups. *New York J. Math.*, 17, 699–712, 2011.

BM10. K. Bou-Rabee and D. B. McReynolds. Bertrand's postulate and subgroup growth. *J. Algebra*, 324(4):793–819, 2010.

BM11. K. Bou-Rabee and D. B. McReynolds. Asymptotic growth and least common multiples in groups. *Bull. Lond. Math. Soc.*, 43(6):1059–1068, 2011.

BM12. K. Bou-Rabee and D. B. McReynolds, Extremal behavior of divisibility functions. *Geometriae Dedicata*, 2014:1-9. 2. 2014.

BK12. K. Bou-Rabee and T. Kaletha. Quantifying residual finiteness of arithmetic groups. *Compos. Math.*, 148(3):907–920, 2012.

Bus09. N. V. Buskin. Economical separability in free groups. *Siberian Mathematical Journal*, 50(4):603–608, 2009.

CCNPW85. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson. An ATLAS of Finite Groups, *Clarendon Press, Oxford* (1985; reprinted with corrections, 2003)

C78. B. N. Cooperstein. Minimal degree for a permutation representation of a classical group *Israel J. Math.* 30, 213–234. 1978.

GKP12. F. Grunewald, B.Kunyavskii and E. Plotkin. New trends in characterization of solvable groups. *to appear*.

Had11. U. Hadad. On the shortest identity in finite simple groups of Lie type *J. Group Theory*, 14(1):37–47, 2011.

Hall59. P. Hall. The theory of groups *The Macmillan Co.*, New York, N.Y., xii+434 pp, 1959.

His84. G. Hiss, Die adjungierten Darstellungen der Chevalley-Gruppen *Arch. Math.* 42, 408-416, 1984.

Hog82. G. M. D. Hogeweij, Almost classical Lie algebras: I, II, *Indag. Math.* 44,, 441–460, 1982.

Jon74. G. A. Jones. Varieties and simple groups. *J. Austral. Math. Soc.*, 17:163–173, 1974.

KL90. W. M. Kantor and A. Lubotzky. The probability of generating a finite classical group. *Geom. Dedicata*, 36(1):67–87, 1990.

KM11. M. Kassabov and F. Matucci. Bounding the residual finiteness of free groups. *Proc. Amer. Math. Soc.*, 139(7):2281–2286, 2011.

KMS12. O. Kharlampovich, A. Myasnikov, and M. Sapir. Algorithmically complex residually finite groups. *submitted*, `http://arxiv.org/abs/1204.6506`.

KN66. L. G. Kovács and M.F. Newman. Cross varieties of groups. *Proc. Roy. Soc. Ser. A*, 292:530–536, 1966.

KT15. G. Kozma and A. Thom Divisibility and laws in finite simple groups. preprint. `http://arxiv.org/abs/1403.2324`.

LS03. A. Lubotzky and D. Segal. *Subgroup growth*, volume 212 of *Progress in Mathematics*. Birkhäuser Verlag, Basel, 2003.

LS95. M. W. Liebeck and A. Shalev. The probability of generating a finite simple group. *Geom. Dedicata*, 56(1):103–113, 1995.

KK00. L. C. Kappe and J. Kirtland. Supplementation in groups. *Glasgow Mathematical Journal*, 42:37–50, 2000.

MP94. A. Moy, G. Prasad, Unrefined minimal K-types for p-adic groups *Invent. math.* 116, 393–408, 1994.

MQR13. N. E. Menezes, M. Quick, C. M. Roney-Dougal. The probability of generating a finite simple group *Israel Journal of Mathematics*, 198(1):371–392, 2013.

Neu67. H. Neumann. *Varieties of groups*, Springer-Verlag New York, Inc., New York, 1967.

NS07. N. Nikolov and D. Segal. On finitely generated profinite groups. I. Strong completeness and uniform bounds. *Ann. of Math. (2)*, 165(1):171–238, 2007.

N87. M. V. Nori. *On subgroups of* $\mathrm{GL}_n(\mathbf{F}_p)$, *Inventiones Mathematicae (88)*, 2:257–275, 1987.

OP64. S. Oates and M. B. Powell Identical relations in finite groups. *J. Algebra*, 1:11–39, 1964.

PR95. V. Platonov and A. Rapinchuk Algebraic groups and number theory. *Pure and Applied Mathematics*, 139, 1994.

Wil09. R. A. Wilson. *The finite simple groups*, volume 251 of *Graduate Texts in Mathematics*. Springer-Verlag London Ltd., London, 2009.

DEPARTMENT OF MATHEMATICS, BOSTON COLLEGE, CARNEY HALL, CHESTNUT HILL, MA 02467-3806, USA
E-mail address: ian.biringer@bc.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MICHIGAN, 2074 EAST HALL, ANN ARBOR, MI 48109-1043, USA
E-mail address: khalidb@umich.edu

DEPARTMENT OF MATHEMATICS, CORNELL UNIVERSITY, MALOTT HALL, ITHACA, NY 14850, USA,
E-mail address: kassabov@math.cornell.edu

DÉPARTEMENT DE MATHÉMATIQUES, FACULTÉ DES SCIENCES D'ORSAY, UNIVERSITÉ PARIS-SUD 11, BÂTIMENT 425, ORSAY, FRANCE
E-mail address: francesco.matucci@math.u-psud.fr