Quantifying residual finiteness of arithmetic groups

Khalid Bou-Rabee and Tasho Kaletha

August 20, 2010

Abstract

The normal Farb growth of a group quantifies how well-approximated the group is by its finite quotients. We show that any S-arithmetic subgroup of a higher rank Chevalley group G has normal Farb growth $n^{\dim(G)}$.

keywords: *Arithmetic groups, normal Farb growth, residual finiteness*

1 Introduction

The quantification of residual finiteness, begun in [B10], seeks to describe how well a residually finite group is approximated by its finite quotients. This is measured by the normal Farb growth of the group. During a geometry seminar at Yale University in December 2009, Daniel Mostow asked the following question:

Question 1.1. (D. Mostow) Does asymptotic information of residual finiteness characterize arithmetic subgroups of a given linear algebraic group?

This paper presents a first major step towards answering this question, by showing that in a fixed Chevalley group G, all S-arithmetic subgroups share the same normal Farb growth, and moreover this growth is $n^{\dim(G)}$. Note that for us, a Chevalley group will be a split simple algebraic group that is not necessarily simply-connected.

To state our results more precisely, we need some notation. Let Γ be a finitely generated, residually finite group, and let X be a finite generating set for Γ. For $\gamma \in \Gamma$, let $\|\gamma\|_X$ denote the word length of γ with respect to X. Define

$$\mathrm{D}_\Gamma(\gamma) := \min\{|Q| \,:\, Q \text{ is a finite quotient of } \Gamma \text{ where } \gamma \neq 1\},$$

and

$$\mathrm{F}_{\Gamma,X}(n) := \max\{\mathrm{D}_\Gamma(\gamma) \,:\, \|\gamma\|_X \leq n\}.$$

The function $F_{\Gamma,X}$ is called the *normal Farb growth function*. It is known that the asymptotic behavior of $F_{\Gamma,X}$ is independent of X (see Section 2). The asymptotic growth of this function is called the *normal Farb growth* of Γ.

The main results of this paper characterize the normal Farb growth of S-arithmetic groups in Chevalley groups. We use the term S-arithmetic subgroup of G to denote any subgroup of $G(\mathbb{C})$ which is commensurable with $G(\mathcal{O}_{K,f})$, where $K \subset \mathbb{C}$ is a number field, $\mathcal{O}_K$ is its ring of integers, and $f \in \mathcal{O}_K \smallsetminus \{0\}$. That is, it is an S-arithmetic subgroup of G in the usual definition for some number field K and some finite set S of places of K which contains the archimedean ones, but we allow K and S to vary. The ingredients used include the structure theory of split semi-simple group schemes, results on the congruence subgroup problem, Moy-Prasad filtrations, Selberg's Lemma, the prime number theorem, and the Cebotarëv density theorem. Furthermore, we use in an essential way the results of Lubotzky-Mozes-Raghunathan [LMR01].

Theorem 1.2. *Let G be a Chevalley group of rank at least 2, K be a number field, and $f \in \mathcal{O}_K \smallsetminus \{0\}$. If Γ is a finitely generated subgroup of $G(\mathbb{C})$ with the property that $\Gamma \cap G(\mathcal{O}_{K,f})$ is of finite-index in $G(\mathcal{O}_{K,f})$, then its normal Farb growth is bounded below by $n^{\dim(G)}$.*

It is interesting to ask whether an analogous result holds in rank 1. So far, the normal Farb growth of a nonabelian free group has been bounded below by $n^{2/3}$ (see [KM10]).

Theorem 1.3. *Let G be a Chevalley group, K be a number field, and $f \in \mathcal{O}_K \smallsetminus \{0\}$. If Γ is a finitely generated subgroup of $G(\mathbb{C})$ with the property that $\Gamma \cap G(\mathcal{O}_{K,f})$ is of finite-index in Γ, then its normal Farb growth is bounded above by $n^{\dim(G)}$.*

As a corollary of Theorems 1.2 and 1.3 we have the following result.

Corollary 1.4. *Let G be a Chevalley group of rank at least 2. Then the normal Farb growth of every S-arithmetic subgroup of G is precisely $n^{\dim(G)}$.*

This result is surprising since in general, if Δ has finite-index in Γ, we cannot hope for $F_\Gamma \approx F_\Delta$ (see Example 2.5 at the end of Section 2). Instead, the most general result in this direction is $F_\Gamma(n) \preceq (F_\Delta(n))^{[\Gamma:\Delta]}$ (see [B10, Lemma 1.3]).

Acknowledgements. It is our pleasure to thank Daniel Mostow for suggesting this pursuit. We are grateful to Martin Kassabov, Alexander Lubotzky, and Gopal Prasad for helpful mathematical conversations, and wish to thank Alexander Premet for providing us with a useful reference. Further, we are thankful to Benson Farb for giving us comments on an earlier draft.

2 Preliminaries

Let Γ be a finitely generated, residually finite group. For $\gamma \in \Gamma \setminus \{1\}$ we define $Q(\gamma,\Gamma)$ to be the set of finite quotients of Γ in which the image of γ is non-trivial. We say that these quotients detect γ. Since Γ is residually finite, this set is non-empty, and thus the natural number

$$\mathrm{D}_\Gamma(\gamma) := \min\{|Q| : Q \in Q(\gamma, G)\}$$

is defined and positive for each $\gamma \in \Gamma \setminus \{1\}$. For a fixed finite generating set $X \subset \Gamma$ we define

$$\mathrm{F}_{\Gamma,X}(n) := \max\{\mathrm{D}_\Gamma(\gamma) \ : \ \gamma \in \Gamma, \|\gamma\|_X \leq n, \gamma \neq 1\}.$$

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

It was shown in [B10] that if X,Y are two finite generating sets for the residually finite group Γ, then $\mathrm{F}_{\Gamma,X} \approx \mathrm{F}_{\Gamma,Y}$. Since we will only be interested in asymptotic behavior, we let F_Γ be the equivalence class (with respect to $\approx$) of the functions $\mathrm{F}_{\Gamma,X}$ for all possible finite generating sets X of Γ. Sometimes, by abuse of notation, F_Γ will stand for some particular representative of this equivalence class, constructed with respect to a convenient generating set.

We will need to use the following auxiliary function in our proofs. For any natural number k, we define

$$\mathrm{D}^k_\Gamma(\gamma) := D_\Gamma(\gamma^k) \ \text{ and } \ \mathrm{F}^k_{\Gamma,X}(n) := \max\{\mathrm{D}^k_\Gamma(\gamma) \ : \ \gamma \in \Gamma, \|\gamma\|_X \leq n, \gamma^k \neq 1\}.$$

The next lemma, which is a consequence of Selberg's Lemma (see [A87]), reveals the potential utility of $\mathrm{F}^k_{\Gamma,X}$.

Lemma 2.1. *Let Γ be an infinite linear group generated by a finite set X and let k a natural number. Then* $\mathrm{F}_{\Gamma,X} \approx \mathrm{F}^k_{\Gamma,X}$.

Proof. The inequality $\mathrm{F}^k_{\Gamma,X}(n) \leq \mathrm{F}_{\Gamma,X}(kn)$ is straightforward. It suffices to prove $\mathrm{F}_{\Gamma,X}(n) \leq \mathrm{F}^k_{\Gamma,X}(n)$ for all but finitely many n. Let γ_n be an element such that $D_\Gamma(\gamma_n) = \mathrm{F}_{\Gamma,X}(n)$ and $\|\gamma_n\|_X \leq n$. If $\gamma_n^k \neq 1$, then $D_\Gamma(\gamma_n) \leq D^k_\Gamma(\gamma_n)$, giving $\mathrm{F}_{\Gamma,X}(n) \leq \mathrm{F}^k_{\Gamma,X}(n)$. The proof will be complete if we show that $\gamma_n^k = 1$ holds for only finitely many n. Suppose otherwise, then by Selberg's Lemma, there exists a finite-index normal subgroup Δ of Γ that is torsion-free, and in particular $\gamma_n \notin \Delta$ for infinitely many n. Since $\mathrm{F}_{\Gamma,X}(n)$ is non-decreasing in n, it must be bounded by $[\Gamma : \Delta]$, but this contradicts the infinitude of Γ. □

Corollary 2.2. *If Γ is an infinite linear group and X,Y are finite generating sets for Γ, then* $\mathrm{F}^k_{\Gamma,X} \approx \mathrm{F}^k_{\Gamma,Y}$.

As with the function F, we will denote the asymptotic equivalence class of $\mathrm{F}^k_{\Gamma,X}$ as X varies by F^k_{Γ}. The following example shows that the linearity assumption cannot be dropped from Lemma 2.1.

Example 2.3. Let Γ be the Lamplighter group $\mathbb{Z}/2\mathbb{Z} \wr \mathbb{Z}$. Set $\Delta = \oplus_{i\in\mathbb{Z}}\mathbb{Z}/2\mathbb{Z}$ to be the base group of Γ so $\Gamma/\Delta \cong \mathbb{Z}$. It is easy to see that for any generating set X of Γ, we have $\mathrm{F}^2_{\Gamma,X}(n) \approx \mathrm{F}_{\mathbb{Z}}(n)$. Thus $\mathrm{F}^2_{\Gamma,X}(n) \approx \log(n)$ by [B10, Corollary 2.3]. We now prove that $\mathrm{F}_\Gamma(n) \succeq (\log(n))^2$, so in particular $\mathrm{F}_\Gamma \not\approx \mathrm{F}^2_{\Gamma,X}$.

Proof. Let $\delta_i \in \Delta$ be the element given by the ith Kronecker delta function. For k a natural number greater than 4, set $\gamma_k := \delta_1 + \delta_{\mathrm{lcm}(1,\dots,k)}$. Let $\phi : \Gamma \to P$ be a homomorphism to a finite quotient of Γ that realizes $\mathrm{D}_\Gamma(\gamma_k)$. We first claim that if $\delta_1 + \delta_{1+n} \in \ker\phi$ for $n \in \mathbb{N}$, then $n \geq k$. Indeed, a simple calculation shows that $\delta_1 + \delta_{1+mn} \in \ker\phi$ for any $m \in \mathbb{N}$. If $n \leq k$, we have that $\mathrm{lcm}(1,\dots,k)$ is a multiple of n, so $\delta_1 + \delta_{\mathrm{lcm}(1,\dots,k)} \in \ker\phi$, which is impossible.

Next, we claim that the set $S := \{(\delta_n,t) : n,t \in \{1,\dots,\lfloor k/4\rfloor\}\} \subseteq \Gamma$ injects into P through ϕ. Suppose not, then $(\delta_n,t)(\delta_{n'},t')^{-1} \in \ker\phi$ for $t,t',n,n' \in \{1,\dots,\lfloor k/4\rfloor\}$ with $(\delta_n,t) \neq (\delta_{n'},t')$. Set $\alpha = (\delta_n,t)(\delta_{n'},t')^{-1} = (\delta_n + \delta_{n'+t-t'}, t-t')$. If $t-t' = 0$, then by our first claim $n = n'$ or $||n|-|n'|| \geq k$. If $n = n'$, then $\alpha = (0,0)$, while the latter possibility contradicts $||n|-|n'|| \leq k/2$. If $t-t' \neq 0$, because $\alpha\delta_i\alpha^{-1}\delta_i^{-1} \in \ker\phi$ for all i, we have $\delta_{1+t-t'} + \delta_1 \in \ker\phi$, where by our first claim, $|t-t'| \geq k$, however $|t-t'| \leq k/2$. Our second claim is now shown.

Since S injects into P, we have $|P| \geq \lfloor k/4\rfloor^2$. Fix a finite generating set X for Γ, by the prime number theorem, there exists a natural number M such that $\|\gamma_k\|_X \leq M3^k$. Set $k = \lfloor \log_3(n)\rfloor$, then because F_Γ is increasing we have, for sufficiently large n,

$$\mathrm{F}_\Gamma(Mn) \geq \mathrm{F}_\Gamma(M3^k) \geq \mathrm{F}_\Gamma(\|\gamma_k\|_X) \geq \lfloor k/4\rfloor^2 \geq \frac{1}{32}\left[\frac{\log(n)}{\log(3)}\right]^2.$$

□

Lemma 2.4. *Let* Γ,Δ *be finitely generated and residually finite. Then*

- *If* $\Delta \subset \Gamma$, *then* $\mathrm{F}_\Delta \preceq \mathrm{F}_\Gamma$.
- *If* $f : \Delta \to \Gamma$ *is surjective with finite kernel, then* $\mathrm{F}_\Delta \preceq \mathrm{F}_\Gamma$. *If moreover* $\ker(f)$ *is central in* Δ *and* Γ *is linear, then* $\mathrm{F}_\Delta \approx \mathrm{F}_\Gamma$.

Proof. The first assertion is [B10, Lemma 1.1]. Consider the second assertion. The inequality $\mathrm{F}_\Delta \preceq \mathrm{F}_\Gamma$ is straightforward. Assuming now that $\ker(f)$ is central in Δ, we will show $\mathrm{F}^k_\Delta \succeq \mathrm{F}_\Gamma$, where $k = |\ker(f)|$. To that end, fix a finite generating set X for Δ and use its image for Γ. Construct F_Δ and F_Γ with respect to these generating sets. Let $g \in \Delta$, $g^k \neq 1$.

Since $g^k = (zg)^k$ for all $z \in \ker(f)$, we see that $\ker(f)N$ is a normal subgroup of Δ not containing g. Thus $\mathrm{D}^k_\Delta(g) \geq \mathrm{D}_\Gamma(f(g))$ for all $g \in \Delta$ with $g^k \neq 1$. We now need to handle torsion elements in Γ.

For each natural number n, let $\gamma_n \in \Gamma$ be an element satisfying $\mathrm{D}_\Gamma(\gamma_n) = \mathrm{F}_\Gamma(n)$ and $\|\gamma_n\| \leq n$. Since f is surjective and by our choice of generating sets, there exists $g_n \in \Delta$ such that $f(g_n) = \gamma_n$ and $\|g_n\| \leq n$. Then if $g_n^k = 1$ for infinitely many n, then $\gamma_n^k = 1$ for infinitely many n. Following the Selberg Lemma application from Lemma 2.1, we see that Γ is finite, which is impossible. Thus, $g_n^k \neq 1$ for all but finitely many n. For such n, we have $\mathrm{D}^k_\Delta(g_n) \geq \mathrm{D}_\Gamma(f(g_n))$ and hence $\mathrm{F}^k_\Delta(n) \succeq \mathrm{F}_\Gamma(n)$. □

We finish the preliminaries section with an example that illustrates that normal Farb growth of a group may be different from that of a finite index subgroup.

Example 2.5. Let Q be the subgroup of $\mathrm{GL}_2(\mathbb{Z})$ generated by

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Let $\Delta = \mathbb{Z} \times \mathbb{Z}$ and set $\Gamma = \Delta \rtimes Q$, where Q acts on Δ via the standard action of $\mathrm{GL}_2(\mathbb{Z})$. Because Q is finite, Γ contains Δ as a subgroup of finite-index. Further, $\mathrm{F}_\Delta(n) \approx \log(n)$ by [B10, Corollary 2.3]. We now prove that $\mathrm{F}_\Gamma(n) \succeq (\log(n))^2$.

Proof. Let X be a generating set for Γ containing $(1,0)$ and $(0,1)$ in Δ. Set γ_k to be $(\mathrm{lcm}(1,\ldots,k),0) \in \Delta$. By the prime number theorem, there exists a natural number M such that $\|\gamma_k\|_X \leq M3^k$. Let $\phi : \Gamma \to P$ be a homomorphism to a finite quotient of Γ that realizes $D_\Gamma(\gamma_k)$ and set $V = \ker\phi \cap \Delta$. We first construct a subgroup of V of the form $d\mathbb{Z} \times d\mathbb{Z}$ for some natural number d. Consider the intersection of V with $\mathbb{Z} \times 0$. This is a subgroup of $\mathbb{Z}$, hence is isomorphic to $d\mathbb{Z}$ for some natural number d. Thus we have $d\mathbb{Z} \times 0 \subset V$, and conjugating by B we also find $0 \times d\mathbb{Z}$ is in V.

Next, we claim that the index of $d\mathbb{Z} \times d\mathbb{Z}$ in V is at most 4: Let $(a,b) \in V$. Then $(2a,0) = (a,b) + A(a,b)A^{-1} \in V$, and similarly $(2b,0) \in V$, so $2a, 2b \in d\mathbb{Z}$, and hence $2(a,b) \in d\mathbb{Z} \times d\mathbb{Z}$, which shows that every element of $V/d\mathbb{Z} \times d\mathbb{Z}$ has order (at most) 2. But V is a free abelian group of rank 2, so $V/d\mathbb{Z} \times d\mathbb{Z}$ is generated by two elements, and the claim follows. We conclude that $d^2 = [\Delta : d\mathbb{Z} \times d\mathbb{Z}] = [\Delta : V][V : d\mathbb{Z} \times d\mathbb{Z}] \leq 4[\Delta : V]$, giving $|P| \geq \frac{1}{4}d^2$.

Finally, since $\gamma_k \notin \ker(\phi)$, we must have that $d \geq k$. Hence, $\mathrm{F}_\Gamma(M3^k) \geq D_\Gamma(\gamma_k) \geq \frac{1}{4}k^2$. Set $k = \lfloor(\log_3(n))\rfloor$, then because F_Γ is increasing we have, for sufficiently large n,

$$\mathrm{F}_\Gamma(Mn) \geq \mathrm{F}_\Gamma(M3^k) \geq \frac{1}{4}k^2 \geq \frac{1}{16}\left(\frac{\log(n)}{\log(3)}\right)^2,$$

giving $\mathrm{F}_\Gamma(n) \succeq (\log(n))^2$, as desired. □

3 Lower bounds

Let G be a Chevalley group, i.e. a split simple group scheme defined over $\mathbb{Z}$, and let $\mathfrak{g}$ be its Lie-algebra. Note that we do not assume that G is simply-connected. For a natural number m, we put $G(m) = G(\mathbb{Z}/m\mathbb{Z})$. For a while, we will focus attention on the powers of a single prime p, and to lighten the notation we put $G_k = G(\mathbb{Z}/p^k\mathbb{Z})$.

Recall from [SGA3, exp.1, 2.3.3+2.3.6] the definition of the center $Z(G)$ of G. It is the subfunctor of G, which assigns to each scheme S the following subgroup of $G(S)$

$$Z(G)(S) := \left\{ g \in G(S) | \; \forall S' \to S : \mathrm{Ad}(g)|_{G(S')} = \mathrm{id}_{G(S')} \right\}$$

where $\mathrm{Ad}(g)|_{G(S')}$ denotes the automorphism of $G(S')$ provided by conjugation by the image of g under the natural map $G(S) \to G(S')$.

It is shown in [SGA3, exp.22, 4.1.8] that the functor $Z(G)$ is representable by a closed $\mathbb{Z}$-subgroup-scheme of G, which is finite and diagonalizable. As such, $Z(G)$ is a product of finitely many groups schemes, each isomorphic to μ_n for some n, where μ_n is the group scheme of n-th roots of unity. In particular, $Z(G)$ is etale over $\mathbb{Z}[\mathrm{ord}(Z(G))^{-1}]$. See [SGA3, exp.8, 2.1].

From the definition it is obvious that $Z(G)(S) \subset Z(G(S))$. We will show that there exists $f \in \mathbb{Z} \setminus \{0\}$ such that if S lies over $\mathrm{Spec}(\mathbb{Z}_f)$, then $Z(G)(S) = Z(G(S))$. The main ingredient in this proof is the following lemma, which asserts the existence of a strongly regular section of the split maximal torus in G over $\mathrm{Spec}(\mathbb{Z}_f)$.

Lemma 3.1. *Let $T \subset G$ be a split maximal torus. There exists $f \in \mathbb{Z} \setminus \{0\}$ and a point $s \in T(\mathbb{Z}_f)$ such that*

$$\mathrm{Cent}(s, G \times \mathrm{Spec}(\mathbb{Z}_f)) = T \times \mathrm{Spec}(\mathbb{Z}_f).$$

Proof. Consider the closed subscheme of T given by

$$\bigcup_{\alpha \in R(T,G)} \ker(\alpha) \cup \bigcup_{w \in W} T^w$$

where $R(T,G)$ is the set of roots of T in G and $W = \mathrm{Norm}(G,T)/T$ is the Weyl group. Let U be its complement in T. Then $U \to T$ is an open immersion, which when composed with an isomorphism $T \cong \mathbb{G}_m^r$ and the open immersion $\mathbb{G}_m^r \to \mathbb{A}_{\mathbb{Z}}^r$ provides an open immersion $U \to \mathbb{A}_{\mathbb{Z}}^r$. Since $\mathbb{A}^r(\mathbb{Q})$ is dense in $\mathbb{A}^r(\overline{\mathbb{Q}})$, it follows that $U(\mathbb{Q}) \neq \emptyset$. As U is of finite type, any map $\mathrm{Spec}(\mathbb{Q}) \to U$ factors as $\mathrm{Spec}(\mathbb{Q}) \to \mathrm{Spec}(\mathbb{Z}_f) \to U$ for some f. Thus we have a point $s : \mathrm{Spec}(\mathbb{Z}_f) \to U$. We claim that this point satisfies the statement of the lemma. To lighten notation, let us base change to $\mathrm{Spec}(\mathbb{Z}_f)$. Consider the centralizer $H := \mathrm{Cent}(s, G)$. It is a closed subscheme of G, hence affine and of finite type over $\mathbb{Z}_f$, and contains T. By generic flatness, we may assume that H is flat, after possibly changing f. By the choice of s, all fibers of H and T coincide. By [SGA3, exp. 10, 4.9], H is a torus, and since T is a maximal torus, it follows that $H = T$. □

Corollary 3.2. *There exists $f \in \mathbb{Z} \setminus \{0\}$ such that for all schemes $S \to \mathrm{Spec}(\mathbb{Z}_f)$ we have*

$$Z(G)(S) = Z(G(S)).$$

Proof. The inclusion $\subset$ is obvious from the definition of $Z(G)$ and we now have to show the converse. Choose f and $s \in T(\mathbb{Z}_f)$ as in the above lemma. Let $S \to \mathrm{Spec}(\mathbb{Z}_f)$ and $x \in Z(G(S))$. If $s_S \in T(S)$ denotes the image of s under $T(\mathbb{Z}_f) \to T(S)$, then

$$x \in \mathrm{Cent}(s_S, G_S)(S) = T(S)$$

We claim that for every root $\alpha \in R(T_S, G_S)$ we have $\alpha(x) = 1$. Assume by way of contradiction that this were not the case. Let $u_\alpha : \mathbb{G}_{a,S} \to G_S$ be the root subgroup corresponding to α, and $y = u_\alpha(1)$. Then $y \in G(S)$ is a point not centralized by x, contrary to the assumptions. It follows that

$$x \in \bigcap_{\alpha \in R(T_S, G_S)} \ker(\alpha)(S) = Z(G)(S)$$

where the last equality is [SGA3, exp. 22, 4.1.6]. □

Corollary 3.3. *There exists a finite set of primes P such that $|Z(G_k)|$ divides $\mathrm{ord}(Z(G))$ for all primes $p \notin P$. In particular, if m is an integer coprime to the elements of P, then the order of every element of $Z(G(m))$ divides $\mathrm{ord}(Z(G))$.*

Proof. The second statement is an immediate consequence of the first, since $Z(G(m)) = \prod_{p^k \| m} Z(G_k)$. To prove the first, let P be the set of primes p for which $Z(G)(\mathbb{Z}/p^k\mathbb{Z})$ is a proper subgroup of $Z(G_k)$. According to Corollary 3.2 the set P is finite. For a prime p not in P, we then have $Z(G_k) = Z(G)(\mathbb{Z}/p^k\mathbb{Z})$. As already remarked, $Z(G)$ is a finite product of μ_n's. Since $(\mathbb{Z}/p^k\mathbb{Z})^\times$ is cyclic, the number $|\mu_n(\mathbb{Z}/p^k\mathbb{Z})|$ divides n. The statements now follows. □

Lemma 3.4. *The natural projection $\mathbb{Z}/p^k\mathbb{Z} \to \mathbb{Z}/p^{k-1}\mathbb{Z}$ induces a surjective homomorphism*

$$G_k \to G_{k-1}$$

For all but finitely many primes p, this homomorphism restricts to an isomorphism

$$Z(G_k) \to Z(G_{k-1}).$$

Proof. The first claim follows directly from the infinitesimal lifting property of smoothness. For the second claim, let p be a prime which does not divide $\mathrm{ord}(Z(G))$ and for which $Z(G_k) = Z(G)(\mathbb{Z}/p^k\mathbb{Z})$ for all k. By Corollaries 3.2 and 3.3 these are all but finitely many primes. Then $Z(G)$ is etale over $\mathbb{Z}_{(p)}$ and this implies the bijectivity of the second map. □

Corollary 3.5. *Assume that G is simply-connected. Then for all but finitely many p,*

$$Z(G_k/Z(G_k)) = \{1\}.$$

Proof. We prove this by induction on k. The base case is $k=1$, which is known, since $G(\mathbb{F}_p)/Z(G(\mathbb{F}_p))$ is simple. For the induction step, let $k>1$. Let $z \in G_k$ be an element which is central in $G_k/Z(G_k)$. Then for all $g \in G_k$, $z_g := gzg^{-1}z^{-1} \in Z(G_k)$. Under the surjection $G_k \to G_{k-1}$, the element z maps to an element $\bar{z}$ with the same property. Applying the induction hypothesis we see that $\bar{z} \in Z(G_{k-1})$. This implies, that $\bar{z}_g = 1$. Lemma 3.4 now implies $z_g = 1$ and the statement follows. □

For $0 \le i \le k$, let $G_k^i := \ker(G_k \to G_i)$. This provides a descending filtration

$$G_k = G_k^0 \ge G_k^1 \ge ... \ge G_k^k = \{1\}.$$

We fix a closed embedding $G \to \mathrm{SL}_m$ defined over $\mathbb{Z}$. This yields an embedding of Lie-algebras $\mathfrak{g} \to \mathrm{sl}_m$ defined over $\mathbb{Z}$. We identify G and $\mathfrak{g}$ with their respective images. Clearly $G_k^i = [1+p^iM_m(\mathbb{Z}/p^k\mathbb{Z})] \cap G_k$, and an element $1+p^ix \in G_k^i$ belongs to G_k^{i+1} if and only if $x \equiv 0 \bmod p$.

The following Lemma is a well-known result from the theory of Moy-Prasad filtrations [MP94].

Lemma 3.6 (Moy-Prasad)**.**

1. $[G_k^i, G_k^j] \subset G_k^{i+j}$.
2. *For* $1 \le i \le k-1$ *the map*

$$G_k^i/G_k^{i+1} \to \mathfrak{g}(\mathbb{F}_p), \qquad 1+p^ix \mapsto x \bmod p$$

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

Remark 3.7. In particular, one sees inductively that each G_k^i for $i>0$ is a p-group.

Lemma 3.8. *There exists positive constants c, C such that for all prime powers $m = p^k$*

$$cm^{\dim(G)} \le |G(m)| \le Cm^{\dim(G)}.$$

Proof. In the case $k=1$ the lemma follows from [S68, Theorem 25, Section 9]. The general case reduces to this, because according to Lemma 3.6 we have $|G_k| = p^{(k-1)\dim(G)}|G(\mathbb{F}_p)|$. □

Lemma 3.9. *For all but finitely many p, the Lie-algebra $\mathfrak{g}(\mathbb{F}_p)$ has no center, and the adjoint action of $G(\mathbb{F}_p)/Z(G(\mathbb{F}_p))$ on $\mathfrak{g}(\mathbb{F}_p)$ is faithful and irreducible.*

Proof. This is a well-known classical result. See for example [H84], [H82]. □

Lemma 3.10. *Assume that p is sufficiently large, and $0 \le i \le k-2$. For every $g \in G_k^i \smallsetminus G_k^{i+1}Z(G_k)$ there exists $h \in G_k^1$ such that $hgh^{-1}g^{-1} \in G_k^{i+1} \smallsetminus G_k^{i+2}Z(G_k)$.*

Proof. Note first that by Lemma 3.4, $G_k^{i+1} \cap (G_k^{i+2}Z(G_k)) = G_k^{i+2}$. Hence it is enough to find h such that $hgh^{-1}g^{-1} \notin G_k^{i+2}$.

Write $h = 1 + py$ with some $y \in M_m(\mathbb{Z}/p^k\mathbb{Z})$ to be determined. We will make use of the following computation: For any $x \in M_m(\mathbb{Z}/p^k\mathbb{Z})$ we have

$$\begin{aligned}(1+py)x(1+py)^{-1} &= (x+pyx)(1+py)^{-1} \\ &= (x+pxy-p[x,y])(1+py)^{-1} \\ &= (x-p[x,y](1+py)^{-1})\end{aligned}$$

where $[x,y] = xy - yx$.

First assume that $i = 0$. Then using the above computation we see that

$$hgh^{-1}g^{-1} = 1 - p[g,y](1+py)^{-1}g^{-1}$$

Clearly the right hand side belongs to G_k^1, and to show that it does not belong to G_k^2 it is enough by Lemma 3.6 to show that the reduction mod p of the matrix $[g,y](1+py)^{-1}g^{-1} \in M_m(\mathbb{Z}/p^k\mathbb{Z})$ is non-zero. Call this reduction T. It belongs to $\mathfrak{g}(\mathbb{F}_p)$. Using the formula

$$(1+py)^{-1} = \sum_{j=0}^{k-1} (-py)^j$$

we compute that $T = [\bar{g},\bar{y}]\bar{g}^{-1} = \bar{g}\bar{y}\bar{g}^{-1} - \bar{y}$. By Lemma 3.4, the preimage of $Z(G(\mathbb{F}_p))$ under $G_k \to G(\mathbb{F}_p)$ is $G_k^1 Z(G_k)$. Thus by assumption, the image $\bar{g}$ of g in $G(\mathbb{F}_p)/Z(G(\mathbb{F}_p))$ is non-trivial, and by Lemma 3.9 there exists $\bar{y} \in \mathfrak{g}(\mathbb{F}_p)$ such that $\bar{g}\bar{y}\bar{g}^{-1} \neq \bar{y}$. According to Lemma 3.6, there exists $h = 1 + py \in G_k^1$ corresponding to this $\bar{y}$. This completes the proof in the case $i = 0$.

Now assume $i > 0$. We write $g = 1 + p^i x$ for some $x \in M_m(\mathbb{Z}/p^k\mathbb{Z})$ whose reduction mod p belongs to $\mathfrak{g}(\mathbb{F}_p)$. Then

$$\begin{aligned}&(1+py)(1+p^ix)(1+py)^{-1}(1+p^ix)^{-1} \\ =\ &(1+p^i(1+py)x(1+py)^{-1})(1+p^ix)^{-1} \\ =\ &(1+p^ix-p^{i+1}[x,y](1+py)^{-1})(1+p^ix)^{-1} \\ =\ &1-p^{i+1}[x,y](1+py)^{-1}(1+p^ix)^{-1}\end{aligned}$$

Again $hgh^{-1}g^{-1} \in G_k^{i+1}$, and we want to choose y so that this element does not belong to G_k^{i+2}. By Lemma 3.6, this is equivalent to the demand that the reduction mod p of the element

$$[x,y](1+py)^{-1}(1+p^ix)^{-1} \in M_m(\mathbb{Z}/p^k\mathbb{Z})$$

be non-trivial. Using the formula for $(1+p^i x)^{-1}$ analogous to that used above for $(1+py)^{-1}$ we compute that this element is equal mod p to $[x,y]$. Now we consider the image of $[x,y] \in M_m(\mathbb{F}_p)$. Of course, this is just the bracket of the images of x and y in $M_m(\mathbb{F}_p)$. But these images, and hence their bracket, lie in $\mathfrak{g}(\mathbb{F}_p)$. Again as in the case $i=0$, specifying h is equivalent to choosing the class of y in $\mathfrak{g}(\mathbb{F}_p)$ in such a way that its bracket with the class of x is non-trivial. Since the Lie-algebra $\mathfrak{g}(\mathbb{F}_p)$ has no center, the class of x is non-central, and so an appropriate y exists. □

Proposition 3.11. *Assume that p is sufficiently large and G is simply-connected. Then every normal subgroup $N < G_k$ which contains $Z(G_k)$ equals $G_k^i Z(G_k)$ for some i.*

Proof. We will first prove under the assumption $k > 1$ by descending induction on i the following statement.

$$\forall 0 \leq i < k: \quad N \cap [G_k^i \setminus G_k^{i+1} Z(G_k)] \neq \emptyset \quad \Rightarrow \quad G_k^i \subset N$$

The base case is when $i = k-1 > 0$. Then the isomorphism of Lemma 3.6 identifies G_k^i with $\mathfrak{g}(\mathbb{F}_p)$ and $N \cap G_k^i$ with an invariant subspace of $\mathfrak{g}(\mathbb{F}_p)$. By assumption this space is non-trivial, and by Lemma 3.9 it is all of $\mathfrak{g}(\mathbb{F}_p)$, hence $N \cap G_k^i = G_k^i$. For the induction step, assume $i \geq 0$. Let $g \in N \cap [G_k^i \setminus G_k^{i+1} Z(G_k)]$. Use Lemma 3.10 to obtain $h \in G_k^1$ such that $hgh^{-1}g^{-1} \in G_k^{i+1} \setminus G_k^{i+2} Z(G_k)$. Then $hgh^{-1}g^{-1} \in N$, and we may apply the induction hypothesis to conclude $G_k^{i+1} \subset N$. Now look at the normal subgroup $(N \cap G_k^i)/G_k^{i+1}$ of G_k^i/G_k^{i+1}. If $i > 0$, then we have the isomorphism $G_k^i/G_k^{i+1} \to \mathfrak{g}(\mathbb{F}_p)$ and the image of that normal subgroup is a non-trivial invariant subspace. If $i = 0$, then we have the isomorphism $G_k^i/G_k^{i+1} \to G(\mathbb{F}_p)$ and the image of that normal subgroup is normal subgroup of $G(\mathbb{F}_p)$ which properly contains $Z(G(\mathbb{F}_p))$. In both cases, we conclude that $(N \cap G_k^i)/G_k^{i+1} = G_k^i/G_k^{i+1}$, and hence $N \cap G_k^i = G_k^i$. This completes the induction.

Now we show how the proposition follows from the above statement. The case $k = 1$ is trivial since $G_1/Z(G_1)$ is simple. Thus assume $k > 1$. If $N = Z(G_k)$ there is nothing to prove. Otherwise there exists a unique smallest index i such that $G_k^i \setminus G_k^{i+1} Z(G_k)$ contains an element of N. By the above statement, $Z(G_k) G_k^i \subset N$, but by minimality of i this must in fact be an equality. □

Proposition 3.12. *Let N be a natural number, and $H = \ker[G(\mathbb{Z}) \to G(N)]$. If G is simply-connected, then for any m coprime to N the projection $G(\mathbb{Z}) \to G(m)$ maps H surjectively onto $G(m)$.*

Proof. We begin with the special case $N = 1$, then $H = G(\mathbb{Z})$. Since G is smooth, the natural projection $G(\mathbb{Z}_p) \to G(\mathbb{Z}/p^k\mathbb{Z})$ is surjective for all primes p and all natural numbers k, and hence the natural projection $G(\widehat{\mathbb{Z}}) \to G(m)$ is surjective for all natural numbers m. By strong approximation ([PR94]), the inclusion $G(\mathbb{Z}) \to G(\widehat{\mathbb{Z}})$ has dense image. Thus, the natural projection $G(\mathbb{Z}) \to G(m)$ is surjective.

For the general case, we have $G(Nm) \cong G(N) \times G(m)$, and by the first part of the proof, the projection $G(\mathbb{Z}) \to G(N) \times G(m)$ is surjective. The preimage in $G(\mathbb{Z})$ of the subgroup $1 \times G(m)$ of $G(N) \times G(m)$ is precisely H, and maps surjectively onto $G(m)$. □

Proposition 3.13. *Assume that the rank of G is at least 2. Let $u : \mathbb{G}_a \to G$ be a root subgroup, and X a finite generating set for $G(\mathbb{Z})$. Then there exists a positive constant M such that for any positive $z \in \mathbb{Z}$*

$$\|u(z)\|_X \leq M \log(z).$$

Proof. Composing u with the chosen closed embedding $G \to \mathrm{SL}_m$, and then further with the natural inclusion $\mathrm{SL}_m \to \mathrm{M}_m$, we obtain a morphism of $\mathbb{Z}$-schemes

$$u' : \mathbb{A}^1_{\mathbb{Z}} \to \mathbb{A}^{m^2}_{\mathbb{Z}}$$

which is given by collection $\{u'_{i,j}\}$ of m^2-many polynomials in one variable with integral coefficients. Let $k = \max \deg(u'_{i,j}) + 1$. Then there exists a positive constant C such that $u'_{i,j}(z) \leq Cz^k$ for all positive integers z and all i, j. Thus $\|u'(z)\| \leq Cz^k$ for all $z \in \mathbb{N}$, where $\| \; \|$ is the maximum norm on $\mathrm{M}_m(\mathbb{R})$. The result now follows from Theorem A in [LMR01]. □

We are now ready to prove our main lower bound. In the proof, we are going to use the fact that if G is simply-connected and has rank at least 2, then $G(\mathbb{Z})$ has the congruence subgroup property. We refer the reader to [PR94, Chap. 9.5] for a discussion of this property. Also recall that a subgroup of $G(m)$ is called *essential* if it does not contain the kernel of the natural map $G(m) \to G(r)$ for any $r|m$ with $r < m$.

Theorem 3.14. *Assume that the rank of G is at least 2. Let K be a number field, $f \in \mathcal{O}_K$, and Δ a finitely generated subgroup of $G(\mathbb{C})$ with the property that $\Delta \cap G(\mathcal{O}_{K,f})$ is of finite-index in $G(\mathcal{O}_{K,f})$. Then*

$$\mathrm{F}_\Delta(n) \succeq n^{\dim(G)}.$$

Proof. Let G_{sc} be the simply connected cover of G, and $p : G_{\mathrm{sc}}(\mathcal{O}_{K,f}) \to G(\mathcal{O}_{K,f})$ the natural map. Then $\Delta_{\mathrm{sc}} := p^{-1}(\Delta \cap G(\mathcal{O}_{K,f}))$ is of finite index in $G_{\mathrm{sc}}(\mathcal{O}_{K,f})$ and the map $p : \Delta_{\mathrm{sc}} \to \Delta$ has finite kernel. By Lemma 2.4 we may assume for the rest of the proof that $G = G_{\mathrm{sc}}$ and $\Delta \subset G(\mathcal{O}_{K,f})$.

Since Δ is of finite-index in $G(\mathcal{O}_{K,f})$, so is $\Delta \cap G(\mathbb{Z})$ of finite-index in $G(\mathbb{Z})$. By virtue of the congruence subgroup property of $G(\mathbb{Z})$, we can find a principal congruence subgroup $\Delta' \subset \Delta \cap G(\mathbb{Z})$. Applying again Lemma 2.4, we may assume for the rest of the proof that $\mathcal{O}_{K,f} = \mathbb{Z}$ and that Δ is a principal congruence subgroup of $G(\mathbb{Z})$.

Let $N = \mathrm{ord}(Z(G))$. By Lemma 2.1, it suffices to find a lower bound for F^N_Δ. Loosely speaking, we will see that working with F^N_Δ instead of F_Δ will aid us in ignoring certain central elements in finite images of Δ.

We first construct candidates that are poorly approximated by finite quotients. Let X and Y be finite generating sets for $G(\mathbb{Z})$ and Δ respectively. Let S be the set of primes p for which at least one of the following conditions fails

- $|Z(G_k)|$ divides N,
- If $Z(G_k) \trianglelefteq N \trianglelefteq G_k$ then $N = G_k^i Z(G_k)$ for some i,
- The projection $G(\mathbb{Z}) \to G_k$ maps Δ surjectively onto G_k.

where as before $G_k = G(\mathbb{Z}/p^k\mathbb{Z})$. By Corollary 3.3 and Propositions 3.11 and 3.12 this set is finite. Put $\alpha = \prod_{p\in S} p$ and $r_k = \alpha^k \operatorname{lcm}(1,\ldots,k)$. Let $u : \mathbb{G}_a \to G$ be a root subgroup, and $B_k = u(r_k)$. Since u is defined over $\mathbb{Z}$, we have $B_k \in G(\mathbb{Z})$, hence $A_k := B_k^{[G(\mathbb{Z}):\Delta]} \in \Delta$. The elements A_k will be our candidates for achieving lower bounds for F_Δ^N.

Next, we bound the word length of A_k, i.e. the function $k \mapsto \|A_k\|_Y$. By Proposition 3.13 there exists a natural number M such that

$$\|A_k\|_X \leq M \log(\operatorname{lcm}(1,\ldots,k)\alpha^k).$$

Hence, by the prime number theorem we may find a potentially different natural number M so that $\|A_k\|_X \leq Mk$. Finally, since $G(\mathbb{Z})$ is quasi-isometric to Δ, we have that

$$\|A_k\|_Y \leq Mk, \tag{1}$$

for a some other natural number M.

The remainder of the proof is devoted to finding a lower bound for the cardinality of any finite quotient $Q = \Delta/H$ which detects A_k^N, in particular to the quotient realizing $D_\Delta^N(A_k)$. We start by taking one such quotient Q. Since we are looking for a lower bound of the cardinality of Q, we may replace it by either a subgroup or a quotient of it, and we will do so repeatedly in the following.

By the congruence subgroup property for $G(\mathbb{Z})$ there exists a natural number m such that the kernel of the projection $\phi : G(\mathbb{Z}) \to G(m)$ lies in H. Let Δ',H', and A_k' be the images of Δ, H, and A_k respectively in $G(m)$. By the Chinese remainder theorem, we may write $G(m) = A \times B$ where

$$A = \prod_{\substack{p^j \| m \\ p \in S}} G(p^j) \qquad \text{and} \qquad B = \prod_{\substack{p^j \| m \\ p \notin S}} G(p^j).$$

and $p^j \| m$ means that j is the greatest power of p which divides m.

We know $(A_k')^N \neq 1$. For any $c \in Z(B)$ we have $\operatorname{ord}(c) | N$ (see Corollary 3.3 and the choices of S and N). Thus we have $(cA_k')^N = (A_k')^N$ for any $c \in Z(B)$, which implies $cA_k' \notin$

H'. Hence, $A'_k \notin H'Z(B)$. Letting A''_k, Δ'', and H'' be the images of A'_k, Δ', and H' in $A \times B/Z(B)$ respectively, we have that $A''_k \notin H''$. Further, $[\Delta'' : H''] \leq [\Delta' : H']$ since Δ''/H'' is an image of $Q = \Delta'/H'$.

We claim that any quotient of $B/Z(B)$ is centerless: Indeed, by the choice of S, for every $p \notin S$, Lemma 3.4 and Corollary 3.5 imply that all quotients of $G(p^j)/Z(G(p^j))$ are centerless. By [LL01, 1.4] every normal subgroup of $B/Z(B)$ is a product of normal subgroups of the factors of $B/Z(B)$, and the statement follows.

Recall that Δ was assumed to be a principal congruence subgroup of $G(\mathbb{Z})$. By Proposition 3.12, $G(\mathbb{Z})$ projects onto $A \times B/Z(B)$. Hence, Δ'' is normal in $A \times B/Z(B)$, and applying [LL01, 1.3,1.4] we see that $\Delta'' = \Delta_1 \times \Delta_2$, where

$$\Delta_1 = \pi_1(\Delta'') \qquad \text{and} \qquad \Delta_2 = \pi_2(\Delta''),$$

where π_1 and π_2 are the natural projection maps of $A \times B/Z(B)$ onto A and $B/Z(B)$ respectively.

By the choice of S we have $\Delta_2 = B/Z(B)$. The subgroup H'' is normal in $\Delta'' = \Delta_1 \times \Delta_2$, and since Δ_2 has no center, [LL01, Corollary 1.4] applies again giving $H'' = H_1 \times H_2$ where $H_1 = \pi_1(H'')$ and $H_2 = \pi_2(H'')$. Now since $A''_k \notin H_1 \times H_2$ we have two cases: $\pi_1(A''_k) \notin \pi_1(H'')$ or $\pi_2(A''_k) \notin \pi_2(H'')$. In both cases, we claim that there exists a natural number M, independent of k, such that $M|Q| \geq k^d$, where $d := \dim(G)$.

We first handle the case $\pi_1(A''_k) \notin \pi_1(H'')$. Write $A = G(m_0)$, let r be the smallest natural number such that the kernel of the natural map $\phi : G(m_0) \to G(r)$ is contained in $\pi_1(H'')$. Then $\phi(\pi_1(A''_k)) \notin \phi(\pi_1(H''))$ and $\phi(\pi_1(H''))$ is essential or trivial. Since the image of A_k in $G(r)$ is nontrivial, r does not divide α^k. But any prime dividing r also divides α (recall the choices of A, r and α), hence $p^k | r$ for some $p \in S$. In the case $\phi(\pi_1(H''))$ is essential, [LS03, Proposition 6.1.2] gives $C[G(r) : \phi(\pi_1(H''))] \geq r \geq p^k$, where C is a natural number that only depends on G. If $\phi(\pi_1(H''))$ is trivial, we get the better bound $C|G(r)| \geq C|G(p^k)| \geq p^{kd}$ by Lemma 3.8 where C is again a natural number that depends only on G. Set $M' = C[G(\mathbb{Z}) : \Delta]$. Since $[G(r) : \phi(\pi_1(\Delta''))] \leq [G(\mathbb{Z}) : \Delta]$, we have

$$M'[\Delta'' : H''] \geq C[G(r) : \phi(\pi_1(\Delta''))][\phi(\pi_1(\Delta'')) : \phi(\pi_1(H''))] = C[G(r) : \phi(\pi_1(H''))] \geq p^k.$$

There exists a natural number M'' such that $M'' p^k \geq k^d$ for all $p \in S$ and $k \in \mathbb{N}$. Setting $M = M'M''$, we see that

$$M[\Delta'' : H''] \geq M'' p^k \geq k^d.$$

Since $|Q| \geq [\Delta'' : H'']$, the claim is shown.

Next we handle the case $\pi_2(A''_k) \notin \pi_2(H'')$. By repeated use of Corollary 1.4 in [LL01], there exists a natural projection $\phi : A \times B/Z(B) \to G_k/Z(G_k)$ with $\phi(A''_k) \notin \phi(H'')$ and $G_k = G(p^k)$ where $p \notin S$. By Proposition 3.11 and the normality of H_2 in $\Delta_2 = B/Z(B)$, we have $\phi(H'') = G^i_k/Z(G_k)$ for some i, hence the image of $\phi(A''_k)$ through the natural projection onto $G_i/Z(G_i)$ is non-trivial. Further, Q maps onto $G_i/Z(G_i)$.

From the estimate $M'|G_i| \geq p^{di}$ (Lemma 3.8), where M' is a natural number, and the fact that p^i does not divide $\mathrm{lcm}(1,\dots,k)$ we obtain $p^i \geq k$, and thus,

$$M'|G_i| \geq p^{id} \geq k^d.$$

Finally, since $|G_i|/|Z(G_i)| \leq |Q|$ and $|Z(G_i)| \leq N$ (by the choice of S), the claim holds with $M = M'N$.

The inequality $M|Q| \geq k^d$ in tandem with Inequality (1) gives some natural number M such that $M\,\mathrm{F}_{\Delta}^{N}(k) \geq k^d$, finishing the proof of the theorem. □

4 Upper bounds

In this section, G continues to be a Chevalley group. Our main upper bound result is a corollary of the following three propositions.

Proposition 4.1. *Let L be a number field with ring of integers $\mathcal{O}_L$. Then*

$$\mathrm{F}_{\mathcal{O}_L}(n) \approx \log(n).$$

Moreover, the finite quotients of the form $\mathbb{Z}/p\mathbb{Z} \cong \mathcal{O}_L/\mathfrak{p}$, where p is a prime number that splits completely in $\mathcal{O}_L$, $\mathfrak{p}|p\mathcal{O}_L$, are enough to obtain the upper bound.

Proof. The fact $\mathrm{F}_{\mathcal{O}_L}(n) \succeq \log(n)$ follows immediately from [B10, Thm. 2.2] and Lemma 2.4. Thus it is enough to prove $\mathrm{F}_{\mathcal{O}_L}(n) \preceq \log(n)$.

Let $S = \{b_1,\dots,b_k\}$ be an integral basis for $\mathcal{O}_L$, and fix a nontrivial g in $\mathcal{O}_L$ with $\|g\|_S = n$. Then $g = \sum_{i=1}^{n} a_i b_i$ where $a_i \in \mathbb{Z}$ and $|a_i| \leq n$. Since $g \neq 0$ there exists k such that $a_k \neq 0$. By the Cebotarëv density theorem, the set P of all primes in $\mathbb{Z}$ that split in $\mathcal{O}_L$ has nonzero natural density in the set of all primes. We claim that there exists $C > 0$, which does not depend on n, and a prime q such that (q) splits in $\mathcal{O}_L$ and $q \leq C\log(n)$ and $a_k \not\equiv 0 \mod q$. Indeed, enumerate $P = \{q_1, q_2, \dots\}$. Let q_{r+1} be the first prime in P such that $a_k \not\equiv 0 \mod q_{r+1}$. Then $q_1 \cdots q_r$ divides a_k and by the prime number theorem and positive density of P, we have that $q_{r+1} \leq Mr\log(r)$ for some $M > 0$, depending only on L. A similar calculation shows that there exists $M' > 0$ such that $q_1 \cdots q_r \geq e^{M'r\log(r)}$. Hence, $q_{r+1} \leq C\log(a_k)$, where $C > 0$ depends only on L. The claim is shown.

Write $(q) = \mathfrak{q}_1 \cdots \mathfrak{q}_c$ with $|\mathcal{O}_L/\mathfrak{q}_i| = q$. Since q does not divide a_k and since the integral basis S gets sent to a $\mathbb{F}_q$-basis of $\mathcal{O}_L/(q)$, we have that $g \neq 1$ in $\mathcal{O}_L/(q)$. Hence, there exists one $\mathfrak{q}_i$ with $g \neq 1$ in $\mathcal{O}_L/\mathfrak{q}_i$. As the cardinality of $\mathcal{O}_L/\mathfrak{q}_i$ is equal to q which is no greater than $C\log(n)$, we have the desired upper bound. □

Proposition 4.2. *Let Γ be a finitely generated subgroup of $G(\mathcal{O}_{L,f})$, where L is a number field and $f \in \mathbb{Z}$. Then*

$$\mathrm{F}_{\Gamma} \preceq n^{\dim(G)}.$$

Proof. Recall that we have fixed a closed embedding $G \to \mathrm{SL}_m$ and are identifying G with its image. Let $\mathcal{X}$ be a finite set of generators for Γ as a semigroup. Let S be an integral basis for $\mathcal{O}_L$. We claim that there exists $\lambda > 0$ such that for any $A \in \Gamma$ with $\|A\|_{\mathcal{X}} = n$ and any non-zero coefficient $a \in \mathcal{O}_{L,f}$ of $A - I$ we have

$$\|f^k a\|_S \leq \lambda^n$$

where k is the least natural number such that $f^k a \in \mathcal{O}_L$.

The prove the claim, let $a' = a+1$ or $a' = a$ according to whether a is a diagonal coefficient or not. Thus a' is a coefficient of A. Let K be the least natural number such that for all $X \in \mathcal{X}$, $f^K X \in \mathrm{M}_m(\mathcal{O}_L)$. Because A is a product of exactly n elements of X, we have $f^{nK} A \in \mathrm{M}_m(\mathcal{O}_L)$, and in particular $k < nK$. Then

$$\|f^k a\|_S \leq \|f^{nK} a\|_S \leq \|f^{nK} a'\|_S + f^{nK}\|1\|_S.$$

This reduces the above claim to the following. There exists $\mu > 0$ such that for any $A \in \Gamma$ with $\|A\|_{\mathcal{X}} = n$ and any non-zero coefficient $a \in \mathcal{O}_{L,f}$ of A we have

$$\|f^{nK} a\|_S \leq \mu^n.$$

We claim that if α denotes the maximum of $\|st\|_S$, where s,t range over the elements of S, and β denotes the maximum of $\|f^K x\|_S$, where x ranges over all entries of all elements of $\mathcal{X}$, then $\mu := m\alpha\beta$ satisfies the last statement. To see this, consider first the case $A = XY$ with $X, Y \in \mathcal{X}$. The entries of A are scalar products of the rows of X and the columns of Y. Thus we are led to study $\|x \cdot y\|_S$ for $x, y \in \mathcal{O}_L^m$, where $\cdot$ denotes scalar product. Clearly we have $\|x \cdot y\|_S \leq m \max\{\|x_i y_i\|_S : 1 \leq i \leq m\}$. In terms of the basis S we can write

$$x_i = \sum_{s \in S} \lambda_{x,i,s} s \qquad \text{and} \qquad y_i = \sum_{s \in S} \lambda_{y,i,s} s$$

where the λ's belong to $\mathbb{Z}$. One computes

$$\|x_i y_i\|_S \leq \|x_i\|_S \|y_i\|_S \max\{\|st\|_S : \ s,t \in S\}.$$

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

To complete the proof of the proposition, let $A \in \Gamma$ be such that $\|A\|_{\mathcal{X}} \leq n$. Let a be a non-zero entry of $A - I$ and k the least integer with $f^k a \in \mathcal{O}_L$. According to Proposition 4.1 and the claim above there exists a natural number M, independent of n, and a homomorphism $\phi : \mathcal{O}_L \to \mathbb{F}_p$ such that $p < Mn$ and $\phi(f^k a) \neq 0$. For all but finitely many primes p, we have that $\phi(f)$ is non-zero in $\mathbb{F}_p$. Hence, we may assume that ϕ extends to a homomorphism $\phi : \mathcal{O}_{L,f} \to \mathbb{F}_p$ and $\phi(a) \neq 0$. The image of A under the induced map $G(\mathcal{O}_{L,f}) \to G(\mathbb{F}_p)$ is non-trivial. Further, according to Lemma 3.8, there exits $M' > 0$ such that $|G(\mathbb{F}_p)| \leq M' p^{\dim(G)}$. Hence, $|G(\mathbb{F}_p)| \leq M'(Mn)^{\dim(G)}$. □

Proposition 4.3. *Let $K \subset \mathbb{C}$ be a number field, $b \in \mathcal{O}_K \smallsetminus \{0\}$, and $\Gamma \subset G(\mathbb{C})$ a finitely generated subgroup, such that $G(\mathcal{O}_{K,b}) \cap \Gamma$ is of finite-index in Γ. Then there exists a finite extension $L \subset \mathbb{C}$ of K, an element $f \in \mathbb{Z} \smallsetminus \{0\}$, and a homomorphism $\Gamma \to G(\mathcal{O}_{L,f})$ with finite kernel.*

Proof. Let $S \subset \Gamma$ be a finite generating set. There exists a field $F \subset \mathbb{C}$, finitely generated over K, such that $S \subset G(F)$. Let $t_1, ..., t_n$ be a transcendence basis for F/K. The extension $F/K(t_1, ..., t_n)$ is finitely generated and algebraic, hence finite. Let $a \in F$ be a primitive element for that extension. Thus $F = K(t_1, ..., t_n, a)$. The ring $\mathcal{O}_{K,b}[t_1, ..., t_n]$ is a free polynomial algebra over $\mathcal{O}_{K,b}$ with field of fractions $K(t_1, ..., t_n)$. There exists $s \in \mathcal{O}_K[t_1, ..., t_n]$ such that the coefficients of the minimal polynomial of a over $K(t_1, ..., t_n)$ lie in the localization $\mathcal{O}_{K,b}[t_1, ..., t_n]_s$. Thus the element a is integral over $\mathcal{O}_{K,b}[t_1, ..., t_n]_s$ and the ring $\mathcal{O}_{K,b}[t_1, ..., t_n]_s[a] \subset F$ has F as its field of fractions. Thus there exists $r \in \mathcal{O}_{K,b}[t_1, ..., t_n]_s[a]$, such that if we put $R = \mathcal{O}_{K,b}[t_1, ..., t_n]_s[a]_r$, then $S \subset G(R)$, and consequently $\Gamma \subset G(R)$.

We can find a homomorphism of $\mathcal{O}_{K,b}$-algebras

$$\phi : \mathcal{O}_{K,b}[t_1, ..., t_n] \to \mathcal{O}_{K,b}$$

such that $\phi(s) \neq 0$. Then ϕ extends to a homomorphism

$$\phi : \mathcal{O}_{K,b}[t_1, ..., t_n]_s \to \mathcal{O}_{K,b\phi(s)}.$$

There exists a finite extension $L \subset \mathbb{C}$ of K such that the composition of ϕ with the natural inclusion $\mathcal{O}_{K,b\phi(s)} \to K$ extends to a homomorphism

$$\phi : \mathcal{O}_{K,b}[t_1, ..., t_n]_s[a] \to L.$$

The element $\phi(a) \in L$ is integral over $\mathcal{O}_{K,b\phi(s)}$, and hence belongs to $\mathcal{O}_{L,b\phi(s)}$. Thus in fact we obtain a homomorphism

$$\phi : \mathcal{O}_{K,b}[t_1, ..., t_n]_s[a] \to \mathcal{O}_{L,b\phi(s)}.$$

We consider $\phi(r) \in \mathcal{O}_{L,b\phi(s)}$. Perturbing ϕ slightly if necessary, we may assume that $\phi(r) \neq 0$. In this way we obtain a homomorphism of $\mathcal{O}_K$-algebras

$$\phi : R \to \mathcal{O}_{L,b\phi(rs)}.$$

The algebra homomorphism $\mathcal{O}_L \otimes_{\mathbb{Z}} \mathbb{Q} \to L$ given by multiplication is an isomorphism. Since $\mathbb{Q} = \varinjlim_{f \in \mathbb{Z}} \mathbb{Z}_f$, we conclude that

$$L \cong \varinjlim_{f \in \mathbb{Z}} \mathcal{O}_L \otimes_{\mathbb{Z}} \mathbb{Z}_f \cong \varinjlim_{f \in \mathbb{Z}} \mathcal{O}_{L,f}.$$

Thus there exists some $f \in \mathbb{Z}$ such that $[b\phi(rs)]^{-1} \in \mathcal{O}_{L,f}$. Composing ϕ with the inclusion $\mathcal{O}_{L,b\phi(rs)} \to \mathcal{O}_{L,f}$ we finally arrive at a homomorphism of $\mathcal{O}_{K,b}$-algebras

$$\phi : R \to \mathcal{O}_{L,f}.$$

It induces a group homomorphism $\phi_* : G(R) \to G(\mathcal{O}_{L,f})$ which fits into the commutative diagram

$$\begin{array}{ccc} G(R) & \xrightarrow{\phi_*} & G(\mathcal{O}_{L,f}) \\ \nwarrow & & \nearrow \\ & G(\mathcal{O}_{K,b}) & \end{array}$$

The restriction of ϕ_* to Γ is the desired homomorphism: Its kernel has trivial intersection with $G(\mathcal{O}_{K,b})$, i.e. it avoids a finite-index subgroup of Γ, and hence must be finite. □

Corollary 4.4. *Let $\Gamma \subset G(\mathbb{C})$ be a finitely generated subgroup. Assume that there exists a finite extension $K \subset \mathbb{C}$ of $\mathbb{Q}$ and $b \in \mathcal{O}_K \smallsetminus \{0\}$ such that $G(\mathcal{O}_{K,b}) \cap \Gamma$ is of finite-index in Γ. Then*

$$\mathrm{F}_\Gamma(n) \preceq n^{\dim(G)}.$$

Proof. This follows immediately from Proposition 4.3, Lemma 2.4 and Proposition 4.2. □

References

[A87] R. C. Alperin, *An elementary account of Selberg's lemma.* Enseign. Math. (2) 33 (1987), no. 3-4, 269–273.

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

[H82] G. M. D. Hogeweij, *Almost classical Lie algebras: I, II*, Indag. Math. 44, (1982), 441–460.

[H84] G. Hiss, *Die adjungierten Darstellungen der Chevalley-Gruppen*, Arch. Math. 42 (1984), 408-416.

[KM10] M. Kassabov and F. Matucci, *Bounding residual finiteness in free groups*, preprint.

[SGA3] M. Demazure, A. Grothendieck, *Schémas en groupes I, II, III, Lecture Notes in Math* 151, 152, 153, Springer- Verlag, New York (1970).

[S68] R.G. Steinberg, *Lectures on Chevalley groups* , Yale Univ. Press (1968).

[LL01] M. Larsen, A. Lubotzky, *On linear groups of polynomal normal subgroup growth; the (G2 F4 E8) theorem*, Algebraic groups & Arithmetic, Ed. S.G.Dani, G. Prasad, Tata inst. Fund. Res. Stud. Math. 441-468, TIFR, Mumbai.

[LMR01] A. Lubotzky, Sh. Mozes, M. S. Raghunathan, *The word and Riemannian metrics on lattices of semisimple groups*, Publ. Math. IHES, No. 91 (2000), 5-53.

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

[MP94] A. Moy, G. Prasad, Unrefined minimal K-types for p-adic groups, Invent. math. 116, 393-408 (1994).

[PR94] V. P. Platonov and A. S. Rapinchuk, *Algebraic groups and number theory*. Translated from the 1991 Russian original by Rachel Rowen. Pure and Applied Mathematics, 139. Academic Press, Inc., Boston, MA, 1994.

Dept. of Mathematics, University of Chicago
5734 University Ave. Chicago, IL 60637
E-mails: khalid@math.uchicago.edu, tkaletha@math.uchicago.edu