Polynomial Representation Growth and the Congruence Subgroup Problem

Alexander Lubotzky and Benjamin Martin

September 1, 2003

Dedicated to Andy Magid for his upcoming sixtieth birthday

Abstract

Let Γ be an S-arithmetic group in a semisimple group. We show that if Γ has the congruence subgroup property then the number of isomorphism classes of irreducible complex n-dimensional characters of Γ is polynomially bounded. In characteristic zero, the converse is also true. We conjecture that the converse also holds in positive characteristic, and we prove some partial results in this direction.

1 Introduction

Let Φ be a group. We denote by $r_n(\Phi)$ (respectively $\widehat{r}_n(\Phi)$) the number of isomorphism classes of irreducible n-dimensional complex representations (respectively with finite image) of Φ. We call $r_n(\Phi)$ the *representation growth* function of Φ. In general $r_n(\Phi)$ may be infinite. There is no known characterisation of the groups Φ such that $r_n(\Phi) < \infty$ for every n; such groups are called *rigid* in [BLMM02]. For finitely generated Φ, $\widehat{r}_n(\Phi) < \infty$ for every n if and only if Φ has the property FAb (that is, $\Phi_0^{\mathrm{ab}} := \Phi_0/[\Phi_0, \Phi_0]$ is finite for every finite index subgroup Φ_0 of Φ) [BLMM02, Proposition 2].

Definition 1.1 We say that Φ has *polynomial representation growth* (PRG) if the function $r_n(\Phi)$ is polynomially bounded: that is, if there exist $c_1, c_2 \in \mathbb{R}$ such that $r_n(\Phi) \leq c_1 n^{c_2}$ for every n. (In particular, this implies that every $r_n(\Phi)$ is finite.)

Let k be a global field and $\mathcal{O}$ its ring of integers. Write V for the set of (equivalence classes of) valuations of k, V_f for the set of finite (that is, nonarchimedean) valuations, and V_∞ for the set of infinite (that is, archimedean) valuations. Fix a finite subset S of V containing V_∞. Let $\mathcal{O}_S := \{x \in k \mid v(x) \geq 0 \ \forall v \in V - S\}$ be the ring of S-integers. Given $v \in V$, we write k_v for the completion of k with respect to v and $\mathcal{O}_v$ for the valuation ring of k_v.

Let G be a semisimple simply connected and connected algebraic group defined over k, with a fixed embedding $G \hookrightarrow \mathrm{GL}_N$. Let $\Gamma = G(\mathcal{O}_S) := G(k) \cap \mathrm{GL}_N(\mathcal{O}_S)$. We assume that $T := \{v \in V \mid G(k_v) \text{ is compact}\}$ is disjoint from $S - V_\infty$, and that $G(\mathcal{O}_S)$ is infinite (equivalently, that $\prod_{v \in S} G(k_v)$ is noncompact).

We say that Γ has the *congruence subgroup property* (CSP for short) if $C := \ker\left(\widehat{G(\mathcal{O}_S)} \xrightarrow{\pi} G(\widehat{\mathcal{O}}_S)\right)$ is finite; here $\widehat{G(\mathcal{O}_S)}$ is the profinite completion of $G(\mathcal{O}_S)$ and $G(\widehat{\mathcal{O}}_S) = \prod_{v \notin S} G(\mathcal{O}_v)$ is the congruence completion of $G(\mathcal{O}_S)$, where $G(\mathcal{O}_v) := G(k_v) \cap \mathrm{GL}_N(\mathcal{O}_v)$. The map π is surjective — that is, Γ is dense in $G(\widehat{\mathcal{O}}_S)$ — by the Strong Approximation Theorem (cf. [PR94, Theorem 7.12] and [Pra77]).

The main goal of this paper is to prove the following theorem.

Theorem 1.2 *Let $\Gamma = G(\mathcal{O}_S)$ be as above, and assume that if* $\operatorname{char} k = 2$ *then G contains no factors of type A_1 or of type C_m for any m. If Γ has the congruence subgroup property then Γ has polynomial representation growth.*

We conjecture that the converse holds in general, but we can prove this completely (and indeed, in a slightly stronger form) only when $\operatorname{char} k = 0$ (Theorem 1.3). As in [Lub95] and [PR93], we assume for Theorem 1.3 that the Platonov-Margulis Conjecture holds: that is, that $G(k)$ has the standard description of normal subgroups. This is known to hold in almost all cases (see [PR94, Chapter 9], [Seg99]).

Theorem 1.3 *Assume that* $\operatorname{char} k = 0$. *If $\Gamma = G(\mathcal{O}_S)$ is as above and $\widehat{r}_n(\Gamma)$ is polynomially bounded then Γ has the congruence subgroup property.*

A striking feature of the proof is that Theorem 1.2 (or rather, the closely related result Proposition 5.1) is needed to prove Theorem 1.3.

The characterisation of the congruence subgroup property by means of polynomial representation growth joins several previous characterisations of the CSP by purely group-theoretic properties: for example, that the profinite completion $\widehat{\Gamma}$ is boundedly generated or that $\log s_n(\Gamma) \leq o((\log n)^2)$ [Lub95], [PR93], where $s_n(\Gamma)$ denotes the number of index n subgroups of Γ. Unfortunately, all of these characterisations so far are true only in characteristic zero and are false in positive characteristic. We believe that the current characterisation is valid in positive characteristic as well, but we were not able to prove this. (The proof of Theorem 1.3 does, however, go a long way in characteristic p.)

The paper is organised as follows. In Section 2 we deal with some preliminary results. In Section 3 we study representations with infinite image. In Section 4 we study representations with finite image; we finish the section with the proof of Theorem 1.2. In Section 5 we prove some consequences of the results in Section 4; these concern estimates for the image size (rather than the number) of n-dimensional representations. Not only do these results have independent interest, but also most of them are needed in Section 6, where Theorem 1.3 is proved.

We are grateful to Nikolay Nikolov and Andrei Jaikin-Zapirain for helpful and informative discussions.

This research was supported by the Israel Science Foundation and the United States Israel Binational Science Foundation. The second author was supported by a Golda Meir Post-Doctoral Fellowship at the Hebrew University of Jerusalem.

2 Preliminaries

All logarithms are to base 2 unless otherwise indicated. We write $[x]$ for the largest integer no greater than x.

Given a group Φ, we write $\mathrm{Rep}_n(\Phi)$ (respectively $\mathrm{Irr}_n(\Phi)$) for the set of isomorphism classes of n-dimensional complex representations (respectively irreducible representations) of Φ. All representations are complex unless otherwise indicated. We say that a representation is *finite* if its image is finite, and *infinite* otherwise.

When we consider subgroups of a profinite group H, we will always mean closed subgroups. We will consider only continuous representations of H; this implies that the kernel of a representation is open and the image is finite, and so $r_n(H) = \widehat{r}_n(H)$. It also implies that if Φ is a discrete group then $\widehat{r}_n(\Phi) = r_n(\widehat{\Phi}) = \widehat{r}_n(\widehat{\Phi})$, where $\widehat{\Phi}$ is the profinite completion of Φ.

Definition 2.1 We define $R_n(\Phi) = \sum_{m=1}^{n} r_m(\Phi)$.

Note that $r_n(\Phi)$ is polynomially bounded if and only if $R_n(\Phi)$ is. On the other hand, even if $r_n(\Phi) = |\mathrm{Irr}_n(\Phi)|$ is polynomially bounded, in general $|\mathrm{Rep}_n(\Phi)|$ is not.

The following result relates the representation growth of a group to that of a finite index subgroup.

Lemma 2.2 *Let Φ' be a finite index subgroup of Φ. Then for all $n \in \mathbb{N}$, we have*

$$R_n(\Phi') \leq [\Phi\colon \Phi'] R_{n[\Phi:\Phi']}(\Phi)$$

and

$$R_n(\Phi) \leq [\Phi\colon \Phi'] R_n(\Phi').$$

Proof For each $m \in \{1, \ldots, n\}$ and each $\tau \in \mathrm{Irr}_m(\Phi')$, choose an irreducible component $\psi(\tau)$ of the induced representation $\mathrm{Ind}_{\Phi'}^{\Phi}\tau$. This gives a map ψ from $\bigcup_{m=1}^{n} \mathrm{Irr}_m(\Phi')$ to $\bigcup_{m=1}^{n[\phi:\phi']} \mathrm{Irr}_m(\Phi)$. Let $\tau \in \mathrm{Irr}_m(\Phi')$ and let $\{\tau_\lambda \mid \lambda \in \Lambda\}$ be the elements of $\psi^{-1}(\psi(\tau))$. Without loss of generality we assume that $\dim \tau$ is minimal among the $\dim \tau_\lambda$. By Frobenius reciprocity, each τ_λ is an irreducible component of $\psi(\tau)|_{\Phi'}$; hence, $\dim \psi(\tau) \geq |\Lambda| \dim \tau$. But $\dim \psi(\tau) \leq [\Phi\colon \Phi'] \dim \tau$, which implies that $|\Lambda| \leq [\Phi\colon \Phi']$. The first inequality follows.

The proof of the second inequality is similar, and we leave it to the reader.

Corollary 2.3 *If Φ' is a finite index subgroup of Φ then Φ has PRG if and only if Φ' has PRG.*

Definition 2.4 We define $A_n(\Phi) = \max\{[\Phi'\colon [\Phi', \Phi']] \mid \Phi' \leq \Phi, [\Phi\colon \Phi'] \leq n\}$.

We will often use the following important fact.

Lemma 2.5 *Every irreducible representation σ of a pronilpotent group H is induced from a one-dimensional representation of some subgroup of index* $\dim \sigma$*.*

Proof Since σ is continuous by assumption, it factors through some finite nilpotent quotient P of H. Finite nilpotent groups are monomial [CR81, Theorem 11.3], so we have $\sigma = \mathrm{Ind}_Q^P \chi$ for some $Q \leq P$ with $[P\colon Q] = \dim \sigma$ and some one-dimensional representation χ of Q. Setting M equal to the preimage of Q in H and regarding χ as a representation of M, it is easily checked that $\sigma = \mathrm{Ind}_M^H \chi$.

This fact allows us to compare the growth rates of $A_n(\Phi)$ and $R_n(\Phi)$.

Lemma 2.6 *Let H be a profinite group.*
(a) $A_n(H) \leq nR_n(H)$. In particular, if $A_n(H)$ is not polynomially bounded then H does not have PRG.
(b) If H is pronilpotent then $r_n(H) \leq A_n(H)s_n(H)$.
(c) If H is compact p-adic analytic then H has PRG if and only if $A_n(H)$ is polynomially bounded.

Proof If $m \leq n$ and M is an index m subgroup of H with abelianisation of size $A_n(H)$ then M admits $A_n(H)$ one-dimensional representations, so (a) follows from the first inequality of Lemma 2.2. If H is pronilpotent then every irreducible n-dimensional representation is induced from a one-dimensional representation (Lemma 2.5), so $r_n(H)$ is bounded by the number of pairs (M, χ), where $M \leq H$, $[H \colon M] = n$ and χ is a one-dimensional representation of H. Part (b) now follows immediately.

Now suppose that H is compact p-adic analytic. If H' is an open subgroup of H then H has PRG if and only if H' does (Corollary 2.3), and it is easy to see that $A_n(H)$ is polynomially bounded if and only if $A_n(H')$ is. Therefore we can assume that H is a p-adic analytic pro-p group. As $s_n(H)$ is polynomially bounded [DdSMS99, Theorem 3.19], (c) follows from (a) and (b).

In fact, for compact p-adic analytic groups we can say something stronger.

Proposition 2.7 *Let H be a p-adic analytic group, and let*

$$K_n(H) = \bigcap \{\ker \rho \mid \rho \colon H \to \mathrm{GL}_n(\mathbb{C}) \text{ is a representation}\}.$$

Suppose that the Lie algebra of H is perfect (we recall the definition of the Lie algebra below). Then $[H \colon K_n(H)]$ is polynomially bounded.

Proof We need to recall some material on uniform pro-p groups and formal group laws; see [DdSMS99, Chapter 8 and Chapter 13] for details. Clearly there is no harm in passing to an open subgroup of H. We assume, therefore, that H is an appropriate open subgroup of a uniform pro-p group, admitting an analytic isomorphism $\psi \colon (p\mathbb{Z}_p)^d \to H$, where $d = \dim H$, such that the group law with respect to these co-ordinates is given by $\mathbf{x}.\mathbf{y} = \mathbf{F}(\mathbf{x}, \mathbf{y})$, where $\mathbf{F}(\mathbf{x}, \mathbf{y})$ is a d-tuple of power series each with coefficients in $\mathbb{Z}_p$. We have

$$\mathbf{F}(\mathbf{x}, \mathbf{y}) = \mathbf{x} + \mathbf{y} + \mathbf{B}(\mathbf{x}, \mathbf{y}) + O'(3),$$

where $\mathbf{B}(\mathbf{x}, \mathbf{y})$ is a bilinear form on $(p\mathbb{Z}_p)^d$ and $O'(3)$ denotes a power series such that each term has total degree at least three and degree at least one in each of the variables. The commutator of a pair of elements in H is given by

$$[\mathbf{x}, \mathbf{y}] = \mathbf{B}(\mathbf{x}, \mathbf{y}) - \mathbf{B}(\mathbf{y}, \mathbf{x}) + O'(3).$$

The map $(\mathbf{x}, \mathbf{y}) \mapsto \mathbf{B}(\mathbf{x}, \mathbf{y}) - \mathbf{B}(\mathbf{x}, \mathbf{y})$ gives $(p\mathbb{Z}_p)^d$ the structure of a Lie algebra over $\mathbb{Z}_p$: call this Lie algebra $\mathcal{L}$. The Lie algebra of H is then given by $\mathcal{L}(\mathbb{Q}_p) := \mathcal{L} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ (this is equivalent to the usual definition of the Lie algebra of a compact p-adic analytic group; cf. [DdSMS99, Exercise 9.13]).

We have a filtration $H = H_1 \supset H_2 \supset \cdots$ of H by normal subgroups, where $H_n = \psi(p^n\mathbb{Z}_p^d)$. Then $H_{n+1} = H^{p^n}$ (see [DdSMS99, Theorems 3.6 and 8.3.1]), where H^{p^n} denotes the closure of the subgroup generated by the p^n-powers in H. It follows that any index p^n subgroup of H contains H_{n+1}.

Suppose that $\mathcal{L}(\mathbb{Q}_p)$ is perfect. Then there exists $r \in \mathbb{N}$ such that $p^r\mathcal{L} \subset [\mathcal{L}, \mathcal{L}]$. Thus for any $n \in \mathbb{N}$, $p^{2n+r}\mathcal{L} \subset [p^n\mathcal{L}, p^n\mathcal{L}]$. We claim that $H_{2n+r} \leq [H_n, H_n]H_{3n}$ for every $n \in \mathbb{N}$. To see this, observe that any $\mathbf{z} \in (p^{2n+r}\mathbb{Z}_p)^d$ can be written as a sum of Lie commutators $[\mathbf{x}_1, \mathbf{y}_1] + \cdots + [\mathbf{x}_s, \mathbf{y}_s]$ for some s, where the $\mathbf{x}_i, \mathbf{y}_i \in (p^n\mathbb{Z}_p)^d$. Using the formula for group commutators above, we see that the product of group commutators $[\mathbf{x}_1, \mathbf{y}_1] \cdots [\mathbf{x}_s, \mathbf{y}_s]$ is equal to $\mathbf{z} +$ (terms in $(p^{3n}\mathbb{Z}_p)^d$), and the claim follows. The claim implies that $[H_n, H_n] \supset H_{3n}$ if $n \geq r + 2$.

Let ρ be an irreducible representation of H of dimension at most p^n, where $n \geq r+2$. Then ρ is induced from a one-dimensional representation of a subgroup M of index at most p^n (Lemma 2.5). Since $M \supset H_{n+1}$, $[M, M]$ contains H_{3n+3}, so $\ker \rho \supset H_{3n+3}$. The index of H_{3n+3} in H is $p^{d(3n+2)}$, which gives the required bound.

Lemma 2.8 *If Φ_1, Φ_2 are groups with PRG then $\Phi_1 \times \Phi_2$ has PRG.*

Proof It is well known that any irreducible n-dimensional representation ρ of the product $\Phi_1 \times \Phi_2$ is isomorphic to a representation of the form $\rho = \rho_1 \otimes \rho_2$, where ρ_i is an irreducible n_i-dimensional representation of Φ_i for $i = 1, 2$, and $n_1 n_2 = n$. If Φ_1, Φ_2 have PRG, with $r_n(\Phi_i) \leq c_i n^{d_i}$, say, then

$$r_n(\Phi_1 \times \Phi_2) \leq \sum_{n_1 n_2 = n} r_{n_1}(\Phi_1) r_{n_2}(\Phi_2) \leq \sum_{n_1 n_2 = n} c_1 n_1^{d_1} c_2 n_2^{d_2} \leq c_1 c_2 n^{d_1 + d_2 + 1},$$

as required.

Lemma 2.8 implies that in order to prove Theorem 1.2, it suffices to consider simple groups G. Moreover, by changing the field we can further assume that G is absolutely simple. We therefore assume throughout this paper that G is absolutely simple. The same remark applies also to Theorem 1.3, as well as to the other theorems we prove (Theorems 4.2 and 4.3).

3 Infinite Representations

Assume for now that k is a number field. Let $\Gamma = G(\mathcal{O}_S)$ be as in Theorem 1.2, and assume that Γ has the congruence subgroup property. Let $H = \mathrm{Res}^k_{\mathbb{Q}}(G)$, where $\mathrm{Res}^k_{\mathbb{Q}}$ denotes restriction of scalars. Then H is a connected simply connected semisimple algebraic group defined over $\mathbb{Q}$, and we have an embedding $\Gamma \hookrightarrow H(\mathbb{Q}) \hookrightarrow H(\mathbb{C})$. A representation of a subgroup Δ of $H(\mathbb{C})$ is said to be *algebraic* if it can be extended to an algebraic representation of $H(\mathbb{C})$.

Lemma 3.1 *There is a finite index subgroup Δ of Γ such that every irreducible finite-dimensional representation is isomorphic to a representation of the form $\rho = \rho_1 \otimes \rho_2$, where ρ_1 is finite and ρ_2 is algebraic.*

Proof Let $A = A(\Gamma)$ be the proalgebraic completion of Γ: that is, $A(\Gamma)$ is a complex proalgebraic group with an embedding $i\colon \Gamma \hookrightarrow A(\Gamma)$ characterised by the fact that every finite-dimensional complex representation ρ of Γ has a unique extension to an algebraic representation $\widetilde{\rho}$ of $A(\Gamma)$ such that $\widetilde{\rho} \circ i = \rho$ (cf. [LM85], [BLMM02]). Let A^0 be the identity component of A, so that we have a short exact sequence

$$1 \to A^0 \to A \xrightarrow{\pi} \widehat{\Gamma} \to 1.$$

Then A has a profinite subgroup P such that $A^0 P = A$ [BLMM02, Corollary 6]. As Γ satisfies the congruence subgroup property, it has superrigidity: this means that every representation of Γ can be extended on a finite index subgroup to an algebraic representation of $H(\mathbb{C})$ [Rag76, Theorem 7.2]. This implies that $A^0 = H(\mathbb{C})$. In particular, A^0 is a finite-dimensional algebraic group, hence its intersection Z with the profinite group P is finite. Let P_1 be an open subgroup of P with $P_1 \cap Z = 1$, so that $P_1 \ltimes A^0$ has finite index in A. Let C be the centraliser $C_{P_1}(A^0)$. Since $\mathrm{Aut}\, A^0 = \mathrm{Aut}\, H(\mathbb{C})$ is a finite-dimensional algebraic group, C is open in P_1 and so $D = C \times A^0$ is a finite index open subgroup of A. It is therefore equal to $A(\Delta)$ for some finite index subgroup Δ of Γ (in fact, $\Delta = i^{-1}(D \cap i(\Gamma))$). As $A(\Delta) = C \times A^0 = \widehat{\Delta} \times A^0$, every irreducible representation of Δ is a tensor product of a finite representation and an algebraic representation, as claimed.

We postpone the treatment of the finite representations to the next section. Here we show that the number of algebraic representations is polynomially bounded.

Proposition 3.2 *Let H be a semisimple linear algebraic group over $\mathbb{C}$. Then the number of isomorphism classes of irreducible n-dimensional algebraic representations of H is polynomially bounded.*

Proof Below we use standard results on the structure theory and representation theory of H; these may be found in [Hum72]. Fix a maximal torus T of H, let Λ be the group of characters of T and let $R \subset \Lambda$ be the set of roots of H with respect to T. Let $(-,-)$ be the canonical Weyl-group-invariant bilinear form on $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$. Choose a decomposition $R = R^+ \cup R^-$ of R into sets of positive and negative roots. We write $\Lambda^+ = \{\lambda \in \Lambda \mid (\lambda, \alpha) \geq 0 \; \forall \alpha \in R^+\}$.

We recall briefly the classification of finite-dimensional irreducible algebraic representations of H (that is, of irreducible rational H-modules). A nonzero rational H-module M can be written as a direct sum of nonzero T-modules M_λ for certain $\lambda \in \Lambda$; the λ that appear are called the *weights* of M. If M is irreducible then there is a unique weight λ_{max}, which belongs to Λ^+, such that λ_{max} is the maximum weight with respect to a natural ordering on the set of weights. For any $\lambda \in \Lambda^+$ there is an irreducible rational H-module $V(\lambda)$ with highest weight λ, and every irreducible M is isomorphic to some $V(\lambda)$.

By [Hum72, 24.3 Corollary], we have

$$\dim V(\lambda) = \frac{\prod_{\alpha \in R^+} (\lambda + \delta, \alpha)}{\prod_{\alpha \in R^+} (\delta, \alpha)},$$

where δ is half of the sum of the positive roots; moreover, the denominator is independent of λ, and each $|(\lambda + \delta, \alpha)|$ is bounded below by $(\alpha, \alpha)/2$.

Since H is semisimple, the positive roots span $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$, so we can define a norm $\| \cdot \|$ on $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$ by $\|\lambda\| = \max_{\alpha \in R^+} |(\lambda, \alpha)|$. For $\|\lambda\|$ sufficiently large we have $\max\{|(\lambda + \delta, \alpha)| \mid \alpha \in R^+\} \geq \frac{1}{2}\|\lambda\|$. The number of weights in the $\| \cdot \|$-ball $B(0, n)$ in $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$ is polynomially bounded, so our result follows.

We turn now to the case of positive characteristic. Recall that Γ is always a lattice (that is, a discrete subgroup of finite covolume) in $H = \prod_{v \in S} G(k_v)$ [Mar91, Chapter 1, Section 3.2]. If $\operatorname{rank}(H) := \sum_{v \in S} \operatorname{rank}_{k_v} G(k_v)$ is one then Γ does not have the CSP [Lub91, Proposition B and Proposition D]. (Indeed, in this case Γ has a finite index subgroup with nonabelian free quotient, so $r_n(\Gamma) = \infty$ for infinitely many n.) On the other hand, if $\operatorname{rank}(H) \geq 2$ then by Margulis [Mar91, Chapter VIII, (3.8) Theorem] (see also [Ven88, Theorem 4.10]), Γ has superrigidity and has **no** infinite complex representations.

Thus in all cases we are reduced to the study of $\widehat{r}_n(\Gamma)$, the growth function of the finite representations. This will be the topic of the next section.

4 Finite Congruence Representations

Let k, G, Γ, etc., be as in the Introduction; we assume now that G is absolutely simple. For $v \in V_f$, let $\mathfrak{m}_v$ be the maximal ideal of $\mathcal{O}_v$. We write $\mathbb{F}_v = \mathcal{O}_v / \mathfrak{m}_v$ for the residue field, $q_v = |\mathbb{F}_v|$, $p_v = \operatorname{char} \mathbb{F}_v$ and $e_v = \log_{p_v} q_v$. In general we denote the field with q elements by $\mathbb{F}_q$ (so that $\mathbb{F}_v = \mathbb{F}_{q_v}$). We write $N_n^{(v)}$ for $G(\mathcal{O}_v) \cap \ker \left(\mathrm{GL}_N(\mathcal{O}_v) \to \mathrm{GL}_N(\mathcal{O}_v / \mathfrak{m}_v^n)\right)$, the nth *principal congruence subgroup* of $G(\mathcal{O}_v)$. Define $G(\mathbb{F}_v)$ to be the image of $G(\mathcal{O}_v)$ in $\mathrm{GL}_N(\mathbb{F}_v)$. Note that $|G(\mathbb{F}_v)| \leq q_v^{N^2}$.

Assumption 4.1 We will always make the following assumption: if $\operatorname{char} k = 2$ then G is not of type A_1 or of type C_m for any m. This ensures that the Lie algebra of G is perfect.

If Γ has the CSP then $C := \ker \left(\widehat{G(\mathcal{O}_S)} \xrightarrow{\pi} G(\widehat{\mathcal{O}}_S)\right)$ is finite. Replacing Γ by a finite index subgroup Γ_0 such that $C \cap \overline{\Gamma_0}$ is trivial, we can assume that C is trivial. By Corollary 2.3, the finite representations of Γ_0 have the same growth as the representations of the congruence completion $G(\widehat{\mathcal{O}}_S)$. The main goal of this section is to show that $r_n(G(\widehat{\mathcal{O}}_S))$ grows polynomially. We do not need to assume that Γ has the CSP to prove this: instead we prove that for any arithmetic group, the number of *congruence representations* is polynomially bounded (where a congruence representation is a representation the kernel of which is a congruence subgroup), since these are precisely the representations that extend to representations of $G(\widehat{\mathcal{O}}_S)$.

Theorem 4.2 *Let k, $\mathcal{O}$, S and G be as above. Then $r_n(G(\widehat{\mathcal{O}}_S))$ is polynomially bounded.*

We recall some properties of the graded Lie algebra associated to the filtration $N_1^{(v)} \geq N_2^{(v)} \geq \ldots$ of $N_1^{(v)}$ (compare [LS03, Section 3.5]). Setting $L_n^{(v)} = N_n^{(v)}/N_{n+1}^{(v)}$, we obtain a graded Lie algebra $L^{(v)} = \sum_{n=1}^{\infty} L_n^{(v)}$ over $\mathbb{F}_v$, where addition is given by

$$xN_{n+1}^{(v)} + yN_{n+1}^{(v)} = xyN_{n+1}^{(v)}$$

and the Lie bracket by

$$[xN_{m+1}^{(v)}, yN_{n+1}^{(v)}] = [x,y]N_{n+m+1}^{(v)}.$$

Each quotient $N_1^{(v)}/N_n^{(v)}$ is a finite p_v-group, and $N_1^{(v)}$ is the inverse limit of the $N_1^{(v)}/N_n^{(v)}$.

Let H be an open subgroup of $N_1^{(v)}$. Setting $L_n^{(v)}(H) = (H \cap N_n^{(v)})N_{n+1}^{(v)}/N_{n+1}^{(v)}$, we obtain a graded $\mathbb{F}_{p_v}$-subalgebra $L^{(v)}(H) = \sum_{n=1}^{\infty} L_n^{(v)}(H)$ of $L^{(v)}$ (this is not an $\mathbb{F}_v$-subalgebra in general). We have

$$[N_1^{(v)} \colon H] = [L^{(v)} \colon L^{(v)}(H)] \tag{1}$$

(compare [LS94, Lemma 2.13]).

Let $\mathcal{P}_1$ be the subset of V_f consisting of all valuations v such that:
(a) $G(\mathbb{F}_v)$ is perfect and is a central extension of a finite simple group of Lie type $H(q_v)$, where H is of the Lie type of G (either twisted or untwisted);
(b) for every $n \in \mathbb{N}$, $|N_n^{(v)}/N_{n+1}^{(v)}| = q_v^{\dim G}$;
(c) for every $m, n \in \mathbb{N}$, $[N_m^{(v)}, N_n^{(v)}] = N_{m+n}^{(v)}$;
(d) $G(\mathcal{O}_v)$ is perfect.

It follows from the discussion before the proof of Theorem 2.1 of [LL] that conditions (a), (b) and (c) hold for almost all $v \in V_f$. Our standing hypothesis Assumption 4.1 implies that the Lie algebra of G is perfect, which implies that $[G(\mathcal{O}_v)/N_2^{(v)}, N_1^{(v)}/N_2^{(v)}] = N_1^{(v)}/N_2^{(v)}$ for almost all $v \in V_f$. This together with conditions (a) and (c) gives condition (d). Therefore $\mathcal{P}_2 := V_f - \mathcal{P}_1$ is finite. Note that (c) implies that $[L_m^{(v)}, L_n^{(v)}] = L_{m+n}^{(v)}$ for every $m, n \in \mathbb{N}$.

To prove Theorem 4.2 we need to prove, in particular, that $r_n(G(\mathcal{O}_v)) \leq c_1 n^{c_2}$ for two constants c_1, c_2 independent of v. In fact, we will prove a stronger result which is of independent interest and will be needed later in Section 6 for the converse theorem.

Theorem 4.3 *There exists $c = c(G, k)$ such that for every $v \in V_f$ and every $n \in \mathbb{N}$, $[G(\mathcal{O}_v) \colon K_n(G(\mathcal{O}_v))] \leq cn^c$, where for a profinite group H, $K_n(H)$ is defined as in Proposition 2.7, namely*

$$K_n(H) = \bigcap\{\ker \rho \mid \rho \colon H \to \mathrm{GL}_n(\mathbb{C}) \textit{ is a representation}\}.$$

Here are two immediate corollaries. Note that the second applies to all representations, not just irreducible ones.

Corollary 4.4 $r_n(G(\mathcal{O}_v)) \leq cn^c$ *for every* $v \in V_f$, $n \in \mathbb{N}$.

Corollary 4.5 $|\rho(G(\mathcal{O}_v))| \leq cn^c$ *for every* $v \in V_f$, $n \in \mathbb{N}$, $\rho \in \mathrm{Rep}_n(G(\mathcal{O}_v))$.

To prove Theorem 4.3 we need:

Proposition 4.6 *There exists $\delta > 0$ such that for every $v \in \mathcal{P}_1$, every nontrivial irreducible representation of $G(\mathcal{O}_v)$ is of dimension at least q_v^δ.*

Proposition 4.6, which we will prove below, is needed in the proof of Theorem 4.3, as well as for proving Theorem 4.2.

Lemma 4.7 *(a) For $n \in \mathbb{N}$, define $f(n)$ to be the number of tuples $(n_1, \dots, n_t)$ of integers such that $n = n_1 \cdots n_t$ and each $n_i > 1$. Then there exists $\mu > 0$ such that $f(n) \leq n^\mu$ for every $n \in \mathbb{N}$.*
(b) There exists $d > 0$, depending only on k, such that the number of $v \in V_f$ with $q_v \leq n$ is bounded by dn, and hence also by n^b for some $b > 0$.

Proof (a) By a result of Kalmar (see [Erd41, Theorem (1)]), we have

$$\sum_{m=1}^{n} f(m) = Dn^\beta(1 + o(1)),$$

where D is constant and β is the unique positive solution of $\zeta(\beta) = 2$ (ζ being the Riemann zeta function). The result follows.
(b) This is a consequence of the Prime Number Theorem (see [Ros02, Theorem 5.12] for the function field case).

Let us now show how Corollary 4.4, Proposition 4.6 and Lemma 4.7 imply Theorem 4.2. We write $G(\widehat{\mathcal{O}}_S)$ as $A \times B$, where $A = \prod_{v \in \mathcal{P}_2 - S} G(\mathcal{O}_v)$ and $B = \prod_{v \in \mathcal{P}_1 - S} G(\mathcal{O}_v)$. Now A is a finite product of groups, each of which has PRG (Corollary 4.4), so A has PRG by Lemma 2.8. The same lemma implies that $G(\widehat{\mathcal{O}}_S)$ has PRG, once we have shown that B has PRG.

To prove this, let $\rho \in \mathrm{Irr}_n(B)$ be nontrivial. Then for some t and some $v_1, \ldots, v_t \in \mathcal{P}_1 - S$, we have nontrivial $\rho_i \in \mathrm{Irr}_{n_i}(G(\mathcal{O}_{v_i}))$ such that $\rho \cong \rho_1 \otimes \cdots \otimes \rho_t$, where the n_i are positive integers such that $n = n_1 \cdots n_t$. Each n_i is greater than 1 by condition (d) in the definition of $\mathcal{P}_1$. The number of possibilities for $(n_1, \ldots, n_t)$ is bounded by n^μ, by Lemma 4.7 (a). Given such a t-tuple $(n_1, \ldots, n_t)$, then for any fixed i between 1 and t, the number of valuations $v_i \in \mathcal{P}_1$ that are possible — that is, such that $G(\mathcal{O}_{v_i})$ admits a nontrivial n_i-dimensional representation — is bounded by $n_i^{b/\delta}$; this follows from Proposition 4.6 and Lemma 4.7 (b). Thus the number of choices for $(v_1, \ldots, v_t)$ is bounded by $\prod_{i=1}^t n_i^{b/\delta} = n^{b/\delta}$. Now given $(n_1, \ldots, n_t)$ and $(v_1, \ldots, v_t)$, for every $i = 1, \ldots, t$, $G(\mathcal{O}_{v_i})$ has at most cn_i^c irreducible representations of dimension n_i (Corollary 4.4). Hence B has at most $n^\mu n^{b/\delta} c^{\log_2 n} n^c$ irreducible n-dimensional representations. Thus B has PRG and Theorem 4.2 is proved (modulo Theorem 4.3 and Proposition 4.6).

We turn now to the proofs of Theorem 4.3 and Proposition 4.6. First we need a result that deals with the finitely many bad primes.

Lemma 4.8 *For every $v \in V_f$, there exists $c > 0$ such that for every $n \in \mathbb{N}$, we have*

$$[G(\mathcal{O}_v) \colon K_n(G(\mathcal{O}_v))] \leq cn^c. \tag{2}$$

Proof As in the proof of Proposition 2.7, we are free to pass to an open subgroup of $G(\mathcal{O}_v)$. Since $G(\mathcal{O}_v)$ is an $\mathcal{O}_v$-analytic group, it has an open subgroup H which is $\mathcal{O}_v$-standard [Ser92, Part II, Chapter IV, Section 8, Theorem]. It can be shown that the Lie algebra $\mathcal{L}(k_v)$ over k_v associated to H (see [DdSMS99, Section 13.3]) is isomorphic to the Lie algebra of the algebraic group $G(k_v)$, which is perfect by Assumption 4.1. If $\mathrm{char}\, k = 0$ then H can be regarded as a $\mathbb{Z}_{p_v}$-standard group; the Lie algebra $\mathcal{L}(\mathbb{Q}_{p_v})$ is just $\mathcal{L}(k_v)$ regarded as a Lie algebra over $\mathbb{Q}_{p_v}$, so it is also perfect. Similarly, if $\mathrm{char}\, k = p > 0$ then H is an $\mathbb{F}_p[[t]]$-standard group with perfect Lie algebra. The result now follows from Proposition 2.7 in characteristic zero, and from the proof of Theorem 6 of [JZ03] in characteristic p.

We need more for the proof of Theorem 4.3: we need to prove the existence of a c in Eqn. (2) that is independent of v, and for this Proposition 4.6 is also required.

Interestingly enough, the proofs of both Theorem 4.3 and Proposition 4.6 need the following lemma.

Lemma 4.9 *Let p be a prime and let $q = p^e$, where $e \in \mathbb{N}$. Let V, W, X be finite-dimensional vector spaces over $\mathbb{F}_q$, and let $T\colon V \times W \to X$ be an $\mathbb{F}_q$-bilinear map such that $T(V \times W)$ spans X over $\mathbb{F}_q$. Suppose that A, B are $\mathbb{F}_p$-subspaces of V, W respectively such that*

$$[V\colon A][W\colon B] < q. \tag{3}$$

Then $T(A \times B)$ spans X over $\mathbb{F}_p$.

Proof First we prove this in the special case that $V = W = X = \mathbb{F}_q$ and T is multiplication. Let $f\colon \mathbb{F}_q \to \mathbb{F}_p$ be any nonzero $\mathbb{F}_p$-linear function. Define an $\mathbb{F}_p$-bilinear form $Q_f\colon \mathbb{F}_q \times \mathbb{F}_q \to \mathbb{F}_p$ by $Q_f(x, y) = f(xy)$. Then Q_f is nondegenerate: for there exists $z \in \mathbb{F}_q$ such that $f(z) \neq 0$, and for any $0 \neq x \in \mathbb{F}_q$ we have $Q_f(x, x^{-1}z) = f(z) \neq 0$. This implies that the orthogonal complement $A^\perp = \{x \in \mathbb{F}_q \,|\, Q_f(x, a) = 0 \text{ for all } a \in A\}$ has $\mathbb{F}_p$-dimension equal to the $\mathbb{F}_p$-codimension of A. By Eqn. (3), the sum of the $\mathbb{F}_p$-dimensions of A and B is greater than e, so $B \not\subset A^\perp$, whence f does not vanish on $T(A \times B)$. But f is arbitrary, so the $\mathbb{F}_p$-span of $T(A \times B)$ must be the whole of $\mathbb{F}_q$.

Now consider the general case. Let Y be the $\mathbb{F}_p$-span of $T(A \times B)$. Eqn. (3) implies that A, B contain $\mathbb{F}_q$-bases for V, W respectively, so Y spans X over $\mathbb{F}_q$. To complete the proof, we therefore need only show that Y is invariant under multiplication by $\mathbb{F}_q$. So let $a \in A, b \in B, w \in \mathbb{F}_q$. We show that $wT(a, b) \in Y$.

Set $A' = \{x \in \mathbb{F}_q \,|\, xa \in A\}$, $B' = \{y \in \mathbb{F}_q \,|\, yb \in B\}$, regarded as $\mathbb{F}_p$-subspaces of $\mathbb{F}_q$. Then $\mathbb{F}_q/A' \cong \mathbb{F}_q.a/(\mathbb{F}_q.a \cap A) \cong (A + \mathbb{F}_q.a)/A \subset V/A$, and similarly $\mathbb{F}_q/B'$ is isomorphic to an $\mathbb{F}_p$-subspace of W/B, so applying Eqn. (3) yields $[\mathbb{F}_q\colon A'][\mathbb{F}_q\colon B'] < q$. By the special case above, there exist $x_1, \ldots, x_m \in A'$ and $y_1, \ldots, y_m \in B'$ for some m such that $w = \sum_{i=1}^m x_i y_i$. We have

$$wT(a, b) = \left(\sum_{i=1}^m x_i y_i\right) T(a, b) = \sum_{i=1}^m T(x_i a, y_i b) \in Y,$$

as required.

We deduce:

Lemma 4.10 *Let $v \in \mathcal{P}_1$ and suppose that $H \leq N_1^{(v)}$ has index smaller than $q_v^{1/2}$. Then $[H, H] = N_2^{(v)}$. In particular, $H \supset N_2^{(v)}$, $H \trianglelefteq N_1^{(v)}$ and $N_1^{(v)}/H$ is elementary abelian.*

Proof We have $[N_1^{(v)} \colon H] = [L^{(v)} \colon L^{(v)}(H)]$, where $L^{(v)}, L^{(v)}(H)$ are the graded Lie algebras defined earlier, so $[L^{(v)} \colon L^{(v)}(H)] < q_v^{1/2}$; in particular, $[L_i^{(v)} \colon L_i^{(v)}(H)] < q_v^{1/2}$ for every $i \in \mathbb{N}$. Applying Lemma 4.9 to $V = L_1^{(v)}$, $W = L_m^{(v)}$, $A = L_1^{(v)}(H), B = L_m^{(v)}(H)$ and with T the Lie bracket, we prove by induction that $L_{m+1}^{(v)}(H) = L_{m+1}^{(v)}$ for every $m \in \mathbb{N}$. Since $[H, H]$ is closed, we deduce that $[H, H] = N_2^{(v)}$. The other assertions follow immediately.

Lemma 4.11 *Let Φ be a perfect finite central extension of a finite simple group of Lie type $H(p^r)$, where $r \in \mathbb{N}$ and p is prime. Then there exists $\delta_1 > 0$, depending neither on p, r nor on the Lie type, such that every nontrivial complex projective representation of Φ has dimension at least $p^{r\delta_1}$. In particular, any proper subgroup Φ' of Φ has index at least $p^{r\delta_1}$.*

Proof If Φ' is a proper subgroup of Φ then the projective representation arising from the permutation representation of Φ on the coset space Φ/Φ' is nontrivial because Φ is perfect, so the second assertion follows from the first. To prove the first assertion, let $\rho \colon \Phi \to \mathrm{PGL}_n(\mathbb{C})$ be a nontrivial projective representation. Then $\rho(\Phi) \subset \mathrm{PGL}_n(K)$ for some number field K, and reducing modulo a suitable prime of K gives a nontrivial projective representation $\rho' \colon \Phi \to \mathrm{PGL}_n(F)$, where F is a field of characteristic $l \neq p$ (compare [Lan93, Chapter XVIII, Exercise 27]). Since $\Phi/\ker \rho'$ is also a perfect central extension of $H(p^r)$, we can assume that ρ' is faithful. The existence of a δ_1 with the required properties then follows from [KL90, Corollary 5.3.3 and Theorem 5.3.9].

We are now ready for:

Proof of Proposition 4.6 We can assume that $\delta < 1/2$. Let $v \in \mathcal{P}_1$ and let (V, ρ) be a nontrivial n-dimensional irreducible representation of $G(\mathcal{O}_v)$. Write $\rho|_{N_1^{(v)}}$ as a direct sum of irreducible representations $W_1 \oplus \cdots \oplus W_m$. Without loss of generality, we assume that $W_1 \oplus \cdots \oplus W_r$ is the isotypic component of W_1, that is, that $W_1, \ldots, W_r$ are precisely the summands that are isomorphic to W_1. Let H be the stabiliser of $W := W_1 \oplus \cdots \oplus W_r$ in $G(\mathcal{O}_v)$, and let σ be the representation of H on W. By Clifford's Theorem, $\rho =$

$\mathrm{Ind}_H^{G(\mathcal{O}_v)}(\sigma)$. Now, if W is a proper subspace of V then H is a proper subgroup of $G(\mathcal{O}_v)$ containing $N_1^{(v)}$; by Lemma 4.11, $[G(\mathcal{O}_v)\colon H] = [G(\mathbb{F}_v)\colon H/N_1^{(v)}]$ is at least $q_v^{\delta_1}$, and we have the required bound for $\dim V$.

Assume, therefore, that $W = V$. Then V is a sum of m isomorphic $N_1^{(v)}$-simple modules, each of dimension s, say. If $s \geq q_v^{1/2}$ then we are done. If not then $s < q_v^{1/2}$, and W_1, being an irreducible representation of the pro-p_v group $N_1^{(v)}$, is induced from a one-dimensional representation of a subgroup M of $N_1^{(v)}$, of index $s < q_v^{1/2}$ (Lemma 2.5). By Lemma 4.10, M contains $N_2^{(v)}$ and $[M, M] = N_2^{(v)}$, which implies that the simple $N_1^{(v)}$-module W_1 is actually a module for the abelian group $N_1^{(v)}/N_2^{(v)}$, and hence is one-dimensional. It follows that $\rho(N_1^{(v)})$ is central in $\rho(G(\mathcal{O}_v))$. Hence ρ gives rise to an n-dimensional projective representation of the quasisimple group $G(\mathbb{F}_v)$, nontrivial because ρ is nontrivial and $G(\mathcal{O}_v)$ is perfect. Lemma 4.11 implies that $n \geq q_v^{\delta_1}$, so the proof of Proposition 4.6 is complete.

Proof of Theorem 4.3 For $v \in \mathcal{P}_1$, we give a precise estimate for $[G(\mathcal{O}_v)\colon K_n(G(\mathcal{O}_v))]$. We claim that for every nontrivial n-dimensional irreducible representation ρ of $G(\mathcal{O}_v)$, we have $\ker\rho \supset N_{4r+6}^{(v)}$, where $r = \left[\frac{\log_{p_v} n}{e_v}\right]$. This will finish the proof of Theorem 4.3, since $[G(\mathcal{O}_v)\colon N_{4r+6}^{(v)}] = |G(\mathbb{F}_v)|[N_1^{(v)}\colon N_{4r+6}^{(v)}] \leq q_v^{N^2} q_v^{(4r+5)\dim G} \leq q_v^{N^2} p_v^{\left(4e_v \frac{\log_{p_v} n}{e_v} + 5e_v\right)\dim G} = n^{4\dim G} q_v^{5\dim G + N^2}$. But since ρ is nontrivial, by Proposition 4.6 we have $q_v \leq n^{1/\delta}$, hence the index of $K_n(G(\mathcal{O}_v))$ is bounded by $n^{(4+5/\delta)\dim G + N^2/\delta}$, as required.

To prove that indeed $\ker\rho \supset N_{4r+6}^{(v)}$, we first restrict ρ to $N_1^{(v)}$ and decompose it into $N_1^{(v)}$-irreducible representations, each of dimension no greater than n. Fix one of these representations and call it σ. As $N_1^{(v)}$ is a pro-p group, σ is induced from a one-dimensional representation of a subgroup H of index at most n (Lemma 2.5). Therefore it suffices to prove:

Proposition 4.12 *Let $v \in \mathcal{P}_1$ and let $H \leq N_1^{(v)}$ have index at most n. Then $H \supset N_{2r+3}^{(v)}$, where $r = \left[\frac{\log_{p_v} n}{e_v}\right]$, and $[H, H] \supset N_{4r+6}^{(v)}$.*

Note that Proposition 4.12 is a stronger version of the standard "index versus level" formula; the usual argument proves only that $H \supset N_{\log_{p_v} n+1}^{(v)}$ [LS03, Proposition 4.3.1]. (Of course, if $\mathrm{char}\, k = 0$ then the usual argument suffices.)

Proof of Proposition 4.12 We have $[N_1^{(v)}\colon H] = [L^{(v)}\colon L^{(v)}(H)]$. Now let $s \geq 2r + 3$. Consider the $r + 1$ pairs of distinct integers $(i, s - i)$ with

$1 \leq i \leq r+1$. By our hypothesis on the index of H, there must exist at least one such pair $(i, s-i)$ such that $[L_i^{(v)} \colon L_i^{(v)}(H)][L_{s-i}^{(v)} \colon L_{s-i}^{(v)}(H)] < q_v$. By Lemma 4.9 we have $[L_i^{(v)}(H), L_{s-i}^{(v)}(H)] = [L_i^{(v)}, L_{s-i}^{(v)}] = L_s^{(v)}$. As H is closed, we deduce that $H \supset N_{2r+3}^{(v)}$. It follows from condition (c) in the definition of $\mathcal{P}_1$ that $[H, H] \supset [N_{2r+3}^{(v)}, N_{2r+3}^{(v)}] = N_{4r+6}^{(v)}$.

This completes the proof of Theorem 4.3 for $v \in \mathcal{P}_1$. For each of the finitely many valuations $v \in \mathcal{P}_2$, Lemma 4.8 gives the result we need, so we have proved Theorem 4.3.

Theorem 1.2 is now proved. Indeed, let $\Gamma = G(\mathcal{O}_S)$ be as in Theorem 1.2 and suppose that Γ has the congruence subgroup property. By Lemma 2.8 and the arguments in Section 3, passing to a finite index subgroup of Γ if necessary, it suffices to show that $\widehat{r}_n(\Gamma)$ is polynomially bounded and that if $\operatorname{char} k = 0$ then the number of algebraic representations of Γ is polynomially bounded. This follows from Theorem 4.2 and Proposition 3.2.

5 Image Growth of Congruence Representations

While proving Theorem 1.2 we showed that the local group $G(\mathcal{O}_v)$ has a normal subgroup $K_n(G(\mathcal{O}_v))$ of polynomial index which is in the kernel of every finite n-dimensional representation. This is not true for the global group $G(\widehat{\mathcal{O}_S})$: a weaker property holds, namely that the image size of every finite **irreducible** representation of dimension n is polynomial in n. For future use (Section 6), we prove a bound for the image size of general finite representations.

Proposition 5.1 *There exists $\gamma \in (0,1)$ such that if n is large enough then for every $\rho \in \operatorname{Rep}_n(G(\widehat{\mathcal{O}_S}))$, we have $|\rho(G(\widehat{\mathcal{O}_S}))| \leq e^{n^\gamma}$.*

We need two lemmas. In the first lemma, the second inequality is obvious, while the first is proved using induction on d and the Binomial Theorem (we leave the details to the reader).

Lemma 5.2 *Let $d, a \in \mathbb{N}$. Then $\frac{1}{a+1} d^{a+1} \leq \sum_{i=1}^{d} i^a \leq d^{a+1}$.*

Let $t \in \mathbb{N}$, let $H_1, \ldots, H_t$ be profinite groups and set $H = H_1 \times \cdots \times H_t$. Given $\rho \in \mathrm{Rep}_n(H)$, let $n_i(\rho)$ denote the maximal dimension of an irreducible component of the restriction of ρ to H_i.

Lemma 5.3 $\sum_{n_i(\rho)>1} n_i(\rho) \leq n$.

Proof We use induction on n. First we suppose that ρ is irreducible. We can write $\rho = \rho_1 \otimes \cdots \otimes \rho_t$, where each $\rho_i \in \mathrm{Rep}_{n_i}(H_i)$ and $n_1 \cdots n_t = n$. Clearly $\rho|_{H_i}$ is a direct sum of copies of ρ_i, so we have $n_i(\rho) = n_i$. Then $\sum_{n_i(\rho)>1} n_i(\rho) = \sum_{n_i>1} n_i \leq n_1 \cdots n_t = n$.

If ρ is reducible, say $\rho = \rho_1 \oplus \rho_2$, then for each i we have $n_i(\rho) = \max\{n_i(\rho_1), n_i(\rho_2)\}$. Applying the induction hypothesis we have

$$\sum_{n_i(\rho)>1} n_i(\rho) \leq \sum_{n_i(\rho_1)>1} n_i(\rho_1) + \sum_{n_i(\rho_2)>1} n_i(\rho_2) \leq \dim \rho_1 + \dim \rho_2 = n,$$

as required.

Proof of Proposition 5.1 Let $\rho \in \mathrm{Rep}_n(G(\widehat{\mathcal{O}_S}))$. We can regard ρ as a representation of $G(\mathcal{O}_{v_1}) \times \cdots \times G(\mathcal{O}_{v_t})$ for some $t \in \mathbb{N}$ and some $v_1, \ldots, v_t \in V_f - S$, such that each restriction $\rho|_{G(\mathcal{O}_{v_i})}$ is nontrivial. Since the set of bad primes $\mathcal{P}_2$ is finite, we can assume (using Theorem 4.3) that each v_i belongs to $\mathcal{P}_1$; compare the beginning of the proof of Theorem 4.2. This implies that $n_1(\rho), \ldots, n_t(\rho) > 1$. We start by finding an upper bound for t in terms of n.

For any $m \in \mathbb{N}$ with $m > 1$, Lemma 4.7 (b) and Proposition 4.6 imply that the number of $v \in \mathcal{P}_1$ such that $G(\mathcal{O}_v)$ admits an irreducible representation of dimension m is at most m^a, for some constant $a \in \mathbb{N}$. In particular, at most m^a of the $n_i(\rho)$ can take the value m. We therefore have

$$n_1(\rho) + \cdots + n_t(\rho) \geq 2^a.2 + 3^a.3 + \cdots + d^a.d, \tag{4}$$

for any $d \in \mathbb{N}$ such that $2^a + 3^a + \cdots + d^a \leq t$. Applying Lemma 5.2 and Lemma 5.3 to the RHS and LHS respectively of Eqn. (4) yields $\frac{1}{a+2} d^{a+2} \leq n$. By Lemma 5.2, we can take $d = [t^{1/(a+1)}]$. Setting $\gamma_0 = \frac{a+1}{a+2}$ and choosing suitable $b > 0$, we therefore have

$$t \leq bn^{\gamma_0}. \tag{5}$$

Consider the function $f(x_1, \ldots, x_t) = x_1 \cdots x_t$ defined on the bounded convex domain $D = \{(x_1, \ldots x_t) \in \mathbb{R}^t \,|\, x_1, \ldots, x_t \geq 0, \sum_{i=1}^t x_i \leq n\}$. Elementary calculus shows that the maximum value of f on D is $(n/t)^t$. Now consider the function $g(y) = (n/y)^y$ on $[1,\alpha]$. By elementary calculus, if $\log_e n - \log_e \alpha \geq 1$ then the maximum value of $g(y)$ is $(n/\alpha)^\alpha$.

It follows that for large enough n and for any $\gamma \in (\gamma_0, 1)$, we have

$$\begin{aligned}
|\rho(G(\widehat{\mathcal{O}_S}))| &\leq c^t(n_1(\rho)\cdots n_t(\rho))^c \text{ by Theorem 4.3} \\
&\leq c^t\left(\frac{n}{t}\right)^{tc} \text{ by the bound for } f(x_1,\ldots,x_t) \\
&\leq c^{bn^{\gamma_0}}\left(\frac{n}{bn^{\gamma_0}}\right)^{cbn^{\gamma_0}} \text{ by Eqn. (5) and the bound for } g(y) \\
&= (b^{-bc}c^b)^{n^{\gamma_0}} n^{(1-\gamma_0)cbn^{\gamma_0}} \\
&\leq e^{n^\gamma},
\end{aligned}$$

as required.

To finish the section we prove another "polynomial image growth" result for local groups, this time for representations over a field of positive characteristic. Only case (i) of the following proposition will be needed in the sequel.

Proposition 5.4 *Let F be a field of characteristic $l \neq 0$, let $v \in V_f$ and let $\rho\colon G(\mathcal{O}_v) \to \mathrm{GL}_n(F)$ be a representation. Set $p = p_v$. Assume that at least one of the following holds:*
(i) $l \neq p$
(ii) $\mathrm{char}\, k = 0$.
Then $|\rho(G(\mathcal{O}_v))| \leq cn^c$ for some constant $c > 0$, depending only on G, k and v.

Proof By assumption, ρ is continuous and has finite image. Assume that $l \neq p$, and let $\sigma = \rho|_{N_1^{(v)}}$. Let $b = [G(\mathcal{O}_v)\colon N_1^{(v)}]$. Since $\sigma(N_1^{(v)})$ is a finite p-group, σ can be lifted to a complex representation $\widetilde{\sigma}$ of $N_1^{(v)}$ (compare [Lan93, Chapter XVIII, Exercise 27]). Inducing $\widetilde{\sigma}$ gives a complex representation $\widetilde{\rho}$ of $G(\mathcal{O}_v)$, with $\ker\widetilde{\rho} \supset K_{bn}(G(\mathcal{O}_v))$. We have $\ker\rho \supset \ker\sigma = \ker\widetilde{\sigma} \supset K_{bn}(G(\mathcal{O}_v)) \cap N_1^{(v)}$. By Theorem 4.3, $K_{bn}(G(\mathcal{O}_v)) \cap N_1^{(v)}$ has polynomial index in $G(\mathcal{O}_v)$, so $|\rho(G(\mathcal{O}_v))|$ is polynomially bounded. This proves (i).

Assume now that $l = p$ and $\mathrm{char}\, k = 0$. Then $N_1^{(v)}$ is a p-adic analytic pro-p group, so $N_1^{(v)}$ is boundedly generated: that is, there exist $x_1,\ldots,x_d \in N_1^{(v)}$ such that every $g \in N_1^{(v)}$ can be written as $g = x_1^{\alpha_1}\cdots x_d^{\alpha_d}$ for some

$\alpha_1, \dots, \alpha_d \in \mathbb{Z}_p$ [DdSMS99, Theorem 3.17]. Now every element of $\mathrm{GL}_n(F)$ of p-power order must be of order at most pn. (Indeed, if $p^m \geq n$ and $y^{p^m} = 1$ then $(y-1)^{p^m} = 0$, so $y - 1$ is a nilpotent element in $M_{n \times n}(F)$ and $(y-1)^n = 0$. This implies that $y^{pp^a} - 1 = (y-1)^{pp^a} = 0$ where $a = [\log_p n]$, so y has order at most pn.) This implies now that $|\rho(N_1^{(v)})| \leq (pn)^d$, so $|\rho(G(\mathcal{O}_v))|$ is polynomially bounded.

6 Arithmetic Groups with Polynomial Representation Growth

In this section we analyse groups $\Gamma = G(\mathcal{O}_S)$ with polynomial representation growth. The goal is to prove Theorem 1.3.

Recall that the profinite and congruence topologies on $G(\mathcal{O}_S)$ can be extended to topologies on $G(k)$; these are called the arithmetic and congruence topologies respectively. The congruence subgroup problem is to study the kernel

$$1 \to C \to \widehat{G(k)} \to \widetilde{G(k)} \to 1,$$

where $\widehat{G(k)}$ (respectively $\widetilde{G(k)}$) is the completion of $G(k)$ with respect to the arithmetic (respectively congruence) topology (see [Ser70], [Rag76]).

Let $C_0 = [C, \widehat{G(k)}]$. By the solution to the metaplectic problem (cf. [PR96]), C_0 is open in C. Note that $G(\mathcal{O}_S)$ has the congruence subgroup property if and only if $C_0 = 1$, so to prove Theorem 1.3, we need to show that C_0 is trivial.

Proposition 6.1 *Suppose that C_0 has an open normal subgroup M with $F := C_0/M$ a nonabelian finite simple group. Then for some $\epsilon > 0$,*

$$R_n(G(\widehat{\mathcal{O}_S})) > n^{\epsilon \log \log n}$$

for infinitely many n. In particular, $\Gamma = G(\mathcal{O}_S)$ does not have PRG.

Proof Let $N = \bigcap_{g \in G(k)} M^g$. It was shown in [Lub95, (2.4)] that N has infinite index in C_0, and since $W := C_0/N$ is a subdirect product of copies of F, we have $W \cong \prod_{i=1}^{\infty} F$. Thus $\widehat{\Gamma}$, after passing to a subgroup of finite index if necessary, is mapped onto a group E of the following type:

$$(*) \qquad 1 \to W \to E \xrightarrow{\pi} H \to 1,$$

where H is an open subgroup of $G(\widehat{\mathcal{O}_S})$. To finish, it is enough to prove the following lemma.

Lemma 6.2 *Let E be a profinite group of the form $(*)$, where F and H are as above. Then for some $\epsilon > 0$, we have*

$$\log R_n(E) > \epsilon \log n \operatorname{loglog} n$$

for infinitely many n.

Proof Since F is simple, we can regard F as a subgroup of $\operatorname{Aut} F$. Fix an irreducible representation (V, σ) of $\operatorname{Aut} F$ such that $\sigma|_F$ is nontrivial. We can write $\sigma|_F$ as a sum of irreducibles $\tau_1 \oplus \cdots \oplus \tau_s$ for some s. Note that no τ_i is trivial (otherwise, as $F \trianglelefteq \operatorname{Aut} F$, the F-fixed points of V form a nonzero invariant subspace, contradicting the irreducibility of σ). Let $c > 1$ be the dimension of σ. Clearly there is no harm in taking logarithms to base c in what follows.

Fix constants $\gamma, \gamma_1, \gamma_2, \gamma_3$ such that $0 < \gamma < \gamma_3 < 1$, $0 < \gamma_1 < \gamma_2 < 1 - \gamma_3$ and γ is as in Proposition 5.1. Choose an open subgroup $U \trianglelefteq E$, and define $E' = E/U$, $W' = W/(W \cap U)$, $H' = H/\pi(U)$. Then W' is the product of a finite number of copies of F, say m copies. We can make m arbitrarily large by an appropriate choice of U. Replacing U by the preimage in E of the centraliser $C_{E'}(W')$, we can assume that $C_{E'}(W')$ is trivial (this does not change m, because $C_{E'}(W') \cap W' = 1$). We can identify $\operatorname{Aut} F^m$ with $\mathfrak{S}_m \ltimes (\operatorname{Aut} F)^m$, where $\mathfrak{S}_m$ is the symmetric group. Thus the action of E' on W' gives rise to a homomorphism $\rho\colon E' \to \mathfrak{S}_m$. Let K be the kernel of this homomorphism. Since E' acts faithfully on W', we can identify K with a subgroup of $(\operatorname{Aut} F)^m$, and we have $F^m \leq K \leq (\operatorname{Aut} F)^m$. As $\mathfrak{S}_m$ embeds into $\mathrm{GL}_m(\mathbb{C})$, Proposition 5.1 implies that

$$[E' \colon K] \leq e^{m^\gamma} \tag{6}$$

for sufficiently large m.

For any $S \subset \{1, \ldots, m\}$, define an irreducible representation σ'_S of $(\operatorname{Aut} F)^m$ by taking σ'_S to be σ on the ith factor of $(\operatorname{Aut} F)^m$ for every $i \in S$ and trivial on the other factors. Choose σ_S to be some irreducible component of the restriction of σ'_S to K. The dimension of σ_S is at most $c^{|S|}$. We claim that if $S_1 \neq S_2$ then $\sigma_{S_1} \neq \sigma_{S_2}$: in fact, $\sigma_{S_1}|_{F^m} \neq \sigma_{S_2}|_{F^m}$. To see this, observe that any irreducible component of $\sigma_S|_{F^m}$ can be written as a tensor product

$\phi_1 \otimes \cdots \otimes \phi_m$, where each ϕ_i is either trivial or equal to one of $\tau_1, \ldots, \tau_s$, and S is precisely the set of indices i such that ϕ_i is nontrivial.

Now let $f \colon \mathbb{N} \to \mathbb{N}$ be any nondecreasing function such that $\lim_{m\to\infty} f(m)/m^{\gamma} = \infty$ and $\lim_{m\to\infty} f(m)/m^{\gamma_3} = 0$ (for example, if $\gamma < \beta < \gamma_3$ then $f(m) = [m^{\beta}]$ will do). For the rest of the proof, assume that m is sufficiently large. We have

$$\begin{aligned}
\binom{m}{f(m)} &= \frac{m!}{(m-f(m))!f(m)!} \\
&\geq \frac{(m-f(m))^{f(m)}}{f(m)^{f(m)}} \\
&\geq \left(c^{-1}\frac{m}{f(m)}\right)^{f(m)} \\
&= c^{f(m)(\log_c m - \log_c f(m) - 1)} \\
&\geq c^{f(m)(\log_c m - \log_c m^{\gamma_3} - 1)} \\
&= c^{f(m)((1-\gamma_3)\log_c m - 1)} \\
&\geq c^{\gamma_2 f(m) \log_c m} \\
&= m^{\gamma_2 f(m)}.
\end{aligned}$$

Thus we have at least $m^{\gamma_2 f(m)}$ isomorphism classes of representations of K of the form σ_S with $|S| = f(m)$, each of dimension at most $c^{f(m)}$. This implies that $R_{c^{f(m)}}(K) \geq m^{\gamma_2 f(m)}$.

Set $n = [E' \colon K]c^{f(m)}$. We have

$$\begin{aligned}
R_n(E) &\geq R_n(E') \\
&\geq \frac{1}{[E' \colon K]} R_{c^{f(m)}}(K) \text{ by the first inequality of Lemma 2.2} \\
&\geq e^{-m^{\gamma}} m^{\gamma_2 f(m)} \text{ by Eqn. (6)} \\
&\geq m^{\gamma_1 f(m)}.
\end{aligned}$$

Taking logarithms gives

$$\log_c R_n(E) \geq \gamma_1 f(m) \log_c m \geq \gamma_1 f(m) \log_c f(m).$$

Fix $\kappa > 1$. Using Eqn. (6), we have $n \leq e^{m^{\gamma}} c^{f(m)} \leq c^{\kappa f(m)}$, which gives

$$\log_c n \leq \kappa f(m)$$

and

$$\log_c \log_c n \leq \log_c \kappa + \log_c f(m) \leq \kappa \log_c f(m).$$

Combining the previous three equations gives

$$\log_c R_n(E) \geq \frac{\gamma_1}{\kappa^2} \log_c n \log_c \log_c n,$$

and we have our required bound.

For the rest of the section, assume that $\operatorname{char} k = 0$. Assume that $\Gamma = G(\mathcal{O}_S)$ does not have the congruence subgroup property. By Rapinchuk's Lemma (see [Lub95, (2.6)] or [LS03, Section 7.1]), Γ has a finite index subgroup Γ_0 such that $\widehat{\Gamma_0}$ has a quotient E with the following property: there exists a short exact sequence of profinite groups

$$(*) \qquad 1 \to W \to E \xrightarrow{\pi} H \to 1,$$

where W is the product of countably many copies of a fixed finite simple group F and one of the following three possibilities occurs:
(a) F is nonabelian and H is an open subgroup of $G(\widehat{\mathcal{O}_S})$;
(b) F is abelian, say $F = C_l$, the cyclic group of order l, and H is an open pro-p_v subgroup of $G(\mathcal{O}_v)$ for some $v \in V_f - S$, with either:

(b1) $l \neq p_v$; or

(b2) $l = p_v$.

Thus, to prove Theorem 1.3 it suffices to show by Corollary 2.3 that in each of these three cases, $r_n(E)$ does not grow polynomially. Case (a) was exactly the case treated in Lemma 6.2.

Let us now treat case (b1). In this case the sequence $(*)$ splits by the Schur-Zassenhaus Theorem and $E = H \ltimes W$. Choose U open and normal in E, and let $E' = E/U$, $W' = W/(W \cap U)$ and $H' = H/\pi(U)$, so that $E' = H' \ltimes W'$. Then $W' \cong C_l^m$ for some m, and m can be made arbitrarily large by a suitable choice of U. Now the centraliser $C_{H'}(W')$ is a normal subgroup of E' which has trivial intersection with W'. Replacing U by the inverse image of $C_{H'}(W')$ in E, we can assume that H' acts faithfully on C_l^m, so that we have a faithful representation of H' into $\mathrm{GL}_m(\mathbb{F}_l)$. We deduce from Proposition 5.4 (i) that $|H'| \leq cm^c$ for some constant c. This implies that $A_{cm^c}(E) \geq l^m$. Lemma 2.6 (a) now implies that for any $\gamma \in (0, 1/c)$, $R_n(E) > e^{n^\gamma}$ for infinitely many n; in particular, E does not have PRG, and case (b1) is proved.

We haven't proven Rapinchuk's Lemma in positive characteristic, but if it is true then the proof of case (b1) works there as well. On the other hand, the following argument, which settles case (b2), works only if $\operatorname{char} k = 0$.

Assume now that we are in case (b2). Set $p := p_v = l$. Then E is a pro-p group. Let E^{p^n} be the closed subgroup of E generated by the p^n-powers in E and let $q_n(E) = [E\colon E^{p^n}]$. Set $E' = E/E^{p^n}$, $H' = H/H^{p^n} = H/\pi(E^{p^n})$. In [DdSMS99, Corollary 11.6] it is shown that if M is a finitely generated pro-p group and $q_n(M) < p^{p^n}$ for some $n \geq 1$ then M is p-adic analytic. Our group E is not p-adic analytic, so $q_n(E) \geq p^{p^n}$ for every n. On the other hand, H is p-adic analytic and so is boundedly generated, and $q_n(H)$ grows polynomially in n [DdSMS99, Theorem 3.16]: say $q_n(H) \leq (p^n)^d$ for some fixed d. Putting these two facts together we deduce that there is a short exact sequence

$$1 \to W' \to E' \to H' \to 1,$$

where $|E'| \geq p^{p^n}$ and $|H'| \leq (p^n)^d$. We conclude that $|W'| \geq p^{p^n - dn}$. As W' is abelian, we deduce that $A_{p^{dn}}(E) \geq p^{p^n-dn}$, which, again by Lemma 2.6 (a), implies that for any $\gamma \in (0, 1/d)$, $R_n(E) > e^{n^\gamma}$, this time for all sufficiently large n. So E does not have PRG. Thus Theorem 1.3 is proved.

We thank A. Jaikin-Zapirain for the main idea in the proof of case (b2).

References

[BLMM02] Hyman Bass, Alexander Lubotzky, Andy R. Magid, and Shahar Mozes, *The proalgebraic completion of rigid groups*, Geom. Dedicata **95** (2002), 19–58.

[CR81] Charles W. Curtis and Irving Reiner, *Methods of representation theory. Vol. I*, John Wiley & Sons Inc, New York, 1981.

[DdSMS99] J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal, *Analytic pro-p groups*, second ed., Cambridge Studies in Advanced Mathematics, vol. 61, Cambridge University Press, Cambridge, 1999.

[Erd41] P. Erdös, *On some asymptotic formulas in the theory of the "factorisation numerorum"*, Ann. of Math. **42** (1941), 989–993.

[Hum72] James E. Humphreys, *Introduction to Lie algebras and representation theory*, Springer-Verlag, New York, 1972, Graduate Texts in Mathematics, Vol. 9.

[JZ03] Andrei Jaikin-Zapirain, *The zeta function of representation of pro-p groups*, preprint, 2003.

[KL90] Peter Kleidman and Martin Liebeck, *The subgroup structure of the finite classical groups*, London Mathematical Society Lecture Note Series, vol. 129, Cambridge University Press, Cambridge, 1990.

[Lan93] Serge Lang, *Algebra*, third ed., Addison-Wesley, Reading, Massachusetts, 1993.

[LL] Michael Larsen and Alexander Lubotzky, *Normal subgroup growth of linear groups: the (G_2, F_4, E_8)-Theorem*, Algebraic Groups and Arithmetic (Mumbai 2001), Tata Inst. Fund. Res. Stud. Math., to appear.

[LM85] Alexander Lubotzky and Andy R. Magid, *Varieties of representations of finitely generated groups*, Mem. Amer. Math. Soc. **58** (1985), no. 336, xi+117.

[LS94] Alexander Lubotzky and Aner Shalev, *On some Λ-analytic pro-p groups*, Israel J. Math. **85** (1994), 307–337.

[LS03] Alexander Lubotzky and Dan Segal, *Subgroup growth*, Progress in Mathematics, vol. 212, Birkhäuser Verlag, Basel, 2003.

[Lub91] Alexander Lubotzky, *Lattices in rank one Lie groups over local fields*, Geom. and Funct. Anal. (GAFA) **1** (1991), 406–431.

[Lub95] ______, *Subgroup growth and congruence subgroups*, Invent. Math. **119** (1995), 267–295.

[Mar91] G. A. Margulis, *Discrete subgroups of semisimple Lie groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 17, Springer-Verlag, Berlin, 1991.

[PR93] V. P. Platonov and A. S. Rapinchuk, *Abstract properties of S-arithmetic groups and the congruence problem*, Russian Acad. Sci. Izv. Math. **40** (1993), 455–476.

[PR94] Vladimir Platonov and Andrei Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139, Academic Press Inc., Boston, MA, 1994.

[PR96] Gopal Prasad and Andrei S. Rapinchuk, *Computation of the metaplectic kernel*, Inst. Hautes Études Sci. Publ. Math. (1996), no. 84, 91–187.

[Pra77] Gopal Prasad, *Strong approximation for semi-simple groups over function fields*, Ann. of Math. **105** (1977), 553–572.

[Rag76] M. S. Raghunathan, *On the congruence subgroup problem*, Inst. Hautes Études Sci. Publ. Math. (1976), no. 46, 107–161.

[Ros02] Michael Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002.

[Seg99] Yoav Segev, *On finite homomorphic images of the multiplicative group of a division algebra*, Ann. of Math. **149** (1999), 219–251.

[Ser70] Jean-Pierre Serre, *Le problème des groupes de congruence pour SL2*, Ann. of Math. **92** (1970), 489–527.

[Ser92] ______, *Lie algebras and Lie groups*, second ed., Lecture Notes in Mathematics, vol. 1500, Springer-Verlag, Berlin, 1992.

[Ven88] T. N. Venkataramana, *On superrigidity and arithmeticity of lattices in semisimple groups over local fields of arbitrary characteristic*, Invent. Math. **92** (1988), 255–306.

Institute of Mathematics
Hebrew University of Jerusalem
Jerusalem 91904
Israel
Email address: `alexlub@math.huji.ac.il`
Email address: `benm@math.huji.ac.il`