SUPER-APPROXIMATION, II:
THE p-ADIC AND BOUNDED POWER OF SQUARE-FREE INTEGERS CASES.

ALIREZA SALEHI GOLSEFIDY

ABSTRACT. Let Ω be a finite symmetric subset of $\mathrm{GL}_n(\mathbb{Z}[1/q_0])$, $\Gamma := \langle \Omega \rangle$, and let π_m be the group homomorphism induced by the quotient map $\mathbb{Z}[1/q_0] \to \mathbb{Z}[1/q_0]/m\mathbb{Z}[1/q_0]$. Then the family of Cayley graphs $\{\mathrm{Cay}(\pi_m(\Gamma), \pi_m(\Omega))\}_m$ is a family of expanders as m ranges over fixed powers of square-free integers and powers of primes that are coprime to q_0 if and only if the connected component of the Zariski-closure of Γ is perfect. Some of the immediate applications, e.g. orbit equivalence rigidity, *largeness* of certain ℓ-adic Galois representations, are also discussed.

CONTENTS

1. Introduction

1.1. **Statement of the main results.** Let Ω be a finite symmetric subset of $\mathrm{GL}_n(\mathbb{Q})$, and $\Gamma = \langle \Omega \rangle$. Since Ω is finite, for some $q_0 \in \mathbb{Z}^+$ we have $\Gamma \subseteq \mathrm{GL}_n(\mathbb{Z}[1/q_0])$. *Strong approximation* implies that (under certain algebraic conditions) the closure of Γ in $\prod_{p \nmid q_0} \mathrm{GL}_n(\mathbb{Z}_p)$ is open in $\prod_{p \nmid q_0} (\mathbb{G}(\mathbb{Q}_p) \cap \mathrm{GL}_n(\mathbb{Z}_p))$, where $\mathbb{G}$ is the Zariski-closure of Γ in $\mathbb{GL}_n$. In combinatorial language, this means that the Cayley graphs

$$\mathrm{Cay}\left(\pi_m(\mathbb{G}(\mathbb{Q}) \cap \mathrm{GL}_n(\mathbb{Z}[1/q_0])), \pi_m(\Omega)\right),$$

where m and q_0 are coprime and π_m is the group homomorphism induced by the quotient map $\pi_m : \mathbb{Z}[1/q_0] \to \mathbb{Z}[1/q_0]/m\mathbb{Z}[1/q_0]$, have at most $C := C(\Omega)$ many connected components. The point being that C does not depend on m. *Super-approximation*[1] tells us that these sparse graphs are *highly connected*, i.e. they form a family of *expanders*. A family $\{X_i\}_{i \in I}$ of d_0-regular graphs is called *expander* if there is $c > 0$ such that for any $i \in I$ and any subset A of the set of vertices $V(X_i)$ of X_i we have

$$c < \frac{|e(A, V(X_i) \setminus A)|}{\min(|A|, |V(X_i) \setminus A|)},$$

where $e(A, V(X_i) \setminus A)$ consists of the edges that connect a vertex in A to a vertex in $V(X_i) \setminus A$.

Expanders are extremely useful in communication and theoretical computer science (e.g. see [HLW06]). In the past decade they have been found useful in a wide range of pure math problems, e.g. affine sieve [BGS10, SGS13], sieve in groups [LM13], variation of Galois representations [EHK12], etc. (see [BO14] for a collection of surveys of related works and applications).

In this article we prove the *best possible* super-approximation results for two families of residue maps. Let $V_f(\mathbb{Q})$ be the set of primes in $\mathbb{Q}$, and $\nu_p(q)$ be the p-valuation of q, i.e. the power of p in q.

Theorem 1. *Let Ω be a finite symmetric subset of $\mathrm{GL}_{N_0}(\mathbb{Z}[1/q_0])$, $\Gamma := \langle \Omega \rangle$, and M_0 be a fixed positive integer. Suppose Γ is an infinite group. Then the family of Cayley graphs $\{\mathrm{Cay}(\pi_m(\Gamma), \pi_m(\Omega))\}_m$ is a family of expanders as m runs through either*

$$\{p^n | \ n \in \mathbb{Z}^+, p \in V_f(\mathbb{Q}), p \nmid q_0\} \ \text{ or } \ \{q | \ \forall p \in V_f(\mathbb{Q}), \nu_p(q) \le M_0\}$$

if and only if the connected component $\mathbb{G}^\circ$ of the Zariski-closure $\mathbb{G}$ of Γ in $\mathbb{GL}_{N_0}$ is perfect, i.e. $[\mathbb{G}^\circ, \mathbb{G}^\circ] = \mathbb{G}^\circ$.

---

[1]Following A. Kontorovich's suggestion, I call this phenomenon super-approximation. It is worth pointing out that this phenomenon has been called superstrong approximation [BO14] by some authors.

In the appendix, a quantitative open image for p-adic analytic maps is proved, which should be of independent interest. In a joint work with Zhang [SGZ], this result is used to generalize a theorem of Burger and Sarnak [BS91] to the setting of *super-approximation* (see Theorem 9 for the statement of this result.).

1.2. **Comparing with the previous related results.** The importance of Theorem 1 lies on the fact that it is an *if-and-only-if* statement. In fact, by Proposition 10, we get that, if $\{\pi_{m_i}(\Gamma), \pi_{m_i}(\Omega)\}$ is a family of expanders for some increasing sequence $\{m_i\}$ of integers that are relatively prime to q_0, then $\{\pi_m(\Gamma), \pi_m(\Omega)\}_m$ is a family of expanders as m runs through integers specified in Theorem 1.

Super-approximation for square-free numbers is the main theorem of [SGV12]. Of course it is a special case of Theorem 1 for $m \in \{q | \forall p \in V_f(\mathbb{Q}), \nu_p(q) \leq M_0\}$ and $M_0 = 1$. It should, however, be noted that our proof relies on [SGV12]. Proof of this part of Theorem 1 is heavily influenced by the relevant part of [BV12]. But here, instead of working with the concrete structure of the congruence quotients of $SL_n(\mathbb{Z})$ as it was done in [BV12], one has to work with arbitrary perfect groups. So it is inevitable to make use of basic theorems from Bruhat-Tits theory to describe structure of a maximal compact subgroup of $\mathbb{H}(\mathbb{Q}_p)$ where $\mathbb{H}$ is a semisimple $\mathbb{Q}_p$-group, and to use *truncated* or *finite logarithmic maps* [Pin98, Section 6] or [SG, Section 2.9]. In addition, one has to understand how such a maximal compact group acts on an open compact subgroup of $\mathbb{U}(\mathbb{Q}_p)$ where $\mathbb{U}$ is a unipotent $\mathbb{Q}_p$-group, which makes the use of the language of schemes necessary.

Proof of Theorem 1 for powers of primes relies on [SG] where the semisimple case is proved.

Prior to [SG], the case of *Zariski-dense* subgroups of $SL_n(\mathbb{Z})$ was studied by Bourgain-Gamburd [BG08-b, BG09] and Bourgain-Varjú [BV12]. As it is pointed out in [SG, Section 1.3], the proofs by Bourgain and Gamburd [BG08-b, BG09] and Bourgain and Varjú [BV12] rely heavily on Archimedean dynamics. In particular, those ideas cannot be implemented for a finitely generated subgroup Γ of $GL_n(\mathbb{Q})$ if Γ is a bounded subgroup of $GL_n(\mathbb{R})$. But it is worth pointing out that, if Γ is a Zariski-dense subgroup of $SL_n(\mathbb{Z})$, Bourgain and Varjú [BV12] prove that $\{Cay(\pi_m(\Gamma), \pi_m(\Omega))\}_m$ is a family of expanders with *no restriction* on m.

Prior to the current work, *no* super-approximation result for powers of primes *beyond semisimple case* was known. To get such a result, one had to use new ideas and combine techniques from p-adic analytic analysis, p-adic analytic pro-p groups, and non-commutative algebra.

1.3. **Applications.**

1.3.1. *Random-walk and spectral gap.* Let Ω be a finite symmetric subset of a compact group G. Let μ be the counting probability measure on Ω and $\Gamma := \langle \Omega \rangle$. Let

$$T_\mu : L^2(\overline{\Gamma}) \to L^2(\overline{\Gamma}), \quad T_\mu(f) := \mu * f,$$

where $(\mu * f)(g) := \sum_{g' \in \text{supp} \mu} \mu(g') f(g'^{-1}g)$ and $\overline{\Gamma}$ is the closure of Γ in G. It is easy to see that T_μ is a self-adjoint operator, the constant function $\mathbb{1}_{\overline{\Gamma}}$ is an eigenfunction with eigenvalue one, i.e. $T_\mu(\mathbb{1}_{\overline{\Gamma}}) = \mathbb{1}_{\overline{\Gamma}}$, and $\|T_\mu\| = 1$. Let

$$\lambda(\mu; G) := \sup\{|\lambda| | \ \lambda \in \text{spec}(T_\mu), \ \lambda < 1\}.$$

We get a fairly good understanding of the random-walk in G with respect to μ if $\lambda(\mu; G) < 1$, in which case it is said that either $\Gamma \curvearrowright \overline{\Gamma}$ or the random-walk with respect to μ has *spectral gap*.

Let us recall a couple of well-known results which give us a connection between having spectral gap and explicit construction of expanders (see [Lub94, Chapter 4.3], [LZ03, Chapter 1.4], [SG, Remark 15]).

Remark 2. (1) *Let Γ be the group generated by a finite symmetric set Ω. Suppose $\{N_i\}_{i \in I}$ is a family of normal, finite-index subgroups of Γ. Suppose, for any $i_1, i_2 \in I$, there is $i_3 \in I$ such that $N_{i_3} \subseteq N_{i_1} \cap N_{i_2}$. Then, by Peter-Weyl theorem, one has*

$$\lambda(\mathcal{P}_\Omega; \varprojlim \Gamma/N_i) = \sup_i \lambda(\mathcal{P}_{\iota_{N_i}(\Omega)}; \Gamma/N_i),$$

where $\iota_{N_i} : \Gamma \to \Gamma/N_i$ is the natural quotient map.

(2) Suppose $\{N_i\}_{i \in I}$ is a family of normal, finite-index subgroups of Γ. Then the family of Cayley graphs $\{\mathrm{Cay}(\Gamma/N_i, \iota_{N_i}(\Omega))\}_{i \in I}$ is a family of expanders if and only if

$$\sup_i \lambda(\mathcal{P}_{\iota_{N_i}(\Omega)}; \Gamma/N_i) < 1.$$

Based on these results, we get that Theorem 1 implies the following.

Corollary 3. Let Ω be a finite symmetric subset of $\mathrm{GL}_{N_0}(\mathbb{Z}[1/q_0])$, and $\mathcal{P}_\Omega$ be the counting probability measure on Ω. Suppose the connected component $\mathbb{G}^\circ$ of the Zariski-closure $\mathbb{G}$ of $\Gamma := \langle \Omega \rangle$ in $\mathbb{GL}_{N_0}$ is perfect. Then for any positive integer M_0 we have

$$\lambda(\mathcal{P}_\Omega; \prod_{p \nmid q_0} \mathrm{GL}_{N_0}(\mathbb{Z}/p^{M_0}\mathbb{Z})) < 1,$$

and

$$\sup_{p \nmid q_0} \lambda(\mathcal{P}_\Omega; \mathrm{GL}_{N_0}(\mathbb{Z}_p)) < 1.$$

Since a stronger form of the *only-if* part of Theorem 1 (see Proposition 10) holds, having spectral gap for a single place implies a uniform spectral gap for all the places.

Corollary 4. Let Ω be a finite symmetric subset of $\mathrm{GL}_{N_0}(\mathbb{Z}[1/q_0])$, and $\mathcal{P}_\Omega$ be the counting probability measure on Ω. Then for some $p \nmid q_0$ we have $\lambda(\mathcal{P}_\Omega; \mathrm{GL}_{N_0}(\mathbb{Z}_p)) < 1$ if and only if

$$\sup_{p \nmid q_0} \lambda(\mathcal{P}_\Omega; \mathrm{GL}_{N_0}(\mathbb{Z}_p)) < 1.$$

Spectral gap has a well-known *weighted equidistribution* consequence.

Corollary 5. In the setting of Corollary 3, there is $\lambda < 1$ such that for any prime p which does not divide q_0 and $\mathbb{G}(\mathbb{Q}_p) \cap \mathrm{GL}_{N_0}(\mathbb{Z}_p)$-finite function f_0 on $\mathbb{G}(\mathbb{Q}_p)$ (which means that f_0 is invariant under an open subgroup of $\mathbb{G}(\mathbb{Q}_p)$) we have

$$|\sum_{\gamma \in \Gamma} \mathcal{P}_\Omega^{(l)}(\gamma) f_0(\gamma) - \int_{\Gamma_p} f_0(g) dg| \leq \|f_0 - \int_{\Gamma_p} f_0(g) dg\|_2 \sqrt{|\Gamma_p \cdot f_0|} \lambda^l,$$

where Γ_p is the closure of Γ in $\mathrm{GL}_{N_0}(\mathbb{Z}_p)$ and it acts on functions on $\mathbb{G}(\mathbb{Q}_p)$ via the right translation, i.e. $(g \cdot f)(g') := f(g'g)$, $\mathcal{P}_\Omega^{(l)}$ is the l-th convolution power of $\mathcal{P}_\Omega$, dg is the probability Haar measure on Γ_p, and $\|f\|_2 := (\int_{g \in \Gamma_p} f(g)^2 dg)^{1/2}$.

Proof. Since Ω is a symmetric set, we have that

$$\sum_{\gamma \in \Gamma} \mathcal{P}_\Omega^{(l)}(\gamma) f_0(\gamma) - \int_{\Gamma_p} f_0(g) dg = T_\mu^l(f_0)(I) - \langle \mathbb{1}_{\Gamma_p}, f_0 \rangle, \tag{1}$$

where I is the identity matrix and $\langle, \rangle$ is the dot product in $L^2(\Gamma_p)$.

On the other hand, by Corollary 3, we have that

$$\|T_\mu^l(f_0) - \langle \mathbb{1}_{\Gamma_p}, f_0 \rangle\|_2 = \|T_\mu^l(f_0 - \langle \mathbb{1}_{\Gamma_p}, f_0 \rangle \mathbb{1}_{\Gamma_p})\|_2 \leq \lambda^l \|f_0 - \langle \mathbb{1}_{\Gamma_p}, f_0 \rangle \mathbb{1}_{\Gamma_p}\|_2, \tag{2}$$

where $\lambda := \sup_{p \nmid q_0} \lambda(\mathcal{P}_\Omega; \mathrm{GL}_{N_0}(\mathbb{Z}_p))$. For any function f, let $\Gamma_{p,f} := \{g \in \Gamma_p | \ g \cdot f = f\}$. Since for any $g \in \Gamma_p$ and $f \in L^2(\Gamma_p)$ we have $T_\mu(g \cdot f) = g \cdot T_\mu(f)$, we get that $\Gamma_{p,f} \subseteq \Gamma_{p,T_\mu(f)}$. So we have

$$\|T_\mu^l(f_0) - \langle \mathbb{1}_{\Gamma_p}, f_0 \rangle\|_2^2 = \int_{\Gamma_p/\Gamma_{p,f_0}} \int_{\Gamma_{p,f_0}} |T_\mu^l(f_0)(gg') - \langle \mathbb{1}_{\Gamma_p}, f_0 \rangle|^2 dg' dg$$

$$= \int_{\Gamma_p/\Gamma_{p,f_0}} \int_{\Gamma_{p,f_0}} |(g' \cdot T_\mu^l(f_0))(g) - \langle \mathbb{1}_{\Gamma_p}, f_0 \rangle|^2 dg' dg$$

$$= \int_{\Gamma_p/\Gamma_{p,f_0}} |T_\mu^l(f_0)(g) - \langle \mathbb{1}_{\Gamma_p}, f_0 \rangle|^2 \int_{\Gamma_{p,f_0}} dg' dg$$

$$= \frac{1}{[\Gamma_p : \Gamma_{p,f_0}]} \sum_{g\Gamma_{p,f_0} \in \Gamma_p/\Gamma_{p,f_0}} |T_\mu^l(f_0)(g) - \langle \mathbb{1}_{\Gamma_p}, f_0 \rangle|^2$$

(3)
$$\geq \frac{|T_\mu^l(f_0)(I) - \langle \mathbb{1}_{\Gamma_p}, f_0 \rangle|^2}{|\Gamma_p \cdot f_0|}.$$

Equations (1), (2), and (3) imply the claim. $\qquad\square$

Corollary 5 is another indication that *super-approximation* is a suitable name for such a phenomenon as it implies a quantitative way to approximate points.

1.3.2. *Orbit equivalence.* Suppose $\Gamma \subseteq G$ and $\Lambda \subseteq H$ are dense subgroups of compact groups G and H. We say the left translation actions $\Gamma \curvearrowright (G, m_G)$ and $\Lambda \curvearrowright (H, m_H)$ are *orbit equivalent* if there exists a measure class preserving Borel isomorphism $\theta : G \to H$ such that $\theta(\Gamma g) = \Lambda\theta(g)$, for m_G-almost every $g \in G$. Surprisingly, if Γ and Λ are amenable, the mentioned actions are orbit equivalent [OW80, CFW81]. In the past decade there have been a lot of progress on this subject, and as a result now it is known that one gets orbit equivalence rigidity under spectral gap assumption [Ioa14-a, Ioa14-b].

Corollary 6. *Let Ω be a finite symmetric subset of $\mathrm{GL}_{N_0}(\mathbb{Z}[1/q_0])$, and $\mathcal{P}_\Omega$ be the counting probability measure on Ω. Suppose the connected component $\mathbb{G}^\circ$ of the Zariski-closure $\mathbb{G}$ of $\Gamma := \langle \Omega \rangle$ in $\mathbb{GL}_{N_0}$ is perfect. Let Γ_p be the closure of Γ in $\mathrm{GL}_{N_0}(\mathbb{Z}_p)$ where $p \nmid q_0$.*

Let Λ be a countable dense subgroup of a profinite group H. Then $\Gamma \curvearrowright (\Gamma_p, m_{\Gamma_p})$ and $\Lambda \curvearrowright (H, m_H)$ are orbit equivalent if and only if there are open subgroups $G_0 \subseteq \Gamma_p$ and $H_0 \subseteq H$ and a continuous isomorphism $\delta : G_0 \to H_0$ such that $[\Gamma_p : G_0] = [H : H_0]$ and $\delta(G_0 \cap \Gamma) = \Lambda \cap H_0$. In particular, H is p-adic analytic.

Proof. This is a direct consequence of Corollary 3 and [Ioa14-a, Theorem A]. $\qquad\square$

1.3.3. *Variations of Galois representations in one-parameter families of abelian varieties.* Since eight years ago, because of a surge of works by various people specially Cadoret, Tamagawa [Cad, CT12, CT13], Hui, and Larsen [Hui12, HL], we have got a much better understanding of the image of ℓ-adic and adelic Galois representations induced by Tate modules of an abelian scheme. On the other hand, Ellenberg, Hall, and Kowalski in [EHK12] gave a beautiful connection between variations of Galois representations and certain spectral gap property[2]. Here we make an observation that Ellenberg-Hall-Kowalski [EHK12] machinery combined with Theorem 1 gives an alternative approach towards [CT12, CT13]; in particular, we do not get any new result on this topic.

In this section, let k be a finitely generated characteristic zero field, $\overline{k}$ be the algebraic closure of k, and U be a smooth algebraic curve over k such that $U \times_k \overline{k}$ is connected. Let $\mathcal{A} \to U$ be an abelian scheme of dimension $g \geq 1$, defined over k. Take an embedding of k into $\mathbb{C}$, and let

$$\rho_0 : \pi_1(U(\mathbb{C}), y_0) \to \mathrm{Aut}_U(\mathcal{A}) \subseteq GL_{2g}(\mathbb{Z})$$

---

[2]Instead of being *expanders*, they only need a weaker assumption on the relevant Schreier graphs, called *esperantist graphs*.

be the monodromy representation. Let $\Gamma := \rho_0(\pi_1(U(\mathbb{C}), y_0))$, and $\mathbb{G}$ be the Zariski-closure of Γ in $(\mathrm{GL}_{2g})_{\mathbb{Q}}$. Let Ω be a finite symmetric generating set of Γ.

For any $x \in U(\overline{k})$, the fiber $\mathcal{A}_x$ over x is an abelian variety defined over the residue field $k(x)$ at x. For any prime l, let $T_{l,x}$ be the Tate module of $\mathcal{A}_x$, i.e.

$$T_{l,x} := \varprojlim \mathcal{A}_x[l^m](\overline{k}),$$

where $\mathcal{A}_x[l^m](\overline{k})$ is the l^m-th torsion elements of $\mathcal{A}_x(\overline{k})$. So $T_{l,x} \simeq \mathbb{Z}_l^{2g}$ and we get the l-adic Galois representation

$$\rho_{l,x} : \mathrm{Gal}(\overline{k}/k(x)) \to \mathrm{Aut}_{\mathbb{Z}_l}(T_{l,x}) \simeq \mathrm{GL}_{2g}(\mathbb{Z}_l).$$

Lemma 7. *In the above setting, the connected component $\mathbb{G}^\circ$ of $\mathbb{G}$ is perfect.*

Proof. By [EHK12, Proposition 16], Γ has a finite index subgroup Λ such that $\pi_l(\Lambda)$ is a perfect group and generated by its order l elements for large enough prime l. In particular, the index of any proper subgroup of $\pi_l(\Lambda)$ is at least l.

Let $\Gamma^\circ := \Gamma \cap \mathbb{G}^\circ$. So Γ° is Zariski-dense in $\mathbb{G}^\circ$. Since $[\pi_l(\Lambda) : \pi_l(\Lambda \cap \Gamma^\circ)] \leq [\Gamma : \Gamma^\circ]$, for large enough prime l we have that $\pi_l(\Lambda) = \pi_l(\Lambda \cap \Gamma^\circ)$.

On the other hand, the quotient map $\mathbb{G}^\circ \xrightarrow{f} (\mathbb{G}^\circ)^{\mathrm{ab}} := \mathbb{G}^\circ/[\mathbb{G}^\circ, \mathbb{G}^\circ]$ is defined over $\mathbb{Q}$. Hence after realizing $(\mathbb{G}^\circ)^{\mathrm{ab}}$ as a subgroup of $(\mathbb{GL}_{n'})_{\mathbb{Q}}$, for large enough l we have that $\pi_l(f(\Gamma^\circ))$ is a homomorphic image of $\pi_l(\Gamma^\circ)^{\mathrm{ab}} := \pi_l(\Gamma^\circ)/[\pi_l(\Gamma^\circ), \pi_l(\Gamma^\circ)]$. Suppose to the contrary that $\mathbb{G}^\circ$ is not perfect. Then $f(\Gamma^\circ)$ is a finitely generated, infinite, abelian group as it is a Zariski-dense subgroup of $(\mathbb{G}^\circ)^{\mathrm{ab}}$. Hence $|\pi_l(f(\Gamma^\circ))| \to \infty$ as l goes to infinity, which implies that $|\pi_l(f(\Gamma^\circ \cap \Lambda))| \to \infty$. Since $\pi_l(f(\Gamma^\circ \cap \Lambda))$ is abelian and a homomorphic image of $\pi_l(\Gamma^\circ \cap \Lambda)$, we get a contradiction. $\square$

Now we can give an alternative proof of the main result of [CT12, CT13].

Proposition 8. *In the above setting, for any integer d and any prime ℓ there is an integer $B := B(d, \ell, \rho_0)$ such that*

$$U_{d,\ell} := \{x \in U(\overline{k})|\ [k(x) : k] \leq d, [\Gamma_\ell : \mathrm{Im}(\rho_{\ell,x}) \cap \Gamma_\ell] > B\},$$

is finite.

Proof. Suppose to the contrary that there is a sequence $\{x_i\}$ of points in $U(\overline{k})$ such that

(1) $x_i \neq x_j$ if $i \neq j$,
(2) $[k(x_i) : k] \leq d$,
(3) $[\Gamma_\ell : \mathrm{Im}(\rho_{\ell,x_i}) \cap \Gamma_\ell] = N_i$ where $N_i \in \mathbb{Z}^+ \cup \{\infty\}$, and $N_i \to \infty$.

By Lemma 38, there is an increasing sequence $\{m_i\}_i$ of positive integers and a sequence of open subgroups $\{H_i\}_i$ of Γ_ℓ such that

$$\lim_{i \to \infty} [\Gamma_\ell : H_i] = \infty,\ \Gamma_\ell \cap \mathrm{Im}(\rho_{\ell,x_i}) \subseteq H_i, \text{and}\ \Gamma_\ell[\ell^{m_i}] \subseteq H_i.$$

Going to a subsequence, if necessary, we can and will assume that $\pi_{\ell^{m_i}}(H_i) = \pi_{\ell^{m_i}}(H_j)$ for any $j \geq i$. Therefore we can and will assume that $H_1 \supsetneq H_2 \supsetneq \cdots$.

For each i, we get an open subgroup of $\pi_1^{et}(U \times_k \overline{k})$, and so we get an étale cover $U_i \xrightarrow{\phi_i} U$ of U that is defined over k. Since $\mathrm{Im}(\rho_{\ell,x_i}) \subseteq H_i$, there is $\widetilde{x}_i \in U_i(k(x_i))$ which is in the fiber over $x_i \in U(k(x_i))$. Moreover, since $\{H_i\}_i$ is a decreasing sequence of open subgroups, we get k-étale covering maps $U_j \xrightarrow{\phi_{ij}} U_i$ for any $i \leq j$ that satisfy $\phi_i \circ \phi_{ij} = \phi_j$. In particular, we have that

$$(4) \qquad \{\phi_{ij}(\widetilde{x}_j)\}_j \subseteq \bigcup_{[k':k] \leq d} U_i(k')$$

is an infinite subset for any i. On the other hand, since $\pi_1^{et}(U_i \times_k \overline{k})$ is the profinite closure of $\pi_1(U_i(\mathbb{C}), x_0)$, the natural embedding induces an isomorphism between the Schreier graphs

$$(5) \qquad \mathrm{Sch}(\pi_1(U(\mathbb{C}), x_0)/\pi_1(U_i(\mathbb{C}), \widetilde{x}_{0,i}); \Omega) \simeq \mathrm{Sch}(\pi_{\ell^{m_i}}(\Gamma_\ell)/\pi_{\ell^{m_i}}(H_i); \pi_{\ell^{m_i}}(\Omega)),$$

where $\widetilde{x}_{0,i}$ is a point over x_0. On the other hand, by Lemma 7 and Theorem 1, we have that

$$(6) \qquad \{\mathrm{Cay}(\pi_{\ell^{m_i}}(\Gamma); \pi_{\ell^{m_i}}(\Omega)\}_i$$

is a family of expanders. Since the Schreier graphs in (5) are quotients of the Cayley graphs in (6) and their size goes to infinity, they form a family of expanders. Therefore by the main result of Ellenberg-Hall-Kowalski [EHK12, Theorem 8] we have that the (geometric) gonality $\gamma(U_i)$ of U_i goes to infinity. Hence by a corollary [CT13, Theorem 2.1] of Falting's theorem [Fal91] on Lang-Mordell conjecture (see [Fer94, Mc95, Maz00]) we have that

$$\bigcup_{[k':k] \leq d} U_i(k')$$

is finite for large enough i. This contradicts (4). $\qquad\square$

1.3.4. *Inducing super-approximation.* As it was mentioned earlier, in the appendix a quantitative open function theorem (see Lemma 53′) is proved, which is of independent interest. This result plays an important role in my joint work with Zhang [SGZ], where we prove that one can induce super-approximation from a subgroup under a mild (and needed) algebraic condition.

Theorem 9. *Let Ω_1 be a finite symmetric subset of $\mathrm{GL}_{N_0}(\mathbb{Z}[1/q_0])$, and $\Gamma_1 := \langle \Omega_1 \rangle$. Let Ω_2 be a finite symmetric subset of Γ_1, and $\Gamma_2 := \langle \Omega_2 \rangle$. Let $\mathbb{G}_i^\circ$ be the connected component of the Zariski-closure of Γ_i in $\mathbb{GL}_{N_0}$ for $i = 1, 2$. Suppose the smallest normal subgroup of $\mathbb{G}_1^\circ$ which contains $\mathbb{G}_2^\circ$ is $\mathbb{G}_1^\circ$. Then, if Γ_2 has super-approximation, then Γ_1 has, too; that is equivalent to say*

$$\lambda(\mathcal{P}_{\Omega_2}; \prod_{p \nmid q_0} \mathbb{Z}_p) < 1 \implies \lambda(\mathcal{P}_{\Omega_1}; \prod_{p \nmid q_0} \mathbb{Z}_p) < 1.$$

Such a result for arithmetic groups was proved by Burger and Sarnak [BS91].

Acknowledgments.

2. Preliminary results and notation.

2.1. **Notation.** In this note, for two real valued functions f and g, and a set of parameters X, we write $f = O_X(g)$ if there are positive functions $C_1(X)$ and $C_2(X)$ of the set of parameters such that for $t \geq C_1(X)$ we have $0 \leq f \leq C_2(X)g$; notice that this is slightly different from the usual Landau symbol as $O_X(g)$ is assumed to be *non-negative*. For two real valued functions f and g of a real variable t and a set of parameters X, we write $f = \Theta_X(g)$ if there are positive functions $C_1(X), C_2(X)$, and $C_3(X)$ such that $C_1(X)g(t) \leq f(t) \leq C_2(X)g(t)$ for any $t \geq C_3(X)$. For two real valued functions f and g of a real variable t and a set of parameters X, we write $f \ll_X g$ if there are positive functions $C_1(X)$ and $C_2(X)$ such that for $t \geq C_2(X)$ we have $f(t) \leq C_1(X)g(t)$. So for two non-negative functions f and g we have $f = O_X(g)$ if and only if $f \ll_X g$; and $f = \Theta_X(g)$ if and only if $g \ll_X f \ll_X g$.

For a (commutative unital) ring R and $a \in R$, $\pi_a : R \to R/aR$ is the quotient map. We denote also the induced group homomorphism $\mathrm{GL}_n(R) \to \mathrm{GL}_n(R/aR)$ and all of its restrictions by π_a. For a subgroup Γ of $\mathrm{GL}_n(R)$, $\Gamma[a]$ denotes $\{\gamma \in \Gamma | \ \pi_a(\gamma) = 1\}$; in particular $\Gamma[1] = \Gamma$.

For a subset A of a group G, we write either $\prod_C A$ or $\underbrace{A \cdot A \cdots \cdots A}_{C \text{ times}}$ for the subset $\{a_1 \cdots a_c | \ a_1, \ldots, a_C \in A\}$; A^{-1} denotes the subset $\{a^{-1} | \ a \in A\}$; and A is called symmetric if $A = A^{-1}$. For an additive group G, $\sum_C A$ denotes the subset $\{a_1 + \cdots + a_C | \ a_1, \ldots, a_C \in A\}$.

For a measure μ on a group G, we let $\mathrm{supp}\, \mu$ be the support of μ. For a measure μ on a group G and $g \in G$, we let $\mu(g) := \mu(\{g\})$. For a measure μ with finite support on a group G and a complex valued function f on G, we let $\mu * f$ be the convolution of μ and f, that means $(\mu * f)(g) = \sum_{s \in \mathrm{supp}(\mu)} \mu(s) f(s^{-1}g)$. For a measure μ with finite support on a group G, we let $\mu^{(l)}$ be the l-fold convolution of μ, that means for any $g \in G$, we have $\mu^{(l)}(g) = (\underbrace{\mu * \cdots * \mu}_{l \text{ times}})(g) = \sum_{g_1 \cdots g_l = g} \mu(g_1) \cdots \mu(g_l)$. We say a measure μ with finite support on a group G is symmetric if $\mu(g^{-1}) = \mu(g)$ for any $g \in G$. For a finite subset X of a group G, we let $\mathcal{P}_X$ be the probability counting measure on X.

The set of (rational) primes is denoted by $V_f(\mathbb{Q})$. For any prime p, $\mathfrak{f}_p$ denotes the finite field with p elements; $\mathbb{Q}_p$ is the field of p-adic numbers; $\mathbb{Z}_p$ is the ring of p-adic integers; and $v_p : \mathbb{Q}_p \setminus \{0\} \to \mathbb{Z}$ (and its restriction to $\mathbb{Q} \setminus \{0\}$) is the p-adic valuation, that means $v_p(x) = n$ if and only if $x \in p^n \mathbb{Z}_p \setminus p^{n+1}\mathbb{Z}_p$. For any prime p and $x \in \mathbb{Q}_p$, we let $|x|_p := (1/p)^{v_p(x)}$ if $x \neq 0$, and $|0|_p := 0$.

2.2. **Necessity.** In this section, we will prove that getting a family of expanders modulo an infinite sequence of integers implies that the connected component of the Zariski-closure is perfect (see Proposition 10). In particular, we get the necessary part of Theorem 1.

Let us remark that proof of [SGV12, Section 5.1] can be adjusted to give the necessary part of Theorem 1 for any fixed prime p. The main point being that the proof in [SGV12] makes use of the fact that the congruence kernels modulo square-free numbers define a topology.

The proof here is rather straightforward and has three parts:

(a) Changing Γ to $\Gamma^\circ := \Gamma \cap \mathbb{G}^\circ$, we can and will assume $\mathbb{G}$ is Zariski-connected;
(b) If $\mathbb{G}$ has infinite abelianization $\mathbb{G}^{\mathrm{ab}} := \mathbb{G}/[\mathbb{G}, \mathbb{G}]$, then the order of the abelianization $\pi_{q_i}(\Gamma)^{\mathrm{ab}}$ of $\pi_{q_i}(\Gamma)$ gets arbitrarily large as q_i goes to infinity.
(c) If S is a finite symmetric generating set of an abelian group A, then the order of A is bounded by a function of $|S|$ and $\lambda(\mathcal{P}_S; A)$ (see [LW93, Corollary 3.3]).

Proposition 10. *Let Ω be a finite symmetric subset of $\mathrm{GL}_n(\mathbb{Z}[1/q_0])$ and $\Gamma = \langle \Omega \rangle \subseteq \mathrm{GL}_n(\mathbb{Z}[1/q_0])$. Let $\mathbb{G}^\circ$ be the Zariski-connected component of the Zariski-closure $\mathbb{G}$ of Γ in $(\mathrm{GL}_n)_{\mathbb{Q}}$. If $\{\mathrm{Cay}(\pi_{q_i}(\Gamma), \pi_{q_i}(\Omega))\}_i$ is a family of expanders for integers $q_1 < q_2 < \cdots$ coprime with q_0, then $\mathbb{G}^\circ$ is perfect, i.e. $[\mathbb{G}^\circ, \mathbb{G}^\circ] = \mathbb{G}^\circ$.*

Proof. Let $\Gamma^\circ := \Gamma \cap \mathbb{G}^\circ$. Then, by [SG, Corollary 17], Γ° has a finite symmetric generating set Ω° and

$$\{\mathrm{Cay}(\pi_{q_i}(\Gamma^\circ), \pi_{q_i}(\Omega^\circ))\}_i$$

is a family of expanders. Therefore for some positive integer C we have $|\pi_{q_i}(\Gamma^\circ)/[\pi_{q_i}(\Gamma^\circ), \pi_{q_i}(\Gamma^\circ)]| < C$ for any i (see [LW93, Corollary 3.3]).

On the other hand, $\mathbb{G}^\circ$ and $[\mathbb{G}^\circ, \mathbb{G}^\circ]$ are $\mathbb{Q}$-groups, and the quotient map $\mathbb{G}^\circ \xrightarrow{f} \mathbb{G}^\circ/[\mathbb{G}^\circ, \mathbb{G}^\circ]$ is a $\mathbb{Q}$-homomorphism. Therefore $\mathbb{G}^\circ/[\mathbb{G}^\circ, \mathbb{G}^\circ]$ can be viewed as a $\mathbb{Q}$-subgroup of $(\mathrm{GL}_{n'})_{\mathbb{Q}}$ such that first the quotient map f induces a $\mathbb{Q}$-homomorphism from $\mathbb{G}$ to $(\mathrm{GL}_{n'})_{\mathbb{Q}}$ and second $f(\Gamma^\circ) \subseteq \mathrm{GL}_{n'}(\mathbb{Z}[1/q_0])$. So there is an integer q' such that for any prime p we have $\|f(\gamma) - I\|_p \leq |q'|_p^{-1} \|\gamma - I\|_p$. Therefore f induces an

epimorphism from $\pi_{q_i}(\Gamma^\circ)/[\pi_{q_i}(\Gamma^\circ), \pi_{q_i}(\Gamma^\circ)]$ onto $\pi_{q_i/\gcd(q_i,q')}(f(\Gamma^\circ))$. Hence for any i we have

$$|\pi_{q_i/\gcd(q_i,q')}(f(\Gamma^\circ))| < C.$$

Since $f(\Gamma^\circ)$ is a Zariski-dense subset of $\mathbb{G}^\circ/[\mathbb{G}^\circ, \mathbb{G}^\circ]$ and modulo arbitrarily large integers it has at most C elements, we have that $\mathbb{G}^\circ/[\mathbb{G}^\circ, \mathbb{G}^\circ]$ is finite. So by the connectedness we have that $\mathbb{G}^\circ$ is perfect. $\qquad\square$

2.3. **A few reductions.** In this section, we make a few reductions and describe the group structure of $\pi_Q(\Gamma)$ using strong approximation [Nor89].

Lemma 11. *It is enough to prove the sufficiency part of Theorem 1 under the following additional assumptions on the Zariski-closure $\mathbb{G}$ of Γ in $(\mathrm{GL}_{n_0})_\mathbb{Q}$:*

There are connected, simply-connected, semisimple $\mathbb{Q}$-group $\mathbb{G}_s$, and unipotent $\mathbb{Q}$-group $\mathbb{U}$ such that $\mathbb{G}_s$ acts on $\mathbb{U}$ and $\mathbb{G} \simeq \mathbb{G}_s \ltimes \mathbb{U}$.

Proof. A similar argument as in the proof of [SG, Lemma 18] works here. For the convenience of the reader, we present an outline of the proof.

By the assumption, $\mathbb{G}^\circ$ is a perfect group. Therefore the radical $\mathbb{U}$ of $\mathbb{G}^\circ$ is unipotent. Let $\mathbb{G}_s$ be a Levi subgroup of $\mathbb{G}^\circ$, $\widetilde{\mathbb{G}}_s$ be the simply-connected cover of $\mathbb{G}_s$, and $\iota : \widetilde{\mathbb{G}}_s \ltimes \mathbb{U} \to \mathbb{G}_s \ltimes \mathbb{U} = \mathbb{G}^\circ$ be the induced covering map. To lift the problem to $\widetilde{\mathbb{G}}$, we consider

$$\widetilde{\Lambda} := \iota^{-1}(\Gamma \cap \mathbb{G}^\circ(\mathbb{Q})) \cap \widetilde{\mathbb{G}}(\mathbb{Q}),$$

and $\Lambda := \iota(\widetilde{\Lambda})$. Since $\mathbb{G}^\circ(\mathbb{Q})/\iota(\widetilde{\mathbb{G}}(\mathbb{Q}))$ is a torsion abelian group and Γ is a finitely generated group, we have that Λ is a normal finite index subgroup of Γ. Therefore by [SG, Corollary 17] we have that Λ has a finite symmetric generating set Ω' and for any family of positive integers $\mathcal{C}$ we have that $\{\mathrm{Cay}(\pi_q(\Gamma), \pi_q(\Omega))\}_{q \in \mathcal{C}}$ is a family of expanders if and only if $\{\mathrm{Cay}(\pi_q(\Lambda), \pi_q(\Omega'))\}_{q \in \mathcal{C}}$ is a family of expanders.

Let us fix an embedding $f : \widetilde{\mathbb{G}} \to (\mathrm{GL}_{n_0'})_\mathbb{Q}$. Since $\Gamma \subseteq \mathrm{GL}_{n_0}(\mathbb{Z}[1/q_0])$, after passing to a (normal) finite index subgroup of Λ, if needed, we can and will assume that $f(\widetilde{\Lambda}) \subseteq \mathrm{GL}_{n_0'}(\mathbb{Z}[1/q_0])$. Since ι is an isogeny defined over $\mathbb{Q}$, there is $q_0' \in \mathbb{Z}$ such that for any positive integer q and $\gamma \in \widetilde{\Lambda}$ we have

$$\pi_q(f(\gamma)) = 1 \ \text{ implies } \ \pi_{q/\gcd(q_0',q)}(\iota(\gamma)) = 1.$$

Hence $\pi_q(\widetilde{\Lambda})$ maps onto $\pi_{q/\gcd(q,q_0')}(\Lambda)$ via the map induced by ι. Therefore if Theorem 1 is proved for the group $\widetilde{\Lambda} \subseteq \mathrm{GL}_{n_0'}(\mathbb{Z}[1/q_0])$, we get the desired result for the group Γ. Hence we can focus on the group $\widetilde{\Lambda}$ which is Zariski-dense in $\widetilde{\mathbb{G}}$; and the claim follows. $\qquad\square$

Lemma 12. *Let $\mathcal{G}$ and $\mathbb{G}$ be the Zariski-closure of Γ in $(\mathrm{GL}_{n_0})_{\mathbb{Z}[1/q_0]}$ and $(\mathrm{GL}_{n_0})_\mathbb{Q}$, respectively. Let $\mathbb{G}_s$ be a semisimple $\mathbb{Q}$-subgroup of $\mathbb{G}$, and $\mathbb{U}$ be a unipotent $\mathbb{Q}$-subgroup of $\mathbb{G}$ such that $\mathbb{G} = \mathbb{G}_s \ltimes \mathbb{U}$.*

It is enough to prove the sufficiency part of Theorem 1 under the following additional assumptions on the closure $\widehat{\Gamma}$ of Γ in $\prod_{p \nmid q_0} \mathrm{GL}_{n_0}(\mathbb{Z}_p)$:

(1) *$\widehat{\Gamma} = \prod_{p \nmid q_0} P_p$ is an open compact subgroup of $\prod_{p \nmid q_0} \mathcal{G}(\mathbb{Z}_p)$.*

(2) *For some non-negative integer q_0' and any prime $p \nmid q_0$, we have $P_p = \mathbb{G}(\mathbb{Q}_p) \cap \mathrm{GL}_{n_0}(\mathbb{Z}_p)[p^{k_p}]$, where $k_p := v_p(q_0')$ and $\mathrm{GL}_{n_0}(\mathbb{Z}_p)[p^{k_p}] := \{g \in \mathrm{GL}_{n_0}(\mathbb{Z}_p)| \ \|g - 1\|_p \le p^{-k_p}\}$. And $P_p = K_p \ltimes U_p$ where $K_p := \mathbb{G}_s(\mathbb{Q}_p) \cap \mathrm{GL}_{n_0}(\mathbb{Z}_p)[p^{k_p}]$, $U_p := \mathbb{U}(\mathbb{Q}_p) \cap \mathrm{GL}_{n_0}(\mathbb{Z}_p)[p^{k_p}]$.*

(3) *There is a prime p_0 such that, for $p \ge p_0$, $K_p = \mathbb{G}_s(\mathbb{Q}_p) \cap \mathrm{GL}_{n_0}(\mathbb{Z}_p)$ is a hyperspecial parahoric subgroup of $\mathbb{G}_s(\mathbb{Q}_p)$, and $U_p = \mathbb{U}(\mathbb{Q}_p) \cap \mathrm{GL}_{n_0}(\mathbb{Z}_p)$.*

(4) *For $p \ge p_0$, the dimension of any non-trivial irreducible representation of $\pi_p(\Gamma) \simeq \mathcal{G}(\mathfrak{f}_p)$ is at least $|\pi_p(\Gamma)|^{O_{\dim \mathbb{G}}(1)}$.*

Proof. By [SG, Corollary 17], we are allowed to pass to a finite-index subgroup of Γ if needed. By Lemma 11 we can and will assume that $\mathbb{G}$ is connected, simply-connected, and perfect. Hence by Strong approximation

we have that $\widehat{\Gamma}$ is an open subgroup of $\prod_{p \nmid q_0} \mathcal{G}(\mathbb{Z}_p)$ (see [Nor89, Theorem 5.4]). So passing to a finite-index subgroup we get part 1. By [Tit79, Section 3.8], for large enough p, K_p is a hyperspecial parahoric. (See the same reference for the definition of hyperspecial; here we use the property that $\pi_p(K_p)$ is a product of quasi-simple groups where the number of factors and their ranks are bounded by $\dim \mathbb{G}_s$.) Since the action of $\mathbb{G}_s$ on $\mathbb{U}$ is defined over $\mathbb{Q}$, one gets the other claims of part 2 and part 3. Moreover, for large enough p, $\pi_p(\Gamma) = \pi_p(K_p) \ltimes \pi_p(U_p)$ is a perfect group. Hence by [SGV12, Corollary 14] the restriction of any non-trivial representation ρ of $\pi_p(\Gamma)$ to $\pi_p(K_p)$ is non-trivial. Since K_p is hyperspecial, $\pi_p(K_p)$ is a product of quasi-simple groups where the number of factors and their ranks are bounded by $\dim \mathbb{G}_s$. Therefore by [LS74] we have $\dim \rho \geq |\pi_p(K_p)|^{O_{\dim \mathbb{G}_s}(1)} \geq |\pi_p(\Gamma)|^{O_{\dim \mathbb{G}}(1)}$. $\qquad\square$

We notice that the restriction of π_q to Γ factors through $\widehat{\Gamma}$, and so

$$\pi_{\prod_i p_i^{n_i}}(\Gamma) \simeq \prod_i \pi_{p_i^{n_i}}(P_{p_i}) \simeq \prod_i \pi_{p_i^{n_i}}(K_{p_i}) \ltimes \pi_{p_i^{n_i}}(U_{p_i}).$$

2.4. **Algebraic homomorphisms and the congruence maps.** In this section, an auxiliary result on the relation between the congruence maps and $\mathbb{Q}$-group homomorphisms is proved (see Lemma 13). This relation is crucial for reducing the proof of the main theorem to the case where the unipotent radical is abelian.

Here is a general formulation of the issue (without a reference to affine group schemes): suppose $\mathbb{H}_1 \subseteq (\mathrm{GL}_{n_1})_{\mathbb{Q}}$ and $\mathbb{H}_2 \subseteq (\mathrm{GL}_{n_2})_{\mathbb{Q}}$ are given, and $\rho : \mathbb{H}_1 \to \mathbb{H}_2$ is a $\mathbb{Q}$-group homomorphism. For any positive integer q and $i = 1, 2$, let π_q be the induced group homomorphism on $\prod_p \mathrm{GL}_{n_i}(\mathbb{Z}_p)$. For any prime p, let $H_{i,p} := \mathbb{H}_i(\mathbb{Q}_p) \cap \mathrm{GL}_{n_i}(\mathbb{Z}_p)$. One would like to have that ρ and π_q *commute*; that means the following (wrong) isomorphism

$$(7) \qquad\qquad \pi_q(\rho(\prod_p H_{1,p})) \simeq \rho(\pi_q(\prod_p H_{1,p})).$$

Equation (7) has two issues: (a) $\rho(\prod_p H_{1,p})$ is not necessarily a subgroup of $\prod_p H_{2,p}$, and so it does not make sense to talk about its congruence quotient, (b) ρ is defined by polynomials with *rational* coefficients that are not necessarily integer. So it does not make sense to talk about ρ of the finite group $\pi_q(\prod_p H_{1,p})$.

In Lemma 13 under the assumption that ρ is surjective with a $\mathbb{Q}$-section, an *almost commuting* of ρ and π_q is proved; in particular, it is proved that, if q does not have small prime factors, then the isomorphism in Equation (7) holds.

The main ingredient in the proof of Lemma 13 is the fact that a $\mathbb{Q}$-homomorphism $\rho : \mathbb{H}_1 \to \mathbb{H}_2$ between two algebraic $\mathbb{Q}$-groups $\mathbb{H}_1$ and $\mathbb{H}_2$ induces a continuous homomorphism between the adelic points $\mathbb{H}_1(\mathbb{A}_{\mathbb{Q}})$ and $\mathbb{H}_2(\mathbb{A}_{\mathbb{Q}})$.

After proving Lemma 13, it will be used for the quotient maps $\rho_1 : \mathbb{G} \to \mathbb{G}_s$ and $\rho_2 : \mathbb{G} \to \mathbb{G}_s \ltimes \mathbb{U}/[\mathbb{U}, \mathbb{U}]$ where $\mathbb{G}_s$ is a Levi $\mathbb{Q}$-subgroup of $\mathbb{G}$, and $\mathbb{U}$ is the unipotent radical of $\mathbb{G}$.

Lemma 13. *Let $\mathbb{H} \subseteq (\mathrm{GL}_{n_1})_{\mathbb{Q}}$ be a $\mathbb{Q}$-subgroup (with a given embedding). Let $\rho : \mathbb{H} \to (\mathrm{GL}_{n_2})_{\mathbb{Q}}$ be a $\mathbb{Q}$-homomorphism. Then the following hold.*

(1) *There is $g \in \mathrm{GL}_{n_2}(\mathbb{Q})$ such that $\rho(\mathbb{H}(\mathbb{Q}) \cap \mathrm{GL}_{n_1}(\mathbb{Z}[1/q_0])) \subseteq g \, \mathrm{GL}_{n_2}(\mathbb{Z}[1/q_0]) g^{-1}$.*

(2) *There is a positive integer q' such that for any prime p and any $h \in \mathbb{H}(\mathbb{Q}_p)$ we have*

$$\|\rho(h) - 1\|_p \leq |q'|_p^{-1} \|h - 1\|_p.$$

(3) *Let $1 \to \mathbb{L} \to \mathbb{H} \xrightarrow{\rho} \bar{\mathbb{H}} \to 1$ be a short exact sequence of $\mathbb{Q}$-groups. Suppose there is a $\mathbb{Q}$-section $s : \bar{\mathbb{H}} \to \mathbb{H}$ such that $s(1) = 1$. Let q_0' be a positive integer and $k_p := v_p(q_0')$. For any prime $p \nmid q_0$, let $Q_p = \mathbb{H}(\mathbb{Q}_p) \cap (1 + q_0' \mathfrak{gl}_{n_1}(\mathbb{Z}_p)) = \{h_p \in \mathbb{H}(\mathbb{Q}_p) | \, \|h_p - 1\| \leq p^{-k_p}\}$. Assume that $\rho(Q_p) \subseteq \mathrm{GL}_{n_2}(\mathbb{Z}_p)$,*

and $s(\rho(Q_p)) \subseteq \mathrm{GL}_{n_1}(\mathbb{Z}_p)$ for any prime $p \nmid q_0$. Then there is a positive integer $q' := \prod_p p^{k'_p}$ such that for non-negative integers $n_p \geq k'_p + k_p$ we have

$$(8) \qquad \prod_{p \nmid q_0} \pi_{p^{n_p + k'_p}}(Q_p)/\pi_{p^{n_p + k'_p}}(\mathbb{L}(\mathbb{Q}_p) \cap Q_p) \twoheadrightarrow \prod_{p \nmid q_0} \pi_{p^{n_p}}(\rho(Q_p)) \twoheadrightarrow \prod_{p \nmid q_0} \pi_{p^{n_p - k'_p}}(Q_p)/\pi_{p^{n_p - k'_p}}(\mathbb{L}(\mathbb{Q}_p) \cap Q_p).$$

Proof. For any p there is $g_p \in \mathrm{GL}_{n_2}(\mathbb{Q}_p)$ such that $g_p \rho(\mathbb{H}(\mathbb{Q}_p) \cap \mathrm{GL}_{n_1}(\mathbb{Z}_p)) g_p^{-1} \subseteq \mathrm{GL}_{n_2}(\mathbb{Z}_p)$. Since ρ is defined over $\mathbb{Q}$, for large enough p, we can assume that $g_p = 1$. Hence there is $\widehat{g} = (g_p) \in \mathrm{GL}_{n_2}(\mathbb{A}_{\mathbb{Q}})$ such that

$$\widehat{g}\Delta(\rho(\mathbb{H}(\mathbb{Q}) \cap \mathrm{GL}_{n_1}(\mathbb{Z}[1/q_0])))\widehat{g}^{-1} \subseteq \mathrm{GL}_{n_2}(\mathbb{R}) \prod_{p \mid q_0} \mathrm{GL}_{n_2}(\mathbb{Q}_p) \prod_{p \nmid q_0} \mathrm{GL}_{n_2}(\mathbb{Z}_p),$$

where Δ is the diagonal embedding. On the other hand, we have

$$\mathrm{GL}_{n_2}(\mathbb{A}_{\mathbb{Q}}) = \Delta(\mathrm{GL}_{n_2}(\mathbb{Q})) \cdot \left(\mathrm{GL}_{n_2}(\mathbb{R}) \prod_{p \mid q_0} \mathrm{GL}_{n_2}(\mathbb{Q}_p) \prod_{p \nmid q_0} \mathrm{GL}_{n_2}(\mathbb{Z}_p) \right).$$

So there is $g \in \mathrm{GL}_{n_2}(\mathbb{Q})$ such that

$$\Delta(g\rho(\mathbb{H}(\mathbb{Q}) \cap \mathrm{GL}_{n_1}(\mathbb{Z}[1/q_0]))g^{-1}) \subseteq \left(\mathrm{GL}_{n_2}(\mathbb{R}) \prod_{p \mid q_0} \mathrm{GL}_{n_2}(\mathbb{Q}_p) \prod_{p \nmid q_0} \mathrm{GL}_{n_2}(\mathbb{Z}_p) \right) \cap \Delta(\mathrm{GL}_{n_2}(\mathbb{Q}))$$

$$= \Delta(\mathrm{GL}_{n_2}(\mathbb{Z}[1/q_0])),$$

which gives us the first part.

The second part is an easy consequence of the fact that ρ can be represented by a polynomial with rational coefficients. Similarly there is a positive integer q' such that

$$(9) \qquad |q'|_p \|s(\rho(h_p)) - 1\|_p \leq \|\rho(h_p) - 1\|_p \leq |q'|_p^{-1} \|h_p - 1\|_p,$$

for any prime p and $h_p \in \mathbb{H}(\mathbb{Q}_p)$. On the other hand,

$$(10) \qquad h_p \in \ker(\pi_{p^n} \circ \rho) \text{ if and only if } \|\rho(h_p) - 1\|_p \leq p^{-n}.$$

These imply that for $h_p \in \ker(\pi_{p^n} \circ \rho)$ we have $\pi_{p^{n-k'_p}}(s(\rho(h_p))) = 1$. And so if $h_p \in Q_p$ and $\pi_{p^n}(\rho(h_p)) = 1$, then we have

$$(11) \qquad h_p = (h_p s(\rho(h_p))^{-1}) \cdot s(\rho(h_p)) \in (\mathbb{L}(\mathbb{Q}_p) \cap Q_p) \ker \pi_{p^{n-k'_p}}.$$

Let $\widetilde{\phi}_1 : Q_p \to \pi_{p^{n_p - k'_p}}(Q_p)/\pi_{p^{n_p - k'_p}}(\mathbb{L}(\mathbb{Q}_p) \cap Q_p), \widetilde{\phi}_1(h_p) := \pi_{p^{n_p - k'_p}}(h_p)\pi_{p^{n_p - k'_p}}(\mathbb{L}(\mathbb{Q}_p) \cap Q_p)$. Then clearly $\widetilde{\phi}_1$ is surjective. By (11), $\widetilde{\phi}_1$ factors through $\pi_{p^{n_p}}(\rho(Q_p))$; that means

$$\pi_{p^{n_p}}(\rho(Q_p)) \twoheadrightarrow \pi_{p^{n_p - k'_p}}(Q_p)/\pi_{p^{n_p - k'_p}}(\mathbb{L}(\mathbb{Q}_p) \cap Q_p).$$

Let $\widetilde{\phi}_2 : Q_p \to \pi_{p^{n_p}}(\rho(Q_p)), \widetilde{\phi}_2(h_p) := \pi_{p^{n_p}}(\rho(h_p))$. So clearly $\widetilde{\phi}_2$ is surjective. By (9) and (10), we have, if $\pi_{p^{n_p + k'_p}}(h_p) = 1$, then $\|\rho(h_p) - 1\|_p \leq |q'|_p^{-1}\|h_p - 1\|_p \leq p^{k'_p}p^{-n_p - k'_p} = p^{-n_p}$; and so $h_p \in \ker \widetilde{\phi}_2$. Therefore $\widetilde{\phi}_2$ factors through $\pi_{p^{n_p + k'_p}}(Q_p)$. By the definition of $\widetilde{\phi}_2$ we have $\mathbb{L}(\mathbb{Q}_p) \cap Q_p \subseteq \ker \widetilde{\phi}_2$. Hence we get a surjection $\pi_{p^{n_p + k'_p}}(Q_p)/\pi_{p^{n_p + k'_p}}(\mathbb{L}(\mathbb{Q}_p) \cap Q_p) \twoheadrightarrow \pi_{p^{n_p}}(\rho(Q_p))$. The claim follows. $\square$

Let $\mathbb{G}_s$ be a simply connected semisimple $\mathbb{Q}$-group which acts on a unipotent $\mathbb{Q}$-group $\mathbb{U}$. Then by the virtue of the proof of [SGV12, Corollary 14] $\mathbb{G} = \mathbb{G}_s \ltimes \mathbb{U}$ is a perfect group if and only if $\mathbb{G}_s \ltimes \mathbb{U}/[\mathbb{U}, \mathbb{U}]$ is perfect. On the other hand, $\mathbb{V} := \mathbb{U}/[\mathbb{U}, \mathbb{U}]$ is a vector $\mathbb{Q}$-group, and the action of $\mathbb{G}_s$ on $\mathbb{U}$ induces a representation $\phi_0 : \mathbb{G}_s \to \mathbb{GL}(\mathbb{V})$ defined over $\mathbb{Q}$. And $\mathbb{G}_s \ltimes \mathbb{V}$ is perfect if and only if the trivial representation is not a subrepresentation of ϕ_0. Consider the following short exact sequences of $\mathbb{Q}$-algebraic groups

$$(12) \qquad 1 \to \mathbb{U} \to \mathbb{G} \xrightarrow{\rho_1} \mathbb{G}_s \to 1 \qquad \text{and} \qquad 1 \to [\mathbb{U}, \mathbb{U}] \to \mathbb{G} \xrightarrow{\rho_2} \mathbb{G}_s \ltimes \mathbb{V} \to 1.$$

We notice that, since the $\mathbb{U}$ is a $\mathbb{Q}$-unipotent group, there is a $\mathbb{Q}$-section from $\mathbb{V}$ to $\mathbb{U}$, which can be extended to a $\mathbb{Q}$-section for the second exact sequence of (12). The first exact sequence clearly splits. We fix certain $\mathbb{Q}$-embeddings $\mathbb{G}_s \subseteq \mathbb{G} \subseteq (\mathrm{GL}_{n_1})_{\mathbb{Q}}$ and $\mathbb{G}_s \ltimes \mathbb{V} \subseteq (\mathrm{GL}_{n_2})_{\mathbb{Q}}$. Let $\Gamma \subseteq \mathbb{G} \cap \mathrm{GL}_{n_1}(\mathbb{Z}[1/q_0])$ be a Zariski-dense subgroup. Then by Lemma 13 after passing to a finite index subgroup, if necessary, we can assume that $\rho_2(\Gamma) \subseteq \mathrm{GL}_{n_2}(\mathbb{Z}[1/q_0])$. By the above comment, we are also allowed to use (8) in Lemma 13 for the p-adic closure of Γ in $\mathbb{G}(\mathbb{Q}_p)$ for any $p \nmid q_0$.

2.5. **Ping-pong players.** As in [SGV12, SG], we work with a Zariski-dense free subgroup of Γ. Following [SG, Proposition 22], using [SGV12, Proposition 7, Proposition 17, Proposition 20] we get the following.

Proposition 14. *Let Ω be a finite symmetric subset of $\mathrm{GL}_n(\mathbb{Q})$ which generates a Zariski-dense subgroup Γ of a Zariski-connected perfect group $\mathbb{G}$. Then there are a finite subset $\overline{\Omega'}$ of Γ and $\delta_0 > 0$ and l_0 (which depend on Ω) such that $\overline{\Omega'}$ freely generates a Zariski-dense subgroup of $\mathbb{G}(\mathbb{Q})$ and*

$$(13) \qquad\qquad \mathcal{P}_{\Omega'}^{(l)}(\mathbb{H}(F)) \le e^{-\delta_0 l}$$

for any field extension $F/\mathbb{Q}$, and any proper subgroup $\mathbb{H} \subsetneq \mathbb{G} \times_{\mathbb{Q}} F$ and $l \ge l_0$, where $\Omega' = \overline{\Omega'} \cup \overline{\Omega'}^{-1}$ and $\mathcal{P}_{\Omega'}$ is the probability counting measure on Ω'. Moreover, $\mathrm{Ad}(\rho_1(\overline{\Omega'}))$ freely generates a subgroup of $\mathrm{Ad}(\mathbb{G}_s(\mathbb{Q}))$, where $\rho_1 : \mathbb{G} \to \mathbb{G}_s$ is the quotient map; in particular, $\ker(\mathrm{Ad} \circ \rho_1) \cap \langle \Omega' \rangle = \{1\}$.

Proof. This is essentially proved in [SGV12, Proposition 7, Proposition 17, Proposition 20]. Here is an outline of the argument.

By [SGV12, Proposition 17] there are irreducible representations η_i of $\mathbb{G} :\to \mathbb{GL}(\mathbb{W}_i)$ defined over local fields F_i and algebraic deformations $\phi_{i,v} : \mathbb{G} \to \mathrm{Aff}(\mathbb{W}_i)$ of η_i where the parameter v varies in an affine space $\mathbb{V}_i$ with the following properties:

(1) for any i, η_i factors through $\mathbb{G}_s$, and at least one of them factors through $\mathrm{Ad}(\mathbb{G}_s)$;
(2) for any i, $\eta_i(\Gamma) \subseteq \mathrm{GL}(\mathbb{W}_i(F_i))$ is unbounded;
(3) the linear part of $\phi_{i,v}$ is η_i for any $v \in \mathbb{V}_i(F_i)$;
(4) for any non-zero vector v, the affine action of $\mathbb{G}(F_i)$ on $\mathbb{W}_i(F_i)$ via $\phi_{i,v}$ has no fixed point;
(5) for any proper algebraic subgroup $\mathbb{H}$ of $\mathbb{G}$ for some i either
   (a) there is a non-zero vector $w \in \mathbb{W}_i(F_i)$ such that $\eta_i(\mathbb{H}(F_i))[w] = [w]$ where $[w]$ is the line $F_i w$, or
   (b) there is a parameter $v \in \mathbb{V}_i(F_i)$ of norm 1 and a point $w \in \mathbb{W}_i(F_i)$ such that w is fixed by $\mathbb{H}$ under the affine action of $\mathbb{G}$ on $\mathbb{W}_i$ given by $\phi_{i,v}$.

By [SGV12, Proposition 20 and Proposition 21], there is a finite subset $\overline{\Omega'} \subseteq \Gamma$ such that

(1) for any i, $\eta_i(\overline{\Omega'})$ freely generates a subgroup of $\eta_i(\Gamma)$; in particular $\mathrm{Ad}(\rho_1(\overline{\Omega'}))$ freely generates a subgroup of $\mathrm{Ad}(\mathbb{G}_s(\mathbb{Q}))$ where $\rho_1 : \mathbb{G} \to \mathbb{G}_s$ is the projection to the semisimple part.
(2) there is $c_0 > 0$ such that, for any index i, and non-zero vector $w_0 \in \mathbb{W}_i(F_i)$, we have

$$|\{\gamma \in B_l(\overline{\Omega'}) \mid \eta_i(\gamma)[w_0] = [w_0]\}| \le |B_l(\overline{\Omega'})|^{1-c_0},$$

and, for any point $w_1 \in \mathbb{W}_i(F_i)$, and parameter $v_i \in \mathbb{V}_i(F_i)$ with norm one,

$$|\{\gamma \in B_l(\overline{\Omega'}) \mid \phi_{i,v}(\gamma)(w_1) = (w_1)\}| \le |B_l(\overline{\Omega'})|^{1-c_0},$$

where $B_l(\overline{\Omega'})$ is the the set of reduced words over $\overline{\Omega'}$ of length l.

Hence, by the above geometric description of proper algebraic subgroups, for any proper algebraic subgroup $\mathbb{H}$ of $\mathbb{G}$ we have

$$|B_l(\overline{\Omega'}) \cap \mathbb{H}(\mathbb{Q})| < |B_l(\overline{\Omega'})|^{1-c_0}.$$

Let $\Omega' := \overline{\Omega'} \cup \overline{\Omega'}^{-1}$. By a result of Kesten [Kes59, Theorem 3] we have $\mathcal{P}_{\Omega'}^{(l)}(I) \leq \left(\frac{2|\overline{\Omega'}|-1}{|\overline{\Omega'}|^2}\right)^l$, where I is the identity matrix. As Ω' is symmetric, we have $\mathcal{P}_{\Omega'}^{(2l)}(I) = \sum_\gamma \mathcal{P}_{\Omega'}^{(l)}(\gamma)^2$. Hence together with the Kesten bound we have

$$(14) \qquad \mathcal{P}_{\Omega'}^{(l)}(\gamma) \leq \mathcal{P}_{\Omega'}^{(2l)}(I) \leq \left(\frac{2|\overline{\Omega'}|-1}{|\overline{\Omega'}|^2}\right)^l.$$

We also notice that, since the random-walk in the group generated by Ω' with respect to the probability counting measure $\mathcal{P}_{\Omega'}$ on Ω' can be identified with the random-walk on a regular tree, $\mathcal{P}_{\Omega'}^{(l)}$ is constant on the set $B_k(\overline{\Omega'})$ of reduced words in $\overline{\Omega'}$ of length k for any positive integer k. Let $p_{l,k} := \mathcal{P}_{\Omega'}^{(l)}(\gamma)$ for some $\gamma \in B_k(\overline{\Omega'})$.

For a proper subgroup $\mathbb{H}$ of $\mathbb{G} \times_{\mathbb{Q}} F$, let $\overline{\overline{\mathbb{H}}}$ be the Zariski-closure of $\Gamma \cap \mathbb{H}(F)$ in $\mathbb{G}$. Then $\overline{\overline{\mathbb{H}}}$ is a subgroup of $\mathbb{G}$ and $\mathcal{P}_{\Omega'}^{(l)}(\mathbb{H}(F)) = \mathcal{P}_{\Omega'}^{(l)}(\overline{\overline{\mathbb{H}}}(\mathbb{Q}))$. Now we can finish the argument as in the proof of [SGV12, Proposition 7]:

$$\mathcal{P}_{\Omega'}^{(l)}(\mathbb{H}(F)) = \mathcal{P}_{\Omega'}^{(l)}(\overline{\overline{\mathbb{H}}}(\mathbb{Q})) = \sum_{k \geq 0} |B_{\overline{\Omega'}}(k) \cap \overline{\overline{\mathbb{H}}}(\mathbb{Q})| \, p_{l,k}$$

$$\leq \left(\sum_{0 \leq k < l/10} (2|\overline{\Omega'}|)^k\right) \left(\frac{2|\overline{\Omega'}|-1}{|\overline{\Omega'}|^2}\right)^l + (2|\overline{\Omega'}|-1)^{-c_0 l/10} \sum_{k \geq l/10} |B_k(\overline{\Omega'})| p_{l,k}$$

$$\leq \frac{(2|\overline{\Omega'}|)^{l/10}}{(|\overline{\Omega'}|/2)^l} + (2|\overline{\Omega'}|-1)^{-c_0 l/10} \leq e^{-\delta_0 l},$$

for some δ_0 and any $l \geq l_0$ where l_0 is a fixed positive integer. $\qquad \square$

Lemma 15. *Let Ω be a finite symmetric subset of $\mathrm{GL}_{n_0}(\mathbb{Z}[1/q_0])$ and $\Gamma = \langle \Omega \rangle$. Assume the Zariski-closure $\mathbb{G}$ of Γ is a connected, simply connected, perfect $\mathbb{Q}$-group. Suppose $\Omega' \subseteq \Gamma$ is a finite symmetric set which generates a Zariski-dense subgroup Λ of $\mathbb{G}$. Then for any set of positive integers $\mathcal{C}$ consisting of integers coprime to q_0 if $\{\mathrm{Cay}(\pi_q(\Lambda), \pi_q(\Omega'))\}_{q \in \mathcal{C}}$ is a family of expanders, then $\{\mathrm{Cay}(\pi_q(\Gamma), \pi_q(\Omega))\}_{q \in \mathcal{C}}$ is a family of expanders.*

Proof. By Nori's strong approximation (see [Nor89, Theorem 5.4]), we have that the closure $\widehat{\Lambda}$ of Λ in $\prod_{p \nmid q_0} \mathrm{GL}_{n_0}(\mathbb{Z}_p)$ is of finite index in the closure $\widehat{\Gamma}$ of Γ in $\prod_{p \nmid q_0} \mathrm{GL}_{n_0}(\mathbb{Z}_p)$. For any q, any representation ρ of $\pi_q(\Gamma)$ can be viewed as a representation of $\widehat{\Gamma}$. The extension of ρ to $\widehat{\Gamma}$ is denoted by ρ too. Only finitely many of them have $\widehat{\Lambda}$ in their kernel. Hence the restriction to Λ of only finitely many such representation is trivial. Let ρ be an irreducible representation of $\pi_q(\Gamma)$ whose restriction to Λ is not trivial. Hence the restriction of ρ to Λ is a subrepresentation of $L^2(\pi_q(\Lambda))^\circ := \{f \in L^2(\pi_q(\Lambda))| \sum_{g \in \pi_q(\Lambda)} f(g) = 0\}$.

Let $u \in V_\rho$ be a unit vector which is an ε-almost invariant vector with respect to Ω; that means

$$\|\rho(\gamma)(u) - u\| < \varepsilon,$$

for any $\gamma \in \Omega$. Since Ω generates Γ and $\Omega' \subseteq \Gamma$, for some r_0 we have $\Omega' \subseteq \prod_{r_0} \Omega$. Thus for any $\lambda \in \Omega'$ we have

$$\|\rho(\lambda)(u) - (u)\| < r_0 \varepsilon.$$

Assuming $\{\mathrm{Cay}(\pi_q(\Lambda), \pi_q(\Omega'))\}_{q \in \mathcal{C}}$ is a family of expanders, there is $\varepsilon_0 > 0$ such that

$$\max_{\lambda \in \Omega'} \|\rho(\lambda)(u) - u\| > \varepsilon_0.$$

Therefore $\varepsilon > \varepsilon_0/r_0$, which implies that no non-trivial irreducible representation of $\pi_q(\Gamma)$ (for $q \in \mathcal{C}$) has an ε'-almost invariant vector for some $\varepsilon' > 0$. $\qquad \square$

Corollary 16. *It is enough to prove the sufficiency part of Theorem 1 under the additional assumptions:*

(1) $\Omega = \overline{\Omega} \cup \overline{\Omega}^{-1}$ *where* $\mathrm{Ad}(\rho_1(\overline{\Omega}))$ *freely generates a Zariski-dense subgroup of* $\mathrm{Ad}(\mathbb{G}_s)$.

(2) *For any field extension $F/\mathbb{Q}$ and proper subgroup $\mathbb{H}$ of $\mathbb{G} \times_{\mathbb{Q}} F$, (13) holds.*

Remark 17. *Notice that by changing Ω, the closure Γ_p of Γ in $\mathrm{GL}_{n_0}(\mathbb{Z}_p)$ is of the form described in Lemma 12 only for large enough p. For small primes Γ_p is still an open subgroup of $\mathbb{G}(\mathbb{Q}_p)$.*

2.6. **Summary of the initial reductions.** In the rest of the article, (unless it is explicitly mentioned otherwise) we assume that $\Omega \subseteq \mathrm{GL}_{n_0}(\mathbb{Z}[1/q_0])$ is a finite symmetric set, and set $\Gamma = \langle \Omega \rangle$. And let $\mathcal{G}$ and $\mathbb{G}$ be the Zariski-closure of Γ in $(\mathrm{GL}_{n_0})_{\mathbb{Z}[1/q_0]}$ and $(\mathrm{GL}_{n_0})_{\mathbb{Q}}$, respectively.

(1) (Zariski closure) By Lemma 11, we can and will assume that $\mathbb{G}$ is a connected, simply connected, perfect group. We let $\mathbb{G}_s$ be a Levi $\mathbb{Q}$-subgroup of $\mathbb{G}$, and $\mathbb{U}$ be the unipotent radical of $\mathbb{G}$.

(2) (Adelic closure) By Lemma 12 and Remark 17, we can and will assume that the closure $\widehat{\Gamma}$ of Γ in $\prod_{p \nmid q_0} \mathrm{GL}_{n_0}(\mathbb{Z}_p)$ is an open subgroup of $\prod_{p \nmid q_0} \mathbb{G}(\mathbb{Q}_p)$ which contains a finite index subgroup of the form $\prod_{p \nmid q_0} P_p$ where $P_p = K_p \ltimes U_p$ and K_p and U_p satisfy the properties mentioned in Lemma 12. In particular, $P_p = \mathbb{G}(\mathbb{Q}_p) \cap \mathrm{GL}_{n_0}(\mathbb{Z}_p)[p^{k_p}]$, $K_p = \mathbb{G}_s(\mathbb{Q}_p) \cap \mathrm{GL}_{n_0}(\mathbb{Z}_p)[p^{k_p}]$, and $U_p = \mathbb{U}(\mathbb{Q}_p) \cap \mathrm{GL}_{n_0}(\mathbb{Z}_p)[p^{k_p}]$ for some non-negative integers k_p that are zero for large enough p.

(3) (Generating set) We can and will assume that Ω is as in Corollary 16. In particular, $\ker(\mathrm{Ad} \circ \rho_1) \cap \Gamma = \{1\}$, and any proper algebraic subgroup of $\mathbb{G}$ intersects Γ in an *exponentially small* subset (see Inequality (13)).

2.7. **Multiplicity bound.** In order to execute Sarnak-Xue [SX91] trick, we need to have a control on the degree of irreducible representations of $\pi_q(\Gamma)$. Here we prove such a result for an arbitrary modulus q which is of independent interest.

Proposition 18. *Let $\Gamma \subseteq \mathrm{GL}_n(\mathbb{Z}[1/q_0])$ be a finitely generated group whose Zariski-closure $\mathbb{G}$ is a Zariski-connected perfect group. Suppose $\mathbb{G}$ is simply-connected; that means $\mathbb{G} = \mathbb{G}_s \ltimes \mathbb{U}$ where $\mathbb{G}_s$ is a simply-connected semisimple group and $\mathbb{U}$ is a unipotent group. Let q be an integer which is co-prime to q_0. Let $\widehat{\Gamma}$ be the closure of Γ in $\prod_{p \nmid q_0} \mathrm{GL}_n(\mathbb{Z}_p)$.*

Then there are a finite set Σ of complex irreducible representations of $\widehat{\Gamma}$ and $\delta > 0$ which depend on Γ such that the following holds.

For any complex irreducible representation ρ of $\pi_q(\Gamma)$ which does not factor through $\pi_{q'}(\Gamma)$ for any proper divisor q' of q, we have that either

(1) *The lift of ρ to $\widehat{\Gamma}$ is in Σ, or*
(2) $\dim \rho \geq |\pi_q(\Gamma)|^{\delta}$.

For a group with entries in a number field and a semisimple Zariski-closure, a similar statement is proved in [SG, Proposition 33]. An identical argument works here, but for the sake of the convenience a proof is included. It is worth pointing out that the main (behind the scene) representation theoretic tool is Howe's Kirillov theory for compact p-adic analytic groups [How77].

For any odd prime p, let $a_0(p) := 1$, and let $a_0(2) := 2$. Then $\exp : p^{a_0(p)}\mathfrak{gl}_n(\mathbb{Z}_p) \to 1 + p^{a_0(p)}\mathfrak{gl}_n(\mathbb{Z}_p)$, and log going backward, can be defined and satisfy the usual properties. Let $b_0(p) := 1$ for any prime $p \geq 5$, and let $b_0(2) = b_0(3) = 2$. Then, by Campbell-Hausdorff formula, we have that for any Lie $\mathbb{Z}_p$-subalgebra $\mathfrak{h}$ of $p^{a_0(p)}\mathfrak{gl}_n(\mathbb{Z}_p)$ we have that $\exp(\mathfrak{h})$ is a subgroup of $1 + p^{a_0(p)}\mathfrak{gl}_n(\mathbb{Z}_p)$.

Lemma 19. *Let $\mathbb{H}$ be an algebraic subgroup of $(\mathrm{GL}_n)_{\mathbb{Q}_p}$. Let $H_c := \mathbb{H}(\mathbb{Q}_p) \cap (1 + p^c \mathfrak{gl}_n(\mathbb{Z}_p))$ for any positive integer c. Let $\mathfrak{h} := \mathrm{Lie}(\mathbb{H})(\mathbb{Q}_p) \cap \mathfrak{gl}_n(\mathbb{Z}_p)$. Suppose $p^{s_0}\mathfrak{h} \subseteq [\mathfrak{h}, \mathfrak{h}]$. Let ρ be an irreducible complex representation of H_c, $c \geq b_0(p) + 1$, and*

$$m_\rho := \min\{m \in \mathbb{Z}^+ | \ H_m \subseteq \ker(\rho)\}.$$

Then $\dim \rho \geq p^{(m_\rho - 1 - c - s_0)/2}$.

Proof. Since the analytic Lie algebra of $\mathbb{H}(\mathbb{Q}_p)$ coincides with $\mathrm{Lie}(\mathbb{H})(\mathbb{Q}_p)$, we get that

$$\log : H_m \to p^m \mathfrak{h}$$

is a bijection and the exponential map is its inverse (for a detailed proof see [SGZ, Proposition 7]). We notice also that $p^{m+s_0}(p^m \mathfrak{h}) \subseteq [\mathfrak{p}^m \mathfrak{h}, \mathfrak{p}^m \mathfrak{h}] \subseteq p^m(p^m \mathfrak{h})$. Hence by [SG, Lemma 32] we have

$$\dim \rho \geq p^{(m_\rho - 1 - c - s_0)/2}.$$

$\square$

Proof of Proposition 18. Let $G_{p,m} := \mathbb{G}(\mathbb{Q}_p) \cap (1 + p^m \mathrm{GL}_n(\mathbb{Z}_p))$ for any prime p and non-negative integer m. Let $\widehat{\Gamma}$ be the closure of Γ in $\prod_{p \nmid q_0} \mathrm{GL}_n(\mathbb{Z}_p)$, let Γ_p be the closure of Γ in $\mathrm{GL}_n(\mathbb{Z}_p)$, and $\Gamma_p[p^m] := \Gamma_p \cap G_{p,m}$. As in Lemma 12, by Nori's strong approximation [Nor89, Theorem 5.4], there is a finite-index subgroup Λ of Γ such that its closure $\widehat{\Lambda}$ in $\prod_{p \nmid q_0} \mathrm{GL}_n(\mathbb{Z}_p)$ is of the form $\prod_{p \nmid q_0} \Lambda_p$, where Λ_p's satisfy the following properties.

(1) For some positive integer c_0 we have that, for any prime $p \geq c_0$, $\Lambda_p = G_{p,0}$ and it is a perfect group, and $\pi_p(\Lambda_p)$ is generated by p-elements;

(2) For any prime $p < c_0$, we have $\Lambda_p = G_{p,c(p)}$ where $c(p)$ is chosen large enough such that $\Lambda_p \subseteq G_{p,8}$.

Since $\mathbb{G}$ is perfect, $[\mathrm{Lie}(\mathbb{G})(\mathbb{Q}), \mathrm{Lie}(\mathbb{G})(\mathbb{Q})] = \mathrm{Lie}(\mathbb{G})(\mathbb{Q})$. Hence there is a positive integer s_0 such that for any prime p we have

$$p^{s_0} \mathfrak{g}_p \subseteq [\mathfrak{g}_p, \mathfrak{g}_p]$$

where $\mathfrak{g}_p := \mathrm{Lie}(\mathbb{G})(\mathbb{Q}_p) \cap \mathfrak{gl}_n(\mathbb{Z}_p)$.

Let $\rho : \pi_q(\Gamma) \to \mathrm{GL}(V)$ be a complex irreducible representation which does not factor through $\pi_{q'}(\Gamma)$ for any proper divisor q' of q. Then $V = \oplus_i \rho(g_i)W$ where W is a simple $\pi_q(\Lambda)$-module and g_i's are some elements of $\pi_q(\Gamma)$. Suppose $q = \prod_i p_i^{n_i}$ is the prime factorization of q. Since $\pi_q(\Lambda) \simeq \prod_i \pi_{p_i^{n_i}}(\Lambda_{p_i})$, there are irreducible representations $\eta_i : \Lambda_{p_i} \to \mathrm{GL}(W_i)$ such that W is isomorphic to $\otimes_i W_i$ as an $\widehat{\Lambda}$-module. In particular, $\dim W = \prod_i \dim W_i$.

Except for finitely many irreducible representations ρ of $\widehat{\Gamma}$, we have that $\widehat{\Lambda}$ acts non-trivially on V, and so $\otimes_i \eta_i$ is a non-trivial irreducible representation of $\widehat{\Lambda}$. Suppose that

$$\Sigma \supseteq \{\rho \in \mathrm{Irr}(\widehat{\Gamma}) | \ \widehat{\Lambda} \subseteq \ker(\rho)\},$$

where $\mathrm{Irr}(\widehat{\Gamma})$ is the set of all the complex irreducible representations of $\widehat{\Gamma}$.

For any i, η_i is an irreducible representation of $\Lambda_{p_i} = G_{p_i,c(p_i)}$ where $c(p_i)$ is 0 for $p \geq c_0$ and given as above for $c < p_0$. Since ρ does not factor through $\pi_{q'}(\Gamma)$ for a proper divisor q' of q, for any i we have

$$m_i := \min\{m \in \mathbb{Z}^+ | \ G_{p_i,m} \subseteq \ker(\eta_i)\} = \max\{n_i, c(p_i)\}.$$

Next we partition the indexes into five types: (1) $n_i - c(p_i) \geq 2s_0 + 2$, and $c(p_i) \geq 8$; (2) $n_i \geq 2s_0 + 10$ and $c(p_i) = 0$; (3) $1 < n_i < 2s_0 + 10$ and $p_i \geq c_0$; (4) $n_i = 1$ and $p_i \geq c_0$; and (5) $p_i < c_0$ and $n_i < 2s_0 + 10$. Now we find a lower bound for the dimension of η_i for the first three types of indexes.

Case 1. $n_i - c(p_i) \geq 2s_0 + 2$ and $c(p_i) \geq 8$.

In this case, by Lemma 19, we have

$$\dim \eta_i \geq p^{(n_i - c(p_i) - 1 - s_0)/2} \geq p^{(n_i - c(p_i))/4} = |\pi_{p_i^{n_i}}(\Lambda_{p_i})|^{\delta_1}$$

where δ_1 is a positive number which depends only on $\dim \mathbb{G}$.

Case 2. $n_i \geq 2s_0 + 10$ and $c(p_i) = 0$.

In this case, the restriction of η_i to $G_{p_i,2}$ is non-trivial. Hence by Lemma 19 we have

$$\dim \eta_i \geq p^{(n_i-2-1-s_0)/2} \geq p^{n_i/4} \geq |\pi_{p_i^{n_i}}(\Lambda_{p_i})|^{\delta_2}$$

where δ_2 is a positive number which depends only on $\dim \mathbb{G}$.

Case 3. $1 < n_i < 2s_0 + 10$ and $p \geq c_0$.

Notice that $\pi_{p_i^{n_i}}(G_{p_i,1})$ is a normal p_i-subgroup of $\pi_{p_i^{n_i}}(\Lambda_{p_i})$. Since the dimension of any irreducible representation of a p_i-group is a power of p_i, we have that either the restriction of η_i to $G_{p_i,1}$ factors through $G_{p_i,1}/[G_{p_i,1}, G_{p_i,1}]$ or $\dim \eta_i \geq p_i \geq |\pi_{p_i^{n_i}}(\Lambda_{p_i})|^{\delta_3}$, where δ_3 is a positive number which depends on $\mathbb{G}$.

Now suppose the restriction of η_i to $G_{p_i,1}$ factors through $G_{p_i,1}/[G_{p_i,1}, G_{p_i,1}]$. Then there is a line l_i in W_i which is invariant under $G_{p_i,1}$ and $W_i = \sum_{g \in G_{p_i,0}} \eta_i(g)(l_i)$. Since $G_{p_i,0}$ is perfect, the stabilizer of l_i should be a proper subgroup of $G_{p_i,0}$. Since $\pi_{p_i^{n_i}}(G_{p_i,0})$ is generated by p_i-elements, we get that the index of the stabilizer of l_i in $G_{p_i,0}$ is at least p_i. And so again $\dim \eta_i \geq p_i \geq |\pi_{p_i^{n_i}}(\Lambda_{p_i})|^{\delta_3}$.

Case 4. $n_i = 1$ and $p_i \geq c_0$.

By [LS74] (see [SGV12, Section 4.2]), we have $\dim \eta_i \geq |\pi_{p_i^{n_i}}(\Lambda_{p_i})|^{\delta_4}$ where δ_4 is a positive number which depends only on $\mathbb{G}$.

Since $\prod_{i \text{ in Case 5}} p_i^{n_i} \ll_{\mathbb{G}} 1$, by the above cases we get that either $q \ll_\Gamma 1$ or $\dim \rho \geq |\pi_q(\Gamma)|^\delta$ where δ is a positive number which depends only on Γ. By enlarging Σ, we can assume that it contains all the irreducible representations of $\widehat{\Gamma}$ which factor through $\pi_q(\Gamma)$ for a positive integer $q \ll_\Gamma 1$. Such Σ and δ satisfy the claimed properties. $\square$

3. Expansion, approximate subgroup, and bounded generation.

3.1. Largeness of level-Q approximate subgroups implies super-approximation.
In this section, the Bourgain-Gamburd machine [BG08-a] is used to reduce a proof of spectral gap at level Q to a proof of the *largeness* of a *generic* level-Q approximate subgroup (see Theorem 20).

We work in the setting of Section 2.6. As in [SG], let us introduce the following notation for convenience: for a finite symmetric subset A of Γ, positive integers l and Q, and a positive number δ, let $\mathfrak{P}_Q(\delta, A, l)$ be the following statement

$$(15) \qquad (\mathcal{P}_\Omega^{(l)}(A) > Q^{-\delta}) \wedge (l > \frac{1}{\delta} \log Q) \wedge (|\pi_Q(A \cdot A \cdot A)| \leq |\pi_Q(A)|^{1+\delta}).$$

One can think of A as a *generic level-Q approximate subgroup* if $\mathfrak{P}_Q(\delta, A, l)$ holds for small enough δ.

Notice that the random-walk in $\pi_Q(\Gamma)$ gets interesting only at steps $O_\Omega(\log|\pi_Q(\Gamma)|) = O_\Omega(\log Q)$ since before this time the random-walk with respect to the probability measure $\mathcal{P}_{\pi_Q(\Omega)}$ is similar to a random-walk in a regular tree. The first two conditions of $\mathfrak{P}_Q(\delta, A, l)$ imply that at $O_\Omega(\log Q)$-range of random-walk the probability of hitting A is not *exponentially small*. And so A should be fairly generic. For instance Proposition 14 implies that A cannot be a subset of a proper algebraic subgroup if δ is small enough. The genericness of such A was crucial in the proof of [SG, Theorem 35] where the largeness of a generic level-Q approximate subgroup for a semisimple group is proved.

Let $\mathcal{C}$ be either $\{p^n | p \in V_f(\mathbb{Q}), p \nmid q_0\}$ or $\{q \in \mathbb{Z}^+ | \gcd(q, q_0) = 1, \forall p \in V_f(\mathbb{Q}), v_p(q_0) \leq N\}$, where $v_p(q)$ is the p-adic valuation of q.

In this section, we deduce Theorem 1 from the following result.

Theorem 20 (Approximate subgroups). *In the above setting, for any $\varepsilon > 0$ there is $\delta > 0$ such that*

$$\mathfrak{P}_Q(\delta, A, l) \text{ implies that } |\pi_Q(A)| \geq |\pi_Q(\Gamma)|^{1-\varepsilon}$$

if $Q \in \mathcal{C}$ and $Q^{\varepsilon^{\Theta_{\mathbb{G}}(1)}} \gg_\Omega 1$.

To show that Theorem 20 implies Theorem 1, we prove the following proposition based on the same proof as in [SG, Section 3.2]. In particular, we see that the reduction to understanding generic level-Q approximate subgroups can be done in much more generality.

Proposition 21. *Let $\overline{\Omega} \subseteq \mathrm{GL}_n(\mathbb{Z}[1/q_0])$ be a finite subset and $\Omega := \overline{\Omega} \cup \overline{\Omega}^{-1}$. Suppose $\overline{\Omega}$ freely generates a subgroup Γ. Let $\mathcal{C}'$ be a family of positive integers which consists of numbers that are corpime to q_0. Suppose $\mathcal{C}'$ is closed under divisibility; that means if $q \in \mathcal{C}'$ and $q'|q$, then $q' \in \mathcal{C}'$. Suppose the assertion of Theorem 20 holds for Ω and $\mathcal{C}'$. Then the family of Cayley graphs $\{\mathrm{Cay}(\pi_q(\Gamma); \pi_q(\Omega))\}_{q \in \mathcal{C}'}$ is a family of expanders.*

Proof. By Remark 2, we have to show $\sup_{q \in \mathcal{C}'} \lambda(\mathcal{P}_{\pi_q(\Omega)}; \pi_q(\Gamma)) < 1$. For $Q \in \mathcal{C}'$, let $T_Q : L^2(\pi_Q(\Gamma)) \to L^2(\pi_Q(\Gamma)), T_Q(f) := \pi_Q[\mathcal{P}_\Omega] * f$ and $\lambda(Q) := \lambda(\mathcal{P}_{\pi_Q(\Omega)}; \pi_Q(\Gamma))$. It is well-known that $\lambda(Q)$ is the second largest eigenvalue of T_Q. Since $L^2(\pi_Q(\Gamma))$ is a completely reducible representation of $\pi_Q(\Gamma)$, there is a unit function $f_0 \in L^2(\pi_Q(\Gamma))$ such that $T_Q(f_0) = \lambda(Q)f_0$ and the $\pi_Q(\Gamma)$-module V_ρ generated by f_0 is a simple $\pi_Q(\Gamma)$-module. Since $\lambda(Q)$ is not one, ρ is not the trivial representation of $\pi_Q(\Gamma)$. Since there are $\dim \rho$-many copies of ρ as subrepresentations of $L^2(\pi_Q(\Gamma))$, we have that the eigenvalue $\lambda(Q)$ of T_Q has multiplicity at least $\dim \rho$. Since $Q \in \mathcal{C}'$ and $\mathcal{C}'$ is closed under divisibility, we can and will assume that ρ does not factor through $\pi_q(\Gamma)$ for some proper divisor q of Q. Hence by Proposition 18 we have that either the lift of ρ to a representation of $\widehat{\Gamma}$, the closure of Γ in $\prod_{p \nmid q_0} \mathrm{GL}_n(\mathbb{Z}_p)$, is in a finite set Σ or $\dim \rho \geq |\pi_Q(\Gamma)|^{\varepsilon_0}$ where ε_0 is a positive number depending only on Γ. As we are seeking a uniform upper bound for $\lambda(Q)$, without loss of generality we can and will assume that the lift of ρ is not in Σ. And so we have that multiplicity of the eigenvalue $\lambda(Q)$ of T_Q is at least $|\pi_Q(\Gamma)|^{\varepsilon_0}$. Therefore for any positive integer l we have

$$|\pi_Q(\Gamma)|^{\varepsilon_0} \lambda(Q)^{2l} \leq \mathrm{Tr}(T_Q^{2l}) = |\pi_Q(\Gamma)| \|\mathcal{P}_{\pi_Q(\Omega)}^{(l)}\|_2^2.$$

So it is enough to show

$$(16) \qquad \|\mathcal{P}_{\pi_Q(\Omega)}^{(l)}\|_2 \leq |\pi_Q(\Gamma)|^{-\frac{1}{2} + \frac{\varepsilon_0}{4}},$$

for some $l \ll_\Omega \log Q$ where the implied constant depends only on Ω; it is worth pointing out that we can and will assume that Q is arbitrarily large depending only on Ω. In particular, we can and will assume *the Largeness of level Q-Approximate Subgroups* in the following sense:

The LAS Assumption: there is $c_2 > 0$ such that, if $Q > 1/c_2$ and $\mathfrak{P}_Q(c_2, A, l)$ holds, then $|\pi_Q(A)| \geq |\pi_Q(\Gamma)|^{1 - \varepsilon_0/8}$.

On the other hand, the first $O_\Omega(\log Q)$ steps of the random-walk with respect to the probability measure $\mathcal{P}_{\pi_Q(\Omega)}$ can be identified with the random-walk with respect to the probability measure $\mathcal{P}_\Omega$. And the latter is the random-walk on a regular infinite tree. Hence by the Kesten bound [Kes59, Theorem 3] we have

$$\|\mathcal{P}_\Omega^{(l)}\|_2^2 = \mathcal{P}_\Omega^{(2l)}(I) \leq \left(\frac{2|\overline{\Omega}| - 1}{|\overline{\Omega}|^2}\right)^l = e^{-c_1 l},$$

where c_1 is a positive number which depends only on Ω. Hence for some positive integer $l_0 = \Theta_\Omega(\log Q)$ where the implied constants depend only on Ω and for some positive number c_3 depending on Ω we have

$$(17) \qquad \|\mathcal{P}_{\pi_Q(\Omega)}^{(l_0)}\|_2 = \|\mathcal{P}_\Omega^{(l_0)}\|_2 \leq |\pi_Q(\Gamma)|^{-c_3}.$$

Equation (17) can be considered as *an initial L^2-flatness.*

An important result of Bourgain and Gamburd roughly indicates that the L^2-norm of a probability measure should substantially drop after a convolution by itself unless an approximate subgroup has a lot of mass [BG08-a] (see also [Var12, Lemma 15]). This result is proved using Tao's non-commutative version of Balog-Szemerédi-Gowers theorem [Tao08]. Here is a precise formulation of their result:

Proposition 22 (Bourgain-Gamburd's L^2-flattening.)**.** *Let μ be a symmetric probability measure with finite support on a group G. Let K be a number more than 2. If $\|\mu * \mu\|_2 \geq \frac{1}{K}\|\mu\|_2$, then there is a finite symmetric subset A of G which satisfies the following properties:*

- *(Size of A is comparable with $\|\mu\|_2^{-2}$) $K^{-R}\|\mu\|_2^{-2} \leq |A| \leq K^R\|\mu\|_2^{-2}$;*
- *(Getting an approximate subgroup) $|A \cdot A \cdot A| \leq K^R|A|$;*
- *(Almost equidistribution on A) $\min_{a \in A}(\mu * \mu)(a) \geq K^{-R}|A|^{-1}$,*

where R is an absolute positive number.

For a small (depending only on Ω and specified later) positive parameter δ, consider the following pseudocode:

Algorithm 1 L^2-flattening process

Give $Q \in \mathcal{C}'$, $\delta \in (0, 1)$;
$l_0 := \lfloor \log Q / 2 \log C(\Omega) \rfloor$; (as in Equation 17)
$\mu_0 := \mathcal{P}_{\pi_Q(\Omega)}^{(l_0)}$;
$i := 0$;
while $(\|\mu_i\|_2 > |\pi_Q(\Gamma)|^{-1/2 + \varepsilon_0/4}$ and $\|\mu_i * \mu_i\|_2 \leq \|\mu_i\|_2^{1+\delta})$ or $(2^i l_0 < (1/\delta)\log Q)$ **do**
  $\mu_{i+1} := \mu_i * \mu_i$;
  $i := i + 1$;
end while

---

where $C(\Omega) := \max_{s \in \Omega} \|s\|$, where $\|s\|$ is the operator norm of $s : \mathbb{R}^n \times \prod_{p|q_0} \mathbb{Q}_p^n \to \mathbb{R}^n \times \prod_{p|q_0} \mathbb{Q}_p^n$ with $\|(v_\infty, v_p)_{p|q_0}\| := \max\{\|v_\infty\|, \|v_p\|_p\}_{p|q_0}$ and the sup norm on $\mathbb{R}^n$ and $\mathbb{Q}_p^n$.

Claim 1. For any $0 < \delta < 1$ and $Q \in \mathcal{C}'$, the number $i_0(\delta, Q)$ of steps in Algorithm 1 is at most $\frac{\log(2/c_3)}{\log(1+\delta)} + \log(\frac{2 \log C(\Omega)}{\delta})$ where c_3 is given in Equation (17).

Proof of Claim 1. By the Young inequality we have $\|\mu_{i+1}\|_2 \leq \|\mu_i\|_2$ for any non-negative integer i. Hence by the initial flatness, Equation (17), we have $\|\mu_i\|_2 \leq \|\mu_0\|_2 \leq |\pi_Q(\Gamma)|^{-c_3}$ for any non-negative integer i. Let j_0 be the smallest integer such that $2^{j_0} l_0 \geq (1/\delta)\log Q$. Then for any $j_0 \leq i < i_0(\delta, Q)$ we have $\|\mu_{i+1}\|_2 \leq \|\mu_i\|_2^{(1+\delta)}$. And so

$$\|\mu_{i_0(\delta, Q)}\|_2 \leq \|\mu_{j_0}\|_2^{(1+\delta)^{i_0 - j_0}}.$$

If $i_0(\delta, Q) > \frac{\log(2/c_3)}{\log(1+\delta)} + \log(\frac{2 \log C(\Omega)}{\delta})$, then $i_0 - j_0 > \frac{\log(2/c_3)}{\log(1+\delta)}$ which implies $\|\mu_{i_0 - 1}\|_2 \leq |\pi_Q(\Gamma)|^{-1}$. And this contradicts $\|\mu_{i_0 - 1}\|_2 > |\pi_Q(\Gamma)|^{-1/2 + \varepsilon_0/4}$. $\qquad\square$

Claim 2. There is a positive number $\delta := \delta(\Omega)$ depending only on Ω, such that, for any $Q \in \mathcal{C}'$ which is at least $1/\delta$, $\|\mu_{i_0(\delta, Q)}\|_2 \leq |\pi_Q(\Gamma)|^{-1/2 + \varepsilon_0/4}$, where $i_0(\delta, Q)$ is given in Claim 1.

Proof of Claim 2. We proceed by contradiction. So to the contrary assumption for any positive number δ there is $Q(\delta) \in \mathcal{C}'$ such that

$$(18) \qquad\qquad Q(\delta) > 1/\delta; \text{ in particular } \lim_{\delta \to 0} Q(\delta) = \infty,$$

$$(19) \qquad\qquad \|\mu_{i_0(\delta, Q(\delta))}\|_2 > |\pi_{Q(\delta)}(\Gamma)|^{-1/2 + \varepsilon_0/4}, \text{ and}$$

$$(20) \qquad\qquad \|\mu_{i_0(\delta, Q(\delta))} * \mu_{i_0(\delta, Q(\delta))}\|_2 \geq \|\mu_{i_0(\delta, Q(\delta))}\|_2^{1+\delta}.$$

Hence by (20) and Proposition 22 (for $K = \|\mu_{i_0(\delta,Q(\delta))}\|_2^{-\delta}$) there is a symmetric subset $\overline{A}(\delta)$ of $\pi_{Q(\delta)}(\Gamma)$ such that

$$\|\mu_{i_0(\delta,Q(\delta))}\|_2^{-2+R\delta} \leq |\overline{A}(\delta)| \leq \|\mu_{i_0(\delta,Q(\delta))}\|_2^{-2-R\delta}, \tag{21}$$

$$|\overline{A}(\delta) \cdot \overline{A}(\delta) \cdot \overline{A}(\delta)| \leq \|\mu_{i_0(\delta)}\|_2^{-R\delta}|\overline{A}(\delta)|, \text{ and} \tag{22}$$

$$\mu_{i_0(\delta,Q(\delta))+1}(\overline{A}(\delta)) \geq \|\mu_{i_0(\delta,Q(\delta))}\|_2^{R\delta}. \tag{23}$$

Hence there is a function $\delta'(\delta)$ of δ such that

$$\lim_{\delta \to 0} \delta'(\delta) = 0 \text{ and } \delta'(\delta) \geq \delta, \tag{24}$$

$$\text{(because of Inequalities (21) and (22),)} \quad |\overline{A}(\delta) \cdot \overline{A}(\delta) \cdot \overline{A}(\delta)| \leq |\overline{A}(\delta)|^{1+\delta'(\delta)} \tag{25}$$

$$\text{(because of Inequalities (19) and (23),)} \quad \mu_{i_0(\delta,Q(\delta))+1}(\overline{A}(\delta)) \geq Q(\delta)^{-\delta'(\delta)}. \tag{26}$$

We notice that $\mu_j = \mathcal{P}^{(2^j l_0(\delta))}_{\pi_{Q(\delta)}(\Omega)}$, and let $A(\delta) := \pi_{Q(\delta)}^{-1}(\overline{A}(\delta)) \cap \mathrm{supp}(\mathcal{P}_{\Omega}^{(l(\delta))})$, where $l(\delta) := 2^{i_0(\delta,Q(\delta))+1}l_0(\delta)$; then we have

$$A(\delta) \text{ is a finite symmetric subset of } \Gamma \text{ because } \overline{A}(\delta) \text{ and } \mathcal{P}_{\Omega} \text{ are symmetric,} \tag{27}$$

$$l(\delta) \geq (1/\delta) \log Q(\delta) \geq (1/\delta'(\delta)) \log Q(\delta) \tag{28}$$

because of the second condition of the loop in Algorithm 1 and the inequality in (24),

$$\mathcal{P}^{(l(\delta))}_{\Omega(\delta)}(A(\delta)) = \mu_{i_0(\delta)+1}(\overline{A}(\delta)) \geq Q(\delta)^{-\delta'(\delta)} \text{ by Inequality (26),} \tag{29}$$

$$|\pi_{Q(\delta)}(A(\delta) \cdot A(\delta) \cdot A(\delta))| \leq |\pi_{Q(\delta)}(A(\delta))|^{1+\delta'(\delta)} \text{ by Inequality (25).} \tag{30}$$

Statements (27), (28), (29), and (30) imply that $\mathfrak{P}_{Q(\delta)}(\delta'(\delta), A(\delta), l(\delta))$ holds for any δ. Now suppose δ is small enough so that $\delta'(\delta)$ is less than c_2 where c_2 is given by the LAS Assumption (this can be done thanks to (24)). Then $Q(\delta) > 1/\delta \geq 1/\delta'(\delta) \geq 1/c_2$, and so by the LAS Assumption we have

$$|\pi_{Q(\delta)}(A(\delta))| = |\overline{A}(\delta)| \geq |\pi_{Q(\delta)}(\Gamma)|^{1-\varepsilon_0/8}. \tag{31}$$

On the other hand, by Inequalities (21) and (19), we have

$$|\overline{A}(\delta)| \leq \|\mu_{i_0(\delta,Q(\delta))}\|_2^{-2-R\delta} \leq |\pi_{Q(\delta)}(\Gamma)|^{1+R\delta/2-\varepsilon_0/2-R\delta\varepsilon_0/4}.$$

Hence, if δ is small enough, we get $|\overline{A}(\delta)| \leq |\pi_{Q(\delta)}(\Gamma)|^{1+R\delta/2-\varepsilon_0/2-R\delta\varepsilon_0/4} \leq |\pi_{Q(\delta)}(\Gamma)|^{1-\varepsilon_0/4}$, which contradicts (31). $\square$

(*Going back to the proof of Proposition 21*) By Claim 1 and Claim 2, for $Q \gg_\Omega 1$ in $\mathcal{C}'$ we have $\|\mathcal{P}^{(l)}_{\pi_Q(\Omega)}\|_2 \leq |\pi_Q(\Gamma)|^{-1/2+\varepsilon_0/4}$ where $l := 2^{i_0(\delta(\Omega),Q)}l_0 \ll_\Omega \log Q$. And this gives us the needed L^2-norm upper bound (see Inequality (16)) for $Q \gg_\Omega 1$. The rest are only finitely many Q's for which we do have spectral gap. $\square$

3.2. Reduction to bounded generation and abelian unipotent radical. The main goal of this section is to deduce Theorem 20 from the following.

Theorem 23 (Bounded generation). *In the setting of Section 2.6, suppose $\mathbb{U}$ is abelian. For any positive integer q, let $\Gamma[q] := \Gamma \cap \mathrm{GL}_{n_0}(\mathbb{Z}[1/q_0])[q]$, where*

$$\mathrm{GL}_{n_0}(\mathbb{Z}[1/q_0])[q] := \ker(\mathrm{GL}_{n_0}(\mathbb{Z}[1/q_0]) \xrightarrow{\pi_q} \mathrm{GL}_{n_0}(\mathbb{Z}[1/q_0]/q\mathbb{Z}[1/q_0])).$$

Then for any $0 < \varepsilon \ll_\Omega 1$ there are $0 < \delta \ll_{\Omega,\varepsilon} 1$ and positive integer $C \gg_{\Omega,\varepsilon} 1$ such that for a finite symmetric subset A of Γ

$$\mathcal{P}^{(l)}_\Omega(A) > Q^{-\delta} \text{ for some } l > (1/\delta)\log Q \text{ implies } \pi_Q(\Gamma[q]) \subseteq \prod_C \pi_Q(A) \text{ for some } q|Q \text{ and } q \leq Q^\varepsilon$$

if $Q \in \mathcal{C}$ and $Q^{\varepsilon^{O_{\mathbb{G}}(1)}} \gg_\Omega 1$.

The idea of the proof of Theorem 20 modulo Theorem 23. It is not clear to the author if a bounded generation result is true when the unipotent radical $\mathbb{U}$ is not abelian (specially since a perfect group might have a non-trivial center.). So to prove the *largeness of a generic level-Q approximate subgroup A of Γ* with Zariki-closure $\mathbb{G} := \mathbb{G}_s \ltimes \mathbb{U}$, first we go to the quotient $\mathbb{G}_s \ltimes \mathbb{U}/[\mathbb{U}, \mathbb{U}]$. Let $\rho_2 : \mathbb{G} \to \mathbb{G}_s \ltimes \mathbb{U}/[\mathbb{U}, \mathbb{U}]$ be the quotient map. For simplicity let us assume ρ_2 commutes with the congruence maps π_Q. This assumption together with the way the generating set Ω is chosen (recall that we have $\Omega = \overline{\Omega} \cup \overline{\Omega}^{-1}$ and $\rho_2(\overline{\Omega})$ freely generates a free group) implies that $\rho_2(A)$ is *a generic level-Q approximate subgroup of $\rho_2(\Gamma)$*. Now by the bounded generation result for $\rho_2(\Gamma)$, we get a *large* congruence subgroup of $\rho_2(\Gamma)$ modulo Q in a *controlled* number of steps. Next we use the techniques of studying a nilpotent group in order to translate our information on $\mathbb{U}/[\mathbb{U}, \mathbb{U}]$ to some data on $\mathbb{U}$. For a unipotent group $\mathbb{U}$ (and in general any nilpotent group), it is a useful method to consider

$$L_{\mathbb{U}} := \gamma_1(\mathbb{U})/\gamma_2(\mathbb{U}) \oplus \gamma_2(\mathbb{U})/\gamma_3(\mathbb{U}) \oplus \cdots \oplus \gamma_c(\mathbb{U})/\gamma_{c+1}(\mathbb{U}),$$

where $\gamma_i(\mathbb{U})$ is the i-th lower central series; that means $\gamma_1(\mathbb{U}) := \mathbb{U}$ and $\gamma_{i+1} := [\gamma_i(\mathbb{U}), \mathbb{U}]$, and $\gamma_{c+1}(\mathbb{U}) = \{1\}$. It is well-known that $[g_i\gamma_{i+1}(\mathbb{U}), g_j\gamma_j(\mathbb{U})] := g_i^{-1}g_j^{-1}g_ig_j\gamma_{i+j+1}(\mathbb{U})$ for $g_i \in \gamma_i(\mathbb{U})$ and $g_j \in \gamma_j(\mathbb{U})$ defines a graded Lie ring structure on $L_{\mathbb{U}}$. And $L_{\mathbb{U}}$ is generated by its degree 1 elements, i.e. $\gamma_1(\mathbb{U})/\gamma_2(\mathbb{U})$, as a Lie ring. So we get an onto multi-linear map

$$\phi_k : \underbrace{\gamma_1(\mathbb{U})/\gamma_2(\mathbb{U}) \times \cdots \times \gamma_1(\mathbb{U})/\gamma_2(\mathbb{U})}_{k\text{-times}} \to \gamma_k(\mathbb{U})/\gamma_{k+1}(\mathbb{U}), \qquad \phi_k(x_1, \ldots, x_k) := [x_1, \ldots, x_k],$$

where $[x_1, \ldots, x_k] := [[x_1, \ldots, x_{k-1}], x_k]$. Having a set X which maps onto a set of representatives for a *large* congruence subgroup modulo Q in $\gamma_1(\mathbb{U})/\gamma_2(\mathbb{U})$, using the above multi-linear maps ϕ_k, we can get a *subset* of $\mathbb{U}$ which is *large* modulo Q. *Notice that at this step we can get a control only on the* size *of the product set* $\pi_Q(\prod_{O_{\mathbb{U}}(1)} X)$. *Though we do get a set of representatives of a* large *congruence subset of the associated graded Lie ring, we do not get such a structural understanding of the product set itself.* Altogether we get that $|\prod_C \pi_Q(A)|$ is *large*. On the other hand, since $|\pi_Q(A) \cdot \pi_Q(A) \cdot \pi_Q(A)| \le |\pi_Q(A)|^{1+\delta}$, by the Ruzsa inequality (see [Hel05, Lemma 2.2]), we get

$$|\textstyle\prod_C \pi_Q(A)| \le |\pi_Q(A)| \left(\frac{|\prod_3 \pi_Q(A)|}{|\pi_Q(A)|}\right)^{C-2} \le |\pi_Q(A)|^{1+(C-2)\delta},$$

which helps us to finish the proof.

Theorem 23 implies Theorem 20. By the contrary assumption, there is $\varepsilon_0 > 0$ such that for any $\delta > 0$ there are a finite symmetric subset A_δ, a positive integer l_δ and $Q_\delta \in \mathcal{C}$ such that $\mathfrak{P}_{Q_\delta}(\delta, A_\delta, l_\delta)$ holds and at the same time $|\pi_{Q_\delta}(A_\delta)| < |\pi_{Q_\delta}(\Gamma)|^{1-\varepsilon_0}$. Since $l_\delta > \log Q_\delta/\delta$, we have $\lim_{\delta \to 0} l_\delta = \infty$. Now we claim that $Q_\delta \to \infty$ as $\delta \to 0$. If not, for infinitely many δ we have $Q_\delta = Q$, and $\pi_Q(A_\delta) = \overline{A}$ is independent of δ. And so

$$\lim_{\delta \to 0} \mathcal{P}^{(l_\delta)}_{\pi_Q(\Omega)}(\pi_Q(A_\delta)) = \frac{|\overline{A}|}{|\pi_Q(\Gamma)|} < \frac{1}{|\pi_Q(\Gamma)|^{\varepsilon_0}}.$$

On the other hand, we have

$$\mathcal{P}^{(l_\delta)}_{\pi_Q(\Omega)}(\pi_Q(A_\delta)) \ge \mathcal{P}^{(l_\delta)}_{\Omega}(A_\delta) > Q_\delta^{-\delta} = Q^{-\delta}.$$

Hence as $\delta \to 0$, we get $|\pi_Q(\Gamma)|^{-\varepsilon_0} > 1$, which is a contradiction.

Let $\{k_p\}_{p \nmid q_0}$ be such that $P_p = \mathbb{G}(\mathbb{Q}_p) \cap \mathrm{GL}_{n_0}(\mathbb{Z}_p)[p^{k_p}]$ where $\{P_p\}_p$ is as in Section 2.6. Let $\rho_2 : \mathbb{G} \to \mathbb{G}_s \ltimes \mathbb{U}/[\mathbb{U}, \mathbb{U}]$ be the quotient map. Let us recall that, by the discussion at the end of Section 2.4, we can and will assume $\rho_2(P_p) \subseteq \mathrm{GL}_{n_2}(\mathbb{Z}_p)$.

Let $q_0' = \prod_{p \nmid q_0} p^{k_p'}$ be a positive integer given by Lemma 13; that means for any sequence $\{m_p\}_{p \nmid q_0} \in \bigoplus_{p \nmid q_0} \mathbb{Z}$ such that $m_p \geq k_p + k_p'$ we have

(32)
$$\prod_{p \nmid q_0} \pi_{p^{m_p + k_p'}}(P_p)/\pi_{p^{m_p + k_p'}}([\mathbb{U}, \mathbb{U}](\mathbb{Q}_p) \cap P_p) \twoheadrightarrow \prod_{p \nmid q_0} \pi_{p^{m_p}}(\rho_2(P_p)) \twoheadrightarrow \prod_{p \nmid q_0} \pi_{p^{m_p - k_p'}}(P_p)/\pi_{p^{m_p - k_p'}}([\mathbb{U}, \mathbb{U}](\mathbb{Q}_p) \cap P_p).$$

In order to use (32), we modify Q_δ so that for any prime p either $v_p(Q_\delta) \geq k_p'$ or $v_p(Q_\delta) = 0$. To this end, it is enough to show that we are allowed to change Q_δ to Q_δ/q_δ' where $q_\delta' := \prod_{p \nmid q_0, 0 < v_p(Q_\delta) < 2k_p' + k_p} p^{v_p(Q_\delta)}$.

Lemma 24. *Let A_δ, Q_δ, and l_δ be as above. Suppose $q_\delta'|Q_\delta$ and $q_\delta' < C'$ (for some constant C'). Then $\mathfrak{P}_{Q_\delta/q_\delta'}(\Theta_{C',\Omega}(\delta), A_\delta, l_\delta)$ holds and $|\pi_{Q_\delta/q_\delta'}(A_\delta)| \leq |\pi_{Q_\delta/q_\delta'}(\Gamma)|^{1-\varepsilon_0/2}$ for $0 < \delta \ll_{C'} 1$.*

Proof. Since $\lim_{\delta \to 0} Q_\delta = \infty$, for $C'' > 1$ and small enough δ we have $Q_\delta/q_\delta' > Q_\delta^{1/C''}$. And so

$$\mathcal{P}^{(l_\delta)}(A_\delta) > Q_\delta^{-\delta} > (Q_\delta/q_\delta')^{-C''\delta}, \quad \text{and} \quad l_\delta > \frac{\log Q_\delta}{\delta} > \frac{\log(Q_\delta/q_\delta')}{C''\delta}.$$

To show that $\mathfrak{P}_{Q_\delta/q_\delta'}(C''\delta, A_\delta, l_\delta)$ holds, it is enough to prove that we have $|\pi_{Q_\delta/q_\delta'}(\prod_3 A_\delta)| \leq |\pi_{Q_\delta/q_\delta'}(A_\delta)|^{1+C''\delta}$ for large enough C''.

We notice that, if c is small enough (depending on Ω), $\pi_{Q_\delta/q_\delta'}$ induces an injection on the ball of radius $c \log(Q_\delta/q_\delta')$ (with respect to the word metric). By [BG09, Remark, page 1060] (see [SG, Lemma 8]), we have $\mathcal{P}^{(\lfloor 2c \log(Q_\delta/q_\delta')\rfloor)}(A_\delta \cdot A_\delta) > Q_\delta^{-2\delta}$. Hence by the Kesten bound (see Inequality (14)) for small enough δ we have

(33)
$$\begin{aligned}
|\pi_{Q_\delta/q_\delta'}(A_\delta \cdot A_\delta)| &= |A_\delta \cdot A_\delta \cap B_{\lfloor 2c \log(Q_\delta/q_\delta')\rfloor}| \\
&\geq \mathcal{P}^{(\lfloor 2c \log(Q_\delta/q_\delta')\rfloor)}(A_\delta \cdot A_\delta)/\|\mathcal{P}^{(\lfloor 2c \log(Q_\delta/q_\delta')\rfloor)}\|_\infty \\
&\geq Q_\delta^{-2\delta} \cdot (2c \log(Q_\delta/q_\delta'))^{\Theta_\Omega(1)} \geq Q_\delta^{\Theta_{C',\Omega}(1)},
\end{aligned}$$

which implies that $|\pi_{Q_\delta/q_\delta'}(A_\delta)| \geq Q_\delta^{\Theta_{C',\Omega}(1)}$.

Since $|\pi_{Q_\delta}(\prod_3 A_\delta)| \leq |\prod_{Q_\delta}(A_\delta)|^{1+\delta}$, by the Ruzsa inequality (see [Hel05, Lemma 2.2]) and [Hel11, Lemma 7.4] we have

$$|\pi_{Q_\delta}(A_\delta)|^{3\delta} \geq \frac{|\pi_{Q_\delta}(\prod_5 A_\delta)|}{|\pi_{Q_\delta}(A_\delta)|} \geq \frac{|\pi_{Q_\delta/q_\delta'}(\prod_3 A_\delta)|}{|\pi_{Q_\delta/q_\delta'}(A_\delta)|},$$

which implies that $|\pi_{Q_\delta/q_\delta'}(\prod_3 A_\delta)|/|\pi_{Q_\delta/q_\delta'}(A_\delta)| \leq |\pi_{Q_\delta/q_\delta'}(A_\delta)|^{C''\delta}$ for large enough C''. Since Q_δ goes to infinity, it is clear that for small enough δ we have $|\pi_{Q_\delta/q_\delta'}(A_\delta)| \leq |\pi_{Q_\delta/q_\delta'}(\Gamma)|^{1-\varepsilon_0/2}$. $\square$

By Lemma 24 we can and will modify $\{Q_\delta\}_\delta$ and assume that, if $k_p + k_p' > 0$, then either $v_p(Q_\delta) = 0$ for any δ or $k_p + 2k_p' \leq \min_\delta v_p(Q_\delta) < \sup_\delta v_p(Q_\delta) = \infty$. In particular, without loss of generality we can and will assume that $q_0'^2|Q_\delta$ for any δ.

On the other hand, by Corollary 16, we have that $\ker(\rho_2) \cap \Gamma = \{1\}$. So $\mathcal{P}_{\rho_2(\Omega)}^{(l_\delta)}(\rho_2(A_\delta)) = \mathcal{P}_\Omega^{(l_\delta)}(A_\delta) > Q_\delta^{-\delta} > (q_0'Q_\delta)^{-\Theta_\Omega(\delta)}$ for suitable constant and small enough δ. Hence by Theorem 23 for any $0 < \varepsilon' \ll_\Omega 1$ there is a positive integer $C = O_{\Omega,\varepsilon'}(1)$ such that for any $0 < \delta \ll_{\varepsilon',\Omega} 1$ we have

(34)
$$\pi_{q_0'Q_\delta}(\rho_2(\Gamma)[q_\delta]) \subseteq \prod_C \pi_{q_0'Q_\delta}(\rho_2(A_\delta))$$

for some $q_\delta|q_0'Q_\delta$ and $q_\delta \leq (q_0'Q_\delta)^{\varepsilon'} \leq Q_\delta^{\Theta(\varepsilon')}$.

On the other hand we have $\pi_{q_0'Q_\delta}(\prod_{p \nmid q_0} \rho_2(U_p)) \subseteq \pi_{q_0'Q_\delta}(\rho_2(\Gamma))$ (recall that $U_p := \mathbb{U}(\mathbb{Q}_p) \cap \mathrm{GL}_{n_0}(\mathbb{Z}_p)[p^{k_p}]$. Let $\overline{U}_p := \mathrm{GL}_{n_2}(\mathbb{Z}_p) \cap \mathbb{U}(\mathbb{Q}_p))$; and so we have that $\overline{U}_p = U_p$ for large enough p, and U_p is an open subgroup of $\overline{U}_p$. By Lemma 24, we can and will assume that $v_p(Q_\delta)$ are either zero or large enough depending on the

index of U_p in $\overline{U}_p$ for all the primes p. And so by enlarging q_δ by a multiplicative constant we can and will assume that

$$\pi_{q'_0 Q_\delta}(\rho_2(\prod_{p \nmid q_0} \overline{U}_p)^{q_\delta}) \subseteq \pi_{q'_0 Q_\delta}(\rho_2(\Gamma)[q_\delta]) \subseteq \prod_C \pi_{q'_0 Q_\delta}(\rho_2(A_\delta)),$$

where $\rho_2(\prod_{p \nmid q_0} \overline{U}_p)^{q_\delta} := \{x^{q_\delta} \mid x \in \rho_2(\prod_{p \nmid q_0} \overline{U}_p)\}$. So there is $B_\delta \subseteq \prod_C A_\delta$ such that

$$(35) \qquad \pi_{q'_0 Q_\delta}(\rho_2(B_\delta)) = \pi_{q'_0 Q_\delta}(\rho_2(\prod_{p \nmid q_0} \overline{U}_p)^{q_\delta}).$$

Lemma 25. *Let $\mathbb{U}$ be a unipotent $\mathbb{Q}$-group with a given $\mathbb{Q}$-embedding in $\mathbb{GL}_n$. For any prime p, let $\overline{U}_p := \mathbb{U}(\mathbb{Q}_p) \cap \mathrm{GL}_n(\mathbb{Z}_p)$. Let $\phi : \mathbb{U} \to \mathbb{U}/[\mathbb{U},\mathbb{U}]$ be the quotient map. Fix a $\mathbb{Q}$-basis $\{\mathbf{e}_i\}$ of $(\mathbb{U}/[\mathbb{U},\mathbb{U}])(\mathbb{Q})$ such that $\phi(\overline{U}_p) \subseteq \sum_i \mathbb{Z}_p \mathbf{e}_i$ for any prime p. Let $q|Q$ be two positive integers. Suppose X is a finite subset of $\prod_p \overline{U}_p$ such $\pi_Q(\phi(X)) = \pi_Q(q \sum_i \mathbb{Z} \mathbf{e}_i)$. Then*

$$|\prod_C \pi_Q(X)| \geq \frac{|\pi_Q(\prod_p \overline{U}_p))|}{C q^C},$$

where C depends on the dimension of $\mathbb{U}$ and the choice of embeddings.

Proof. Let $\gamma_i(\mathbb{U})$ be the i-th lower central series; that means $\gamma_1(\mathbb{U}) := \mathbb{U}$ and $\gamma_{i+1}(\mathbb{U}) := [\gamma_i(\mathbb{U}), \mathbb{U}]$. It is well-known that the long commutators $(g_1, \ldots, g_k) := ((g_1, \ldots, g_{k-1}), g_k)$, where $(g_1, g_2) := g_1^{-1} g_2^{-1} g_1 g_2$, induce multilinear maps f_k from $\mathbb{U}/[\mathbb{U},\mathbb{U}] \times \cdots \times \mathbb{U}/[\mathbb{U},\mathbb{U}]$ (k times) to $\gamma_k(\mathbb{U})/\gamma_{k+1}(\mathbb{U})$, and the $\mathbb{Q}$-span of $\{f_k(\mathbf{e}_{i_1}, \ldots, \mathbf{e}_{i_k})\}$ is $(\gamma_k(\mathbb{U})/\gamma_{k+1}(\mathbb{U}))(\mathbb{Q})$. For any k, let $\phi_k : \gamma_k(\mathbb{U}) \to \gamma_k(\mathbb{U})/\gamma_{k+1}(\mathbb{U})$. Then for any k we have

$$\pi_Q(\phi_k(\prod_{4k} X \cap \gamma_k(\mathbb{U})(\prod_p \mathbb{Q}_p)) \supseteq \cup_{i_1, \ldots, i_k} \pi_Q(q^k \mathbb{Z} f_k(\mathbf{e}_{i_1}, \ldots, \mathbf{e}_{i_k})),$$

and so

$$\pi_Q(\phi_k(\prod_{4k \dim \mathbb{U}} X \cap \gamma_k(\mathbb{U})(\prod_p \mathbb{Q}_p))) \supseteq \pi_Q(q^k \sum_{i_1, \ldots, i_k} \mathbb{Z} f_k(\mathbf{e}_{i_1}, \ldots, \mathbf{e}_{i_k}))$$

In particular, we have

$$(36) \qquad |\pi_Q(\phi_k(\prod_{4k \dim \mathbb{U}} X \cap \gamma_k(\mathbb{U})(\prod_p \mathbb{Q}_p)))| \geq (Q/q^k)^{\dim \gamma_k(\mathbb{U}) - \dim \gamma_{k+1}(\mathbb{U})}.$$

Since ϕ_k's are regular morphisms defined over $\mathbb{Q}$, there is a positive integer q'_1 depending on the embedding of $\mathbb{U}$ and the choice of $\{\mathbf{e}_i\}$) such that for any prime power p^m we have

$$\phi_k \left(\gamma_k(\mathbb{U})(\prod_p \mathbb{Q}_p) \cap \prod_p \overline{U}_p[q'_1 Q] \right) \subseteq \prod_p (Q \sum_{i_1, \ldots, i_k} \mathbb{Z}_p f_k(\mathbf{e}_{i_1}, \ldots, \mathbf{e}_{i_k})).$$

And so ϕ_k induces homomorphism $\overline{\phi}_k : \pi_{q'_1 Q}(\gamma_k(\mathbb{U})(\prod_p \mathbb{Q}_p) \cap \prod_p \overline{U}_p) \to \pi_Q(\sum_{i_1, \ldots, i_k} \mathbb{Z} f_k(\mathbf{e}_{i_1}, \ldots, \mathbf{e}_{i_k}))$, and we have $\overline{\phi}_k \circ \pi_{q'_1 Q} = \pi_Q \circ \phi_k$. Thus by (36) we have

$$(37) \qquad |\pi_{q'_1 Q}(\prod_{4 \dim \mathbb{U}^3} X)| \geq \prod_k |\pi_Q(\phi_k(\prod_{4k \dim \mathbb{U}} X \cap \gamma_k(\mathbb{U})(\prod_p \mathbb{Q}_p)))| \geq (Q/q^{\dim \mathbb{U}})^{\dim \mathbb{U}}.$$

Since $\mathbb{U}$ is a $\mathbb{Q}$-unipotent, there is a positive integer q'_2 (depending on the embedding and $\mathbb{U}$) such that $q'_2{}^{-1} Q^{\dim \mathbb{U}} \leq |\pi_Q(\prod_p \overline{U}_p)| \leq q'_2 Q^{\dim \mathbb{U}}$. And so

$$|\pi_Q(\prod_{4 \dim \mathbb{U}^3} X)| \geq \frac{|\pi_Q(\prod_p \overline{U}_p)|}{q'_2{}^2 q'_1{}^{\dim \mathbb{U}} q^{\dim \mathbb{U}^2}};$$

and the claim follows. $\qquad \square$

By (35) there is $X_\delta \subseteq \prod_p U_p$ such that $\pi_{q'_0 Q_\delta}(X_\delta) = \pi_{q'_0 Q_\delta}(B_\delta)$, which implies that $\pi_{Q_\delta}(\rho_2(X_\delta)) = \pi_{Q_\delta}(\rho_2(B_\delta))$. Hence by Lemma 25 we have

$$(38) \qquad |\pi_{Q_\delta}(\prod_{O_{\Omega, \varepsilon'}(1)} A_\delta) \cap \pi_{Q_\delta}(\prod_{p \nmid q_0} \overline{U}_p)| \geq \frac{|\pi_{Q_\delta}(\prod_{p \nmid q_0} \overline{U}_p)|}{\Theta_{\dim \mathbb{U}}(1) q_\delta^{\Theta_{\mathbb{U}}(1)}} \geq \frac{|\pi_{Q_\delta}(\prod_{p \nmid q_0} \overline{U}_p)|}{Q_\delta^{\Theta_{\dim \mathbb{U}}(\varepsilon')}} \geq |\pi_{Q_\delta}(\prod_{p | Q_\delta} \overline{U}_p)|^{1 - \Theta_{\mathbb{U}}(\varepsilon')},$$

for small enough δ (depending on ε') as $\lim_{\delta \to 0} Q_\delta = \infty$.

On the other hand, by (34), we have

$$\pi_{Q_\delta}(\textstyle\prod_{p\nmid q_0} K_p[q_\delta]) \subseteq \prod_C \pi_{Q_\delta}(A_\delta).$$

Therefore we have

(39) $$|\pi_{Q_\delta}(\textstyle\prod_C A_\delta) \cap \pi_{Q_\delta}(\textstyle\prod_{p|Q_\delta} K_p)| \geq |\pi_{Q_\delta}(\textstyle\prod_{p|Q_\delta} K_p)|^{1-\Theta_{\mathbb{G}_s}(\varepsilon')},$$

for small enough δ (depending on ε') as $\lim_{\delta\to 0} Q_\delta = \infty$.

By (38), (39), $\lim_{\delta\to 0} Q_\delta = \infty$, and the fact that $\prod_{p\nmid q_0} K_p \ltimes U_p$ is of finite index in $\widehat{\Gamma}$, we have

(40) $$|\pi_{Q_\delta}(\textstyle\prod_C A_\delta)| \geq |\pi_{Q_\delta}(\Gamma)|^{1-\Theta_\Omega(\varepsilon')},$$

for small enough δ (depending on ε').

On the other hand, since $|\pi_{Q_\delta}(\prod_3 A_\delta)| \leq |\pi_{Q_\delta}(A_\delta)|^{1+\delta}$ by the Ruzsa inequality (see [Hel05]), we have

(41) $$|\pi_{Q_\delta}(\textstyle\prod_C A_\delta)| \leq |\pi_{Q_\delta}(A_\delta)|^{1+(C-2)\delta} \leq |\pi_{Q_\delta}(\Gamma)|^{(1-\varepsilon_0)(1+(C-2)\delta)}.$$

By (40) and (41), for any ε' and small enough δ (in particular it can approach zero), we have

$$1 - \Theta_\Omega(\varepsilon') \leq (1-\varepsilon_0)(1+(C(\varepsilon')-2)\delta),$$

which is a contradiction. $\qquad\square$

4. SUPER-APPROXIMATION: BOUNDED POWER OF SQUARE-FREE INTEGERS CASE.

By Section 3.2, to prove Theorem 1 for $\mathcal{C}_N := \{q \in \mathbb{Z}^+ | \ \forall p \nmid q_0, v_p(q) \leq N\}$ it is enough to prove Theorem 23 (Bounded generation) for $\mathcal{C}_N$. In particular, we can assume that $\mathbb{U}$ is abelian. Since I believe it is interesting to know if some of the auxiliary results are true for more general perfect groups, I do not assume $\mathbb{U}$ is abelian till towards the end of this section. As a result some extra lemmas are proved which are not necessary for the proof of Theorem 23 for $\mathcal{C}_N$.[3]

4.1. **The residue maps do not split.** The main goal of this section is to show Lemma 29 which roughly asserts that π_p does split under mild conditions.

Lemma 26. *Let $\mathbb{G} = \mathbb{H} \ltimes \mathbb{U}$ be a $\mathbb{Q}$-group with a given $\mathbb{Q}$-embedding into $(\mathrm{GL}_n)_\mathbb{Q}$, where $\mathbb{H}$ is a connected semisimple $\mathbb{Q}$-group and $\mathbb{U}$ is a unipotent $\mathbb{Q}$-group. Let $\mathcal{G}$ (resp. $\mathcal{H}, \mathcal{U}$) be the Zariski-closure of $\mathbb{G}$ (resp. $\mathbb{H}, \mathbb{U}$) in the $\mathbb{Z}$-group scheme $(\mathrm{GL}_n)_\mathbb{Z}$, and $\mathfrak{g} = \mathrm{Lie}(\mathcal{G})$, $\mathfrak{h} = \mathrm{Lie}(\mathcal{H})$, and $\mathfrak{u} = \mathrm{Lie}(\mathcal{U})$. For large enough p, if $V \subsetneq \mathfrak{g}(\mathfrak{f}_p)$ is a $\mathcal{G}(\mathfrak{f}_p)$-invariant proper subspace, then $V + [\mathfrak{u}(\mathfrak{f}_p), \mathfrak{u}(\mathfrak{f}_p)]$ is a proper subspace. Moreover if $\mathbb{G}$ is perfect, then $V + \mathfrak{z}(\mathfrak{f}_p)$ is also a proper subspace, where $\mathfrak{z} = \mathrm{Lie}(Z(\mathcal{G}))$ is the Lie ring of the schematic center of $\mathcal{G}$.*

Proof. Let $A_G := \mathfrak{f}_p[\mathrm{Ad}(\mathcal{G}(\mathfrak{f}_p))] \subseteq \mathrm{End}_{\mathfrak{f}_p}(\mathfrak{g}(\mathfrak{f}_p))$ be the $\mathfrak{f}_p$-span of $\mathrm{Ad}(\mathcal{G}(\mathfrak{f}_p))$, and $A_H := \mathfrak{f}_p[\mathrm{Ad}(\mathcal{H}(\mathfrak{f}_p))]$ be its subalgebra. Since $\mathbb{H}$ is connected semisimple, for large enough p, $\mathfrak{g}(\mathfrak{f}_p)$ is a faithful completely reducible A_H-module. Thus A_H is a semisimple algebra, and so its Jacobson radical $J(A_H)$ is zero. Let $\mathfrak{a}$ be the ideal generated by $\{u - 1| \ u \in \mathcal{U}(\mathfrak{f}_p)\}$. Then we have the following short exact sequence of A_G-modules:

$$0 \to \mathfrak{a} \to A_G \to A_H \to 0.$$

Since A_H is semisimple, $J(A_G) \subseteq \mathfrak{a}$. On the other hand, since $\mathbb{U}$ is a unipotent normal subgroup of $\mathbb{G}$, $\mathfrak{a}$ is a nilpotent ideal. So overall we have $\mathfrak{a} = J(A_G)$.

Suppose to the contrary that there is a proper A_G-submodule V of $\mathfrak{g}(\mathfrak{f}_p)$ such that $V + [\mathfrak{u}(\mathfrak{f}_p), \mathfrak{u}(\mathfrak{f}_p)] = \mathfrak{g}(\mathfrak{f}_p)$. If we show that $J(A_G)\mathfrak{g}(\mathfrak{f}_p) \supseteq [\mathfrak{u}(\mathfrak{f}_p), \mathfrak{u}(\mathfrak{f}_p)]$, then we get that $V + J(A_G)\mathfrak{g}(\mathfrak{f}_p) = \mathfrak{g}(\mathfrak{f}_p)$. And so by Nakayama's lemma we have $V = \mathfrak{g}(\mathfrak{f}_p)$, which is a contradiction.

---

[3]If the reader is only interested in the proof of Theorem 23 for $\mathcal{C}_N$, s/he can skip Lemma 26, Lemma 27, and Lemma 31.

Since $\mathbb{U}$ is unipotent, log and exp define $\mathbb{Q}$-morphisms between $\mathbb{U}$ and its Lie algebra. And for large enough p they induce bijections between $\mathcal{U}(\mathfrak{f}_p)$ and $\mathfrak{u}(\mathfrak{f}_p)$. Furthermore for any $t \in \mathfrak{f}_p$, $x, y \in \mathfrak{u}(\mathfrak{f}_p)$ we have

$$\tag{42} \mathrm{Ad}(\exp(tx))(y) = \exp(t \, \mathrm{ad}(x))(y).$$

Thus for $t \in \mathfrak{f}_p$, $x, y \in \mathfrak{u}(\mathfrak{f}_p)$ we have

$$\tag{43} t^{-1}(\mathrm{Ad}(\exp(tx))(y) - y) = [x, y] + \sum_{i=1}^{\dim \mathbb{U}} \frac{t^i}{i!} \, \mathrm{ad}(x)^i(y) \in J(A_G)\mathfrak{g}(\mathfrak{f}_p).$$

Therefore for large enough p by the Vandermonde determinant we have that $[x, y] \in J(A_G)\mathfrak{g}(\mathfrak{f}_p)$ which shows our claim.

To finish the proof, it is enough to notice that $\mathbb{G}$ is perfect if and only if $\mathbb{H}$ acts without a non-zero fixed vector on $\mathbb{U}/[\mathbb{U}, \mathbb{U}]$. And so when $\mathbb{G}$ is perfect, for large enough p we have $\mathfrak{z}(\mathfrak{f}_p) \subseteq [\mathfrak{u}, \mathfrak{u}](\mathfrak{f}_p) = [\mathfrak{u}(\mathfrak{f}_p), \mathfrak{u}(\mathfrak{f}_p)]$. $\qquad\square$

Lemma 27. *Let $\mathbb{U} \subseteq (\mathrm{GL}_n)_{\mathbb{Q}_p}$ be a $\mathbb{Q}_p$-subgroup, and $U := \mathbb{U}(\mathbb{Q}_p) \cap \mathrm{GL}_n(\mathbb{Z}_p)$. Then if p is large enough depending only on n, then we have*

$$\pi_{p^2}(U) = \langle g \in \pi_{p^2}(U)| \ g^p \neq 1 \rangle, \quad and \quad U[p^m] = U^{p^m} := \{u^{p^m}| \ u \in U\},$$

for any positive integer m.

Proof. Let exp and log define $\mathbb{Q}_p$-morphisms between $\mathrm{Lie}(\mathbb{U})$ and $\mathbb{U}$. And so for large enough prime p we have

$$\tag{44} \|\exp x - I\|_p = \|x\|_p, \ \|\log u\|_p = \|u - I\|_p \qquad \text{if } \|x\|_p, \|u\|_p \leq 1 \text{ and } x^n = 0, (u - I)^n = 0.$$

Hence exp and log induce homeomorphisms between $\mathfrak{u} := \mathrm{Lie}(\mathbb{U})(\mathbb{Q}_p) \cap \mathfrak{gl}_n(\mathbb{Z}_p)$ and U, and moreover for any positive integer m

$$\tag{45} U[p^m] = U^{p^m} := \{u^{p^m}| \ u \in U\}.$$

We have (45) because of the following observation:

$$u \in U[p^m] \Leftrightarrow \|u - I\|_p \leq p^{-m} \Leftrightarrow u = \exp x, \ x \in \mathrm{Lie}(\mathbb{U})(\mathbb{Q}_p) \text{ and } \|x\|_p \leq p^{-m},$$
$$\Leftrightarrow u = \exp(p^m x') = (\exp x')^{p^m} \text{ and } x' \in \mathfrak{u},$$
$$\Leftrightarrow u \in U^{p^m}.$$

If $g^p = 1$ for some $g \in \pi_{p^2}(U)$, then for some $u \in U$ we have $g = \pi_{p^2}(u)$ and $u^p \in \ker(\pi_{p^2})$. So there is a (unique) $u' \in U \setminus U^p$ such that $u'^{p^m} = u^p$ for some $m \in \mathbb{Z}^{\geq 2}$. Another use of the logarithm map, we have $u = u'^{p^{m-1}}$. Hence

$$\pi_{p^2}(U) = \{g^{p^i}| \ g \in \pi_{p^2}(U), \ g^p \neq 1, \ i = 0, 1, 2\}.$$

$\qquad\square$

Lemma 28. *Let $\mathbb{H}$ be a simply-connected semisimple $\mathbb{Q}$-group with a given embedding into $(\mathrm{GL}_n)_{\mathbb{Q}}$. Let $P_0 = \mathbb{H}(\mathbb{Q}_p) \cap \mathrm{GL}_n(\mathbb{Z}_p)$ and $P_1 := \ker(P_0 \xrightarrow{\pi_p} \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z}))$. Then for large enough p we have*

$$P_i = \overline{\langle \mathbb{U}(\mathbb{Q}_p) \cap P_i| \ \mathbb{U} \subseteq \mathbb{H} \ unipotent \ \mathbb{Q}_p\text{-}subgroup \rangle},$$

for $i = 0, 1$.

Proof. For large enough p, we have that $\mathbb{H}$ is quasi-split over $\mathbb{Q}_p$, and splits over an unramified extension of $\mathbb{Q}_p$, and P_0 is a hyper-special parahoric subgroup. Let $Q_i = \langle \mathbb{U}(\mathbb{Q}_p) \cap P_i| \ \mathbb{U} \subseteq \mathbb{H} \ \text{unipotent } \mathbb{Q}_p\text{-subgroup} \rangle$. Then clearly Q_i is a normal subgroup of P_0. By the Bruhat-Tits theory, there is a smooth $\mathbb{Z}_p$-group scheme $\mathcal{H}$ such that

(1) $P_0 = \mathcal{H}(\mathbb{Z}_p)$,
(2) The generic fiber of $\mathcal{H}$ is isomorphic to $\mathbb{H}$,

(3) The special fiber $\mathcal{H}_p := \mathcal{H} \otimes_{\mathbb{Z}_p} \mathfrak{f}_p$ is a simply-connected semisimple $\mathfrak{f}_p$-group since $\mathbb{H}$ is simply connected quasi-split over $\mathbb{Q}_p$ and splits over an unramified extension of $\mathbb{Q}_p$,

(4) $\pi_p(P_0) = \mathcal{H}_p(\mathfrak{f}_p)$ is a product of quasi-simple groups.

Since $\mathbb{H}$ is quasi-split over $\mathbb{Q}_p$, $\pi_p(Q_0)$ intersects any quasi-simple factor subgroup of $\mathcal{H}_p(\mathfrak{f}_p)$ in a non-central subgroup. As $\pi_p(Q_0)$ is a normal subgroup of $\mathcal{H}_p(\mathfrak{f}_p)$, $\mathcal{H}_p(\mathfrak{f}_p)^+$ is contained in $\pi_p(Q_0)$. As $\mathcal{H}_p$ is simply-connected, we get that $\pi_p(Q_0) = \pi_p(P_0)$. For any positive integer i, let $P_i := \ker(P \xrightarrow{\pi_{p^i}} \mathcal{H}_p(\mathbb{Z}_p/p^i\mathbb{Z}_p))$. It is well-known that P_i/P_{i+1} as an $\mathcal{H}_p(\mathfrak{f}_p)$-module is isomorphic to $\mathrm{Lie}(\mathcal{H}_p)(\mathfrak{f}_p)$ via the adjoint action. Let's identify $\pi_{p^i}(Q_1 \cap P_{i+1})$ with $\mathfrak{h}_i \subseteq \mathrm{Lie}(\mathcal{H}_p)(\mathfrak{f}_p)$. Since $Q_1 \lhd P$, $\mathfrak{h}_i$ is $\mathcal{H}_p(\mathfrak{f}_p)$-invariant. On the other hand, since $\mathbb{H}$ is quasi-split, $\mathfrak{h}_i$ intersects each one of the Lie algebras of the simple factors of $\mathcal{H}_p$. Since for large enough p the $\mathfrak{f}_p$-points of the Lie algebra of the simple factors of $\mathcal{H}_p$ are simple $\mathcal{H}_p(\mathfrak{f}_p)$-module, $\mathfrak{h}_i = \mathrm{Lie}(\mathcal{H}_p)(\mathfrak{f}_p)$. Hence by induction we have $\pi_{p^i}(Q_j) = \pi_{p^i}(P_j)$ for $j = 0, 1$ and any positive integer i, which finishes the proof. $\qquad\square$

Lemma 29. *Let $\mathbb{G} \subseteq (\mathrm{GL}_n)_{\mathbb{Q}}$ be a perfect $\mathbb{Q}$-group. Assume that the semisimple part of $\mathbb{G}$ is simply-connected; that means $\mathbb{G} \simeq \mathbb{H} \ltimes \mathbb{U}$ where $\mathbb{H}$ is a simply-connected semisimple $\mathbb{Q}$-group and $\mathbb{U}$ is a unipotent $\mathbb{Q}$-group. Let $P_p = \mathbb{G}(\mathbb{Q}_p) \cap \mathrm{GL}_n(\mathbb{Z}_p)$, $\mathcal{G}$ be the closure of $\mathbb{G}$ in $(\mathrm{GL}_n)_{\mathbb{Z}}$, and $\mathfrak{g} = \mathrm{Lie}(\mathcal{G})$. Then*

(1) *For large enough p, the following is a short exact sequence:*

$$1 \to \mathfrak{g}(\mathfrak{f}_p) \to \pi_{p^2}(P_p) \to \pi_p(P_p) \to 1.$$

(2) *For large enough p and any proper subgroup $V \subsetneq \mathfrak{g}(\mathfrak{f}_p)$ which is a normal subgroup of $\pi_{p^2}(P_p)$, the following short exact sequence does not split*

$$1 \to \mathfrak{g}(\mathfrak{f}_p)/V \to \pi_{p^2}(P_p)/V \to \pi_p(P_p) \to 1$$

Proof. For large enough p, $Q_p := \mathbb{H}(\mathbb{Q}_p) \cap \mathrm{GL}_n(\mathbb{Z}_p)$ is a hyperspecial parahoric subgroup which acts on $U_p := \mathbb{U}(\mathbb{Q}_p) \cap \mathrm{GL}_n(\mathbb{Z}_p)$, and $P_p = Q_p \ltimes U_p$. Furthermore for large enough p, the assumptions of Lemma 28 hold and so $\pi_{p^i}(P_p) = \pi_{p^i}(\langle P_p \cap \mathbb{U}'(\mathbb{Q}_p)| \mathbb{U}' \text{ unipotent } \mathbb{Q}_p\text{-subgroup}\rangle)$. Hence by Lemma 27 we have

$$\pi_{p^2}(P_p) = \langle g \in \pi_{p^2}(P_p \cap \mathbb{U}'(\mathbb{Q}_p))| \mathbb{U}' \text{ unipotent } \mathbb{Q}_p\text{-subgroup}, \ g^p \neq 1\rangle.$$

On the other hand, if for any $\mathbb{Q}_p$-unipotent subgroup $\mathbb{U}'$ of $\mathbb{G}$ we have $\pi_{p^2}(P_p[p] \cap \mathbb{U}'(\mathbb{Q}_p)) \subseteq V$, then by Lemma 28 we get that $\pi_{p^2}(P_p[p]) \subseteq V$ which is a contradiction. Hence for some unipotent $\mathbb{Q}_p$-subgroup $\mathbb{U}'$ there is $x \in \pi_{p^2}(P_p[p] \cap \mathbb{U}'(\mathbb{Q}_p)) \setminus V$. By Lemma 27 there is $g \in \mathrm{GL}_n(\mathbb{Z}_p) \cap \mathbb{U}'(\mathbb{Q}_p)$ such that $\pi_{p^2}(g^p) = x$. Since $\mathbb{U}'$ is a $\mathbb{Q}_p$-subgroup of $\mathbb{G}$ and $P_p = \mathrm{GL}_n(\mathbb{Z}_p) \cap \mathbb{G}(\mathbb{Q}_p)$, we have that $g \in P_p$, and the order of $\pi_{p^2}(g)$ in $\pi_{p^2}(P_p)/V$ is p^2. Now suppose to the contrary that the given exact sequence splits; then $\pi_{p^2}(P_p)/V \simeq \pi_p(P_p) \ltimes (\mathfrak{g}(\mathfrak{f}_p)/V)$, and the latter is a linear group over $\mathfrak{f}_p$. However any p-element of a linear group over $\mathfrak{f}_p$ is unipotent, and so it is of order p (for large enough p), which is a contradiction. $\qquad\square$

4.2. Statistical non-splitting of residue maps. In this section, following [BV12], we prove that any section of π_p is statistically far from being a group homomorphism.

Lemma 30. *Let $\mathbb{G}$, $\mathfrak{g}$, and P_p be as in Lemma 29. Then there is a positive number δ (depending on $\mathbb{G}$) such that for large enough p (depending on $\mathbb{G}$ and its embedding in $(\mathrm{GL}_n)_{\mathbb{Q}}$) the following holds: Let $V \subsetneq \mathfrak{g}(\mathfrak{f}_p)$ be a proper subgroup which is normal in $\pi_{p^2}(P_p)$, and $\psi : \pi_p(P_p) \to \pi_{p^2}(P_p)/V$ be a section of the quotient map $\pi : \pi_{p^2}(P_p)/V \to \pi_p(P_p)$; that means $\pi \circ \psi = \mathrm{id}_{\pi_p(P_p)}$. Let $\mu = \mathcal{P}_{\pi_p(P_p)}$ be the probability Haar measure (i.e. the normalized counting measure) on $\pi_p(P_p)$. Then*

$$(\mu \times \mu)(\{(x,y) \in \pi_p(P_p) \times \pi_p(P_p)| \ \psi(x)\psi(y) = \psi(xy)\}) < p^{-\delta}.$$

Proof. We notice that by Lemma 26, for large enough p, $V + \mathfrak{z}(\mathfrak{f}_p)$ is a proper subspace of $\mathfrak{g}(\mathfrak{f}_p)$ (which is normal in $\pi_{p^2}(P_p)$). And so without loss of generality we can assume that V contains $\mathfrak{z}(\mathfrak{f}_p)$.

Let $\mathcal{A} := \{(x, y) \in \pi_p(P_p) \times \pi_p(P_p) | \ \psi(x)\psi(y) = \psi(xy)\}$ and suppose to the contrary that $(\mu \times \mu)(\mathcal{A}) \geq p^{-\delta}$. We will get a contradiction if δ is small enough. Let ν be the push-forward of μ via ψ. For any $g \in \pi_p(P_p)$ we have

$$(\nu * \nu)(\psi(g)) = \sum_{h_1 h_2 = \psi(g)} \nu(h_1)\nu(h_2) = \sum_{\substack{x, \, y \, \in \, \pi_p(P_p) \\ \psi(x)\psi(y) \, = \, \psi(g)}} \mu(x)\mu(y) \qquad \text{(since supp } \nu = \mathrm{Im}\psi)$$

$$= \sum_{\substack{(x, \, y) \, \in \, \mathcal{A} \\ xy \, = \, g}} \mu(x)\mu(y). \qquad \begin{aligned}&\text{(since } g = \pi(\psi(g)) = \pi(\psi(x)\psi(y)) \\ &\quad = \pi(\psi(x))\pi(\psi(y)) = xy.)\end{aligned}$$

In particular, we have $(\nu * \nu)(\mathrm{supp}\,\nu) = (\mu \times \mu)(\mathcal{A})$. And so by the Cauchy-Schwarz inequality, we get

$$\sqrt{|\,\mathrm{supp}\,\nu|}\|\nu * \nu\|_2 \geq (\nu * \nu)(\mathrm{supp}\,\nu) = (\mu \times \mu)(\mathcal{A}) \geq p^{-\delta}.$$

Hence $\|\nu * \nu\|_2 \geq p^{-\delta}\|\nu\|_2$. Thus by [Var12, Lemma 15] (which is based on [BG08-a] (see Proposition 22)) there is a symmetric subset $S \subseteq \pi_{p^2}(P_p)/V$ with the following properties:

  (P1) $|\pi_p(P_p)|^{1-\Theta_\mathbb{G}(\delta)} \leq |S| \leq |\pi_p(P_p)|^{1+\Theta_\mathbb{G}(\delta)}$,
  (P2) $|\prod_3 S| \leq |\pi_p(P_p)|^{\Theta_\mathbb{G}(\delta)}|S|$,
  (P3) $\min_{s \in S}(\widetilde{\nu} * \nu)(s) \geq (|\pi_p(P_p)|^{\Theta_\mathbb{G}(\delta)}|S|)^{-1}$.

Since the push-forward $\pi[\nu]$ of ν via π is the probability Haar measure of $\pi_p(P_p)$, we have $\mu = \pi[\widetilde{\nu}*\nu]$. And so the third part of properties of S implies that $\mu(\pi(S)) \geq |\pi_p(P_p)|^{-\Theta_\mathbb{G}(\delta)}$. Therefore $|\pi(S)| \geq |\pi_p(P_p)|^{1-\Theta_\mathbb{G}(\delta)}$. On the other hand, by [SGV12, Corollary 14] and the main theorem of [LS74], we have that $\pi_p(P_p)$ is a quasi-random group; that means the minimal degree of its non-trivial irreducible representations is at least $|\pi_p(P_p)|^{\Theta_\mathbb{G}(1)}$ for large enough p. Thus by Gowers's result [Gow08] (we use the formulation in [NP11, Corollary 1]) we have that $\pi(\prod_3 S) = \pi_p(P_p)$ if δ is small enough. So $S' = \prod_3 S$ has the following properties:

  (1) $\pi(S') = \pi_p(P_p)$,
  (2) S' is a $|\pi_p(P_p)|^{\Theta_\mathbb{G}(\delta)}$-approximate subgroup by [Tao08, Corollary 3.11],
  (3) $|S'| \leq |\pi_p(P_p)|^{1+\Theta_\mathbb{G}(\delta)}$ by properties (P1) and (P2) of S.

Next we prove that there is $0 \neq x \in \prod_3 S' \cap (\mathfrak{g}(\mathfrak{f}_p)/V)$. We proceed by contradiction. For any $s_1, s_2 \in S'$, there is $s_3 \in S'$ such that $\pi(s_1 s_2) = \pi(s_3)$. Hence $s_1 s_2 s_3^{-1} \in \prod_3 S' \cap (\mathfrak{g}(\mathfrak{f}_p)/V)$, and so by the contrary assumption we have $s_1 s_2 = s_3$. Thus S' is a subgroup which contradicts Lemma 29.

Since V contains $\mathfrak{z}(\mathfrak{f}_p)$, $\pi(S) = \pi_p(P_p)$ acts on $(\mathfrak{g}(\mathfrak{f}_p)/V)$ via the adjoint action without non-zero fixed point for large enough p. Hence by [SGV12, Lemma 30], $\sum_{O_\mathbb{G}(1)} \pi(S') \cdot x$ contains a non-zero subspace of $\mathfrak{g}(\mathfrak{f}_p)/V$. Therefore $|\prod_{O_\mathbb{G}(1)} S' \cap (\mathfrak{g}(\mathfrak{f}_p)/V)| \geq p$, and we get $|\prod_{O_\mathbb{G}(1)} S'| \geq p|\pi_p(P_p)|$. Since S' is an approximate subgroup, we get

$$p|\pi_p(P_p)| \leq |\prod_{O_\mathbb{G}(1)} S'| \leq |\pi_p(P_p)|^{1+\Theta_\mathbb{G}(\delta)}.$$

So $p \leq |\pi_p(P_p)|^{\Theta_\mathbb{G}(\delta)}$ which is a contradiction for small enough δ (independent of p). $\square$

4.3. Bounded generation of perfect groups by commutators.

Lemma 31. *Let P be a finite p-group. Suppose $|P| = p^n$ and $|P/[P, P]| = p^m$. Then*

$$\prod_{n-m}\{[g_1, g_2] | \ g_1, g_2 \in P\} = [P, P],$$

where $[g_1, g_2] := g_1 g_2 g_1^{-1} g_2^{-1}$.

Proof. We proceed by induction on the nilpotency class of P. If P is abelian, there is nothing to prove. Now suppose the nilpotency class of P is c; that means its $c+1$-th lower central series $\gamma_{c+1}(P)$ is trivial and $\gamma_c(P)$

is not trivial. It is well-known that $\gamma_c(P)$ is an $\mathfrak{f}_p$-vector space which is spanned by the long commutators. So $\gamma_c(P)$ is contained in $\prod_{\dim_{\mathfrak{f}_p} \gamma_c(P)} \{[g_1, g_2] | g_1, g_2 \in P\}$. By the induction hypothesis, we have

$$\prod_{n-m-\dim_{\mathfrak{f}_p} \gamma_c(P)} \{[\bar{g}_1, \bar{g}_2] | \bar{g}_1, \bar{g}_2 \in P/\gamma_c(P)\} = P/\gamma_c(P).$$

And so $\prod_{n-m} \{[g_1, g_2] | g_1, g_2 \in P\} = P$. □

Lemma 32. *Let $\mathbb{G}$ be a Zariski-connected perfect $\mathbb{Q}$-subgroup of $(\mathrm{GL}_n)_{\mathbb{Q}}$, and let $\mathcal{G}$ be its Zariski-closure in $(\mathrm{GL}_n)_{\mathbb{Z}}$. Suppose that $\mathbb{G}$ is simply-connected; that means its semisimple part is simply-connected. Then there is a positive integer C depending on $\mathbb{G}$ such that for large enough prime p we have*

$$\prod_C \{[g_1, g_2] | g_1, g_2 \in \mathcal{G}_p(\mathfrak{f}_p)\} = \mathcal{G}_p(\mathfrak{f}_p),$$

where $\mathcal{G}_p = \mathcal{G} \times_{\mathrm{Spec}\,\mathbb{Z}} \mathrm{Spec}\,\mathfrak{f}_p$.

Proof. As it was mentioned earlier, for large enough p, $\mathcal{G}_p \simeq \mathcal{H}_p \ltimes \mathcal{U}_p$ is a perfect $\mathfrak{f}_p$-group, where $\mathcal{H}_p$ is a simply connected semisimple $\mathfrak{f}_p$-group and $\mathcal{U}_p$ is a unipotent $\mathfrak{f}_p$-group. Moreover $\mathcal{G}_p(\mathfrak{f}_p) = \mathcal{H}_p(\mathfrak{f}_p) \ltimes \mathcal{U}_p(\mathfrak{f}_p)$, and $V_p := \mathcal{U}_p(\mathfrak{f}_p)/[\mathcal{U}_p(\mathfrak{f}_p), \mathcal{U}_p(\mathfrak{f}_p)]$ is a completely reducible $\mathcal{H}_p(\mathfrak{f}_p)$-module with no non-zero fixed vector. Let $w(x_1, x_2) = [x_1, x_2]$ and, for any group K, let $w(K) := \{w(k_1, k_2) | k_1, k_2 \in K\}$. Then by [Sha09, Theorem 1.1] (see an alternative approach in [NP11, Theorem 3]) we have that $\prod_3 w(\mathcal{H}_p(\mathfrak{f}_p)) = \mathcal{H}_p(\mathfrak{f}_p)$ for large enough p.

Let $H_p = \mathcal{H}_p(\mathfrak{f}_p)$ and $G_p = H_p \ltimes V_p$. Let $\rho : H_p \to \mathrm{GL}(V_p)$ be the homomorphism induced from the action of H_p on V_p. Then $\prod_7 w(G_p)$ contains

$$\{\rho(h)((\rho(h') - I)(v)) | h, h' \in H_p, \ v \in V_p\}.$$

And so $\prod_{7\dim_{\mathfrak{f}_p} V_p} w(G_p)$ contains the $\mathfrak{f}_p[H_p]$-submodule M_p of V_p generated by $\{(\rho(h) - I)(v) | h \in H_p, \ v \in V_p\}$. Therefore H_p acts trivially on V_p/M_p. Since V_p is a completely reducible H_p-module with no non-zero fixed vectors, $M_p = V_p$. Thus

$$\prod_{O(\dim \mathbb{G})} w(G_p) = G_p.$$

And so by Lemma 31 applied for $P := \mathcal{U}_p(\mathfrak{f}_p)$ the claim follows. □

Lemma 33. *Let $\mathbb{G}$ and $\mathcal{G}$ be as in Lemma 32, and N be a positive integer. Suppose the unipotent radical of $\mathbb{G}$ is abelian. Then there is a positive integer C depending on $\mathcal{G}$ and N such that for large enough p we have*

$$\prod_C \{[g_1, g_2] | g_i \in \mathcal{G}(\mathbb{Z}/p^N\mathbb{Z})\} = \mathcal{G}(\mathbb{Z}/p^N\mathbb{Z}).$$

Proof. By Lemma 32 we get the case of $N = 1$. It is well-known that π_p induces the following short exact sequence

$$1 \to \mathfrak{g}(\mathfrak{f}_p) \to \mathcal{G}(\mathbb{Z}/p^2\mathbb{Z}) \xrightarrow{\pi_p} \mathcal{G}(\mathfrak{f}_p) \to 1,$$

where $\mathfrak{g} = \mathrm{Lie}(\mathcal{G})$, and the conjugation action of $\mathcal{G}(\mathbb{Z}/p^2\mathbb{Z})$ on $\mathfrak{g}(\mathfrak{f}_p)$ factors through the adjoint action of $\mathcal{G}(\mathfrak{f}_p)$. Let $\mathfrak{u}$ be the Lie algebra of the Zariski-closure of the unipotent radical of $\mathbb{G}$ in $\mathcal{G}$. For large enough p, $\mathcal{G}(\mathfrak{f}_p)$ and $\mathfrak{g}(\mathfrak{f}_p)$ are perfect, and $\mathfrak{g}(\mathfrak{f}_p)$ is a completely reducible $\mathcal{G}(f_p)$-module without any non-zero invariant vectors (as $\mathbb{U}$ is abelian). So by a similar argument as in the proof of Lemma 32, we have

$$\prod_{O_{\mathbb{G}}(1)} w(\mathcal{G}(\mathbb{Z}/p^2\mathbb{Z})) \supseteq \mathfrak{g}(\mathfrak{f}_p),$$

and so by Lemma 32, we have that

$$\prod_{O_{\mathbb{G}}(1)} w(\mathcal{G}(\mathbb{Z}/p^2\mathbb{Z})) = \mathcal{G}(\mathbb{Z}/p^2\mathbb{Z}).$$

Now using the facts that $\mathcal{G}(\mathbb{Z}_p)[p^i]/\mathcal{G}(\mathbb{Z}_p)[p^{i+1}] \simeq \mathfrak{g}(\mathfrak{f}_p)$, the group commutators are mapped to the Lie algebra commutators, and $\mathfrak{g}(f_p)$ is perfect, we get the desired result. (See [SG, Lemma 34] for the relations between the group commutators and the Lie algebra commutators.) □

4.4. **Proof of Theorem 1 for bounded powers of square-free integers.** Now we go to the proof of Theorem 1 for $\mathcal{C}_N := \{q \in \mathbb{Z}^+ | \gcd(q, q_0) = 1, \forall p \in V_f(\mathbb{Q}), v_p(q_0) \leq N\}$. Having the above lemmas the rest of the proof is a modification of the argument in [BV12, Section 3].

By Section 3.2, it is enough to prove Theorem 23 for $\mathcal{C}_N$. First we point out that it is enough to prove Theorem 23 for $\mathcal{C}_N^{\geq p_0} := \{q \in \mathbb{Z}^+ | \gcd(q, q_0) = 1, \forall p \in V_f(\mathbb{Q}), v_p(q_0) \leq N, \forall p \leq p_0, v_p(q_0) = 0\}$. This Lemma helps us to avoid all the small primes p where $\pi_p(\Gamma)$ does not behave nicely; in particular we will be able to assume Lemmas 26-33 to hold for all the prime divisors of Q.

Lemma 34. *Let p_0 be a prime number. Then a bounded generation in the sense of Theorem 23 for $\mathcal{C}_N^{\geq p_0}$ implies Theorem 23 for $\mathcal{C}_N$ where the implied constants depend also on p_0.*

Proof. Fix a positive number $\delta_0 := \delta_0(\varepsilon, \Omega, p_0)$ and a positive integer $C_0 := C_0(\varepsilon, \Omega, p_0)$ for which Theorem 23 holds for $\mathcal{C}_N^{\geq p_0}$.

For $Q \in \mathcal{C}_N$, let $q_0 := \prod_{p|Q, p \leq p_0} p^{v_p(Q)}$. Since $q_0 < p_0^{Np_0}$, we have $[\Gamma : \Gamma[q_0]] \ll_{\mathbb{G}, p_0, N} 1$. Suppose Q is large enough (depending only on $\varepsilon, \Omega, p_0, N$) such that the bounded generation for $\mathcal{C}_N^{\geq p_0}$ can be applied for $Q/q_0 \in \mathcal{C}_N^{\geq p_0}$. Moreover we assume Q is large enough (again depending only on $\varepsilon, \Omega, p_0, N$) such that $Q^{-\delta_0/2}/[\Gamma, \Gamma[q_0]] > (Q/q_0)^{-\delta_0}$. Now suppose δ is a positive number which is at most $\delta_0/4$, A is a symmetric set, and l is a positive integer which is more than $(1/\delta)\log Q$ such that $\mathcal{P}_\Omega^{(l)}(A) > Q^{-\delta}$. Then

$$\mathcal{P}_\Omega^{(2l)}(A \cdot A \cap \Gamma[q_0]) \geq Q^{-2\delta}/[\Gamma : \Gamma[q_0]] > Q^{-\delta_0/2}/[\Gamma : \Gamma[q_0]] > (Q/q_0)^{-\delta_0}.$$

Hence $\mathfrak{P}_{Q/q_0}(\delta_0, A \cdot A \cap \Gamma[q_0], l)$ holds. Therefore by the bounded generation for $\mathcal{C}_N^{\geq p_0}$ we have that

$$(46) \qquad \qquad \pi_{Q/q_0}(\Gamma[q]) \subseteq \pi_{Q/q_0}(\textstyle\prod_{C_0}(A \cdot A \cap \Gamma[q_0])),$$

for some $q|Q/q_0$ and $q \leq (Q/q_0)^\varepsilon$. Since Q and Q/q_0 are coprime, $\pi_Q(\Gamma)$ can be diagonally embedded into $\pi_{q_0}(\Gamma) \oplus \pi_{Q/q_0}(\Gamma)$, and by enlarging p_0, if needed, we can and will assume that $\pi_Q(\Gamma[qq_0])$ gets identified with $\{1\} \oplus \pi_{Q/q_0}(\Gamma[q])$ under the diagonal embedding of $\pi_Q(\Gamma)$ into $\pi_{q_0}(\Gamma) \oplus \pi_{Q/q_0}(\Gamma)$. Notice that $\pi_Q(A \cdot A \cap \Gamma[q_0])$ gets mapped to a subset of $\{1\} \oplus \pi_{Q/q_0}(\Gamma[q])$ and so by (46) we get that

$$\pi_Q(\Gamma[qq_0]) \subseteq \textstyle\prod_{2C_0} \pi_Q(A).$$

And we have $qq_0|Q$ and $qq_0 \leq Q^\varepsilon q_0^{1-\varepsilon} \leq Q^{2\varepsilon}$ for large enough Q (again depending on $\varepsilon, \Omega, p_0, N$). $\square$

Next we show a reduction which works for any family of positive integers $\mathcal{C}'$:

Lemma 35. *To prove Theorem 23 for Q in a family of positive integers $\mathcal{C}'$, it is enough to prove the bounded generation claim for a subset A for which $\mathfrak{P}_Q(\delta, A, l)$ and $\mathfrak{P}_Q(\delta, \rho_1(A), l)$ hold (where $\rho_1 : \mathbb{G} \to \mathbb{G}_s$ is the quotient map). That means for any $0 < \varepsilon \ll_\Omega 1$ there are $0 < \delta \ll_{\Omega,\varepsilon} 1$ and positive integer $C \gg_{\Omega,\varepsilon} 1$ for which the following holds:*

(Restricted BG): *$\mathfrak{P}_Q(\delta, A, l) \wedge \mathfrak{P}_Q(\delta, \rho_1(A), l)$ implies $\pi_Q(\Gamma[q]) \subseteq \prod_C \pi_Q(A)$ for some $q|Q$ such that*
$$q \leq Q^\varepsilon \text{ if } Q \in \mathcal{C}' \text{ and } Q^{\varepsilon^{O_\mathbb{G}(1)}} \gg_\Omega 1.$$

Proof. Suppose δ is a positive number and $\mathcal{P}_\Omega^{(l)}(A) > Q^{-\delta}$ for a symmetric set A and a positive integer $l > (1/\delta)\log Q$. Since $\ker(\rho_1) \cap \Gamma = \{1\}$, we have $\mathcal{P}_{\rho_1(\Omega)}^{(l)}(\rho_1(A)) > Q^{-\delta}$. Then by a similar argument as in (33) (based on the Kesten bound (see Inequality (14))) we have

$$(47) \qquad \qquad |\pi_Q(A)| > Q^{\eta_0} \text{ and } |\pi_Q(\rho_1(A))| > Q^{\eta_0},$$

for small enough δ (depending only on Ω) and some positive number $\eta_0 := \eta_0(\Omega)$ which depends only on Ω.

Fix a positive number $\delta_0 := \delta_0(\varepsilon, \Omega)$ and a positive integer $C_0 := C_0(\varepsilon, \Omega)$ for which the **Restricted BG** holds. And let

(48) $$I_A := \{i \in \mathbb{Z}^+ | \, |\textstyle\prod_{3^{i+1}} \pi_Q(A)| \leq |\textstyle\prod_{3^i} \pi_Q(A)|^{1+\delta_0}\} \text{ and}$$

(49) $$I_{\rho_1(A)} := \{i \in \mathbb{Z}^+ | \, |\textstyle\prod_{3^{i+1}} \pi_Q(\rho_1(A))| \leq |\textstyle\prod_{3^i} \pi_Q(\rho_1(A))|^{1+\delta_0}\}.$$

Notice that $|\pi_Q(\Gamma)| \leq Q^{N_0(\mathbb{G})}$ and $|\pi_Q(\rho_1(\Gamma))| \leq Q^{N_0(\mathbb{G})}$ for some positive integer N_0 which depends only on the dimension of $\mathbb{G}$. Now let $N_1 := N_1(\delta_0)$ be the smallest positive integer such that

(50) $$(1 + \delta_0)^{N_1}\eta_0 > N_0.$$

So by Inequalities (47) and (50), the complements of I_A and $I_{\rho_1(A)}$ in $\mathbb{Z}^+$ have at most N_1 elements. Hence there is a positive integer $C_1 \leq 3^{2N_1+1} \ll_{\Omega,\varepsilon} 1$ such that

$$|\pi_Q(\textstyle\prod_{C_1}\rho_1(A)) \cdot \pi_Q(\textstyle\prod_{C_1}\rho_1(A)) \cdot \pi_Q(\textstyle\prod_{C_1}\rho_1(A))| \leq |\pi_Q(\textstyle\prod_{C_1}\rho_1(A))|^{1+\delta_0} \text{ and}$$
$$|\pi_Q(\textstyle\prod_{C_1}A) \cdot \pi_Q(\textstyle\prod_{C_1}A) \cdot \pi_Q(\textstyle\prod_{C_1}A)| \leq |\pi_Q(\textstyle\prod_{C_1}A)|^{1+\delta_0}.$$

Therefore, if $\delta < \delta_0$, then $\mathfrak{P}_Q(\delta_0, \prod_{C_1}A, l)$ and $\mathfrak{P}_Q(\delta_0, \prod_{C_1}(\rho_1(A)), l)$ hold. Thus, by the **Restricted BG** and the fact that $C_1 C_0 \ll_{\Omega,\varepsilon} 1$, we are done. $\qquad\square$

(Going back to the proof of Theorem 23 for $\mathcal{C}_N$:) Suppose p_0 is a prime number such that $p_0 \ll_\Omega 1$ and all the claims of Lemmas 26-33 hold for all the primes $p \geq p_0$ (later we will assume p_0 is large enough depending on Ω to gain additional properties for $\pi_p(\Gamma)$ where p is a prime divisor of Q.). So by Lemma 34 we can assume that all the prime factors of Q are at least p_0. By Lemma 35 (for $\mathcal{C}' := \mathcal{C}_N^{\geq p_0}$), without loss of generality we can and will assume that $\mathfrak{P}_Q(\delta, A, l)$ and $\mathfrak{P}_Q(\delta, \rho_1(A), l)$ hold.

Let $Q_s := \prod_{p|Q} p$ (, and so $Q|Q_s^N$). By [SGV12, Theorem 1], [SG, Lemma 31], and $l > \frac{N}{\delta}\log Q_s$ we have that

$$\left| \mathcal{P}^{(l)}_{\pi_{Q_s}(\Omega)}(\pi_{Q_s}(A)) - \frac{|\pi_{Q_s}(A)|}{|\pi_{Q_s}(\Gamma)|} \right| \leq \frac{1}{|\pi_{Q_s}(\Gamma)|}$$

for small enough δ. And so we have

$$Q_s^{-N\delta} \leq Q^{-\delta} \leq \mathcal{P}^{(l)}_{\pi_{Q_s}(\Omega)}(\pi_{Q_s}(A)) \leq \frac{|\pi_{Q_s}(A)| + 1}{|\pi_{Q_s}(\Gamma)|},$$

which implies that $|\pi_{Q_s}(A)| \geq |\pi_{Q_s}(\Gamma)|Q_s^{-\Theta_{\Omega,N}(\delta)}$. Since we assumed that the prime factors of Q are large enough, we have that $\pi_{Q_s}(\Gamma) \simeq \prod_{p|Q}\pi_p(\Gamma)$. Writing $Q_s = \prod_{j=1}^l p_j$, to the product set $\prod_{i=1}^l \pi_{p_i}(\Gamma)$ one can associate a rooted tree with l levels. The root is considered to be the zero level. The vertices of the j-th level are elements of $\prod_{i=1}^j \pi_{p_i}(\Gamma)$, and each vertex is connected to its projection in the previous level. By a regularity argument similar to the proof of [SG, Lemma 12] (see [BGS10, Lemma 5.2] or [Var12, Page 26]), one can show that there are a set $A' \subseteq A$ and a sequence of integers $\{k_i\}_{i=1}^l$ such that for any $g \in A'$ and for any $1 \leq i \leq l$ we have

$$|\{x \in \pi_{p_i}(\Gamma)| \, \exists h \in A' : \, \pi_{p_1\cdots p_{i-1}}(h) = \pi_{p_1\cdots p_{i-1}}(g) \text{ and } \pi_{p_i}(h) = x\}| = k_i,$$

and

$$|A'| = \prod_{i=1}^l k_i \geq (\prod_{i=1}^l 2\log|\pi_{p_i}(\Gamma)|)^{-1}|A|.$$

By [SGV12, Corollary 14] and the main theorem of [LS74], $\pi_p(\Gamma)$ is a quasi-random group for large enough p; that means the dimension of any non-trivial irreducible representation of $\pi_p(\Gamma)$ is at least $|\pi_p(\Gamma)|^{\Theta_{\mathbb{G}}(1)}$ (for $p \gg_\Omega 1$) (see also Proposition 18). So by a result of Gowers [Gow08] (see [NP11, Corollary 1]) there is a positive number c_0 depending on $\mathbb{G}$ such that for large enough p the following holds: if $A, B, C \subseteq \pi_p(\Gamma)$

and $|A|, |B|, |C| \geq |\pi_p(\Gamma)|^{1-c_0}$, then $A \cdot B \cdot C = G$. We assume that the prime factors of Q are large enough so that $2 \log |\pi_{p_i}(\Gamma)| < |\pi_{p_i}(\Gamma)|^{c_0 \varepsilon}$. Hence

$$\prod_{i=1}^{l} k_i \geq |\pi_{Q_s}(\Gamma)|^{1-\Theta_{\mathbb{G}}(\delta)-c_0\varepsilon}.$$

Let $I := \{i|\ k_i < |\pi_{p_i}(\Gamma)|^{1-c_0}\}$; then we have

$$|\pi_{Q_s}(\Gamma)|/\prod_{i\in I} |\pi_{p_i}(\Gamma)|^{c_0} \geq \prod_{i=1}^{l} k_i \geq |\pi_{Q_s}(\Gamma)|^{1-\Theta_{\mathbb{G}}(\delta)-c_0\varepsilon},$$

and so

$$\prod_{i\in I} p_i \leq Q_s^{\Theta_{\mathbb{G}}(\delta)+2\varepsilon} \leq Q_s^{4\varepsilon},$$

for small enough δ (depending on Ω, N and ε). Now by a similar argument as in [Var12, Page 26] (using the mentioned result of Gowers) one can show that

(51) $\pi_{\prod_{i\notin I} p_i}(A \cdot A \cdot A) = \pi_{\prod_{i\notin I} p_i}(\Gamma).$

Let $Q'_s = \prod_{i\notin I} p_i$ and $q' = Q_s/Q'_s$. By (51) there is a function $f_1 : \pi_{Q'_s}(\Gamma) \to \pi_{q'^N}(\Gamma)$ such that $\{(g, f_1(g))|\ g \in \pi_{Q'_s}(\Gamma)\}$ is contained in $\pi_{Q'_s q'^N}(\prod_3 A)$. Thus there is a fiber of f_1 with at least $Q_s^{1-\Theta_{\mathbb{G},N}(\varepsilon)}$-many elements. Hence, as before by a regularization argument and another application of the mentioned Gowers's result (for $\varepsilon \ll_{\mathbb{G},N} 1$), there is $q''|Q'_s$ and a function $f_2 : \pi_{Q'_s/q''}(\Gamma) \to \pi_{q''}(\Gamma)$ such that $q'' \leq Q^{\Theta_{\mathbb{G},N}(\varepsilon)}$ and

$$\{(g, f_2(g), 1) \in \pi_{Q'_s/q''}(\Gamma) \times \pi_{q''}(\Gamma) \times \pi_{q'^N}(\Gamma)|g \in \pi_{Q'_s/q''}(\Gamma)\}$$

is contained in $\pi_{Q'_s q'^N}(\prod_{O_{\mathbb{G}}(1)} A)$. Hence, for any $g_1, g_2 \in \pi_{Q'_s/q''}(\Gamma)$, we have

$$([g_1, g_2], 1, 1) = [(g_1, f_2(g_1), 1), (g_2, 1, f_1(g_2, 1))] \in \pi_{Q'_s q'^N}(\prod_{O_{\mathbb{G}}(1)} A).$$

Therefore by Lemma 32

$$\pi_{Q'_s q'^N}(\Gamma[q'^N]) \subseteq \pi_{Q'_s q'^N}(\prod_{Q_{\mathbb{G}}(1)} A).$$

Let A' be a subset of $\prod_{Q_{\mathbb{G}}(1)} A$ such that $\pi_{Q'_s q'^N}(\Gamma[q'^N]) = \pi_{Q'_s q'^N}(A')$. Now we will go to the second level; that means we will show that there are a positive integer C and $\bar{q}|Q'_s$ such that $\bar{q} \leq Q^{\Theta_{\mathbb{G}}(\varepsilon)}$ and $\pi_{Q'_s{}^2}(\prod_C A')$ contains $\pi_{Q'_s{}^2}(\Gamma[\bar{q}^2])$.

Lemma 36. *In the above setting, assume $\mathbb{U}$ is abelian. Then for any $\varepsilon > 0$ there are $\delta > 0$ and a positive integer C such that the following holds.*

Assume $A \subseteq \Gamma$ and a square-free integer Q_s have the following properties:

   (1) *$Q_s^\varepsilon \gg_\Omega 1$.*
   (2) *The prime factors of Q_s are sufficiently large (depending on Ω); in particular the assertions of Lemma 29 hold, and $\pi_{Q_s^2}(\Gamma) \simeq \prod_{p|Q_s} \pi_{p^2}(\Gamma)$.*
   (3) *$\pi_{Q_s}(A) = \pi_{Q_s}(\Gamma)$.*
   (4) *For any prime factor p of Q_s, let $V_p \subsetneq \mathfrak{g}(\mathfrak{f}_p)$ be a $\pi_p(\Gamma)$-invariant under the adjoint action. And $\prod_{p|Q_s} V_p \subseteq \pi_{Q_s^2}(A)$.*

Then there are Q'_s and $\{M_p\}_{p|Q'_s}$ such that

   (1) *$Q'_s|Q_s$ and $Q_s^{1-\varepsilon} \leq Q'_s$.*
   (2) *For any p, we have $V_p \subsetneq M_p \subseteq \mathfrak{g}(\mathfrak{f}_p)$, and M_p is $\pi_p(\Gamma)$-invariant under the adjoint action.*
   (3) *$\prod_{p|Q'_s} M_p \oplus \prod_{p|(Q_s/Q'_s)} \{0\} \subseteq \pi_{Q_s^2}(\prod_C A).$*

Proof. Since $V_p \subseteq \mathfrak{g}(\mathfrak{f}_p)$, the map $\pi_p : \pi_{p^2}(\Gamma) \to \pi_p(\Gamma)$ factors through $\pi_{p^2}(\Gamma)/V_p$. Let us abuse the notation and still denote the induce homomorphism by $\pi_p : \pi_{p^2}(\Gamma)/V_p \to \pi_p(\Gamma)$. Let $\psi : \pi_{Q_s}(\Gamma) \to A \subseteq \Gamma$ be a section of π_{Q_s}, and $\psi_p : \pi_{Q_s}(\Gamma) \to \pi_{p^2}(\Gamma)/V_p$ be $\psi_p(g) = \pi_{p^2}(\psi(g))V_p$. As in the proof of [BV12, Proposition 3], let us consider the following expectation with respect to the probability Haar measure:

$$(52) \qquad \mathbb{E}\left(\sum_{p|Q_s,\ \psi_p(xy)=\psi_p(x)\psi_p(y)} \log p\right) = \sum_{p|Q_s} \log p \cdot (\mathcal{P}_{\pi_p(\Gamma)} \times \mathcal{P}_{\pi_p(\Gamma)})(\{(x,y)|\ \psi_p(xy) = \psi_p(x)\psi_p(y)\})$$

$$\leq \sum_{p|Q_s} p^{-\Theta_{\mathbb{G}}(1)} \log p \leq \log(Q_s^\varepsilon),$$

where the first inequality is given by Lemma 30 and the second inequality holds for $Q_s^\varepsilon \gg_{\mathbb{G}} 1$. Inequality (52) implies that

$$\mathbb{E}\left(\log\left(\prod_{p|Q_s\psi_p(x)\psi_p(y)\psi_p(xy)^{-1}\neq 1} p\right)\right) \geq \log(Q_s^{1-\varepsilon}).$$

So there are $x, y \in \pi_{Q_s}(\Gamma)$ and $Q_s'|Q_s$ such that $Q_s' \geq Q_s^{1-\varepsilon}$ and for any prime $p|Q_s'$ we have $z_p := \psi_p(x)\psi_p(y)\psi_p(xy)^{-1} \neq 1$. Hence there is $a \in \prod_3 A$ such that for any $p|Q_s'$ we have that $\pi_{p^2}(a)$ belongs to $\mathfrak{g}(\mathfrak{f}_p) \setminus V_p$ where $\mathfrak{g}(\mathfrak{f}_p)$ is identified with $\pi_{p^2}(\Gamma[p])$. By our assumptions on $\mathbb{G}$, $\pi_p(\Gamma)$ is generated by its p-elements and $\mathfrak{g}(\mathfrak{f}_p)$ is a completely reducible $\pi_p(\Gamma)$-module with no non-zero invariant vector (the latter holds as $\mathbb{G}$ is perfect and its unipotent radical is abelian). Therefore by [SGV12, Corollary 31] $\sum_{O_{\mathbb{G}}(1)} \pi_p(\Gamma) \cdot z_p$ is the $\pi_p(\Gamma)$-subspace M_p/V_p of $\mathfrak{g}(\mathfrak{f}_p)/V_p$ that is generated by z_p.

In the group $\pi_{Q_s^2}(\Gamma)/\prod_{p|Q_s} V_p$, for any $\gamma \in \Gamma$, we have

$$(53) \qquad \pi_{Q_s^2}(\gamma)\pi_{Q_s^2}(a)\pi_{Q_s^2}(\gamma)^{-1}\left(\prod_{p|Q_s} V_p\right) = (\pi_p(\gamma) \cdot z_p)_{p|Q_s} \in \prod_{p|Q_s} \mathfrak{g}(\mathfrak{f}_p)/V_p.$$

Since $\pi_{Q_s}(A) = \pi_{Q_s}(\Gamma)$ and $a \in \prod_3 A$, by (53) we have that $\pi_{Q_s'^2}(\prod_{O_{\mathbb{G}}(1)} A)\left(\prod_{p|Q_s} V_p\right)$ (as a subset of $\pi_{Q_s^2}(\Gamma)/\prod_{p|Q_s} V_p$) contains

$$\sum_{O_{\mathbb{G}}(1)} \pi_{Q_s'}(A) \cdot (z_p)_{p|Q_s'} = \prod_{p|Q_s'} \sum_{O_{\mathbb{G}}(1)} \pi_p(\Gamma) \cdot z_p = \prod_{p|Q_s'} M_p/V_p.$$

(Here $\pi_{Q_s^2}(\Gamma)/\prod_{p|Q_s} V_p$ is viewed as $(\pi_{Q_s'^2}(\Gamma)/\prod_{p|Q_s'} V_p) \oplus (\pi_{(Q_s/Q_s')^2}(\Gamma)/\prod_{p|Q_s/Q_s'} V_p)$.) And so

$$\prod_{p|Q_s'} M_p \subseteq \pi_{Q_s^2}(\prod_{O_{\mathbb{G}}(1)} A);$$

and the claim follows. $\qquad\square$

(Going back to the proof of Theorem 23 for $\mathcal{C}_N$:) By Equation (51) and a repeated use of Lemma 36 (for $O_{\mathbb{G}}(1)$-many times), we get that there is $q|Q_s$ such that $q \leq Q_s^{\Theta_{\mathbb{G}}(\varepsilon)}$ (if $Q_s^\varepsilon \gg_{\mathbb{G}} 1$) and

$$(54) \qquad \pi_{Q_s^2}(\prod_{O_{\mathbb{G}}(1)} A) \supseteq \pi_{Q_s^2}(\Gamma[q^2]) = \prod_{p|(Q_s/q)} \pi_{p^2}(\Gamma) \times \prod_{p|q}\{1\}.$$

Let us recall that for large enough p (depending only on Ω) we have that, for any positive integer i, there is a $\pi_p(\Gamma)$-module isomorphism $\Psi_{p^i}^{p^{i+1}} : \Gamma[p^i]/\Gamma[p^{i+1}] \to \mathfrak{g}(\mathfrak{f}_p)$; and for any $g_i \in \Gamma[p^i]$ and $g_j \in \Gamma[p^j]$ we have $[g_i, g_j] := g_i g_j g_i^{-1} g_j^{-1} \in \Gamma[p^{i+j}]$ and

$$(55) \qquad \Psi_{p^{i+j}}^{p^{i+j+1}}([g_i, g_j]\Gamma[p^{i+j+1}]) = [\Psi_{p^i}^{p^{i+1}}(g_i\Gamma[p^{i+1}]), \Psi_{p^j}^{p^{j+1}}(g_j\Gamma[p^{j+1}])],$$

where the right hand side is the Lie bracket in $\mathfrak{g}(\mathfrak{f}_p)$. (These maps are called the *truncated or finite logarithmic maps*. We refer the interested reader to [SG, Section 2.9] for a general and quick treatment of these maps and their basic properties.) Equation (55) defines a graded Lie algebra structure on

$$\Gamma[p]/\Gamma[p^2] \oplus \Gamma[p^2]/\Gamma[p^3] \oplus \cdots \oplus \Gamma[p^{N-1}]/\Gamma[p^N]$$

and shows that it is isomorphic to the graded Lie algebra $\mathfrak{g}(\mathfrak{f}_p) \otimes (t\mathfrak{f}_p[t]/t^N \mathfrak{f}_p[t])$ where $\mathfrak{f}_p[t]$ is the ring of polynomials in a single variable t, $[x_i \otimes \bar{t}^i, x_j \otimes \bar{t}^j] := [x_i, x_j] \otimes \bar{t}^{i+j}$ for any $x_i, x_j \in \mathfrak{g}(\mathfrak{f}_p)$, and $\bar{t} := t + t^N \mathfrak{f}_p[t]$. Since, for large enough p (depending only on Ω), $\mathfrak{g}(\mathfrak{f}_p)$ is a perfect Lie algebra, $\mathfrak{g}(\mathfrak{f}_p) \otimes (t\mathfrak{f}_p[t]/t^N \mathfrak{f}_p[t])$ is generated by the degree one elements, that means $\mathfrak{g}(\mathfrak{f}_p) \otimes \bar{t}$. So by (54) and (55) we get that

$$(56) \qquad \pi_{(Q_s/q)^N}\left(\prod_{O_{\mathbb{G},N}(1)} A\right) = \pi_{(Q_s/q)^N}(\Gamma) = \prod_{p \mid (Q_s/q)} \pi_{p^N}(\Gamma).$$

Hence there is a function $f_1 : \pi_{(Q_s/q)^N}(\Gamma) \to \pi_{q^N}(\Gamma[q])$ such that $G(f_1) := \{(g, f_1(g)) | g \in \pi_{(Q_s/q)^N}(\Gamma)\}$ is contained in $\pi_{Q_s^N}\left(\prod_{O_{\mathbb{G},N}(1)} A\right)$. Let $w(x_1, x_2) := x_1 x_2 x_1^{-1} x_2^{-1}$ and for any subset X of a group $w(X) := \{w(x_1, x_2) | x_1, x_2 \in X\}$. Then $w(G(f_1)) \subseteq \pi_{(Q_s/q)^N}(\Gamma) \times \pi_{q^N}(\Gamma[q^2])$. And so by Lemma 33 we have that there is a function $f_2 : \pi_{(Q_s/q)^N}(\Gamma) \to \pi_{q^N}(\Gamma[q^2])$ such that its graph $G(f_2)$ is contained in $\pi_{Q_s^N}\left(\prod_{O_{\mathbb{G},N}(1)} A\right)$. Repeating this argument $\log N$ times we get that $\pi_{Q_s^N}(\Gamma[q^N])$ is contained in $\pi_{Q_s^N}\left(\prod_{O_{\mathbb{G},N}(1)} A\right)$, which finishes the proof of Theorem 23 for $\mathcal{C}_N$.

5. Super-approximation: the p-adic case.

To prove Theorem 1 for $\mathcal{C} := \{p^m | p \in V_f(\mathbb{Q}), p \nmid q_0, m \in \mathbb{Z}^+\}$, by Section 3.2, it is enough to Prove Theorem 23 for $\mathcal{C}$.

In this section, we work in the setting of Section 2.6. In addition, we assume that $\mathbb{U}$ is abelian. So we assume that $\mathbb{V}$ is a vector $\mathbb{Q}$-group, $\mathbb{G}_s$ is a connected, simply-connected, semisimple $\mathbb{Q}$-group, there is a $\mathbb{Q}$-homomorphism $\mathbb{G} \to \mathbb{GL}(\mathbb{V})$ with no non-zero fixed vector, and $\mathbb{G} = \mathbb{G}_s \ltimes \mathbb{V}$ is the Zariski-closure of $\Gamma = \langle \Omega \rangle$. We also fix a $\mathbb{Q}$-embedding $\mathbb{G} \subseteq (\mathrm{GL}_{N_0})_{\mathbb{Q}}$.

By Lemma 35 (for $\mathcal{C}' := \mathcal{C}$), we can and will assume that $\mathfrak{P}_Q(\delta, A, l)$ and $\mathfrak{P}_Q(\delta, \rho_1(A), l)$ hold where $\rho_1 : \mathbb{G} \to \mathbb{G}_s$ is the quotient map.

It is worth pointing out that Theorem 23 for semisimple groups and powers of primes is proved in [SG, Theorem 36].

5.1. **Escape from proper subgroups.** In this section, we explore the pro-p structure of an open subgroup of the p-adic closure Γ_p of Γ. The main goal is to escape proper subgroups of $\pi_Q(\Gamma)$ where $Q = p^n$ is a power of a prime p.

Proposition 37. *In the above setting, there is a positive number δ (depending on Ω) such that for any $n \gg_\Omega 1$ and any proper subgroup H of $\pi_{p^n}(\Gamma)$ we have*

$$\mathcal{P}^{(l)}_{\pi_{p^n}(\Omega)}(H) \le [\pi_{p^n}(\Gamma) : H]^{-\delta},$$

for $l \ge \frac{n}{\delta} \log p$.

We start with a (well-known) lemma which gives us the Frattini subgroup of the congruence subgroups of $\mathcal{G}(\mathbb{Z}_p)$, where (as before) $\mathcal{G}$ is the closure of $\mathbb{G}$ in $(\mathrm{GL}_{N_0})_{\mathbb{Z}_S}$. This kind of result for semisimple groups and large p goes back to Weisfeiler [Wei84].

Lemma 38. *Let $\mathcal{G}$ be as above, and $G := \mathcal{G}(\mathbb{Z}_p)$. Suppose either $p \gg_{\mathcal{G}} 1$ or $m_0 \gg_{\mathcal{G}} 1$. If $\widetilde{H}$ is a closed subgroup of $G[p^{m_0}]$ and $\widetilde{H} G[p^{m_0+1}] = G[p^{m_0}]$, then $\widetilde{H} = G[p^{m_0}]$. And so the Frattini subgroup $\Phi(G[p^{m_0}]) = G[p^{m_0+1}]$.*

Proof. By induction on k we prove that $\widetilde{H}G[p^{m_0+k}] = G[p^{m_0}]$. The base of the induction is given by the assumption. To get the induction step, it is enough to prove that $(\widetilde{H} \cap G[p^{m_0+k}])G[p^{m_0+k+1}] = G[p^{m_0+k}]$. Let $\mathfrak{g} := \mathrm{Lie}(\mathcal{G})(\mathbb{Z}_p)$. By [SG, Lemma 34], we have $\Psi_{p^{m_0}}^{p^{m_0+1}} : G[p^{m_0}]/G[p^{m_0+1}] \to \mathfrak{g}/p\mathfrak{g}$ is an isomorphism if either $p \gg_{\mathcal{G}} 1$ or $m_0 \gg_{\mathcal{G}} 1$ (see [SG, Section 2.9] for the definition and properties of *finite logarithmic map* $\Psi_{p^{m_0}}^{p^{m_0+1}}$). And so by the assumption, for any $x \in \mathfrak{g}$ there is $h \in \widetilde{H}$ such that $\pi_{p^{m_0+1}}(h) = \pi_{p^{m_0+1}}(I + p^{m_0}x)$. On the other hand, if $m_0 \geq 2$, then $\pi_p(((I+p^{m_0}x')^p - I)/p^{m_0+1}) = \pi_p(x')$. And so $\Psi_{p^{m_0+k}}^{p^{m_0+k+1}}(\pi_{p^{m_0+k+1}}(h^{p^k})) = \pi_p(x)$. Since, by [SG, Lemma 34], $\Psi_{p^{m_0+k}}^{p^{m_0+k+1}} : G[p^{m_0+k}]/G[p^{m_0+k+1}] \to \mathfrak{g}/p\mathfrak{g}$ is a bijection, we get the induction step. Since $\widetilde{H}$ is a closed subgroup, we have that $\widetilde{H} = G[p^{m_0}]$. $\square$

The following lemma which is a module theoretic version of [SG05, Lemma 3.5] is proved next. It will be needed in the following sections, too.

Lemma 39. *Let $R \subseteq M_{n_0}(\mathbb{Z}_p)$ be a $\mathbb{Z}_p$-subalgebra (not necessarily with the identity element). Suppose $\mathbb{Q}_p^{n_0}$ is a simple $\mathbb{Q}_p[R]$-module, where $\mathbb{Q}_p[R]$ is the $\mathbb{Q}_p$-span of R. Then*

$$\sup_{v \in \mathbb{Z}_p^{n_0} \setminus p\mathbb{Z}_p^{n_0}} [\mathbb{Z}_p^{n_0} : Rv] < \infty.$$

Proof. Suppose to the contrary that there is a sequence of unit vectors v_i such that $[\mathbb{Z}_p^{n_0} : Rv_i]$ goes to infinity as i goes to infinity. Since the set of unit vectors is a compact set, by passing to a subsequence we can assume that $\lim_{i \to \infty} v_i = v$ where v is a unit vector. Since $\mathbb{Q}_p^{n_0}$ is a simple $\mathbb{Q}_p[R]$-module, the $\mathbb{Q}_p$-span of Rv is $\mathbb{Q}_p^{n_0}$. And so Rv is of finite-index in $\mathbb{Z}_p^{n_0}$. Therefore Rv contains $p^{k_0}\mathbb{Z}_p^{n_0}$ for some positive integer k_0. If i is large enough, $v - v_i \in p^{k_0+1}\mathbb{Z}_p$. So $Rv_i + p^{k_0+1}\mathbb{Z}_p^{n_0} = Rv + p^{k_0+1}\mathbb{Z}_p^{n_0} \supseteq p^{k_0}\mathbb{Z}_p^{n_0}$. Since Rv_i is complete and the Frattini subgroup of $p^{k_0}\mathbb{Z}_p^{n_0}$ is $p^{k_0+1}\mathbb{Z}_p^{n_0}$, $Rv_i \supseteq p^{k_0}\mathbb{Z}_p^{n_0}$ which is a contradiction. $\square$

The following lemma roughly shows that an almost invariant subspace of $\mathrm{Lie}(\mathbb{G}_s)(\mathbb{Q}_p)$ is close to an invariant subspace.

Lemma 40. *Let $\mathbb{G}_s \subseteq (\mathrm{GL}_{N_0})_{\mathbb{Q}}$ be (as before) a semisimple group. Let $G := \mathbb{G}_s(\mathbb{Q}_p) \cap \mathrm{GL}_{N_0}(\mathbb{Z}_p)[p^{k_0}]$ for a fixed positive integer k_0. Suppose m is large enough depending on the embedding of $\mathbb{G}_s$ in $(\mathrm{GL}_{N_0})_{\mathbb{Q}}$ and k_0. Then the following holds:*

Suppose W is a subspace of $\mathrm{Lie}(\mathbb{G}_s)(\mathbb{Q}_p)$ such that $\pi_{p^m}(W \cap \mathfrak{gl}_{N_0}(\mathbb{Z}_p))$ is invariant under G. Then there is a normal closed subgroup $\mathbb{G}_W$ of $\mathbb{G}_s$ and a positive integer C which depends only on the embedding of $\mathbb{G}_s$ in $(\mathrm{GL}_{N_0})_{\mathbb{Q}}$ and k_0 such that

$$(57) \qquad p^{2C}\pi_{p^{m-C}}(\mathfrak{g}_W) \subseteq p^C \pi_{p^{m-C}}(W \cap \mathfrak{gl}_{N_0}(\mathbb{Z}_p)) \subseteq \pi_{p^{m-C}}(\mathfrak{g}_W),$$

where $\mathfrak{g}_W := \mathrm{Lie}(\mathbb{G}_W)(\mathbb{Q}_p) \cap \mathfrak{gl}_{N_0}(\mathbb{Z}_p)$.

Proof. Since $\mathbb{G}_s$ is semisimple, it is the almost product of $\mathbb{Q}_p$-simple factors $\mathbb{G}_i$. And so $\mathrm{Lie}(\mathbb{G}) = \oplus_i \mathrm{Lie}(\mathbb{G}_i)(\mathbb{Q}_p)$. Let $\mathfrak{g} := \mathrm{Lie}(\mathbb{G})(\mathbb{Q}_p) \cap \mathfrak{gl}_{N_0}(\mathbb{Z}_p)$ and $\mathfrak{g}_i := \mathrm{Lie}(\mathbb{G}_i)(\mathbb{Q}_p) \cap \mathfrak{gl}_{N_0}(\mathbb{Z}_p)$. Then there is a positive number c_1 which depends only on the embedding of $\mathbb{G}_s$ in $(\mathrm{GL}_{N_0})_{\mathbb{Q}}$ such that

$$(58) \qquad \bigoplus_i \mathfrak{g}_i \subseteq \mathfrak{g} \subseteq \bigoplus_i p^{-c_1}\mathfrak{g}_i;$$

in particular, for any $x \in \mathrm{Lie}(\mathbb{G})(\mathbb{Q}_p)$, we have

$$(59) \qquad \|x\|_p \leq \max_i \|x_i\|_p \leq p^{c_1}\|x\|_p,$$

where $x = \sum_i x_i$ and $x_i \in \mathrm{Lie}(\mathbb{G}_i)(\mathbb{Q}_p)$.

Let $\mathfrak{W} := W \cap \mathfrak{gl}_{N_0}(\mathbb{Z}_p)$. For $x \in \mathfrak{W}$, let $x_i \in \mathrm{Lie}(\mathbb{G}_i)(\mathbb{Q}_p)$ be such that $x = \sum_i x_i$. For any $g_j \in \mathbb{G}_j(\mathbb{Q}_p) \cap \mathrm{GL}_{N_0}(\mathbb{Z}_p)[p^{k_0}]$, $\mathrm{Ad}(g_j)$ changes only the j-th component. So, using the assumption that $\pi_{p^m}(\mathfrak{W})$ is invariant under $\mathrm{Ad}(g_j)$, we get that

$$(60) \qquad \mathrm{Ad}(g_j)x_j - x_j \in \mathfrak{W} + p^m \mathfrak{gl}_{N_0}(\mathbb{Z}_p).$$

Hence $\mathfrak{a}_j x_j \subseteq \mathfrak{W} + p^m \mathfrak{gl}_{N_0}(\mathbb{Z}_p)$ where $\mathfrak{a}_j$ is the $\mathbb{Z}_p$-span of $\{\mathrm{Ad}(g_j) - I \mid g_j \in \mathbb{G}_j(\mathbb{Q}_p) \cap \mathrm{GL}_{N_0}(\mathbb{Z}_p)[p^{k_0}]\}$ (here we restrict to the action on $\mathrm{Lie}(\mathbb{G}_j)$, and consider $\mathfrak{a}_j$ as a subset of $\mathrm{End}_{\mathbb{Q}_p}(\mathrm{Lie}\,\mathbb{G}_j(\mathbb{Q}_p))$). Notice that $\mathfrak{a}_j$ is an ideal of the $\mathbb{Z}_p$-span R_j of $\mathrm{Ad}(\mathbb{G}_j(\mathbb{Q}_p) \cap \mathrm{GL}_{N_0}(\mathbb{Z}_p)[p^{k_0}])$. And $\mathrm{Lie}(\mathbb{G}_j)(\mathbb{Q}_p)$ is a simple $\mathbb{Q}_p[R_j]$-module, where $\mathbb{Q}_p[R_j]$ is the $\mathbb{Q}_p$-span of R_j. Hence $\mathbb{Q}_p[R_j]$ is a simple $\mathbb{Q}_p$-algebra as it has a simple faithful module. Therefore the $\mathbb{Q}_p$-span $\mathbb{Q}_p[\mathfrak{a}_j]$ of $\mathfrak{a}_j$ is R_j, and $\mathrm{Lie}(\mathbb{G}_j)(\mathbb{Q}_p)$ is a simple $\mathbb{Q}_p[\mathfrak{a}_j]$-module. Hence, by Lemma 38, there is a positive integer c_2 which depends only on k_0 and the embedding of $\mathbb{G}_s$ in $(\mathrm{GL}_{N_0})_{\mathbb{Q}}$ such that

$$(61) \qquad \bigoplus_j p^{c_2} \|x_j\|^{-1} \mathfrak{g}_j \subseteq \bigoplus_j \mathfrak{a}_j x_j \subseteq \mathfrak{W} + p^m \mathfrak{gl}_{N_0}(\mathbb{Z}_p).$$

Let $I_W := \{j \mid \exists x \in W, \|x\|_p = 1 \text{ and } \|x_j\|_p \geq 1, \text{ where } x = \sum_i x_i, \text{ and } x_i \in \mathrm{Lie}(\mathbb{G}_i)(\mathbb{Q}_p)\}$, $\mathbb{G}_W$ be the product of the simple factors $\mathbb{G}_i$ for $i \in I_W$; and so $\mathfrak{g}_W := (\oplus_{i \in I_W} \mathrm{Lie}(\mathbb{G}_i)(\mathbb{Q}_p)) \cap \mathfrak{gl}_{N_0}(\mathbb{Z}_p)$.

We can and will assume that $c_2 \geq c_1$, and we claim that (57) holds for $C := c_1 + c_2$ and $\mathfrak{g}_W$. We start with the *first inclusion* in (57).

For any $j \in I_W$, there is $x \in \mathfrak{W}$ such that its j-th simple component x_j has norm at least 1. Therefore by (61) we have $p^{c_2} \mathfrak{g}_j \subseteq \mathfrak{W} + p^m \mathfrak{gl}_{N_0}(\mathbb{Z}_p)$. And so by (58) we have

$$(62) \qquad p^{c_1+c_2} \mathfrak{g}_W \subseteq \bigoplus_{j \in I_W} p^{c_2} \mathfrak{g}_j \subseteq \mathfrak{W} + p^m \mathfrak{gl}_{N_0}(\mathbb{Z}_p).$$

To show the *second inclusion* in (57), we proceed by contradiction. So assume to the contrary that there is $x \in \mathfrak{W}$ such that $p^C \pi_{p^{m-C}}(x) \notin \pi_{p^{m-C}}(\mathfrak{g}_W)$. By (58) there are $x_j \in \mathfrak{g}_j$ such that $p^{c_1}x = \sum_j x_j$. By (62), there are $x' \in \mathfrak{W}$ and $e \in \mathfrak{g}$ such that

$$(63) \qquad p^{c_2} \sum_{i \in I_W} x_i = x' + p^m e.$$

Hence

$$(64) \qquad x'' := p^{c_1+c_2} x - x' = \sum_{j \notin I_W} p^{c_2} x_j + p^m e = \sum_{j \notin I_W} (p^{c_2} x_j + p^m e_j) + \sum_{j \in I_W} p^m e_j,$$

where $e = \sum_i e_i$ and $e_i \in \mathrm{Lie}(\mathbb{G}_i)(\mathbb{Q}_p)$, is contained in $\mathfrak{W}$. Since $e \in \mathfrak{g}$, we have $\|e\|_p \leq 1$. Therefore, by (59), we have

$$(65) \qquad \|p^m e_i\|_p \leq p^{-m+c_1}.$$

On the other hand, since $p^C \pi_{p^{m-C}}(x) \notin \pi_{p^{m-C}}(\mathfrak{g}_W)$ and $p^C x = p^{c_2} \sum_{i \in I_W} x_i + p^{c_2} \sum_{i \notin I_W} x_i \in \mathfrak{g}_W + p^{c_2} \sum_{i \notin I_W} x_i$, we have $\|p^{c_2} \sum_{j \notin I_W} x_j\|_p > p^{-m+C}$, which implies that there is $j_0 \notin I_W$ such that

$$(66) \qquad \|p^{c_2} x_{j_0}\|_p > p^{-m+C}.$$

So by the inequalities given in (65) and (66) we have

$$(67) \qquad \|p^{c_2} x_{j_0} + p^m e_{j_0}\| = \max\{\|p^{c_2} x_{j_0}\|_p, \|p^m e_{j_0}\|_p\} > p^{-m+C}.$$

Therefore

$$
\begin{aligned}
\|x''\|_p &\geq p^{-c_1} \|p^{c_2} x_{j_0} + p^m e_{j_0}\| && \text{(by (64) and (59))} \\
&> p^{-c_1} p^{-m+C} = p^{-m+c_2} \geq p^{-m+c_1} && \text{(by (67))} \\
&\geq \|p^m e_i\|_p. && \text{(by (65))}
\end{aligned}
$$

So after normalizing x'', we get a vector $\overline{x} \in W$ such that $\|\overline{x}\|_p = 1$ and, for any $i \in I_W$, $\|\overline{x}_i\|_p < 1$, where $\overline{x} = \sum_i \overline{x}_i$ and $\overline{x}_i \in \mathrm{Lie}(\mathbb{G}_i)(\mathbb{Q}_p)$. This is contrary to the definition of I_W.

$\square$

Lemma 41. *As before let $\mathbb{G} = \mathbb{G}_s \ltimes \mathbb{V} \subseteq (\mathrm{GL}_{N_0})_{\mathbb{Q}}$, where $\mathbb{G}_s$ is a semisimple connected simply-connected $\mathbb{Q}$-group and $\mathbb{V}$ is a $\mathbb{Q}$-vector group. Let $G := \mathbb{G}(\mathbb{Q}_p) \cap \mathrm{GL}_{N_0}(\mathbb{Z}_p)[p^{k_0}]$ for a fixed positive integer k_0. Suppose m is large enough depending on the embedding of $\mathbb{G}$ in $(\mathrm{GL}_{N_0})_{\mathbb{Q}}$ and k_0. Then the following holds:*

Suppose W is a subspace of $\mathrm{Lie}(\mathbb{G})(\mathbb{Q}_p)$ such that the projection of W onto $\mathrm{Lie}(\mathbb{G}_s)(\mathbb{Q}_p)$ is onto and $\pi_{p^m}(W \cap \mathfrak{gl}_{N_0}(\mathbb{Z}_p))$ is invariant under G. Then $W = \mathrm{Lie}(\mathbb{G})(\mathbb{Q}_p)$.

Proof. Without loss of generality we can and will assume that $\mathbb{V}$ is non-zero. Suppose $\mathbb{G}_s$ acts on $\mathbb{V}$ via $\rho : \mathbb{G}_s \to \mathrm{GL}(\mathbb{V})$; that means for any $g \in \mathbb{G}_s(R)$ and $v \in \mathbb{V}(R)$ we have $(g, 0)(1, v)(g, 0)^{-1} := (1, \rho(g)(v))$ in $\mathbb{G}(R)$ for any $\mathbb{Q}$-algebra R. To get a clear computation of the adjoint action, we use the *dual numbers* $\mathbb{Q}_p[\varepsilon] := \mathbb{Q}_p \oplus \mathbb{Q}_p \varepsilon$ where $\varepsilon^2 = 0$ (this lemma is the only place where ε is *not* a real number, and it is an element of the dual numbers.). Recall that we can identify $\mathrm{Lie}(\mathbb{G})(\mathbb{Q}_p)$ with

$$\ker \left(\mathbb{G}_s(\mathbb{Q}_p[\varepsilon]) \ltimes \mathbb{V}(\mathbb{Q}_p[\varepsilon]) \xrightarrow{\pi_\varepsilon} \mathbb{G}_s(\mathbb{Q}_p) \ltimes \mathbb{V}_p(\mathbb{Q}_p) \right)$$

where π_ε is the group homomorphism induced by the ring homomorphism $\pi_\varepsilon : \mathbb{Q}_p[\varepsilon] \to \mathbb{Q}_p$. Under this identification the adjoint action is given by conjugation; that means, for $x \in \mathrm{Lie}(\mathbb{G})(\mathbb{Q}_p)$, we have $1 + \varepsilon x \in \mathbb{G}(\mathbb{Q}_p[\varepsilon])$; and for $g \in \mathbb{G}(\mathbb{Q}_p)$, we have $1 + \varepsilon \mathrm{Ad}(g)(x) = g(1 + \varepsilon x)g^{-1}$.

The identity element of $\mathbb{G} = \mathbb{G}_s \ltimes \mathbb{V}$ is $(1, 0)$. And so $(x, w) \in \mathrm{Lie}(\mathbb{G})(\mathbb{Q}_p)$ if and only if $(1 + \varepsilon x, \varepsilon w) \in \mathbb{G}(\mathbb{Q}_p[\varepsilon])$; and to compute $\mathrm{Ad}(v)(x, w)$ we have to compute $(1, v)(1 + \varepsilon x, \varepsilon w)(1, v)^{-1}$ in $\mathbb{G}(\mathbb{Q}_p[\varepsilon])$. We have

$$(1, v)(1 + \varepsilon x, \varepsilon w)(1, -v) = (1, v)(1 + \varepsilon x, 0)(1, \varepsilon w - v)$$
$$= (1 + \varepsilon x, \rho(1 - \varepsilon x)(v) - v + \varepsilon w) = (1 + \varepsilon x, \varepsilon(d\rho(x)(v) + w)),$$

which means $\mathrm{Ad}(1, v)(x, w) = (x, d\rho(x)(v) + w)$. Notice that we are slightly abusing the notation and use the addition for the group operation of $\mathbb{V}$ though it is realized as a subgroup of $(\mathrm{GL}_{N_0})_{\mathbb{Q}}$. By this computation, for any $(x, w) \in W$ and $v \in \mathbb{V}(\mathbb{Q}_p) \cap \mathrm{GL}_{N_0}(\mathbb{Z}_p)$, we have

$$p^{k_0} d\rho(x)(v) := (0, p^{k_0} d\rho(x)(v)) = \mathrm{Ad}(p^{k_0} v)(x, w) - (x, w) \in (W \cap \mathfrak{gl}_{N_0}(\mathbb{Z}_p)) + p^m \mathfrak{gl}_{N_0}(\mathbb{Z}_p).$$

Thus we have

$$p^{k_0} d\rho \left(\mathrm{Lie}(\mathbb{G}_s)(\mathbb{Q}_p) \cap \mathfrak{gl}_{N_0}(\mathbb{Z}_p) \right) \left(\mathbb{V}(\mathbb{Q}_p) \cap \mathfrak{gl}_{N_0}(\mathbb{Z}_p) \right) \subseteq (W \cap \mathfrak{gl}_{N_0}(\mathbb{Z}_p)) + p^m \mathfrak{gl}_{N_0}(\mathbb{Z}_p).$$

Since $\mathbb{V}$ is a completely reducible $\mathbb{G}_s$ module with no trivial factors, we have

$$d\rho \left(\mathrm{Lie}(\mathbb{G}_s)(\mathbb{Q}_p) \cap \mathfrak{gl}_{N_0}(\mathbb{Z}_p) \right) \left(\mathbb{V}(\mathbb{Q}_p) \cap \mathfrak{gl}_{N_0}(\mathbb{Z}_p) \right) \supseteq p^{O(1)}(\mathbb{V}(\mathbb{Q}_p) \cap \mathfrak{gl}_{N_0}(\mathbb{Z}_p)),$$

where the implied constant depends on $\mathbb{G}$ and its embedding into $(\mathrm{GL}_{N_0})_{\mathbb{Q}}$. Therefore $\mathbb{V}(\mathbb{Q}_p) \subseteq W$; and the claim follows. $\square$

The next lemma is crucial in proving the bounded generation claim and its proof is fairly involved. By the strong-approximation, we know that the S-arithmetic group $\Gamma_0 := \mathbb{G}(\mathbb{Q}) \cap \mathrm{GL}_{N_0}(\mathbb{Z}_S)$, when infinite, is dense in $G_p := \mathbb{G}(\mathbb{Q}_p) \cap \mathrm{GL}_{N_0}(\mathbb{Z}_p)$ for any prime p which is not in S (here $\mathbb{G}$ is as before a simply-connected, connected, perfect $\mathbb{Q}$-group.). And so for any open subgroup $\widetilde{H}$ of G_p, $\Gamma_0 \cap \widetilde{H}$ is dense in $\widetilde{H}$. The next lemma shows that elements of $\Gamma_0 \cap \widetilde{H}$ with the S-norm at most $[G_p : \widetilde{H}]^{O_{\Gamma_0}(1)}$ are, however, trapped within a proper algebraic subgroup of $\mathbb{G}$.

Let ν_∞ be the Archimedean place of $\mathbb{Q}$, and $\widetilde{S} := \{\nu_\infty\} \cup S$. Notice that $\mathbb{Z}_S$ can be diagonally embedded in $\prod_{\nu \in \widetilde{S}} \mathbb{Q}_\nu$ as a discrete subgroup. Let $\|\mathbf{x}\|_{\nu_\infty} := \sqrt{\sum_i x_i^2}$ for $\mathbf{x} = (x_1, \dots, x_{N_0}) \in \mathbb{R}^{N_0}$, and $\|\mathbf{x}\|_p := \max\{|x_i|_p\}_i$ for $\mathbf{x} = (x_1, \dots, x_{N_0}) \in \mathbb{Q}_p^{N_0}$. For any $(\mathbf{x}_\nu) \in \prod_{\nu \in \widetilde{S}} \mathbb{Q}_\nu^{N_0}$, let $\|(\mathbf{x}_\nu)\|_{\widetilde{S}} := \max_{\nu \in \widetilde{S}} \|\mathbf{x}_\nu\|_\nu$. For any $\lambda \in \mathrm{GL}_{N_0}(\mathbb{Z}_S)$, we let $\|\lambda\|_S$ be the operator norm of $\lambda : \prod_{\widetilde{S}} \mathbb{Q}_\nu^{N_0} \to \prod_{\widetilde{S}} \mathbb{Q}_\nu^{N_0}$.

Lemma 42. *As before, let* $\mathbb{G} = \mathbb{G}_s \ltimes \mathbb{V} \subseteq (\mathrm{GL}_{N_0})_{\mathbb{Q}}$, *where* $\mathbb{G}_s$ *is a semisimple, connected, simply-connected* $\mathbb{Q}$-*group and* $\mathbb{V}$ *is a* $\mathbb{Q}$-*vector group. Let* $\mathcal{G}$ *be the Zariski-closure of* $\mathbb{G}$ *in* $(\mathrm{GL}_{N_0})_{\mathbb{Z}}$; *in particular* $\mathcal{G}(\mathbb{Z}_S) = \mathbb{G}(\mathbb{Q}) \cap \mathrm{GL}_{N_0}(\mathbb{Z}_S)$ *for any finite set of primes* S. *Let* S *be a finite set of primes such that* $\mathcal{G}(\mathbb{Z}_S)$ *is infinite.* *Suppose either* $p \gg_{\mathcal{G}} 1$ *or* $m_0 \gg_{\mathcal{G}} 1$. *Let* $G := \mathcal{G}(\mathbb{Z}_p)$. *Then there is a positive number* δ *such that for any prime* $p \notin S$ *and an open subgroup* $\widetilde{H}$ *of* $G[p^{m_0}]$ *the set*

$$\mathcal{L}_{\delta}(\widetilde{H}) := \{\lambda \in \mathcal{G}(\mathbb{Z}_S) \cap \widetilde{H} | \ \|\lambda\|_S \leq [\mathcal{G}(\mathbb{Z}_p) : \widetilde{H}]^{\delta}\}$$

is in a proper Zariski-closed subgroup of $\mathbb{G}$.

Proof. Since $\mathrm{GL}_{N_0}(\mathbb{Z}_S)$ is a discrete set with respect to the S-norm, we can and will assume that $[\mathcal{G}(\mathbb{Z}_p) : \widetilde{H}]$ is large enough. Otherwise choosing δ small enough, we have that $\mathcal{L}_{\delta}(\widetilde{H})$ is a subset of a finite subgroup and we are done.

Suppose p or m_0 are large enough so that Lemma 38 holds. Let $G := \mathcal{G}(\mathbb{Z}_p)$, $\mathfrak{g} := \mathrm{Lie}(\mathcal{G})(\mathbb{Z}_p)$, and

$$l(\widetilde{H}) := \min\{k \in \mathbb{Z}^+ | \ \widetilde{H} \supseteq G[p^k]\}.$$

Notice that, since $\widetilde{H}$ is an open subgroup, $l(\widetilde{H})$ is finite. By Lemma 38, for any $m_0 \leq k \leq l(\widetilde{H}) - 1$, we have that $(\widetilde{H} \cap G[p^k])G[p^{k+1}]/G[p^{k+1}]$ is a proper $\mathfrak{f}_p$-subspace of $G[p^k]/G[p^{k+1}] \simeq \mathfrak{g}/p\mathfrak{g}$. Thus we have

$$(68) \qquad\qquad\qquad p^{l(\widetilde{H})-m_0} \leq [G[p^{m_0}] : \widetilde{H}] \leq p^{d(l(\widetilde{H})-m_0)},$$

where $d = \dim_{\mathfrak{f}_p} \mathfrak{g}/p\mathfrak{g}$.

Our first goal is to find a *linear separation* of an $\mathrm{Ad}(\widetilde{H})$-orbit with a *good margin* (see Claim 1) when $l(\widetilde{H})$ is large enough depending only on $\mathcal{G}$. To achieve this goal, we start with finding *primitive* $\mathbb{Z}_p$-submodules of $\mathfrak{g}$ and $\mathfrak{g}_s := \mathrm{Lie}(\mathbb{G}_s)(\mathbb{Q}_p) \cap \mathfrak{g}$ that are *almost* $\mathrm{Ad}(\widetilde{H})$-invariant (see (71) and (80)).

Notice that, since $\mathbb{V}$ is a direct sum of non-trivial simple $\mathbb{G}_s$-modules, for any prime p, $\mathbb{G}(\mathbb{Q}_p) = \mathbb{G}_s(\mathbb{Q}_p) \ltimes \mathbb{V}(\mathbb{Q}_p)$ is compactly generated. Hence, by a result of Kneser [Kne64], $\mathcal{G}(\mathbb{Z}_S)$ is a finitely generated group. We fix a finite generating set Ω' of $\mathcal{G}(\mathbb{Z}_S)$.

Claim 1. For any constant $C_0 > 1$ (later it will depend on $\dim \mathbb{G}$), there is $c(\mathcal{G})$ such that, if $l(\widetilde{H}) \gg_{\mathcal{G}, C_0} 1$, then for some $w \in \mathfrak{g}$ and $L \in \mathfrak{g}^* := \mathrm{Hom}_{\mathbb{Z}_p}(\mathfrak{g}, \mathbb{Z}_p)$ the following holds

(1) for any $h \in \widetilde{H}$, $|L(\mathrm{Ad}(h)(w))|_p \leq [\mathcal{G}(\mathbb{Z}_p) : \widetilde{H}]^{-c}$;
(2) for some $\gamma \in \Omega'$, $|L(\mathrm{Ad}(\gamma)(w))|_p \geq [\mathcal{G}(\mathbb{Z}_p) : \widetilde{H}]^{-c/C_0}$.

Proof of Claim 1. Let

$$\overline{V} := \Psi^{p^l}_{p^{l'}}((\widetilde{H} \cap G[p^{l'}])G[p^l]/G[p^l]) \subseteq \mathfrak{g}/p^{l-l'}\mathfrak{g},$$

where $l := l(\widetilde{H})$ and $l' := \lceil l/2 \rceil + m_0$ (Recall that $\Psi^{p^l}_{p^{l'}}(1 + p^{l'}x) := \pi_{p^{l-l'}}(x)$ is a *finite logarithmic map*.). So there are a $\mathbb{Z}_p$-basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_d\}$ of $\mathfrak{g}$ and positive integers $n_1 \leq \cdots \leq n_{d'}$ such that $\overline{V} = \pi_{p^{l-l'}}(\sum_{i=1}^{d'} p^{n_i}\mathbb{Z}_p\mathbf{e}_i)$ (for some $d' \leq d$). Since

$$0 = n_0 \leq n_1 \leq \cdots \leq n_{d'} \leq \lfloor l/2 \rfloor - m_0 =: n_{d'+1},$$

there is i_0 such that

$$(69) \qquad\qquad\qquad (1/2d)l - m_0 - 1 < n_{i_0} - n_{i_0-1} \leq (1/2)l - m_0.$$

Let $\mathfrak{W}_1 := \sum_{i=1}^{i_0-1} p^{n_i}\mathbb{Z}_p\mathbf{e}_i \subset \mathfrak{g}$ (if $i_0 = 1$, then $\mathfrak{W}_1 = 0$). So

$$(70) \qquad\qquad\qquad \mathrm{Ad}(\widetilde{H})(\mathfrak{W}_1) \subseteq \mathfrak{W}_1 + p^{n_{i_0}}\mathfrak{g}.$$

Let $\mathfrak{W}_2 := \sum_{i=1}^{i_0-1} \mathbb{Z}_p \mathbf{e}_i$. Notice that $\mathfrak{W}_2 = W_1 \cap \mathfrak{g}$ where $W_1 = \sum_{i=1}^{i_0-1} \mathbb{Q}_p \mathbf{e}_i$ is the $\mathbb{Q}_p$-span of $\mathfrak{W}_1$. Since $\pi_{p^{n_{i_0}}}(\mathfrak{W}_1)$ is $\widetilde{H}$-invariant, for any $1 \le i \le i_0 - 1$ and $h \in \widetilde{H}$ we have

$$\mathrm{Ad}(h)(p^{n_i}\mathbf{e}_i) = \sum_{j=1}^{i_0-1} c_j p^{n_j} \mathbf{e}_j + \sum_{j=1}^{d} p^{n_{i_0}} c'_j \mathbf{e}_j,$$

where $c_j, c'_j \in \mathbb{Z}_p$. Therefore

$$\mathrm{Ad}(h)(\mathbf{e}_i) = \sum_{j=1}^{i_0-1} (c_j p^{n_j - n_i} + p^{n_{i_0} - n_i} c'_j) \mathbf{e}_j + \sum_{j=i_0}^{d} p^{n_{i_0} - n_i} c'_j \mathbf{e}_j.$$

Since $\mathfrak{g}$ is $\widetilde{H}$-invariant, we have $c_j p^{n_j - n_i} + p^{n_{i_0} - n_i} c'_j \in \mathbb{Z}_p$. Since n_j is increasing, we have $p^{n_{i_0} - n_i} \ge p^{n_{i_0} - n_{i_0 - 1}}$ for any $i < i_0$. Hence we have

$$(71) \qquad \mathrm{Ad}(\widetilde{H})(\mathfrak{W}_2) \subseteq \mathfrak{W}_2 + p^{n_{i_0} - n_{i_0 - 1}} \mathfrak{g}.$$

Next we would like to get some invariance in the semisimple part of $\mathfrak{g}$. We notice that $\mathrm{Lie}(\mathbb{G})(\mathbb{Q}_p) = \mathrm{Lie}(\mathbb{G}_s)(\mathbb{Q}_p) \oplus \mathbb{V}(\mathbb{Q}_p)$ (we are identifying $\mathbb{V}$ with its Lie algebra.). For any $x \in \mathrm{Lie}(\mathbb{G})(\mathbb{Q}_p)$, we write its components in the above decomposition by x_s and x_v; that means $x = x_s + x_v$ where $x_s \in \mathrm{Lie}(\mathbb{G}_s)(\mathbb{Q}_p)$ and $\mathrm{Lie}(\mathbb{V})(\mathbb{Q}_p)$. There is a positive integer d_1 depending only on $\mathcal{G}$ such that

$$(72) \qquad \|x\|_p \le \max\{\|x_s\|_p, \|x_v\|_p\} \le p^{d_1} \|x\|_p \qquad \text{and} \qquad \mathfrak{g}_s \oplus \mathfrak{V} \subseteq \mathfrak{g} \subseteq p^{-d_1}(\mathfrak{g}_s \oplus \mathfrak{V}),$$

where $\mathfrak{g}_s := \mathrm{Lie}(\mathbb{G}_s)(\mathbb{Q}_p) \cap \mathfrak{g}$ and $\mathfrak{V} := \mathbb{V}(\mathbb{Q}_p) \cap \mathfrak{g}$. Let $\mathfrak{W}_{2,s} := \{x_s \mid x \in \mathfrak{W}_2\}$ be the projection to $\mathrm{Lie}(\mathbb{G}_s)(\mathbb{Q}_p)$ of $\mathfrak{W}_2$. And so, by (71) and the fact that $\mathbb{V}$ is a normal subgroup of $\mathbb{G}$, we have

$$(73) \qquad \mathrm{Ad}(\widetilde{H})(\mathfrak{W}_{2,s}) \subseteq \mathfrak{W}_{2,s} + \mathbb{V}(\mathbb{Q}_p) + p^{n_{i_0} - n_{i_0 - 1}} \mathfrak{g}.$$

By (72), $p^{d_1} \mathfrak{W}_{2,s}$ is a $\mathbb{Z}_p$-submodule of $\mathfrak{g}_s$. Hence $\mathfrak{g}_s$ has a $\mathbb{Z}_p$-basis $\mathbf{f}_1, \ldots, \mathbf{f}_{d_s}$ such that

$$(74) \qquad \mathfrak{W}_{2,s} = \sum_{i=1}^{d'_s} p^{n'_i} \mathbb{Z}_p \mathbf{f}_i$$

for some integers $-d_1 =: n'_0 \le n'_1 \le \cdots \le n'_{d'_s} < n'_{d'_s + 1} := \infty$. Let j_0 be the smallest index such that

$$(75) \qquad n'_{j_0 + 1} - n'_{j_0} \ge \frac{n_{i_0} - n_{i_0 - 1} - d_1}{2 d_s}.$$

(Notice that, since $n'_0 := 0$ and $n'_{d'_s + 1} := \infty$, there is such j_0.) In particular, we have

$$(76) \qquad n'_{j_0} < \frac{n_{i_0} - n_{i_0 - 1} - d_1}{2}.$$

Let $\mathfrak{W}_{3,s} := \sum_{i=1}^{j_0} \mathbb{Z}_p \mathbf{f}_i$. Notice that $\mathfrak{W}_{3,s} = W_{3,s} \cap \mathfrak{g}_s$ where $W_{3,s} = \sum_{i=1}^{j_0} \mathbb{Q}_p \mathbf{f}_i$. So by (73) and (72) for any $1 \le i \le j_0$ and $h \in \widetilde{H}$, we have

$$\mathrm{Ad}(h)(p^{n'_i} \mathbf{f}_i) = \sum_{j=1}^{d'_s} p^{n'_j} c_{j,s} \mathbf{f}_j + p^{n_{i_0} - n_{i_0 - 1}} \sum_{j=1}^{d_s} p^{-d_1} c'_{j,s} \mathbf{f}_j + v_i,$$

where $c_{j,s}, c'_{j,s} \in \mathbb{Z}_p$ and $v_i \in \mathbb{V}(\mathbb{Q}_p)$. Therefore

$$(77) \qquad (\mathrm{Ad}(h)(\mathbf{f}_i))_s = \sum_{j=1}^{d'_s} (p^{n'_j - n'_i} c_{j,s} + p^{n_{i_0} - n_{i_0 - 1} - d_1 - n'_i} c'_{j,s}) \mathbf{f}_j + \sum_{j=d'_s}^{d_s} p^{n_{i_0} - n_{i_0 - 1} - d_1 - n'_i} c'_{j,s} \mathbf{f}_j.$$

Since, for any $x_s \in \mathfrak{g}_s$ and $h \in \widetilde{H}$, $(\mathrm{Ad}(h)(x_s))_s \in \mathfrak{g}_s$, we have $p^{n'_j - n'_i} c_{j,s} + p^{n_{i_0} - n_{i_0-1} - d_1 - n'_i} c'_{j,s} \in \mathbb{Z}_p$ and $p^{n_{i_0} - n_{i_0-1} - d_1 - n'_i} c'_{j,s} \in \mathbb{Z}_p$. By (76) we have

$$(78) \qquad n_{i_0} - n_{i_0-1} - d_1 - n'_i > \frac{n_{i_0} - n_{i_0-1} - d_1}{2}.$$

By (75), for $j \geq j_0 + 1$ and $i \leq j_0$, we have

$$(79) \qquad n'_j - n'_i \geq \frac{n_{i_0} - n_{i_0-1} - d_1}{2d_s}.$$

By (77), (78), and (79), we get

$$(80) \qquad \mathrm{Ad}(\widetilde{H})(\mathfrak{W}_{3,s}) \subseteq \mathfrak{W}_{3,s} + \mathbb{V}(\mathbb{Q}_p) + p^{\lfloor (n_{i_0} - n_{i_0-1} - d_1)/(2d_s) \rfloor} \mathfrak{g}_s.$$

Having (71) and (80), we are ready to find the desired *linear separation* of an $\mathrm{Ad}(\widetilde{H})$-orbit. We do this considering various cases.

Case 1. *Suppose*

$$(81) \qquad \mathrm{Ad}(\mathcal{G}(\mathbb{Z}_S))(\mathfrak{W}_{3,s}) \not\subseteq \mathfrak{W}_{3,s} + \mathbb{V}(\mathbb{Q}_p) + p^{\lfloor (n_{i_0} - n_{i_0-1} - d_1)/(4d_s C_0) \rfloor} \mathfrak{g}_s.$$

By (81), we have that there is $\lambda \in \Omega'$ and $1 \leq i \leq j_0$ such that

$$(82) \qquad (\mathrm{Ad}(\lambda)(\mathbf{f}_i))_s \notin \mathfrak{W}_{3,s} + p^{\lfloor (n_{i_0} - n_{i_0-1} - d_1)/(4d_s C_0) \rfloor} \mathfrak{g}_s.$$

For $1 \leq i \leq j_0$, let $\mathbf{f}_i^* : \mathfrak{g} \to \mathbb{Z}_p$ be a $\mathbb{Z}_p$-linear map such that

$$\mathbf{f}_i^*(\mathbf{f}_i) = p^{d_1}, \ \mathbf{f}_i^*(\mathbf{f}_j) = 0 \text{ for } j \neq i, \text{ and } \mathbf{f}_i^*(x) = \mathbf{f}_i^*(x_s).$$

(Here x_s is the $\mathrm{Lie}(\mathbb{G}_s)(\mathbb{Q}_p)$-component of x; and notice that because of (72) the image of $\mathbf{f}_i^*$ is a subset of $\mathbb{Z}_p$.) By (82), we have that there is $j > j_0$ such that

$$(83) \qquad |\mathbf{f}_j^*(\mathrm{Ad}(\lambda)(\mathbf{f}_i))|_p > p^{-\lfloor (n_{i_0} - n_{i_0-1} - d_1)/(4d_s C_0) \rfloor}.$$

And, by (80) and $j > j_0 \geq i$, for any $h \in \widetilde{H}$, we have

$$(84) \qquad |\mathbf{f}_j^*(\mathrm{Ad}(h)(\mathbf{f}_i))|_p \leq p^{-\lfloor (n_{i_0} - n_{i_0-1} - d_1)/(2d_s) \rfloor}.$$

So by (69), for $l(\widetilde{H}) \gg_{\mathcal{G},C_0} 1$, we get that (83) and (84) imply $w := \mathbf{f}_i$ and $L := \mathbf{f}_j^*$ satisfy the conditions of Claim 1.

Case 2. *Suppose* $\mathrm{Lie}(\mathbb{G}_s)(\mathbb{Q}_p)$ *is the* $\mathbb{Q}_p$-*span* $W_{3,s}$ *of* $\mathfrak{W}_{3,s}$.

Let us recall that W_1 is the $\mathbb{Q}_p$-span of $\mathfrak{W}_1$. And $\mathfrak{W}_{3,s}$ is a subset of the projection of W_1 to $\mathrm{Lie}(\mathbb{G}_s)(\mathbb{Q}_p)$. So by the assumption of Case 2, we have that the projection of W_1 onto $\mathrm{Lie}(\mathbb{G}_s)(\mathbb{Q}_p)$ is onto. Since W_1 is a proper subspace of $\mathrm{Lie}(\mathbb{G})(\mathbb{Q}_p)$, by Lemma 41 and the strong approximation there is $c_3 \ll_{\mathcal{G}} 1$ such that $\pi_{p^{c_3}}(W_1 \cap \mathfrak{g})$ is not $\mathcal{G}(\mathbb{Z}_S)$-invariant. Recall that $\mathfrak{W}_2 = W_1 \cap \mathfrak{g} = \sum_{i=1}^{i_0} \mathbb{Z}_p \mathbf{e}_i$. So there is $\lambda \in \Omega'$ and $1 \leq i \leq i_0$ such that

$$(85) \qquad \mathrm{Ad}(\lambda)(\mathbf{e}_i) \notin \mathfrak{W}_2 + p^{c_3} \mathfrak{g}.$$

Let $\{\mathbf{e}_1^*, \ldots, \mathbf{e}_d^*\}$ be the dual of $\{\mathbf{e}_1, \ldots, \mathbf{e}_d\}$. Then, by (85) we have that there is $j \geq i_0$ such that

$$(86) \qquad |\mathbf{e}_j^*(\mathrm{Ad}(\lambda)(\mathbf{e}_i))|_p > p^{-c_3}.$$

And by (71) and $j \geq i_0 > i$, for any $h \in \widetilde{H}$, we have

$$(87) \qquad |\mathbf{e}_j^*(\mathrm{Ad}(h)(\mathbf{e}_i))|_p \leq p^{-(n_{i_0} - n_{i_0-1})}.$$

So by (69), for $l(\widetilde{H}) \gg_{\mathcal{G},C_0} 1$, we get that (86) and (87) imply $w := \mathbf{e}_i$ and $L := \mathbf{e}_j^*$ satisfy the conditions of Claim 1.

Case 3. *Suppose*

$$(88) \qquad \mathrm{Ad}(\mathcal{G}(\mathbb{Z}_S))(\mathfrak{W}_{3,s}) \subseteq \mathfrak{W}_{3,s} + \mathbb{V}(\mathbb{Q}_p) + p^{\lfloor (n_{i_0} - n_{i_0-1} - d_1)/(4d_s C_0) \rfloor} \mathfrak{g}_s,$$

and $\mathrm{Lie}(\mathbb{G}_s)(\mathbb{Q}_p)$ *is not the* $\mathbb{Q}_p$-*span* $W_{3,s}$ *of* $\mathfrak{W}_{3,s}$.

By the strong approximation, the projection K_p of the closure of $\mathcal{G}(\mathbb{Z}_S)$ to $\mathbb{G}_s(\mathbb{Q}_p)$ contains $\mathbb{G}_s(\mathbb{Q}_p) \cap \mathrm{GL}_{N_0}(\mathbb{Z}_p)[p^{k_0}]$ where k_0 depends only on $\mathcal{G}$. So by Lemma 40 and (88), there are a positive integer c_4, which depends only on $\mathcal{G}$, and a normal subgroup $\mathbb{G}_{W_{3,s}}$ of $\mathbb{G}_s$ such that

$$(89) \qquad p^{2c_4} \pi_{p^{m-c_4}}(\mathfrak{g}_{W_{3,s}}) \subseteq p^{c_4} \pi_{p^{m-c_4}}(\mathfrak{W}_{3,s}) \subseteq \pi_{p^{m-c_4}}(\mathfrak{g}_{W_{3,s}}),$$

where $\mathfrak{g}_{W_{3,s}} := \mathrm{Lie}(\mathbb{G}_{W_{3,s}})(\mathbb{Q}_p) \cap \mathfrak{g}$ and $m := \lfloor (n_{i_0} - n_{i_0-1} - d_1)/(4d_s C_0) \rfloor$.

Since $W_{3,s}$ is a proper subspace of $\mathrm{Lie}(\mathbb{G}_s)(\mathbb{Q}_p)$, by the first inclusion in (89) we have that $\mathbb{G}_{W_{3,s}}$ is a proper normal subgroup of $\mathbb{G}_s$. So at least one simple factor $\mathbb{G}_{i_0'}$ is missing in $\mathrm{Lie}(\mathbb{G}_{W_{3,s}})(\mathbb{Q}_p)$. Let $\mathfrak{g}_{i_0'} := \mathrm{Lie}(\mathbb{G}_{i_0'})(\mathbb{Q}_p) \cap \mathfrak{g}$. Then we have that $\mathfrak{g}_{i_0'} \cap \mathfrak{g}_{W_{3,s}} = \{0\}$ and $[\mathfrak{g}_{i_0'}, \mathfrak{g}_{W_{3,s}}] = \{0\}$. Let $x_0 \in \mathfrak{g}_{i_0'}$ be a unit vector. Next we show that $\mathfrak{W}_{3,s} + \mathbb{Z}_p x_0 + \mathbb{V}(\mathbb{Q}_p)$ is *almost* $\mathrm{Ad}(\widetilde{H})$-invariant.

Let $h \in \widetilde{H}$ and suppose $h \in G[p^k] \setminus G[p^{k+1}]$ for some $k < l' := \lceil l/2 \rceil + m_0$. Then

$$\log h \in (p^k \mathfrak{gl}_{N_0}(\mathbb{Z}_p) \cap \mathfrak{g}) \setminus p^{k+1} \mathfrak{gl}_{N_0}(\mathbb{Z}_p).$$

So

$$\log h^{p^{l'-k}} = p^{l'-k} \log h \in p^{l'} \mathfrak{gl}_{N_0}(\mathbb{Z}_p) \cap \log \widetilde{H}.$$

Hence $\pi_{p^{n_{i_0}}}(p^{-k} \log h) \in \pi_{p^{n_{i_0}}}(\mathfrak{W}_1)$. This implies that there is $y_h \in \mathfrak{W}_{2,s}$ such that

$$p^{-k} \log h \in y_h + p^{n_{i_0}} \mathfrak{g} + \mathbb{V}(\mathbb{Q}_p).$$

And so $y_h = \sum_{i=1}^{d_s'} a_i p^{n_i'} \mathbf{f}_i$, for some $a_i \in \mathbb{Z}_p$, which implies

$$(90) \qquad p^{-k} \log h \in \mathfrak{W}_{3,s} + p^{\min\{n_{i_0}, n_{i_0'+1}'\}} \mathfrak{g} + \mathbb{V}(\mathbb{Q}_p).$$

By (75), we have

$$(91) \qquad \min\{n_{i_0}, n_{i_0'+1}'\} \geq \frac{n_{i_0} - n_{i_0-1} - d_1}{2d_s} - d_1 \geq 2C_0 m - d_1.$$

Hence by (90) and (91), we have

$$(92) \qquad p^{-k} \log h \in \mathfrak{W}_{3,s} + p^{2C_0 m - d_1} \mathfrak{g} + \mathbb{V}(\mathbb{Q}_p).$$

By (89) and (92), we have

$$(93) \qquad p^{c_4 - k} \log h \in \mathfrak{g}_{W_{3,s}} + p^{\min\{2C_0 m - d_1, m - c_4\}} \mathfrak{g} + \mathbb{V}(\mathbb{Q}_p).$$

By (93) and the fact that $[\mathfrak{g}_{W_{3,s}}, x_0] = \{0\}$, we have

$$(94) \qquad \mathrm{ad}(\log h)(x_0) \in p^{\min\{2C_0 m - d_1, m - c_4\} - c_4} \mathfrak{g} + \mathbb{V}(\mathbb{Q}_p).$$

Thus by $m = \lfloor (n_{i_0} - n_{i_0-1} - d_1)/(4d_s C_0) \rfloor$, (69), and (94), for $l(\widetilde{H}) \gg_{\mathcal{G}, C_0} 1$ we have

$$(95) \qquad \mathrm{Ad}(h)(x_0) = \exp(\mathrm{ad}(\log h))(x_0) \in x_0 + p^{\min\{2C_0 m - d_1, m - c_4\} - c_4} \mathfrak{g} + \mathbb{V}(\mathbb{Q}_p).$$

So by (80) and (95), we have

$$(96) \qquad \mathrm{Ad}(\widetilde{H})(\mathfrak{W}_{3,s} + \mathbb{Z}_p x_0) \subseteq \mathfrak{W}_{3,s} + \mathbb{Z}_p x_0 + p^{\min\{2C_0 m - d_1, m - c_4\} - c_4} \mathfrak{g} + \mathbb{V}(\mathbb{Q}_p).$$

On the other hand, looking at the action of $\mathcal{G}(\mathbb{Z}_S)$ on $\mathfrak{g}_{i_0'}$, we can choose $x_0 \in \mathfrak{g}_{i_0'}$, $L_0 \in \mathrm{Hom}_{\mathbb{Z}_p}(\mathfrak{g}_{i_0'}, \mathbb{Z}_p)$, and a positive integer c_5 which depends only on $\mathcal{G}$ such that for some $\lambda \in \Omega'$ we have

$$(97) \qquad |L_0((\mathrm{Ad}(\lambda)(x_0))_s)|_p \geq p^{-c_5}, \text{ and } L_0(x_0) = 0.$$

Now let $\mathrm{Lie}(\mathbb{G}_s)(\mathbb{Q}_p) = \oplus_i \mathrm{Lie}(\mathbb{G}_{s,i})(\mathbb{Q}_p)$ be the decomposition of $\mathrm{Lie}(\mathbb{G}_s)(\mathbb{Q}_p)$ to its simple factors; and for any $x \in \mathrm{Lie}(\mathbb{G})(\mathbb{Q}_p)$ let $x = x_v + \sum_i x_{s,i}$ be the such that $x_v \in \mathrm{Lie}(\mathbb{V})(\mathbb{Q}_p)$ and $x_{s,i} \in \mathrm{Lie}(\mathbb{G}_{s,i})(\mathbb{Q}_p)$. Then for some positive integer c_6 which depends only on $\mathcal{G}$ we have

$$p^{c_6} \|x\|_p \geq \max\{\|x_{s,i}\|_p\}_i.$$

So there is a well-defined $\mathbb{Z}_p$-linear map $L : \mathfrak{g} \to \mathbb{Z}_p, L(x) := L_0(p^{c_6} x_{s,i_0'})$. We notice that

(98) $$|L(\mathrm{Ad}(\lambda)(x_0))|_p \geq p^{-c_5}, \text{ and } L(\mathfrak{W}_{3,s} + \mathbb{Z}_p x_0) = 0.$$

And so by (96), for any $h \in \widetilde{H}$, we have

(99) $$|L(\mathrm{Ad}(h)(x_0))|_p \leq p^{- \min\{2C_0 m - d_1, m - c_4\} - c_4}.$$

So by (69), for $l(\widetilde{H}) \gg_{\mathcal{G},C_0} 1$, we get that (98) and (99) imply $w := x_0$ and L satisfy the conditions of Claim 1. $\qquad\square$

Next we will show elements with *small height* in $\widetilde{H}$ are in a proper quadratic subvariety. Let $\underline{\mathfrak{g}} := \mathrm{Lie}\,\mathcal{G}$. So there are finitely many $\mathbb{Z}_S$-linear maps f_i (for $1 \leq i \leq s_0$) viewed as regular functions on the affine scheme $(\mathfrak{gl}_{N_0})_{\mathbb{Z}_S}$ of N_0-by-N_0 matrices such that for any (unital commutative) $\mathbb{Z}_S$-algebra R, we have

(100) $$\underline{\mathfrak{g}}(R) = \{x \in \mathfrak{gl}_{N_0}(R)| \forall i, f_i(x) = 0\}.$$

Let us view $\mathfrak{gl}_{N_0}(R)$ as $R^{N_0^2}$, and write its elements as vectors. This way we write $f_i(x_1, \ldots, x_{N_0^2}) := \sum_j a_{ij} x_j$, where $a_{ij} \in \mathbb{Z}_S$. And consider the matrix $A := [a_{ij}] \in M_{s_0 \times N_0^2}(\mathbb{Z}_S)$. Since $\mathbb{Z}_S$ is a PID, there are $\gamma_1 \in \mathrm{GL}_{s_0}(\mathbb{Z}_S)$, $\gamma_2 \in \mathrm{GL}_{N_0^2}(\mathbb{Z}_S)$, and positive integers $r_1|r_2|\cdots|r_{N_0^2-d}$ such that

(101) $$A = \gamma_1 \begin{bmatrix} 0 & 0 \\ 0 & \mathrm{diag}(r_1, \ldots, r_{N_0^2-d}) \end{bmatrix} \gamma_2,$$

where $\mathrm{diag}(r_1, \ldots, r_{N_0^2-d})$ is the diagonal matrix with diagonal entries r_i's (this is known as the Smith normal form when the diagonal block is at the top left corner.). Let us view the rows of γ_2 as a $\mathbb{Z}_S$-basis $\{\mathbf{e}_1^*, \ldots, \mathbf{e}_{N_0^2}^*\}$ of the dual of $\mathbb{Z}_S^{N_0^2}$. And let $\{\mathbf{e}_1, \ldots, \mathbf{e}_{N_0^2}\}$ be the dual $\mathbb{Z}_S$-basis of $\mathbb{Z}_S^{N_0^2}$. So by (100) and (101), for any $\mathbb{Z}_S$-algebra R with *no additive torsion* element, we have

(102) $$x \in \underline{\mathfrak{g}}(R) \iff \mathbf{e}_{d+1}^*(x) = \cdots = \mathbf{e}_{N_0^2}^*(x) = 0 \iff x \in \bigoplus_{i=1}^d R\mathbf{e}_i.$$

And so in this case we have

(103) $$\underline{\mathfrak{g}}^*(R) := \mathrm{Hom}_R(\underline{\mathfrak{g}}(R), R) = \bigoplus_{i=1}^d R\mathbf{e}_i^*.$$

Claim 2. Suppose $\{\mathbf{e}_1, \ldots, \mathbf{e}_{N_0^2}\}$ is a $\mathbb{Z}_S$-basis of $\mathfrak{gl}_{N_0}(\mathbb{Z}_S)$ such that (102) and (103) hold for any $\mathbb{Z}_S$-algebra R with no additive torsion element. For $(w_1, \ldots, w_d) \in R^d$, $(l_1, \ldots, l_d) \in R^d$, and $g \in \mathcal{G}(R)$, let

$$\eta_g(w_1, \ldots, w_d; l_1, \ldots, l_d) := \sum_{i,j} \mathbf{e}_i^*(\mathrm{Ad}(g)(\mathbf{e}_j)) l_i w_j.$$

If δ is small enough, there is $(w_1, \ldots, w_d, l_1, \ldots, l_d) \in \overline{\mathbb{Q}}^{2d}$ ($\overline{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$) such that

(1) For any $h \in \mathcal{L}_\delta(\widetilde{H})$ we have $\eta_h(w_1, \ldots, w_d; l_1, \ldots, l_d) = 0$,
(2) For some $\gamma \in \Omega'$ we have $\eta_\gamma(w_1, \ldots, w_d; l_1, \ldots, l_d) \neq 0$.

Proof of Claim 2. By Claim 1, there are $w \in \underline{\mathfrak{g}}(\mathbb{Z}_p)$ and $L \in \underline{\mathfrak{g}}(\mathbb{Z}_p)^*$ such that for any $h \in \widetilde{H}$ and some $\gamma \in \Omega'$ we have

(104) $$|L(\mathrm{Ad}(\gamma)(w))|_p \geq [\mathcal{G}(\mathbb{Z}_p) : \widetilde{H}]^{-c/C_0}, \text{ and } |L(\mathrm{Ad}(h)(w))|_p \leq [\mathcal{G}(\mathbb{Z}_p) : \widetilde{H}]^{-c},$$

for some c which depends only on $\mathcal{G}$ and some large positive number C_0 which will be specified later.

Suppose $L(\mathrm{Ad}(\lambda)(w))^{-1}w = \sum_{i=1}^{d} x_i\mathbf{e}_i$ and $L = \sum_{i=1}^{d} y_i\mathbf{e}_i^*$; and let $\mathbf{x}_0 := (x_1,\ldots,x_d)$ and $\mathbf{y}_0 := (y_1,\ldots,y_d)$. Since $\underline{\mathfrak{g}}(\mathbb{Z}_p) = \mathfrak{g} = \mathrm{Lie}(\mathbb{G})(\mathbb{Q}_p) \cap \mathfrak{gl}_{N_0}(\mathbb{Z}_p)$, it is a primitive $\mathbb{Z}_p$-submodule of $\mathfrak{gl}_{N_0}(\mathbb{Z}_p)$; and so

$$(105) \qquad \|\mathbf{x}_0\|_p = |L(\mathrm{Ad}(h)(w))|_p^{-1}\|w\|_p \leq [\mathcal{G}(\mathbb{Z}_p):\widetilde{H}]^{c/C_0}.$$

And clearly $\|\mathbf{y}_0\|_p \leq 1$. By (104) and the way $\mathbf{x}_0$ and $\mathbf{y}_0$ are defined, we get that for any $h \in \widetilde{H}$ and some $\gamma \in \Omega'$ we have

$$(106) \qquad \eta_\gamma(\mathbf{x}_0,\mathbf{y}_0) = 1, \text{ and } |\eta_h(\mathbf{x}_0,\mathbf{y}_0)| \leq [\mathcal{G}(\mathbb{Z}_p):\widetilde{H}]^{-c(1-1/C_0)}.$$

To prove the claim, we proceed by contradiction and use an effective version of Nullstellensatz theorem [BY91] (or [MW, Theorem IV]).

Suppose the following has no solution over $\overline{\mathbb{Q}}$:

$$\forall\, h \in \mathcal{L}_\delta(\widetilde{H}),\ \eta_h(\mathbf{x},\mathbf{y}) = 0,\ \eta_\gamma(\mathbf{x},\mathbf{y}) = 1,$$

where $\gamma \in \Omega'$ is the one given in (106). Notice that the total degree of η_g is two for any $g \in \mathcal{G}(\mathbb{Z}_p)$; and the S-norm of the coefficients of η_h for $h \in \mathcal{L}_\delta(\widetilde{H})$ is at most $[\mathcal{G}(\mathbb{Z}_p):\widetilde{H}]^{\Theta_\Omega(\delta)}$. So by the effective Nullstellensatz, there are polynomials $q_\gamma, q_h \in \mathbb{Z}_S[T_1,\ldots,T_{2d}]$ and $D_0 \in \mathbb{Z}_S$ such that

$$(107) \qquad q_\gamma(\mathbf{x},\mathbf{y})(\eta_\gamma(\mathbf{x},\mathbf{y})-1) + \sum_{h\in\mathcal{L}_\delta(\widetilde{H})} q_h(\mathbf{x},\mathbf{y})\eta_h(\mathbf{x},\mathbf{y}) = D_0, \text{ and}$$

$$(108) \qquad \deg q_\gamma, \deg q_h \leq N(d), \text{ and } \|D_0\|_S \leq [\mathcal{G}(\mathbb{Z}_p):\widetilde{H}]^{\Theta_\Omega(\delta)},$$

where $h \in \mathcal{L}_\delta(\widetilde{H})$ and $N(d)$ is a positive integer which depends only on $d := \dim\mathbb{G}$. So by (108), (105), and the fact that $\mathbf{y}_0 \in \mathbb{Z}_p^d$, we have

$$(109) \qquad |q_h(\mathbf{x}_0,\mathbf{y}_0)|_p \leq [\mathcal{G}(\mathbb{Z}_p):\widetilde{H}]^{N(d)c/C_0}.$$

Hence by (109) and (106), for any $h \in \mathcal{L}_\delta(\widetilde{H})$ we have

$$(110) \qquad |q_h(\mathbf{x}_0,\mathbf{y}_0)\eta_h(\mathbf{x}_0,\mathbf{y}_0)|_p \leq [\mathcal{G}(\mathbb{Z}_p):\widetilde{H}]^{-c\left(1-\frac{N(d)+1}{C_0}\right)}.$$

Now suppose $C_0 = 2N(d)+2$; so by (106), (107), and (110), we have

$$(111) \qquad |D_0|_p = \left| q_\gamma(\mathbf{x}_0,\mathbf{y}_0)(\eta_\gamma(\mathbf{x}_0,\mathbf{y}_0)-1) + \sum_{h\in\mathcal{L}_\delta(\widetilde{H})} q_h(\mathbf{x}_0,\mathbf{y}_0)\eta_h(\mathbf{x}_0,\mathbf{y}_0) \right|_p \leq [\mathcal{G}(\mathbb{Z}_p):\widetilde{H}]^{-c/2}.$$

Hence by (108) and (111) we get

$$[\mathcal{G}(\mathbb{Z}_p):\widetilde{H}]^{c/2} \leq \|D_0\|_S \leq [\mathcal{G}(\mathbb{Z}_p):\widetilde{H}]^{\Theta_\Omega(\delta)},$$

which gives us a contradiction for $\delta \ll_\Omega 1$. $\qquad\square$

(*Going back to the proof of Lemma 42.*) For a given $(\mathbf{w},\mathbf{l}) \in \overline{\mathbb{Q}}^d \times \overline{\mathbb{Q}}^d$, let

$$V_{\mathbf{w},\mathbf{l}}(\overline{\mathbb{Q}}) := \{g \in \mathbb{G}(\overline{\mathbb{Q}})|\ \eta_g(\mathbf{w},\mathbf{l}) = 0\}.$$

Then $V_{\mathbf{w},\mathbf{l}}$ gives us a closed subvariety of $\mathbb{G}$. And since it is coming from an intersection of a hyperplane in $\mathfrak{gl}_{N_0}(\overline{\mathbb{Q}})$ and $\mathbb{G}(\overline{\mathbb{Q}})$, both its number of irreducible components and their degrees are bounded by a positive integer $N_1 := N_1(\mathbb{G})$ which depends only on $\mathbb{G}$.

Hence by [EMO05, Proposition 3.2] and its proof, there is a positive integer $N_2 := N_2(\mathbb{G})$ such that for any subset A of $\mathbb{G}(\overline{\mathbb{Q}})$ which generates a Zariski-dense subgroup of $\mathbb{G}(\overline{\mathbb{Q}})$ we have

$$(112) \qquad \prod\nolimits_{N_2} A \not\subseteq V_{\mathbf{w},\mathbf{l}}(\overline{\mathbb{Q}}),$$

for any $(\mathbf{w}, \mathbf{l}) \in \overline{\mathbb{Q}}^d \times \overline{\mathbb{Q}}^d$. By Claim 2, if $\delta \ll_{\mathcal{G}} 1$, there is $(\mathbf{w}, \mathbf{l}) \in \overline{\mathbb{Q}}^d \times \overline{\mathbb{Q}}^d$ such that $\mathcal{L}_{N_2 \delta}(\widetilde{H}) \subseteq V_{\mathbf{w}, \mathbf{l}}(\overline{\mathbb{Q}})$. And so

$$(113) \qquad \prod\nolimits_{N_2} \mathcal{L}_{\delta}(\widetilde{H}) \subseteq \mathcal{L}_{N_2 \delta}(\widetilde{H}) \subseteq V_{\mathbf{w}, \mathbf{l}}(\overline{\mathbb{Q}}).$$

Therefore by (112) and (113) we have that $\mathcal{L}_{\delta}(\widetilde{H})$ does not generate a Zariski-dense subgroup of $\mathbb{G}(\overline{\mathbb{Q}})$; proving Lemma. $\qquad \square$

Proof of Proposition 37. By Nori's strong approximation [Nor89, Theorem 5.4] we know that $[\mathcal{G}(\mathbb{Z}_p) : \overline{\Gamma}] \ll_{\Gamma} 1$, where $\overline{\Gamma}$ is the closure of Γ in $\mathcal{G}(\mathbb{Z}_p)$. For a proper subgroup H of $\pi_{p^n}(\Gamma)$, let $\widetilde{H} := \{h \in \mathcal{G}(\mathbb{Z}_p) | \ \pi_{p^n}(h) \in H\}$. So by Lemma 42 we have that $\mathcal{L}_{\delta_1}(\widetilde{H})$ is in a proper algebraic subgroup $\mathbb{H}$ of $\mathbb{G}$ for small enough δ_1. So by Proposition 14 we have that

$$(114) \qquad \mathcal{P}^{(l)}(\{\gamma \in \Gamma | \ \pi_{p^n}(\gamma) \in H\}) \leq e^{-\delta_0 l}$$

if $1 \ll l \ll \delta_1 \log[\pi_{p^n}(\Gamma) : H]$ where δ_0 is given by Proposition 14 and δ_1 is given by Lemma 42.

If for some $l \geq \frac{n}{\delta} \log p$ we have $\mathcal{P}^{(l)}_{\pi_{p^n}(\Omega)}(H) \geq [\pi_{p^n}(\Gamma) : H]^{-\delta}$, then by [BG09, Remark, page 1060] (see [SG, Lemma 8]) for any $l' \leq \frac{n}{\delta} \log p$ we have $\mathcal{P}^{(2l')}_{\pi_{p^n}(\Omega)}(H) \geq [\pi_{p^n}(\Gamma) : H]^{-2\delta}$. This contradicts (114) if δ is small enough. $\qquad \square$

5.2. Getting a large ideal by adding/subtracting a congruence subgroup boundedly many times.
The main goal of this section is to prove Proposition 43. At the end we also provide a few lemmas that are needed for using Proposition 43 in the context of modules. The results of this section rely on properties of p-adic analytic maps that are proved in the appendix.

Proposition 43. *Let $\mathbb{G}_s \subseteq (\mathrm{GL}_{N_0})_{\mathbb{Q}}$ be a semisimple $\mathbb{Q}$-subgroup. Let $\rho : \mathbb{G}_s \to \mathbb{GL}(\mathbb{V})$ be a $\mathbb{Q}$-homomorphism, where $\mathbb{V}$ is a $\mathbb{Q}$-vector group. Suppose no non-zero vector of $\mathbb{V}(\overline{\mathbb{Q}})$ is $\rho(\mathbb{G}_s(\overline{\mathbb{Q}}))$-invariant. For a prime p, let $P[p^l] := \{g \in \mathbb{G}_s(\mathbb{Q}_p) \cap \mathrm{GL}_{N_0}(\mathbb{Z}_p) | \ \pi_{p^l}(g) = 1\}$. Then for $l \gg_{\mathbb{G}_s, \rho} 1$ we have*

$$\sum\nolimits_{\Theta_{\mathbb{G}_s, \rho}(1)} \rho(P[p^l]) - \sum\nolimits_{\Theta_{\mathbb{G}_s, \rho}(1)} \rho(P[p^l]) \supseteq p^{\Theta_{\mathbb{G}_s, \rho}(l)} \mathbb{Z}_p[\rho(P[1])].$$

(Notice that the implied constants are independent of p.)

Let us point out that the same proof gives us also the local version of Proposition 43.

Proposition 43'. *Let $\mathbb{G}_s \subseteq (\mathrm{GL}_{N_0})_{\mathbb{Q}}$ be a semisimple $\mathbb{Q}_p$-subgroup. Let $\rho : \mathbb{G}_s \to \mathbb{GL}(\mathbb{V})$ be a $\mathbb{Q}_p$-homomorphism, where $\mathbb{V}$ is a $\mathbb{Q}_p$-vector group. Let $P[p^l] := \{g \in \mathbb{G}_s(\mathbb{Q}_p) \cap \mathrm{GL}_{N_0}(\mathbb{Z}_p) | \ \pi_{p^l}(g) = 1\}$. Suppose that $\mathbb{V}(\mathbb{Q}_p)$ has no non-zero $\mathbb{G}_s(\mathbb{Q}_p)$ fixed vector. Then for $l \gg_{\mathbb{G}_s, \rho} 1$ we have*

$$\sum\nolimits_{\Theta_{\mathbb{G}_s, \rho}(1)} \rho(P[p^l]) - \sum\nolimits_{\Theta_{\mathbb{G}_s, \rho}(1)} \rho(P[p^l]) \supseteq p^{\Theta_{\mathbb{G}_s, \rho}(l)} \mathbb{Z}_p[\rho(P)].$$

Lemma 44. *Let K be a field (only in this Lemma), and G be a subgroup of $\mathrm{GL}_{N_0}(K)$. Suppose $V := K^{N_0}$ is a completely reducible G-module, and V has no non-zero G-fixed vector. Then there is no $a \in M_{N_0}(K)$ such that $\mathrm{Tr}(ag) = 1$ for any $g \in G$.*

Proof. Suppose to the contrary that there is such $a \in M_{N_0}(K)$. Let $A := K[G]$ be the K-span of G. Since A has a faithful semisimple finite dimensional A-module, A is a semisimple K-algebra. Let

$$\mathfrak{a} := \langle g - 1 | \ g \in G \rangle$$

be the ideal generated by $G - 1$ in A. Since $\mathrm{Tr}(ag) = 1$ for any $g \in G$, we have that $\mathrm{Tr}(ax) = 0$ for any $x \in \mathfrak{a}$. Thus $\mathfrak{a}$ is a proper ideal. On the other hand, since A is semisimple, by the idempotent decomposition there are $\alpha_1, \alpha_2 \in A$ such that

(1) $\alpha_i^2 = \alpha_i$,
(2) $\alpha_1 + \alpha_2 = 1$,
(3) $\mathfrak{a} = A\alpha_1$.

Since $\mathfrak{a}$ is a proper ideal, $\alpha_1 \neq 1$. And so there is a non-zero vector $v \in V$ in the kernel of α_1, which implies that $\mathfrak{a}v = A\alpha_1 v = 0$. Therefore for any $g \in G$ we have $gv = v$ which contradicts the assumption that V does not have a non-zero G-fixed point. $\square$

Proof of Proposition 43. Since $\mathbb{G}_s$ is a semisimple group, $\mathbb{V}(\overline{\mathbb{Q}}_p)$ is a completely reducible $\overline{\mathbb{Q}}_p[\rho(\mathbb{G}_s(\overline{\mathbb{Q}}_p))]$-module, for any prime p. As $\mathbb{G}_s(\mathbb{Q}_p)$ is Zariski-dense in $\mathbb{G}_s(\overline{\mathbb{Q}}_p)$, we have that $\overline{\mathbb{Q}}_p[\rho(\mathbb{G}_s(\overline{\mathbb{Q}}_p))] = \overline{\mathbb{Q}}_p[\rho(\mathbb{G}_s(\mathbb{Q}_p))]$. Therefore $\overline{\mathbb{Q}}_p[\rho(\mathbb{G}_s(\mathbb{Q}_p))]$ has a faithful completely reducible module, which implies that $\overline{\mathbb{Q}}_p[\rho(\mathbb{G}_s(\mathbb{Q}_p))]$ is a semisimple algebra. Hence the nilradical of $\mathbb{Q}_p[\rho(\mathbb{G}_s(\mathbb{Q}_p))]$ is zero, too. Thus $\mathbb{Q}_p[\rho(\mathbb{G}_s(\mathbb{Q}_p))]$ is a semisimple algebra and $\mathbb{V}(\mathbb{Q}_p)$ is a completely reducible $\mathbb{Q}_p[\rho(\mathbb{G}_s(\mathbb{Q}_p))]$-module.

Next we show that $\mathbb{V}(\mathbb{Q}_p)$ does not have a non-zero $\mathbb{G}_s(\mathbb{Q}_p)$-invariant vector. If not, $\mathbb{V}(\mathbb{Q}_p)^{\mathbb{G}_s(\mathbb{Q})} := \{v \in \mathbb{V}(\mathbb{Q}_p) | \rho(\mathbb{G}_s(\mathbb{Q}))(v) = v\}$ is non-zero. For $v_0 \in \mathbb{V}(\mathbb{Q}_p)^{\mathbb{G}_s(\mathbb{Q})}$ we have $v_0 = \sum_i a_i v_i$ where $a_i \in \mathbb{Q}_p$ are $\mathbb{Q}$-linearly independent and $v_i \in \mathbb{V}(\mathbb{Q})$. Since ρ is defined over $\mathbb{Q}$, for $g \in \mathbb{G}_s(\mathbb{Q})$ we have $\rho(g)(v_i) \in \mathbb{V}(\mathbb{Q})$ for any i. Hence $\rho(g)(v_0) = v_0$ implies that for any i we have $\rho(g)(v_i) = v_i$. Since $\mathbb{G}_s(\mathbb{Q})$ is Zariski-dense in $\mathbb{G}_s$, we get that $\rho(\mathbb{G}_s(\overline{\mathbb{Q}}))(v_i)$, which is a contradiction.

Hence Lemma 44 implies that the constant function $\mathbb{1}$ does not belong to the linear span of the analytic functions ρ_{ij} where ρ_{ij} are the entries of $\rho : \mathbb{G}_s(\mathbb{Q}_p) \to \mathrm{GL}(\mathbb{V}(\mathbb{Q}_p))$ with respect to a $\mathbb{Q}_p$-basis of $\mathbb{V}(\mathbb{Q}_p)$. So we get the desired result by Corollary 50. $\square$

Next we prove a corollary of Lemma 39.

Corollary 45. *Let $R \subseteq M_{n_0}(\mathbb{Z}_p)$ be a $\mathbb{Z}_p$-subalgebra. Let*

$$0 = W_{k_0+1} \subseteq W_{k_0} \subseteq \ldots \subseteq W_1 = \mathbb{Q}_p^{n_0}$$

be a composition series of $\mathbb{Q}_p^{n_0}$ as an $\mathbb{Q}_p[R]$-module, where $\mathbb{Q}_p[R]$ is the $\mathbb{Q}_p$-span of R. Suppose $v_i \in M_i := W_i \cap \mathbb{Z}_p^{n_0}$ and $\|\overline{v_i}\| := \inf\{\|v_i + w\|_p| w \in W_{i+1}\} \geq q^{-1}$, where q is a power of p. Then

$$\sum_{i=1}^{k_0} Rv_i \supseteq q^{\Theta_{R,\{W_j\}}(1)} \mathbb{Z}_p^{n_0}.$$

Proof. For any $1 \leq i \leq k_0$, we get a ring homomorphism from R to $\mathrm{End}_{\mathbb{Q}_p}(W_i/W_{i+1})$. Let R_i be its image. Notice that M_i/M_{i+1} can be embedded into W_i/W_{i+1} and for any $v \in M_i$ we have $R_i(v+M_{i+1}) = Rv + M_{i+1}$. So by Lemma 39 for the ring R_i we have that,

$$q^{\Theta_{R,W_i}(1)} M_i \subseteq Rv_i + M_{i+1} \subseteq M_i.$$

By induction on i one can easily see that, for any $1 \leq i \leq k_0$, we have

$$q^{\Theta_{R,\{W_j\}}(1)} \mathbb{Z}_p^{n_0} = q^{\Theta_{R,\{W_j\}}(1)} M_1 \subseteq \sum_{j=1}^{i} Rv_j + M_{i+1}.$$

$\square$

Lemma 46. *Let $R \subseteq M_{n_0}(\mathbb{Z}_S)$ be a $\mathbb{Z}_S$-subalgebra. Assume the $\mathbb{Q}$-span $\mathbb{Q}[R]$ of R is a semisimple algebra. Suppose p is a large prime number (depending on R), and W is a composition factor of $\mathbb{Q}_p^{n_0}$; that means there are two $\mathbb{Q}_p[R]$-submodules $W_1 \subseteq W_2$ such that $W = W_2/W_1$ is a simple $\mathbb{Q}_p[R]$-module. Then for any $v \in W_{\mathbb{Z}_p} := (W_2 \cap \mathbb{Z}_p^{n_0}) + W_1/W_1$ we have $\mathbb{Z}_p[R]v = W_{\mathbb{Z}_p}$ if $v \notin pW_{\mathbb{Z}_p}$.*

Proof. By Wedderburn theorem and Artin-Brauer-Noether theorem, for large enough p we have that

(1) $\mathbb{Q}_p[R] \simeq \bigoplus_i M_{n_i}(K_i)$ where K_i are finite extensions of $\mathbb{Q}_p$,
(2) under the above identification $\mathbb{Z}_p[R]$ gets identified with $\bigoplus_i M_{n_i}(\mathcal{O}_{K_i})$,
(3) under the above identification $\mathbb{Z}_p^{n_0}$ naturally gets identified with $\bigoplus_i \mathcal{O}_{K_i}^{n_i}$.

Hence $W_{\mathbb{Z}_p}$ is isomorphic to $\mathcal{O}_{K_i}^{n_i}$ where $\mathbb{Z}_p[R]$ acts via $M_{n_i}(\mathcal{O}_{K_i})$. It is clear that for any unit vector $v \in \mathcal{O}_{K_i}^{n_i}$ we have $M_{n_i}(\mathcal{O}_{K_i})v = \mathcal{O}_{K_i}^{n_i}$. $\qquad\square$

Corollary 47. *Let $R \subseteq M_{n_0}(\mathbb{Z}_S)$ be a $\mathbb{Z}_S$-subalgebra. Assume the $\mathbb{Q}$-span $\mathbb{Q}[R]$ of R is a semisimple algebra. Let*

$$0 = W_{k_0+1} \subseteq W_{k_0} \subseteq \ldots \subseteq W_1 = \mathbb{Q}_p^{n_0}$$

be a composition series of $\mathbb{Q}_p^{n_0}$ as an $\mathbb{Q}_p[R]$-module, where $\mathbb{Q}_p[R]$ is the $\mathbb{Q}_p$-span of R. Suppose $v_i \in M_i := W_i \cap \mathbb{Z}_p^{n_0}$ and $\|\overline{v_i}\| := \inf\{\|v_i + w\|_p| \ w \in W_{i+1}\} = 1$. Then, for large enough p, we have

$$\mathbb{Z}_p^{n_0} = \sum_{i=1}^{k_0} Rv_i.$$

Proof. It is a direct corollary of Lemma 46. $\qquad\square$

5.3. **Getting a p-adically large vector in a submodule in boundedly many steps.** The main goal of this short section is proving a key lemma (Lemma 48). Using this Lemma, we will be able to get a $\mathbb{Q}_p$-basis of $\mathbb{V}(\mathbb{Q}_p)$ consisting of *large* vectors in *boundedly many steps*.

Lemma 48. *Let Ω, Γ and $\mathbb{G}$ be as above. In particular, $\mathbb{G} = \mathbb{G}_s \ltimes \mathbb{V}$ where $\mathbb{G}_s$ is a semisimple $\mathbb{Q}_p$-group and $\mathbb{V}$ is a $\mathbb{Q}_p$-vector group; and for some non-negative integer $k_p \ll_\Omega 1$ (which is zero for large enough p) $Q_p[p^{k_p}] = K_p \ltimes V_p$ where Q_p is the closure of Γ in $\mathbb{G}(\mathbb{Q}_p)$, $Q_p[p^{k_p}] := Q_p \cap \mathrm{GL}_{N_0}(\mathbb{Z}_p)[p^{k_p}]$, $K_p := \mathbb{G}_s(\mathbb{Q}_p) \cap \mathrm{GL}_{N_0}(\mathbb{Z}_p)[p^{k_p}]$, and $V_p := \mathbb{V}(\mathbb{Q}_p) \cap \mathrm{GL}_{N_0}(\mathbb{Z}_p)[p^{k_p}]$ (see Section 2.6).*

Let $\mathbb{V}' \subseteq \mathbb{V}$ be a non-zero $\mathbb{Q}_p$-subgroup which is $\mathbb{G}_s$-invariant. For any $0 < \varepsilon \ll_{\Omega,\mathbb{V}'} 1$, there are $\delta > 0$ and a positive integer C such that the following holds:

Suppose p is a prime number, $Q = p^n$, and $n\varepsilon \gg_{\Omega,\mathbb{V}'} 1$.

If $\mathfrak{P}_Q(\delta, A, l)$ holds and $\pi_Q(\Gamma[q_2]) \subseteq \pi_Q(\prod_C A)\pi_Q(V_p \cap \mathbb{V}'(\mathbb{Q}_p))$ where $q_2 = p^{n_2}$ and $n_2 \leq \varepsilon^2 n$, then

$$\tag{115} \{v \in \mathbb{V}'(\mathbb{Q}_p)| \ \|v\|_p > Q^\varepsilon, \ \pi_Q(v) \in \pi_Q(\prod_{4C} A)\}$$

is non-empty.

Proof. Since $\mathbb{V}'$ is $\mathbb{G}_s$-invariant and it commutes with $\mathbb{V}$, $\mathbb{V}'$ is a normal subgroup of $\mathbb{G}$. On the other hand, $\mathrm{GL}_{N_0}(\mathbb{Z}_p)[p^{k_p}]$ is a normal subgroup of $\mathrm{GL}_{N_0}(\mathbb{Z}_p)$ and $Q_p \subseteq \mathrm{GL}_{N_0}(\mathbb{Z}_p)$; and so $V_p \cap \mathbb{V}'(\mathbb{Q}_p) = \mathbb{V}'(\mathbb{Q}_p) \cap \mathrm{GL}_{N_0}(\mathbb{Z}_p)[p^{k_p}]$ is a normal subgroup of Q_p. Let $\eta_{q_1} : \pi_{q_1}(Q_p) \to \pi_{q_1}(Q_p)/\pi_{q_1}(V_p \cap \mathbb{V}'(\mathbb{Q}_p))$ be the projection map where $q_1 = p^{n_1}$ and $n_1 = \lfloor \varepsilon n \rfloor$. So by the assumption there is a section

$$s : \eta_{q_1}(\pi_Q(Q_p[q_2])) \to \pi_{q_1}(Q_p)$$

such that the image of s is a subset of $\pi_{q_1}(\prod_C A)$ (by section we mean $\eta_{q_1}(s(x)) = x$). Notice that

$$\eta_{q_1}(s(x_1^{-1}x_2)^{-1}s(x_1)s(x_2^{-1})) = \eta_{q_1}(s(x_1^{-1}x_2))^{-1}\eta_{q_1}(s(x_1))\eta_{q_1}(s(x_2^{-1})) = (x_1^{-1}x_2)^{-1}(x_1)(x_2^{-1}) = 1.$$

Hence $s(x_1^{-1}x_2)^{-1}s(x_1)s(x_2^{-1}) \in \pi_{q_1}(\prod_{3C} A) \cap \pi_{q_1}(V_p \cap \mathbb{V}'(\mathbb{Q}_p))$. Now if we assume to the contrary that the set in (115) is empty, then we get that $\pi_{q_1}(\prod_{3C} A) \cap \pi_{q_1}(V_p \cap \mathbb{V}'(\mathbb{Q}_p)) = \{1\}$. And so s is a group homomorphism. So $H := \mathrm{Im}(s)$ is a subgroup of $\pi_{q_1}(Q_p)$, and $[\pi_{q_1}(Q_p) : H] \geq |\pi_{q_1}(V_p \cap \mathbb{V}'(\mathbb{Q}_p))| \geq p^{\Theta_{\mathbb{V}'}(n\varepsilon)}$. By Proposition 37 we have that

$$\tag{116} \mathcal{P}_{\pi_{q_1}(\Omega)}^{(2l)}(H) \leq [\pi_{q_1}(\Gamma) : H]^{-\Theta_\Omega(1)} \leq p^{-\Theta_{\Omega,\mathbb{V}'}(n\varepsilon)}.$$

On the other hand, if $x \in \pi_{q_1}(\prod_{2C} A) \cap \pi_{q_1}(\Gamma[q_2])$, then

$$x^{-1}s(\eta_{q_1}(x)) \in \pi_{q_1}(\prod_{4C} A) \cap \pi_{q_1}(V_p \cap \mathbb{V}'(\mathbb{Q}_p)).$$

So by the contrary assumption we have that $x \in H$, which means

$$\tag{117} \pi_{q_1}(\prod_{2C} A) \cap \pi_{q_1}(\Gamma[q_2]) \subseteq H.$$

By the assumption we have $\mathcal{P}_\Omega^{(l)}(A) > Q^{-\delta}$ (where δ is small positive number to be determined later). So

$$\mathcal{P}_\Omega^{(l)}(A \cap \pi_{q_2}^{-1}(x')) > Q^{-\delta}|\pi_{q_2}(\Gamma)|^{-1} = p^{-\Theta_\Omega(n\varepsilon^2)} = p^{-n(\delta+\Theta_\Omega(\varepsilon^2))},$$

for some $x' \in \pi_{q_2}(\Gamma)$. Hence $\mathcal{P}^{(2l)}(A \cdot A \cap \Gamma[q_2]) > p^{-n\Theta_\Omega(\varepsilon^2)}$ for small enough δ. Therefore by (117) and (116) we have

$$-n\Theta_\Omega(\varepsilon^2) < -n\Theta_{\Omega,\mathbb{V}'}(\varepsilon),$$

which is a contradiction if $0 < \varepsilon \ll_{\Omega,\mathbb{V}'} 1$. $\qquad\square$

5.4. **Proof of super-approximation: the p-adic case.** Let us recall that $\mathbb{G} = \mathbb{G}_s \ltimes \mathbb{V}$ where $\mathbb{G}_s$ is a semisimple $\mathbb{Q}_p$-group and $\mathbb{V}$ is a $\mathbb{Q}_p$-vector group; let $\rho : \mathbb{G}_s \to \mathbb{GL}(\mathbb{V})$ be the $\mathbb{Q}_p$-representation which gives us the action of $\mathbb{G}_s$ on $\mathbb{V}$. Let us recall that, since $\mathbb{G}$ is perfect, no non-zero vector of $\mathbb{V}(\mathbb{Q}_p)$ is $\rho(\mathbb{G}_s(\mathbb{Q}_p))$-invariant. Let $\mathbb{V}_i$ be $\mathbb{Q}_p$-subgroups of $\mathbb{V}$ such that

(1) $\mathbb{V}_i(\mathbb{Q}_p)$ are irreducible $\mathbb{G}_s(\mathbb{Q}_p)$-modules.
(2) $\mathbb{V} = \oplus_{i=1}^{k_0} \mathbb{V}_i$.

Let $P[p^k] := \{g \in \mathbb{G}_s(\mathbb{Q}_p)| \|g - 1\|_p \leq p^{-k}\}$ for any non-negative integer k.

Inductively we do the following simultaneously:

(1) construct a permutation $\sigma : \{1, \ldots, k_0\} \to \{1, \ldots, k_0\}$,
(2) find vectors $v_j \in W_j := \bigoplus_{i \in \{1,\ldots,k_0\}\setminus\{\sigma(1),\ldots,\sigma(j-1)\}} \mathbb{V}_{\sigma(i)}(\mathbb{Q}_p)$,

such that the following holds:

(1) for small enough δ, large enough C (depending on ε, Ω, and $\mathbb{V}_i$) and any $1 \leq j \leq k_0$ we have

$$(118) \qquad \pi_Q\left(\Gamma[p^{n(\varepsilon^{\Theta_\mathbb{G}(1)})}]\right) \subseteq \pi_Q(\textstyle\prod_{\Theta(C)} A)\pi_Q(V_p \cap W_j);$$

(2) $v_j \in W_j$;
(3) $\overline{v}_1, \ldots, \overline{v}_j$ generate W_1/W_{j+1} as a $\mathbb{G}_s(\mathbb{Q}_p)$-module, where $\overline{v}_i$ is the projection of v_i.
(4) $\log_p \|\overline{v}_j\|_p \gg n\varepsilon^{\Theta_\mathbb{G}(1)}$;
(5) $\sum_{i=1}^{j} \left(\sum_{\Theta_\mathbb{G}(1)} \rho(P[p^{n(\varepsilon^{\Theta_\mathbb{G}(1)})}])(v_i) - \sum_{\Theta_\mathbb{G}(1)} \rho(P[p^{n(\varepsilon^{\Theta_\mathbb{G}(1)})}])(v_i)\right) + W_{j+1} \supseteq p^{n(\varepsilon^{\Theta_\mathbb{G}(1)})}V_p$.

By [SG, Theorem 36], if δ is small enough and C is large enough, (118) holds for $j = 1$. Now we suppose (118) holds for $1 \leq j \leq j_0$ and we have already found $v_1, \ldots, v_{j_0-1}$ as desired. We will define $\sigma(j_0)$ and find v_{j_0} so that the above properties hold.

Since (118) holds for $j = j_0$, by Lemma 48 there is $v_{j_0} \in W_{j_0}$ such that

$$(119) \qquad \log_p \|v_{j_0}\|_p \gg n\varepsilon^{\Theta_\mathbb{G}(1)}, \text{ and } \pi_Q(v_{j_0}) \in \pi_Q(\textstyle\prod_{\Theta(C)} A).$$

Since $\log_p \|v_{j_0}\|_p \gg n\varepsilon^{\Theta_\mathbb{G}(1)}$, the projection $\overline{v}_{j_0}$ of v_{j_0} to $\mathbb{V}_{\sigma(j_0)}$ for some

$$\sigma(j_0) \in \{1, \ldots, k_0\} \setminus \{\sigma(1), \ldots, \sigma(j_0 - 1)\}$$

has length at least $\Theta_{\mathbb{V}_i}(p^{\Theta(n\varepsilon^{\Theta_\mathbb{G}(1)})})$. Now by Proposition 43, and Corollaries 45 and 47 one gets all the mentioned properties except the first one.

By [SG, Theorem 36] we have that for small enough δ and large enough C

$$(120) \qquad \pi_Q(P[p^{n\varepsilon^{\Theta(1)}}]) \subseteq \pi_Q(\textstyle\prod_C A)\pi_Q(V_p).$$

To simplify our notation let us drop the constant power of ε in the rest of the argument. Hence by (119) we have

$$(121) \qquad \pi_Q(p^{n\varepsilon}V_p) \subseteq \pi_Q(\textstyle\prod_{\Theta(C)} A)\pi_Q(V_p \cap W_j).$$

For any $g_1, g_2 \in P[p^{n\varepsilon}]$ and $v_1, v_2 \in V_p$, we have

$$[(g_1, v_1), (g_2, v_2)] \in P[p^{2n\varepsilon}] \ltimes (p^{n\varepsilon} V_p).$$

Hence by (120) and (121) we have

(122) $$\pi_Q(\{[g_1, g_2] | \ g_1, g_2 \in P[p^{n\varepsilon}]\}) \subseteq \pi_Q(\textstyle\prod_{\Theta(C)} A) \pi_Q(V_p \cap W_j).$$

Let $X := \{[g_1, g_2] | \ g_1, g_2 \in P[p^{n\varepsilon}]\}$. Using properties of the finite logarithmic maps (see [SG, Lemma 34]), we have

$$(\textstyle\prod_{\dim \mathbb{G}_s} X \cap P[p^{kn\varepsilon + \Theta(1)}]) P[p^{2kn\varepsilon}] = P[p^{kn\varepsilon + \Theta(1)}],$$

for any integer $k \geq 2$. Therefore $\pi_Q(\prod_{\Theta(-\log \varepsilon)} X) \supseteq \pi_Q(P[p^{n\Theta(\varepsilon)}])$. Hence

(123) $$\pi_Q(P[p^{n\Theta(\varepsilon)}]) \subseteq \pi_Q(\textstyle\prod_{\Theta(C)} A) \pi_Q(V_p \cap W_j).$$

And so by (121) and (123) we have

$$\pi_Q(\Gamma[p^{n\Theta(\varepsilon)}]) \subseteq \pi_Q(\textstyle\prod_{\Theta(C)} A) \pi_Q(V_p \cap W_j),$$

which finishes the proof.

6. Appendix A: quantitative open image for p-adic analytic maps.

The main goal of this appendix is to prove that one can get a *large open set* by adding the image of an analytic function in controlled number of times (see Proposition 49).

Proposition 49. *Let K be a characteristic zero non-Archimedean local field. Let $\mathcal{O} := \mathcal{O}_K$ be its ring of integers, and $\mathfrak{p}$ be a uniformizing element. Let $U \subseteq K^{n_0}$ be a neighborhood of the origin, and $F := (f_1, \ldots, f_{d_0}) : U \to K^{d_0}$ be an analytic function. Suppose the constant function $\mathbb{1}$ is not in the K-span of f_i. Then for any $l \gg_F 1$ we have*

$$\textstyle\sum_{\Theta_F(1)} F(\mathfrak{p}^l \mathcal{O}^{n_0}) - \sum_{\Theta_F(1)} F(\mathfrak{p}^l \mathcal{O}^{n_0}) \supseteq (K\text{-span of } F(U)) \cap \mathfrak{p}^{\Theta_F(l)} \mathcal{O}^{d_0}.$$

In fact, we prove the following refinement of Proposition 49. In Proposition 49′, we pinpoint how the implied constants depend on the given analytic functions (with a few extra technical assumptions). This type of control helps us to prove Corollary 50. Corollary 50 is the only result in the appendix that is needed in the main part of the article. In Corollary 50, we deal with polynomial maps that are defined over a number field, and prove that their images in all the non-Archimedean completions are *uniformly large*.

Proposition 49′. *Let K be a characteristic zero non-Archimedean local field. Let $\mathcal{O} := \mathcal{O}_K$ be its ring of integers, and $\mathfrak{p}$ be a uniformizing element. Let $F := (f_1, \ldots, f_{d_0}) : \mathcal{O}^{n_0} \to \mathcal{O}^{d_0}$ be an analytic function of the form*

$$F(\mathbf{x}) = \sum_{\mathbf{i}} (c_{\mathbf{i},1} \mathbf{x}^{\mathbf{i}}, \ldots, c_{\mathbf{i},d_0} \mathbf{x}^{\mathbf{i}}),$$

where $\mathbf{i} = (i_1, \ldots, i_{n_0})$ ranges over multi-indexes non-negative integers and $\mathbf{x}^{\mathbf{i}} = x_1^{i_1} \cdots x_{n_0}^{i_{n_0}}$. Suppose

(1) $|c_{\mathbf{i},j}|_{\mathfrak{p}} \leq 1$ *for any $\mathbf{i} = (i_1, \ldots, i_m)$ and any $1 \leq j \leq d_0$,*

(2) $L : K^{d_0'} \to K^{d_0}$ *is a linear embedding such that $F(\mathbf{x}) = L(f_{j_1}(\mathbf{x}), \ldots, f_{j_{d_0'}}(\mathbf{x}))$ for some indexes $1 \leq j_u \leq d_0$,*

(3) $|\det(c_{\mathbf{i}_i, j_u})_{1 \leq i, u \leq d_0'}|_{\mathfrak{p}} = |\mathfrak{p}^{k_0}|_{\mathfrak{p}}$ *for some multi-indexes $\mathbf{i}_1, \ldots, \mathbf{i}_{d_0'}$ whose coordinates add up to a number at most m_0 and some indexes $j_1, \ldots, j_{d_0'}$.*

Then for any $l \gg_{d_0', n_0, m_0, k_0, \|L\|_{\mathfrak{p}}} 1$ we have

$$\textstyle\sum_{\Theta(1)} F(\mathfrak{p}^l \mathcal{O}^{n_0}) - \sum_{\Theta(1)} F(\mathfrak{p}^l \mathcal{O}^{n_0}) \supseteq (K\text{-span of } F(U)) \cap \mathfrak{p}^{\Theta(l)} \mathcal{O}^{d_0},$$

where all the implied constants depend on d_0, n_0, m_0 and k_0.

Corollary 50. *Let κ be a number field. Let $f_1, \ldots, f_{d_0} \in \kappa[x_1, \ldots, x_{n_0}]$. Suppose $\mathbb{1}, f_1, \ldots, f_{d_0}$ are linearly independent where $\mathbb{1}$ is the constant polynomial one. Let $F := (f_1, \ldots, f_{d_0})$. Then for any $l \gg_F 1$ and any $\mathfrak{p} \in V_f(\kappa)$ we have*

$$\sum\nolimits_{\Theta_F(1)} F(\mathfrak{p}^l \mathcal{O}_{\mathfrak{p}}^{n_0}) - \sum\nolimits_{\Theta_F(1)} F(\mathfrak{p}^l \mathcal{O}_{\mathfrak{p}}^{n_0}) \supseteq (\kappa_{\mathfrak{p}}\text{-span of } F(\mathcal{O}_{\mathfrak{p}})) \cap \mathfrak{p}^{\Theta_F(l)} \mathcal{O}_{\mathfrak{p}}^{d_0},$$

where $\kappa_{\mathfrak{p}}$ is the completion of κ with respect to the finite place $\mathfrak{p} \in V_f(\kappa)$, $\mathcal{O}_{\mathfrak{p}}$ is the ring of integers of $\kappa_{\mathfrak{p}}$, and $\mathfrak{p}$ also shows a uniformizing element of $\mathcal{O}_{\mathfrak{p}}$.

Let us recall the needed notation from $\mathfrak{p}$-adic analysis. If U is an open subset of K, then $\nabla^k U := \{(x_1, \ldots, x_k) \in U \times \cdots \times U \mid x_i \neq x_j \text{ if } i \neq j\}$. If $f : U \to K$, then $\Phi^k f : \nabla^{k+1} U \to K$ is defined recursively

$$\Phi^k f(x_1, \ldots, x_k) := \frac{\Phi^{k-1} f(x_1, x_3, \ldots, x_k) - \Phi^{k-1} f(x_2, \ldots, x_k)}{x_1 - x_2},$$

and $\Phi^0 f = f$. If f is an analytic function, then $\Phi^n f$ can be uniquely extended to a continuous function $\overline{\Phi}^n f : U^{n+1} \to K$ for any n and $f^{(i)}(a) = i! \overline{\Phi}^i f(a, \ldots, a)$. Similarly for open subsets $U_i \subseteq K$ and a (multi-variable) function $f : U_1 \times \cdots \times U_m \to K$ we can define the kth order difference quotient $\Phi_i^k f$ of f with respect to the ith variable. And then for a multi-index $\mathbf{i} := (i_1, \ldots, i_m)$ we set

$$\Phi_{\mathbf{i}} f : \nabla^{i_1+1} U_1 \times \cdots \times \nabla^{i_m+1} U_m \to K, \qquad \Phi_{\mathbf{i}} f := \Phi_1^{i_1} \circ \Phi_2^{i_2} \circ \cdots \circ \Phi_m^{i_m} f.$$

If f is analytic, then $\Phi_{\mathbf{i}} f$ can be uniquely extended to a continuous function $\overline{\Phi}_{\mathbf{i}} f : U_1^{i_1+1} \times \cdots \times U_m^{i_m+1} \to K$, and

$$\partial_{\mathbf{i}} f(a_1, \ldots, a_m) = \mathbf{i}! \overline{\Phi}_{\mathbf{i}} f(\theta_{\mathbf{i}}(a_1, \ldots, a_m)),$$

where $\mathbf{i}! := i_1! i_2! \cdots i_m!$ and

$$\theta_{\mathbf{i}}(a_1, \ldots, a_m) := (\underbrace{a_1, \ldots, a_1}_{i_1+1-\text{times}}, \underbrace{a_2, \ldots, a_2}_{i_2+1-\text{times}}, \ldots, \underbrace{a_m, \ldots, a_m}_{i_m+1-\text{times}}).$$

Let $U := U_1 \times \cdots \times U_m \subseteq K^m$ be an open subset, $f_i : U \to K$ be analytic functions, and $F := (f_1, \ldots, f_d) : U \to K^d$ (in computations, it is considered as a d-by-1 column matrix). Then $dF(\mathbf{x})$ is a d-by-m matrix

$$dF(\mathbf{x}) := [\partial_j f_i(\mathbf{x})].$$

For any $1 \leq i, j \leq m$, let $\overline{\Phi}_{\mathbf{e}_i + \mathbf{e}_j} F(\bullet)$ be the column vector whose kth entry is $\overline{\Phi}_{\mathbf{e}_i + \mathbf{e}_j} f_k(\bullet)$. In the above setting, by Taylor expansion we have

(124) $$F(\mathbf{x}_0 + \mathbf{x}) = F(\mathbf{x}_0) + dF(\mathbf{x}_0)\mathbf{x} + R_2 F(\mathbf{x}_0 + \mathbf{x}, \mathbf{x}_0),$$

where $R_2 F(\mathbf{x}_0 + \mathbf{x}, \mathbf{x}_0)$ is of the form $\sum_{i,j} x_i x_j \overline{\Phi}_{\mathbf{e}_i + \mathbf{e}_j} F(\bullet)$ (the entries are the entries of either $\mathbf{x}_0 + \mathbf{x}$ or $\mathbf{x}_0$) and $\mathbf{x} = (x_1, \ldots, x_m)$.

For a d-by-m matrix $X = [\mathbf{v}_1 \cdots \mathbf{v}_m]$ with entries in K, let

$$N(X) := \max_{1 \leq i_1 \leq \cdots \leq i_d \leq m} |\det[\mathbf{v}_{i_1} \cdots \mathbf{v}_{i_d}]|.$$

Let $\{\mathbf{e}_i\}_i$ be the standard basis of K^n; and for any $I := \{i_1 < i_2 < \cdots < i_m\} \subseteq \{1, \ldots, n\}$, let $\mathbf{e}_I := \mathbf{e}_{i_1} \wedge \ldots \wedge \mathbf{e}_{i_m}$. It is well-known that $\{\mathbf{e}_I\}_{I \subseteq \{1, \ldots, n\}, |I|=m}$ is a basis of $\bigwedge^m(K^n)$. For any

$$\mathbf{x} = \sum_{I \subseteq \{1, \ldots, n\}, |I|=m} x_I \mathbf{e}_I \in \bigwedge\nolimits^m(K^n), \text{ we let } \|\mathbf{x}\| := \max\{|x_I| \mid I \subseteq \{1, \ldots, n\}, |I| = m\}.$$

Lemma 51.   (1) *If $\mathbf{w}_1, \ldots, \mathbf{w}_d$ are the rows of $X \in M_{d,m}(K)$, then $N(X) = \|\mathbf{w}_1 \wedge \cdots \wedge \mathbf{w}_d\|$; in particular $N(X) = 0$ if $\mathrm{rank}(X) < d$.*
   (2) *If $X \in M_{d,m}(\mathcal{O})$ and $N(X) \geq |\mathfrak{p}^{k_0}|$, then for any positive integer l and $\mathbf{y} \in \mathfrak{p}^{l+k_0} \mathcal{O}^d$ there is $\mathbf{x} \in \mathfrak{p}^l \mathcal{O}^m$ such that $X\mathbf{x} = \mathbf{y}$.*
   (3) *For any $1 \leq i \leq m$ and vectors $\mathbf{v}_j$ we have*

$$N[\mathbf{v}_1 \cdots \mathbf{v}_i (\mathbf{v}_{i+1} - \mathbf{v}_i) \cdots (\mathbf{v}_m - \mathbf{v}_i)] \leq (d+1) N[\mathbf{v}_1 \cdots \mathbf{v}_m].$$

Proof. The first part is clear. Now suppose that $N(X) \geq |\mathfrak{p}^{k_0}|$; then there are d columns $\mathbf{v}_{i_1}, \ldots, \mathbf{v}_{i_d}$ such that $|\det[\mathbf{v}_{i_1} \cdots \mathbf{v}_{i_d}]| \geq |\mathfrak{p}^{k_0}|$. Let $X_I = [\mathbf{v}_{i_1} \cdots \mathbf{v}_{i_d}]$. Then $X_I \mathrm{adj}(X_I) \mathbf{y} = \det(X_I) \mathbf{y}$, and so there is $\mathbf{x}' \in \mathfrak{p}^l \mathcal{O}^d$ such that $X_I \mathbf{x}' = \mathbf{y}$. Therefore there is $\mathbf{x} \in \mathfrak{p}^l \mathcal{O}^m$ such that $X\mathbf{x} = \mathbf{y}$.

For the third part, we get an upper-bound for the determinant of a d-by-d submatrix:

$$|\det[\mathbf{v}_{i_1} \cdots \mathbf{v}_{i_j}(\mathbf{v}_{i_{j+1}} - \mathbf{v}) \cdots (\mathbf{v}_{i_d} - \mathbf{v})]| = \|\mathbf{v}_{i_1} \wedge \cdots \wedge \mathbf{v}_{i_j} \wedge (\mathbf{v}_{i_{j+1}} - \mathbf{v}) \wedge \cdots \wedge (\mathbf{v}_{i_d} - \mathbf{v})\|$$

$$= \left\| \mathbf{v}_{i_1} \wedge \cdots \wedge \mathbf{v}_{i_d} - \sum_{k=j+1}^{d} \mathbf{v}_{i_{j+1}} \wedge \cdots \wedge \mathbf{v}_{i_{k-1}} \wedge \mathbf{v} \wedge \mathbf{v}_{i_{k+1}} \wedge \cdots \wedge \mathbf{v}_{i_d} \right\|$$

$$\leq (d+1)N([\mathbf{v}_1 \cdots \mathbf{v}_m]),$$

where $\mathbf{v}$ is either 0 or $\mathbf{v}_i$. $\square$

In what follows, a series of Lemmas are proved in pairs. In the first ones the constants depend on F, and they are geared towards proving Proposition 49. In the second ones, we make the needed modification and make them suitable for proving Proposition 49′.

Lemma 52 (Hensel's lemma). *Let $\mathbf{x}_0 \in K^m$ and $U \subseteq K^m$ be an open neighborhood of $\mathbf{x}_0$. Let $f_i : U \to K$ be analytic functions and $F = (f_1, \ldots, f_d)$. Suppose there is a positive integer k_0 such that*

    (1) $\mathbf{x}_0 + \mathfrak{p}^{k_0} \mathcal{O}^m \subseteq U$,
    (2) $\|dF(\mathbf{x}_0)\| \leq 1$,
    (3) *for any i, j, if $\|\mathbf{x}' - \theta_{\mathbf{e}_i+\mathbf{e}_j}(\mathbf{x}_0)\| \leq |\mathfrak{p}^{k_0}|$, then $\|\overline{\Phi}_{\mathbf{e}_i+\mathbf{e}_j} F(\mathbf{x}')\| \leq 1$,*
    (4) $N(dF(\mathbf{x}_0)) \geq |\mathfrak{p}^{k_0}|$.

Then for any $l \geq k_0$ and any $\mathbf{y} \in \mathcal{O}^d$ there is $\mathbf{x}_1 \in \mathbf{x}_0 + \mathfrak{p}^l \mathcal{O}^m$ such that

$$\|F(\mathbf{x}_1) - F(\mathbf{x}_0) - \mathfrak{p}^{l+k_0} \mathbf{y}\| \leq |\mathfrak{p}^{2l}|.$$

Proof. By (124) we have that

$$(125) \qquad \|F(\mathbf{x}_0 + \mathfrak{p}^l \mathbf{x}) - F(\mathbf{x}_0) - \mathfrak{p}^l dF(\mathbf{x}_0)\mathbf{x}\| = \|\sum_{i,j}(\mathfrak{p}^l x_i)(\mathfrak{p}^l x_j)\overline{\Phi}_{\mathbf{e}_i+\mathbf{e}_j} F(\mathbf{x}_{ij})\|,$$

where $\mathbf{x} = (x_1, \ldots, x_m)$, $\|\mathbf{x}\| \leq 1$ and $\|\mathbf{x}_{ij} - \theta_{\mathbf{e}_i+\mathbf{e}_j}(\mathbf{x}_0)\| \leq |\mathfrak{p}^l|$. Now by Lemma 51 for any $\mathbf{y} \in \mathcal{O}^d$ there is $\mathbf{x} \in \mathcal{O}^m$ such that $dF(\mathbf{x}_0)\mathbf{x} = \mathfrak{p}^{k_0}\mathbf{y}$. And so by (125)

$$\|F(\mathbf{x}_0 + \mathfrak{p}^l \mathbf{x}) - F(\mathbf{x}_0) - \mathfrak{p}^{l+k_0} \mathbf{y}\| \leq |\mathfrak{p}^{2l}|.$$

$\square$

Lemma 53 (Quantitative open function theorem). *Let $\mathbf{x}_0 \in K^m$ and $U \subseteq K^m$ be an open neighborhood of $\mathbf{x}_0$. Let $f_i : U \to K$ be analytic functions and $F = (f_1, \ldots, f_d)$. Suppose*

    (1) $\|dF(\mathbf{x}_0)\| \leq 1$,
    (2) $\|\partial_{ij} F(\mathbf{x}_0)\| \leq 1$, *for any i, j,*
    (3) $N(dF(\mathbf{x}_0)) \geq |\mathfrak{p}^{k_0}|$, *for some positive integer k_0.*

Then for any large enough integer l (depending on F and U) we have

$$F(\mathbf{x}_0 + \mathfrak{p}^l \mathcal{O}^m) \supseteq F(\mathbf{x}_0) + \mathfrak{p}^{l+k_0} \mathcal{O}^d.$$

Proof. By the continuity of dF and $\overline{\Phi}_{\mathbf{e}_i+\mathbf{e}_j} F$, for large enough l (in particular $l > k_0$), we have that

    (1) $\|dF(\mathbf{x})\| \leq 1$ if $\|\mathbf{x} - \mathbf{x}_0\| \leq |\mathfrak{p}^l|$,
    (2) $\|\overline{\Phi}_{\mathbf{e}_i+\mathbf{e}_j} F(\mathbf{x}')\| \leq 1$ if $\|\mathbf{x}' - \theta_{\mathbf{e}_i+\mathbf{e}_j}(\mathbf{x}_0)\| \leq |\mathfrak{p}^l|$,
    (3) $N(dF(\mathbf{x})) \geq |\mathfrak{p}^{k_0}|$ if $\|\mathbf{x} - \mathbf{x}_0\| \leq |\mathfrak{p}^l|$.

By induction on i we prove that for any $\mathbf{y} \in \mathcal{O}^d$ there are $\mathbf{x}_i \in \mathbf{x}_0 + \mathfrak{p}^l \mathcal{O}^m$ and integers $l_i \geq 2l$ such that

(1) $l_1 := 2l$ and $l_{i+1} := 2(l_i - k_0)$,
(2) $\|F(\mathbf{x}_i) - F(\mathbf{x}_0) - \mathfrak{p}^{l+k_0}\mathbf{y}\| \leq |\mathfrak{p}^{l_i}|$.

Lemma 52 gives us the base of the induction. By induction hypothesis, there is $\mathbf{x}_i \in \mathbf{x}_0 + \mathfrak{p}^l \mathcal{O}^m$ such that

$$F(\mathbf{x}_i) - F(\mathbf{x}_0) - \mathfrak{p}^{l+k_0}\mathbf{y} \in \mathfrak{p}^{l_i}\mathcal{O}^d.$$

Hence by Lemma 52 there is $\mathbf{x}_{i+1} \in \mathbf{x}_i + \mathfrak{p}^{l_i - k_0}\mathcal{O}^m \subseteq \mathbf{x}_0 + \mathfrak{p}^l \mathcal{O}^m$ such that

$$\|F(\mathbf{x}_{i+1}) - F(\mathbf{x}_i) + (F(\mathbf{x}_i) - F(\mathbf{x}_0) - \mathfrak{p}^{l+k_0}\mathbf{y})\| \leq |\mathfrak{p}^{2(l_i - k_0)}| = |\mathfrak{p}^{l_{i+1}}|.$$

This proves the induction step. One can easily see that $\{l_i\}$ is a strictly increasing integer sequence. So $\{\mathbf{x}_i\}$ is a Cauchy sequence. Therefore $\lim_{i\to\infty} \mathbf{x}_i = \mathbf{x} \in \mathbf{x}_0 + \mathfrak{p}^l \mathcal{O}^m$ by the compactness of $\mathbf{x}_0 + \mathfrak{p}^l \mathcal{O}^m$, and by the continuity of F we have $F(\mathbf{x}) = F(\mathbf{x}_0) + \mathfrak{p}^{l+k_0}\mathbf{y}$. $\qquad\square$

Lemma 53′. *Let $F := (f_1, \ldots, f_{d_0}) : \mathcal{O}^{n_0} \to \mathcal{O}^{d_0}, F(\mathbf{x}) = \sum_{\mathbf{i}}(c_{\mathbf{i},1}\mathbf{x}^{\mathbf{i}}, \ldots, c_{\mathbf{i},d_0}\mathbf{x}^{\mathbf{i}})$ be an analytic function such that*

(1) $|c_{\mathbf{i},j}| \leq 1$ *for any $\mathbf{i}$ and j,*
(2) $N(dF(\mathbf{0})) \geq |\mathfrak{p}^{k_0}|$ *for some positive integer k_0.*

Then for any $l \gg_{k_0} 1$ we have

$$F(\mathfrak{p}^l \mathcal{O}) \supseteq F(\mathbf{0}) + \mathfrak{p}^{l+k_0}\mathcal{O}^{d_0}.$$

Proof. Since $F(\mathbf{x}) := \sum_{\mathbf{i}}(c_{\mathbf{i},1}\mathbf{x}^{\mathbf{i}}, \ldots, c_{\mathbf{i},d_0}\mathbf{x}^{\mathbf{i}})$ and $|c_{\mathbf{i},j}| \leq 1$, we have $\|dF(\mathbf{x})\| \leq 1$ and $\|\overline{\Phi}_{\mathbf{e}_i+\mathbf{e}_j}F(\mathbf{x}')\| \leq 1$ for any $\|\mathbf{x}\| \leq 1$ and $\|\mathbf{x}'\| \leq 1$.

Since $|c_{\mathbf{i},j}| \leq 1$ and $N(dF(\mathbf{0})) \geq |\mathfrak{p}^{k_0}|$, we have that $N(dF(\mathbf{x})) \geq |\mathfrak{p}^{k_0}|$ for any $\mathbf{x} \in \mathfrak{p}^{k_0+1}\mathcal{O}$. One can finish the argument as in the proof of Lemma 53. $\qquad\square$

Lemma 54. *Let U be a neighborhood of $0 \in K$, and $f_i : U \to K$ be analytic functions. Suppose $\mathbb{1}, f_1, \ldots, f_d$ are linearly independent. Then for large enough m (depending on f_i) and large enough l (depending on f_i and m) we have that, for any $x_1, \ldots, x_m \in \mathfrak{p}^l \mathcal{O}$,*

$$N([f_i'(x_j)]) \gg \prod_{1 \leq i < j \leq m} |(x_i - x_j)|,$$

where the implied constant depends on f_i.

Proof. Notice that we can rescale, i.e. change f_i to $g_i(x) := f_i(\mathfrak{p}^k x)$, and make sure that $|f_i^{(j)}(0)| \leq 1$ for any $1 \leq i \leq d$ and any positive integer j.

Since f_i are analytic and $\mathbb{1}, f_1, \ldots, f_d$ are linearly independent, for large enough m we have that $\text{rank}([f_i^{(j)}(0)]) = d$, where $1 \leq i \leq d$ and $1 \leq j \leq m$. So $N([f_i^{(j)}(0)]) = |\mathfrak{p}^{k_0}|$ for some non-negative integer k_0. Hence by the continuity of $\overline{\Phi}^j f_i$, for large enough l, we have that $N([\overline{\Phi}^j f_i(\mathbf{x}_j)]) \gg 1$ if $\mathbf{x}_j \in \mathfrak{p}^l \mathcal{O}^{j+1}$ for any $1 \leq j \leq m$.

Let $F(x)$ be the column vector $[f_1(x) \cdots f_d(x)]^T$. Then by the repeated use of the third part of Lemma 51 we have

$$
\begin{aligned}
N([f_i'(x_j)]) &= N[F'(x_1) \cdots F'(x_m)] \\
&\geq (d+1)^{-1} N[F'(x_1)(F'(x_2) - F'(x_1)) \cdots (F'(x_m) - F'(x_1))] \\
&\geq (d+1)^{-1} \left(\prod_{i=2}^{m} |x_i - x_1| \right) N[F'(x_1)\overline{\Phi}^1 F'(x_2, x_1) \cdots \overline{\Phi}^1 F'(x_m, x_1)] \\
&\geq \cdots \\
&\geq (d+1)^{-m} \left(\prod_{1 \leq i < j \leq m} |x_i - x_j| \right) N[F'(x_1)\overline{\Phi}^1 F'(x_2, x_1)\overline{\Phi}^2 F'(x_3, x_2, x_1) \cdots \overline{\Phi}^{m-1} F'(x_m, \ldots, x_1)] \\
&\gg \prod_{1 \leq i < j \leq m} |x_i - x_j|.
\end{aligned}
$$

$\square$

Lemma 54'. *Let $F := (f_1, \ldots, f_{d_0}) : \mathcal{O} \to \mathcal{O}^{d_0}, F(x) = \sum_i (c_{i,1} x^i, \ldots, c_{i,d_0} x^i)$ be an analytic function such that*

(1) $|c_{i,j}| \leq 1$ *for any i and j,*
(2) $|\det(c_{i_e, j})| = |\mathfrak{p}^{k_0}|$ *for some indexes $i_1, \ldots, i_{d_0} \leq m_0$ and some positive integer k_0.*

Then for any $l \gg_{k_0} 1$ we have that, for any $x_1, \ldots, x_{m_0} \in \mathfrak{p}^l \mathcal{O}$,

$$
N([f_i'(x_j)]) \geq |\mathfrak{p}^{\Theta_{k_0, d_0, m_0}(1)}| \prod_{1 \leq i < j \leq m_0} |x_i - x_j|.
$$

Proof. Since $|c_{i,j}| \leq 1$ and $|\det(c_{i,j})| = |\mathfrak{p}^{k_0}|$, we have that $N(\overline{\Phi}^j f_i(\mathbf{x}_j)) \geq |\det(\overline{\Phi}^{i_e} f_j(\mathbf{x}_{i_e}))| = |\mathfrak{p}^{k_0}|$ for any $\mathbf{x}_j \in \mathfrak{p}^{k_0+1} \mathcal{O}^j$. Now one gets the claim as in the proof of Lemma 54. $\square$

Lemma 55. *Let U be a neighborhood of $0 \in K$, and $f_i : U \to K$ be analytic functions. Suppose $\mathbb{1}, f_1, \ldots, f_d$ are linearly independent. Let $F = (f_1, \ldots, f_d)$. Then for any $l \gg_F 1$ we have*

$$
\sum\nolimits_{\Theta_F(1)} F(\mathfrak{p}^l \mathcal{O}) - \sum\nolimits_{\Theta_F(1)} F(\mathfrak{p}^l \mathcal{O}) \supseteq \mathfrak{p}^{\Theta_F(l)} \mathcal{O}^d.
$$

Proof. By Lemma 54 for large enough m_0 (depending on F) and large enough l (depending on F and m_0) we have

$$
N(d\widetilde{F}(\mathbf{x})) \gg \prod_{1 \leq i < j \leq m_0} |x_i - x_j|,
$$

where $\widetilde{F}(\mathbf{x}) = F(x_1) + \cdots + F(x_{m_0})$ and $\mathbf{x} = (x_1, \ldots, x_{m_0})$ has norm at most $|\mathfrak{p}^l|$. Let $\mathbf{x}_0 = (x_1, \ldots, x_{m_0})$ be such that $|x_i| \leq |\mathfrak{p}^l|$ for any i and $|x_i - x_j| \geq |\mathfrak{p}^{2l}|$ for any $i \neq j$. So $N(d\widetilde{F}(\mathbf{x}_0)) \gg \mathfrak{p}^{\Theta_{F, m_0}(l)}$. By rescaling, if needed, we can assume that $|f_i^{(j)}(0)| \leq 1$ for any $1 \leq i \leq d$ and any positive integer j. And so $\|d\widetilde{F}(\mathbf{x}_0)\| \leq 1$ and $\|\partial_{ij} \widetilde{F}(\mathbf{x}_0)\| \leq 1$. Therefore by Lemma 53 we have

$$
\widetilde{F}(\mathfrak{p}^l \mathcal{O}^{m_0}) = \widetilde{F}(\mathbf{x}_0 + \mathfrak{p}^l \mathcal{O}^{m_0}) \supseteq \widetilde{F}(\mathbf{x}_0) + \mathfrak{p}^{\Theta_{m_0, F}(l)} \mathcal{O}^d,
$$

and so

$$
\sum\nolimits_{m_0} F(\mathfrak{p}^l \mathcal{O}) - \sum\nolimits_{m_0} F(\mathfrak{p}^l \mathcal{O}) = \widetilde{F}(\mathfrak{p}^l \mathcal{O}^{m_0}) - \widetilde{F}(\mathfrak{p}^l \mathcal{O}^{m_0}) \supseteq \mathfrak{p}^{\Theta_{m_0, F}(l)} \mathcal{O}^d.
$$

$\square$

Lemma 55'. *Let $F := (f_1, \ldots, f_{d_0}) : \mathcal{O} \to \mathcal{O}^{d_0}, F(\mathbf{x}) = \sum_i (c_{i,1} x^i, \ldots, c_{i,d_0} x^i)$ be an analytic function such that*

(1) $|c_{i,j}| \leq 1$ *for any i and j,*

(2) $|\det(c_{i_e,j})| = |\mathfrak{p}^{k_0}|$ *for some indexes* $i_1, \dots, i_{d_0} \le m_0$ *and some positive integer* k_0.

Then for any $l \gg_{k_0,m_0} 1$ *we have*

$$\textstyle\sum_{m_0} F(\mathfrak{p}^l \mathcal{O}) - \sum_{m_0} F(\mathfrak{p}^l \mathcal{O}) \supseteq \mathfrak{p}^{\Theta_{m_0,d_0,k_0}(l)} \mathcal{O}^{d_0}.$$

Proof. As in the proof of Lemma 55, let $\widetilde{F}(\mathbf{x}) = \sum_{i=1}^{m_0} F(x_i)$. Hence by Lemma 54′ for $l \gg_{k_0} 1$ we have

$$N(d\widetilde{F}(\mathbf{x})) \ge |\mathfrak{p}^{\Theta_{k_0,d_0,m_0}(1)}| \prod_{1 \le i < j \le m_0} |x_i - x_j|,$$

for any $\mathbf{x} \in \mathfrak{p}^l \mathcal{O}^{m_0}$. Let $\mathbf{x}_0 \in \mathfrak{p}^l \mathcal{O}^{m_0}$ be such that $|x_i - x_j| \ge |\mathfrak{p}^{2l}|$ for any $i \ne j$. Notice that, since $l \gg_{m_0} 1$, there is such $\mathbf{x}_0$. Hence

$$N(d\widetilde{F}(\mathbf{x}_0)) \ge |\mathfrak{p}^{\Theta_{m_0,d_0,k_0}(l)}|.$$

Let $F_{\mathbf{x}_0}(\mathbf{x}) := \widetilde{F}(\mathbf{x} + \mathbf{x}_0)$. Hence $F_{\mathbf{x}_0}$ has a Taylor series expansion and its coefficients have norm at most one. Moreover $N(dF_{\mathbf{x}_0}(\mathbf{0})) \ge |\mathfrak{p}^{\Theta_{m_0,d_0,k_0}(l)}|$. Therefore by Lemma 53′ we have

$$F_{\mathbf{x}_0}(\mathfrak{p}^l \mathcal{O}) \supseteq F_{\mathbf{x}_0}(\mathbf{0}) + \mathfrak{p}^{\Theta_{m_0,d_0,k_0}(l)} \mathcal{O}^{d_0}.$$

One can finish the proof as above. $\qquad\square$

Lemma 56. *Let $U \subseteq K^{n_0}$ be a non-empty open subset. Let $f_i : U \to K$ be analytic functions such that $\mathbb{1}, f_1, \dots, f_d$ are linearly independent. Then there is a polynomial curve $r : K \to K^{n_0}$ such that $\mathbb{1}, f_1 \circ r, \dots, f_d \circ r$ are linearly independent, and defined on a neighborhood of $0 \in K$.*

Proof. Let $\mathbf{x}_0$ be a point in U. After rescaling, if needed, we can assume that $|\partial_{\mathbf{i}} f_j(\mathbf{x}_0)/\mathbf{i}!| \le 1$ for any $\mathbf{i}$ which is not zero. Since $\mathbb{1}, f_1, \dots, f_d$ are linearly independent, for large enough m we have that

$$\operatorname{rank}[\partial_{\mathbf{i}} f_j(\mathbf{x}_0)]_{1 \le \|\mathbf{i}\|_1 \le m, \ 1 \le j \le d} = d.$$

Thus

(126) $$N([\partial_{\mathbf{i}} f_j(\mathbf{x}_0)/\mathbf{i}!]) = |\mathfrak{p}^{k_0}|,$$

where k_0 is a non-negative integer. Now let

$$r(t) := \mathbf{x}_0 + \mathfrak{p}(t, t^s, t^{s^2}, \dots, t^{s^{n_0-1}})$$

where s is sufficiently large (to be determined later). By the Taylor expansion of f_j we have

$$f_j(r(t)) = \sum_{\mathbf{i}} a_{\mathbf{i}}^{(j)} \mathfrak{p}^{\|\mathbf{i}\|_1} t^{\sum_{k=1}^{n_0} i_k s^{k-1}},$$

where $\mathbf{i} = (i_1, \dots, i_{n_0})$ and $a_{\mathbf{i}}^{(j)} = \partial_{\mathbf{i}} f_j/\mathbf{i}!$. And so

(127) $$f_j(r(t)) = \sum_{n=0}^{\infty} \left(\sum_{\{\mathbf{i} \mid \sum_k i_k s^{k-1} = n\}} a_{\mathbf{i}}^{(j)} \mathfrak{p}^{\|\mathbf{i}\|_1} \right) t^n.$$

We make the following two observations:

(1) $\sum_{\{\mathbf{i} \mid \sum_k i_k s^{k-1} = n\}} a_{\mathbf{i}}^{(j)} \mathfrak{p}^{\|\mathbf{i}\|_1} \equiv \sum_{\{\mathbf{i} \mid \|\mathbf{i}\|_\infty < s, \ \sum_k i_k s^{k-1} = n\}} a_{\mathbf{i}}^{(j)} \mathfrak{p}^{\|\mathbf{i}\|_1} \pmod{\mathfrak{p}^s}$,
(2) If $\|\mathbf{i}\|_\infty, \|\mathbf{i}'\|_\infty < s$ and $\sum_k i_k s^{k-1} = \sum_k i'_k s^{k-1}$, then $\mathbf{i} = \mathbf{i}'$.

In particular we have

$$\sum_{\{\mathbf{i} \mid \sum_k i_k s^{k-1} = n\}} a_{\mathbf{i}}^{(j)} \mathfrak{p}^{\|\mathbf{i}\|_1} \equiv \begin{cases} 0 & \text{if } n \ge s^{n_0} \\ a_{\mathbf{i}(n)}^{(j)} \mathfrak{p}^{\|\mathbf{i}(n)\|_1} & 0 \le n \le s^{n_0} - 1 \end{cases} \pmod{\mathfrak{p}^s}$$

where $\mathbf{i}(n) := (i_1, \ldots, i_{n_0})$ gives us the s-adic digits of n; that means $n = \sum_k i_k s^{k-1}$. Therefore we have

$$(128) \qquad N\left(\left[\sum_{\{\mathbf{i}\mid \sum_k i_k s^{k-1}=n\}} a_{\mathbf{i}}^{(j)}\mathfrak{p}^{\|\mathbf{i}\|_1}\right]_{1\leq n\leq s^{n_0}-1,\ 1\leq j\leq d}\right) \equiv N([a_{\mathbf{i}(n)}^{(j)}\mathfrak{p}^{\|\mathbf{i}(n)\|_1}]) \pmod{\mathfrak{p}^s}.$$

Now suppose $s > dm + k_0$; in particular, if $\|\mathbf{i}\|_1 \leq m$, then $\mathbf{i} = \mathbf{i}(n)$ for some $n < s^{n_0}$. And so we have

$$(129) \qquad\qquad\qquad N([a_{\mathbf{i}(n)}^{(j)}\mathfrak{p}^{\|\mathbf{i}(n)\|_1}]) \geq |\mathfrak{p}^{md+k_0}|.$$

Hence by (128), (129) and $s > dm + k_0$ we have

$$N\left(\left[\sum_{\{\mathbf{i}\mid \sum_k i_k s^{k-1}=n\}} a_{\mathbf{i}}^{(j)}\mathfrak{p}^{\|\mathbf{i}\|_1}\right]_{1\leq n\leq s^{n_0}-1,\ 1\leq j\leq d}\right) \not\equiv 0 \pmod{\mathfrak{p}^s},$$

which implies that

$$\mathrm{rank}\left(\left[\sum_{\{\mathbf{i}\mid \sum_k i_k s^{k-1}=n\}} a_{\mathbf{i}}^{(j)}\mathfrak{p}^{\|\mathbf{i}\|_1}\right]_{1\leq n\leq s^{n_0}-1,\ 1\leq j\leq d}\right) = d,$$

and $\mathbb{1}, f_1 \circ r, \ldots, f_d \circ r$ are linearly independent. $\qquad\square$

Lemma 56′. *Let* $F := (f_1, \ldots, f_{d_0}) : \mathcal{O}^{n_0} \to \mathcal{O}^{d_0}$ *be an analytic function of the form*

$$F(\mathbf{x}) = \sum_{\mathbf{i}} (c_{\mathbf{i},1}\mathbf{x}^{\mathbf{i}}, \ldots, c_{\mathbf{i},d_0}\mathbf{x}^{\mathbf{i}}),$$

where $\mathbf{i} = (i_1, \ldots, i_{n_0})$ *ranges over multi-indexes non-negative integers and* $\mathbf{x}^{\mathbf{i}} = x_1^{i_1} \cdots x_{n_0}^{i_{n_0}}$. *Suppose*

   (1) $|c_{\mathbf{i},j}| \leq 1$ *for any* $\mathbf{i} = (i_1, \ldots, i_m)$ *and any* $1 \leq j \leq d_0$,
   (2) $|\det(c_{\mathbf{i}_i,j})| = |\mathfrak{p}^{k_0}|$ *for some multi-indexes* $\mathbf{i}_1, \ldots, \mathbf{i}_{d_0}$ *whose coordinates add up to a number at most* m_0 *and some positive integer* k_0.

Then there is a polynomial curve $r : \mathcal{O} \to \mathcal{O}^{n_0}$ *such that* $|\det(c'_{i_e,j})| \geq |\mathfrak{p}^{\Theta_{m_0,d_0,k_0}(1)}|$ *for some indexes* $i_e \ll_{m_0,n_0,d_0,k_0} 1$ *where* $f_j \circ r(x) = \sum_i c'_{i,j}x^i$.

Proof. A close examination of proof of Lemma 56 yields that (128), (129) imply

$$N([c'_{i,j}]_{1\leq i\leq(d_0m_0+k_0+1)^{n_0}-1, 1\leq j\leq d}) \geq |\mathfrak{p}^{m_0d_0+k_0}|,$$

which gives us the claim. $\qquad\square$

Corollary 57. *Let* $U \subseteq K^{m_0}$ *be a non-empty open set. Let* $f_j : U \to K$ *be analytic functions, and* $F := (f_1, \ldots, f_d)$. *Suppose* $\mathbb{1}, f_1, \ldots, f_d$ *are linearly independent. Then for any* $l \gg_F 1$ *we have*

$$\sum_{\Theta_F(1)} F(\mathfrak{p}^l\mathcal{O}) - \sum_{\Theta_F(1)} F(\mathfrak{p}^l\mathcal{O}) \supseteq \mathfrak{p}^{\Theta_F(l)}\mathcal{O}^d.$$

Proof. By Lemma 56 there is a polynomial curve r such that $\mathbb{1}, f_1 \circ r, \ldots, f_d \circ r$ are linearly independent and defined on a neighborhood of $0 \in K$. Hence by Lemma 54 we are done. $\qquad\square$

Corollary 57′. *Let* $F := (f_1, \ldots, f_{d_0}) : \mathcal{O}^{n_0} \to \mathcal{O}^{d_0}$ *be an analytic function of the form*

$$F(\mathbf{x}) = \sum_{\mathbf{i}} (c_{\mathbf{i},1}\mathbf{x}^{\mathbf{i}}, \ldots, c_{\mathbf{i},d_0}\mathbf{x}^{\mathbf{i}}),$$

where $\mathbf{i} = (i_1, \ldots, i_{n_0})$ *ranges over multi-indexes non-negative integers. Suppose*

   (1) $|c_{\mathbf{i},j}| \leq 1$ *for any* $\mathbf{i} = (i_1, \ldots, i_m)$ *and any* $1 \leq j \leq d_0$,
   (2) $|\det(c_{\mathbf{i}_i,j})| = |\mathfrak{p}^{k_0}|$ *for some multi-indexes* $\mathbf{i}_1, \ldots, \mathbf{i}_{d_0}$ *whose coordinates add up to a number at most* m_0 *and some positive integer* k_0.

Then for $l \gg_{m_0,n_0,d_0,k_0} 1$ we have

$$\sum\nolimits_{\Theta(1)} F(\mathfrak{p}^l \mathcal{O}) - \sum\nolimits_{\Theta(1)} F(\mathfrak{p}^l \mathcal{O}) \supseteq \mathfrak{p}^{\Theta(l)} \mathcal{O}^{d_0},$$

where all the implied constants depend on m_0, n_0, d_0, k_0.

Proof. This is direct corollary of Lemma 55$'$ and Lemma 56$'$. $\square$

Proof of Proposition 49. Suppose $\{f_{i_1}, \ldots, f_{i_d}\}$ is a basis of $\sum_i K f_i$. So $\mathbb{1}, f_{i_1}, \ldots, f_{i_d}$ are linearly independent. And moreover there is an injective linear map $L : K^d \to K^{d_0}$ such that $F = L \circ \overline{F}$, where $\overline{F}(\mathbf{x}) = (f_{i_1}(\mathbf{x}), \ldots, f_{i_d}(\mathbf{x}))$. By Corollary 57 we have that

$$\sum\nolimits_{\Theta_{\overline{F}}(1)} \overline{F}(\mathfrak{p}^l \mathcal{O}) - \sum\nolimits_{\Theta_{\overline{F}}(1)} \overline{F}(\mathfrak{p}^l \mathcal{O}) \supseteq \mathfrak{p}^{\Theta_{\overline{F}}(l)} \mathcal{O}^d.$$

for any $l \gg_{\overline{F}} 1$. Applying L to the both sides and using the linearity of L we have

$$\sum\nolimits_{\Theta_F(1)} F(\mathfrak{p}^l \mathcal{O}) - \sum\nolimits_{\Theta_F(1)} F(\mathfrak{p}^l \mathcal{O}) \supseteq \mathfrak{p}^{\Theta_F(l)} L(\mathcal{O}^d) \supseteq \mathfrak{p}^{\Theta_F(l)} \mathcal{O}^{d_0} \cap \mathrm{Im}(L).$$

$\square$

Proof of Proposition 49$'$. By a similar argument as in the proof of Proposition 49, Corollary 57$'$ implies the desired result. $\square$

Proof of Corollary 50. Let $\mathcal{O}_\kappa$ be the ring of integers of κ. There is $a \in \mathcal{O}_\kappa$ such that for any i

$$\overline{f}_i(\mathbf{x}) := f_i(a\mathbf{x}) \in \mathcal{O}_\kappa[x_1, \ldots, x_{n_0}].$$

Suppose $\overline{f}_{j_1}, \ldots, \overline{f}_{j'_{d_0}}$ is a basis of $\sum_{i=1}^{d_0} \kappa \overline{f}_i$. So there is a linear embedding $L : \kappa^{d'_0} \to \kappa^{d_0}$ such that

$$(\overline{f}_1(\mathbf{x}), \ldots, \overline{f}_{d_0}(\mathbf{x})) = L(\overline{f}_{j_1}, \ldots, \overline{f}_{j_{d'_0}}).$$

So the operator norm of the induced linear embedding $L_\mathfrak{p} : \kappa_\mathfrak{p}^{d'_0} \to \kappa_\mathfrak{p}^{d_0}$ are uniformly bounded from infinity and zero.

Since $\overline{f}_{j_1}, \ldots, \overline{f}_{j_{d'_0}}$ are linearly independent, there are multi-indexes $\mathbf{i}_1, \ldots, \mathbf{i}_{d'_0}$ such that

$$0 \neq \det(c_{\mathbf{i}_i, j_u}) \in \mathcal{O}_\kappa,$$

where $\overline{f}_j(\mathbf{x}) = \sum_\mathbf{i} c_{\mathbf{i},j} \mathbf{x}^\mathbf{i}$. So $|\det(c_{\mathbf{i}_i, j_u})|_\mathfrak{p} = 1$ for almost all $\mathfrak{p} \in V_f(\kappa)$.

By the above discussion, one can easily finish the proof using Proposition 49$'$. $\square$

REFERENCES

[BY91]   C. Bernstein, A. Yger, *Effective Bézout identities in $\mathbb{Q}[z_1, \ldots, z_n]$*, Acta Math. **166** (1991) 69–120.

[BG08-a]   J. Bourgain, A. Gamburd, *Uniform expansion bounds for Cayley graphs of $\mathrm{SL}_2(\mathfrak{f}_p)$*, Annals of Mathematics **167** (2008) 625–642.

[BG08-b]   J. Bourgain, A. Gamburd, *Expansion and random walks in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$:I*, Journal of the European Mathematical Society **10** (2008) 987–1011.

[BG09]   J. Bourgain, A. Gamburd, *Expansion and random walks in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$:II. With an appendix by J. Bourgain*, Journal of the European Mathematical Society **11**, no. 5., (2009) 1057–1103.

[BGS10]   J. Bourgain, A. Gamburd, P. Sarnak, *Affine linear sieve, expanders, and sum-product,* Inventiones mathematicae **179**, no. 3., (2010) 559–644.

[BV12]   J. Bourgain, P. Varjú, *Expansion in $\mathrm{SL}_d(\mathbb{Z}/q\mathbb{Z})$, q arbitrary*, Inventiones mathematicae **188**, no 1, (2012) 151–173.

[BO14]   E. Breuillard, H. Oh (editors), Thin groups and superstrong approximation, MSRI Publ. **61**, Cambridge Univ. Press., Cambridge 2014.

[BS91]   M. Burger and P. Sarnak, *Ramanujan duals II,* Inventiones mathematicae **106**, no. 1, (1991) 1–11.

[Cad]   A. Cadoret, *An open adelic image theorem for abelian schemes,* to appear in International Mathematics Research Notices.

[CT12]   A. Cadoret, A. Tamagawa, *A uniform open image theorem for l-adic representations, I,* Duke Mathematical Journal **161** (2012) 2605–2634.

[CT13]   A. Cadoret, A. Tamagawa, *A uniform open image theorem for l-adic representations, II,* Duke Mathematical Journal **162** (2013) 2301–2344.

[CFW81]   A. Connes, J. Feldman, B.Weiss, *An amenable equivalence relations is generated by a single transformation,* Ergodic Theory and Dynamical Systems **1** (1981) 431–450.

[Din06]   O. Dinai, *Poly-log diameter bounds for some families of finite groups,* Proceeding of the American Mathematical Society **134**, no 11, (2006) 3137–3142.

[EHK12]   J. Ellenberg, C. Hall, E. Kowalski, *Expander graphs, gonality, and variation of Galois representations,* Duke Mathematical Journal **161**, no.7, (2012) 1233–1275.

[EMO05]   A. Eskin, S. Mozes, H. Oh, *On uniform exponential growth for linear groups,* Inventiones mathematicae **160**, no. 1, (2005) 1–30.

[Fal91]   G. Faltings, *Diophantine approximation on abelian varieties,* Annals of Mathematics (2) **133** (1991) 549–576.

[Fer94]   G. Frey, *Curves with infinitely many points of fixed degree,* Israel J. Math. **85** (1994) 79–85.

[GS04]   A. Gamburd, M. Shahshahani, *Uniform diameter bounds for some families of Cayley graphs,* International Mathematics Research Notices **71** (2004) 3813–3824.

[Gow08]   W.T. Gowers, *Quasirandom Groups,* Combinatorics, Probability and Computing **17** (2008) 363–387.

[Hel05]   H. Helfgott, *Growth and generation in* $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, Annals of Mathematics **167** (2008) 601–623.

[Hel11]   H. Helfgott, *Growth in* $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$, Journal of the European Mathematical Society **13**, no. 3, (2011) 761–851.

[HLW06]   S. Hoory, N. Linial, A. Widgerson, *Expander graphs and their application,* Bull. American Mathematical Society **43**, no. 4, (2006) 439–561.

[How77]   R. Howe, *Kirillov theory for compact p-adic groups,* Pacific Journal of Mathematics **73**, no. 2, (1977) 365–381.

[Hui12]   C.-Y. Hui, *Specialization of monodromy and ℓ-independence,* C. R. Acad. Sci. Paris, Ser. I **350** (2012) 5–7.

[HL]   C.-Y. Hui, M. Larsen, *Adelic openness without the Mumford-Tate conjecture,* preprint. Available online: `http://arxiv.org/pdf/1312.3812v2.pdf`

[Ioa14-a]   A. Ioana, *Orbit equivalence and Borel reducibility rigidity for profinite actions with spectral gap,* to appear in Journal of the European Mathematical Society. Available online: `http://arxiv.org/pdf/1309.3026v4.pdf`

[Ioa14-b]   A. Ioana, *Strong ergodicity, property (T), and orbit equivalence rigidity for translation actions,* to appear in J. Reine Angew. Math. Available online: `http://arxiv.org/pdf/1406.6628.pdf`

[Kes59]   H. Kesten, *Symmetric random walks on groups,* Transactions of the American Mathematical Society **92** (1959) 336–354.

[Kne64]   M. Kneser, *Erzeugende und Relationen verallgemeinerter Einheitengruppen,* J. Reine Angew. Math. **214-215** (1964) 345–349.

[LS74]   V. Landazuri, G. M. Seitz, *On the minimal degrees of projective representations of the finite Chevalley groups,* Journal of Algebra **32** (1974) 418–443.

[Lub94]   A. Lubotzky, Discrete Groups, Expanding Graphs and Invariant Measures, Birkhäuser, 1994.

[LM13]   A. Lubotzky, C. Meiri, *Sieve methods in group theory I: powers in linear groups,* Journal of the American Mathematical Society **25**, no. 4, (2012) 1119–1148.

[LW93]   A. Lubotzky, B. Weiss, *Groups and expanders,* In Expanding graphs (Princeton, NJ, 1992) DIMACS Series **10**, Discrete Mathematics and Theoretical Computer Science 95–109. American Mathematical Society, Providence, RI, 1993.

[LZ03]   A. Lubotzky, A. Żuk, Property(τ), preliminary version, 2003. `http://www.ma.huji.ac.il/~alexlub/BOOKS/On\ %20property/On\%20property.pdf`.

[MW]   D. W. Masser, G. Wüstholz, *Fields of large transcendence degree generated by values of elliptic functions*, Inventiones mathematicae **72**, no. 3 ,(1983) 407–464.

[Maz00]   B. Mazur, *Abelian varieties and the Mordell–Lang conjecture,* 199-227; in D. Haskell, A. Pillay, C. Steinhorn (ed.), Model theory, algebra, and geometry, MSRI Publ. **39**, Cambridge Univ. Press., Cambridge, 2000.

[Mc95]   M. McQuillan, *Division points on semi-abelian varieties,* Inventiones mathematicae **120** (1995) 143–159.

[NP11]   N. Nikolov, L. Pyber, *Product decompositions of quasirandom groups and a Jordan type theorem,* Journal of the European Mathematical Society **13**, no. 4, (2011) 1063–1077.

[Nor89]   M. V. Nori, *On subgroups of* $\mathrm{GL}_n(\mathfrak{f}_p)$, Inventiones mathematicae **88**, no. 2, (1987) 257–275.

[OW80]   D. Ornstein, B.Weiss, *Ergodic theory of amenable groups. I. The Rokhlin lemma.,* Bulletin of the American Mathematical Society (N.S.) **1** (1980) 161–164.

[Pin98]   R. Pink, *Compact subgroups of linear algebraic groups,* Journal of Algebra **206** (1998) 438–504.

[SG05]   A. Salehi Golsefidy, *Character degrees of p-groups and pro-p groups,* Journal of Algebra **286** (2005) 476–491.

[SG]   A. Salehi Golsefidy, *Super-approximation, I:* $\mathfrak{p}$*-adic semisimple case,* to appear in International Mathematics Research Notices. `https://doi.org/10.1093/imrn/rnw208`

[SGS13]   A. Salehi Golsefidy, P. Sarnak, *Affine sieve,* Journal of the American Mathematical Society **26**, no. 4, (2013) 1085–1105.

[SGV12]   A. Salehi Golsefidy, P. Varjú, *Expansions in perfect groups,* Geometric And Functional Analysis **22**, no. 6, (2012) 1832–1891.

[SGZ]   A. Salehi Golsefidy, X. Zhang, *Inducing super-approximation,* preprint.

[SX91]   P. Sarnak and X. Xue, *Bounds for multiplicities of automorphic representations,* Duke Mathematical Journal **64**, no. 1, (1991) 207–227.

[Sha09]   A. Shalev, *Word maps, conjugacy classes, and a noncommutative Waring-type theorem,* Annals of Mathematics (2) **170**, no. 3, (2009) 1383–1416.

[Tao08]   T. Tao, *Product set estimates for non-commutative groups,* Combinatorica **28**, no. 5, (2008) 547–594.

[Tit79]   J. Tits, *Reductive groups over local fields,* Proceedings of symposia in pure mathematics **33** (1979), part 1, 29–69.

[Var12]   P. Varjú, *Expansion in* $\mathrm{SL}_d(\mathcal{O}_K/I)$*, I square-free,* Journal of the European Mathematical Society **14**, no. 1, (2012) 273–305.

[Wei84]   B. Weisfeiler, *Strong approximation for Zariski-dense subgroups of semisimple algebraic groups,* Annals of Mathematics **120** (1984) 271–315.

Mathematics Dept, University of California, San Diego, CA 92093-0112

E-mail address: `golsefidy@ucsd.edu`