JOURNAL OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 26, Number 4, October 2013, Pages 1085–1105
S 0894-0347(2013)00764-X
Article electronically published on April 1, 2013

THE AFFINE SIEVE

ALIREZA SALEHI GOLSEFIDY AND PETER SARNAK

1. Introduction

The purpose of this paper is to complete the program initiated in [BGS10] of developing a Brun combinatorial sieve in the context of a group of affine linear motions. As explained below, this is possible in part thanks to recent developments concerning expansion in graphs which are associated with orbits of such groups. We review briefly the set up in [BGS10]. Let Γ be a finitely generated group of affine linear motions of $\mathbb{Q}^n$, that is, transformations of the form $\phi : x \mapsto Ax+b$ with $A \in \mathrm{GL}_n(\mathbb{Q})$ and $b \in \mathbb{Q}^n$. It will be convenient for us to realize Γ as a subgroup of linear transformations of $\mathbb{Q}^{n+1}$ by setting

$$\phi = \begin{bmatrix} A & b^t \\ 0 & 1 \end{bmatrix}.$$

Fix $v \in \mathbb{Q}^n$ and let $\mathcal{O} = \Gamma v$ be the orbit of v under Γ in $\mathbb{Q}^n$. Since Γ is finitely generated, the points of $\mathcal{O}$ have coordinates in the ring of S-integers $\mathbb{Z}_S$ (that is, their denominators have all of their prime factors in the finite set S). In what follows, we will suppress the behavior of our points at these places in S and we will even extend S to a fixed finite set S' when convenient. This is done for technical simplicity and an analysis of what happens at these places can probably be examined and controlled, but we will not do so here.

Denote by $\mathrm{Zcl}(\mathcal{O})$ the Zariski closure of $\mathcal{O}$ in $\mathbb{A}^n_{\mathbb{Q}}$. Let $f \in \mathbb{Q}[x_1, \dots, x_n]$ and denote by $V(f)$ its zeros. We will assume henceforth that $\dim(V(f) \cap \mathrm{Zcl}(\mathcal{O})) < \dim(\mathrm{Zcl}(\mathcal{O}))$, i.e., f is not constantly zero on any of the irreducible components of $\mathrm{Zcl}(\mathcal{O})$. We seek points $x \in \mathcal{O}$ such that $f(x)$ has at most a fixed number of prime factors outside of S (or an enlarged S'). For $m \geq 1$ and S' fixed (and finite) set

$$\mathcal{O}_{m,S'} := \{x \in \mathcal{O} |\ f(x) \text{ has at most } m \text{ prime factors outside } S'\}. \tag{1}$$

Thus $\mathcal{O}_{1,S'} \subseteq \mathcal{O}_{2,S'} \subseteq \cdots$, $\mathcal{O} = \bigcup_{m=1}^{\infty} \mathcal{O}_{m,S'}$, and $\bigcup_{m=1}^{\infty} \mathrm{Zcl}(\mathcal{O}_{m,S'}) \subseteq \mathrm{Zcl}(\mathcal{O})$. We say that the pair $(\mathcal{O}, f)$ saturates if $\mathrm{Zcl}(\mathcal{O}) = \mathrm{Zcl}(\mathcal{O}_{r,S'})$ for some $r < \infty$. In words, this happens if there is a finite set S' of primes and a finite number r such that the set of points $x \in \mathcal{O}$ at which $f(x)$ has at most r prime factors outside of S' (that is to say, at most r prime factors as an S'-integer) is Zariski dense in $\mathrm{Zcl}(\mathcal{O})$.

In [BGS10] many classical examples and applications of such saturation (or conjectured saturation) are given. Here we simply point to Brun's original work. If $n = 1$ and $\mathbb{G} = \mathrm{Zcl}(\Gamma)$ contains no tori, then $\mathcal{O}$ (if it is infinite) is essentially an arithmetic progression. In this case, the pair $(\mathcal{O}, f)$ saturates by Brun's results,

Received by the editors October 13, 2011 and, in revised form, January 7, 2013.
2010 *Mathematics Subject Classification.* Primary 20G35, 11N35.
The first author was partially supported by the NSF grants DMS-0635607 and DMS-1001598.
The second author was partially supported by an NSF grant.

which assert that there are infinitely many $x \in \mathbb{Z}$ (infinite is equivalent to Zariski density in $\mathbb{A}^1$) such that $f(x)$ has at most a fixed number $r = r_f$ prime factors. In this case after Brun, much effort has gone into reducing the number r (for example if $f(x) = x(x+2)$, then $r_f = 2$ is equivalent to the twin prime conjecture and $r_f = 3$ is known [Ch73]). On the other hand, in this one-dimensional case if $\mathbb{G} = \mathrm{Zcl}(\Gamma)$ is a torus, then it is quite likely that $(\mathcal{O}, f)$ does not saturate for certain f's. For example if $\Gamma = \{2^n | \ b \in \mathbb{Z}\}$, $v = 1$, and $f(x) = (x-1)(x-2)$, then standard heuristic probabilistic arguments (see for example [HW79, p. 15] or [BLMS05] for a related conjecture and heuristic argument) suggest that the number of odd distinct prime factors of $(2^m - 2)(2^m - 1)$ tends to infinity as m goes to infinity. That is, $(\mathcal{O}, f)$ does not saturate.

This feature persists (see the Appendix) for any group which does not satisfy one of the following equivalent conditions for a group $\mathbb{G} = \mathrm{Zcl}(\Gamma)$.

(1) The character group $X(\mathbb{G}^\circ)$ of $\mathbb{G}^\circ$ is trivial, where $\mathbb{G}^\circ$ is the connected component of $\mathbb{G}$.
(2) No torus is a homomorphic image of $\mathbb{G}^\circ$.
(3) $X(R(\mathbb{G})) = 1$, where $R(\mathbb{G})$ is the radical of $\mathbb{G}$.
(4) $\mathbb{G}/R_u(\mathbb{G})$ is a semisimple group, where $R_u(\mathbb{G})$ is the unipotent radical of $\mathbb{G}$.
(5) $\mathbb{G} \simeq \mathbb{G}_{ss} \ltimes \mathbb{U}$, where $\mathbb{G}_{ss}$ is a semisimple group and $\mathbb{U}$ is a unipotent group.
(6) The Levi factor of $\mathbb{G}$ is semisimple.

If $\mathbb{G}$ satisfies the above properties, we call it *Levi-semisimple*. We can now state our main result, which is a proof of the *fundamental saturation theorem* that was conjectured in [BGS10].

Theorem 1. *Let Γ, $\mathcal{O}$, and f be as above and assume that $\mathbb{G} = \mathrm{Zcl}(\Gamma)$ is Levi-semisimple. Then $(\mathcal{O}, f)$ saturates. That is, there are a positive integer r and finite set of primes S' such that $\mathrm{Zcl}(\mathcal{O}_{r,S'}) = \mathrm{Zcl}(\mathcal{O})$.*

Remark 2. (1) The condition on $\mathbb{G}$ which is quite mild and easily checked in examples, is probably necessary for saturation (in particular it is needed in executing a Brun-like sieve), when considering all pairs $(\mathcal{O}, f)$ for which $\mathrm{Zcl}(\Gamma) = \mathbb{G}$. We discuss the heuristics leading to this belief in the Appendix. (It is worth emphasizing however that we have no example of a pair $(\mathcal{O}, f)$ for which we can prove that it does not saturate!) These heuristics indicate what we expect is the case that the condition on $\mathbb{G}$ in the theorem is the exact one that leads to saturation.

(2) The proof of Theorem 1 is effective in the sense that given a pair $(\mathcal{O}, f)$, there is an algorithm which will terminate with a value r and the set S'. However without imposing strong conditions on Γ (such as it being a lattice in the corresponding group G_S, as is done in [NS10]), the bounds for r that would emerge from our proof would be absurdly large and very far from the minimal r (called the saturation number in [BGS10]).

We outline the proof of Theorem 1. We start by pulling back f to a regular function on $\mathbb{G}$ and reformulate Theorem 1 to the following form.

Theorem 3. *Let Γ be a finitely generated subgroup of $\mathrm{SL}_n(\mathbb{Q})$. Let $\mathbb{G}$ be the Zariski closure of Γ in $(\mathbb{SL}_n)_{\mathbb{Q}}$ and let $f \in \mathbb{Q}[\mathbb{G}]$ which is not constantly zero on any of the irreducible components of $\mathbb{G}$. If $\mathbb{G}$ is Levi-semisimple, then there are a positive*

integer r and a finite set S of primes such that

$$\Gamma_{r,S}(f) := \{\gamma \in \Gamma |\ f(\gamma) \text{ has at most } r \text{ prime factors outside } S\} \tag{2}$$

is Zariski dense in $\mathbb{G}$.

To prove Theorem 3, first we find a perfect normal subgroup $\mathbb{H}$ of $\mathbb{G}$ such that $\Gamma \cap \mathbb{H}$ is Zariski dense in $\mathbb{H}$ and $\mathbb{G}/\mathbb{H}$ is a unipotent group. Let π denote the projection map $\pi : \mathbb{G} \to \mathbb{G}/\mathbb{H}$. Since $\mathbb{G}/\mathbb{H}$ is a $\mathbb{Q}$-unipotent group, there is a $\mathbb{Q}$-section $\phi : \mathbb{G}/\mathbb{H} \to \mathbb{G}$ and, as a $\mathbb{Q}$-variety, $\mathbb{G}$ can be identified with the product of $\mathbb{H}$ and $\mathbb{U}$ (see Section 5 for more details). Thus there are polynomials p and $p_i \in \mathbb{Q}[\mathbb{U}]$ and regular functions $f_i \in \mathbb{Q}[\mathbb{H}]$ such that $\gcd(p_i) = 1$ and

$$f(g) = p(\pi(g)) \cdot \left[\sum_i p_i(\pi(g))\ f_i(\phi(\pi(g))^{-1} g)\right] = p(\pi(g)) \cdot \left[\sum_i p_i(\pi(g)) L_{\phi(\pi(g))}(f_i)(g)\right], \tag{3}$$

where $L_g : \mathbb{Q}[\mathbb{G}] \to \mathbb{Q}[\mathbb{G}]$ is the left multiplication operator, i.e., $L_g(f)(g') = f(g^{-1}g')$.

In the second step, we prove the following stronger version of Theorem 3 for a unipotent group to get a control on the values of p and the p_i's.

Theorem 4. *Let $\mathbb{U}$ be a unipotent $\mathbb{Q}$-group. Let Γ be a finitely generated, Zariski dense subgroup of $\mathbb{U}(\mathbb{Q})$, and let $p, p_1, \ldots, p_m \in \mathbb{Q}[\mathbb{U}]$ such that $\gcd(p_i) = 1$. Then there are a finite set S of primes and a positive integer r such that,*

$$\{\gamma \in \Gamma \mid p(\gamma) \text{ has at most } r \text{ prime factors in } \mathbb{Z}_S \text{ and } \gcd(p_i(\gamma)) \text{ is a unit in } \mathbb{Z}_S\}$$

is Zariski dense in $\mathbb{U}$.

The major inputs in the proof of Theorem 4 are Malcev theory of lattices in nilpotent Lie groups and Brun's combinatorial sieve.

In using Theorem 4, to prove Theorem 3, one needs to prove its stronger form for perfect groups, which also provides a uniform control on r and S for all the coprime linear combinations of a finite set of regular functions f_i's. We get this control in two steps. Before stating the precise formulation of our results, let us briefly recall parts of Nori's results from [N87] and introduce some notation.

As we said earlier, $\Gamma \subseteq \mathrm{SL}_n(\mathbb{Z}_{S_0})$ for some finite set of primes S_0. Let $\mathcal{G}$ be the Zariski closure of Γ in $(\mathbb{SL}_n)_{\mathbb{Z}_{S_0}}$. It is worth mentioning that $\mathbb{G}$ is just the generic fiber of $\mathcal{G}$. If $\mathbb{G}$ is generated by its 1-parameter unipotent subgroups, then, by [N87], there is a finite set $S_0 \subseteq S_\Gamma$ of primes such that:

(1) The projection map $\mathcal{G} \times \mathrm{Spec}(\mathbb{Z}_{S_\Gamma}) \to \mathrm{Spec}(\mathbb{Z}_{S_\Gamma})$ is smooth.
(2) All the fibers of the projection map $\mathcal{G} \times \mathrm{Spec}(\mathbb{Z}_{S_\Gamma}) \to \mathrm{Spec}(\mathbb{Z}_{S_\Gamma})$ are geometrically irreducible and have the same dimension.
(3) $\pi_p(\Gamma) = \mathcal{G}_p(\mathfrak{f}_p)$ for any p outside of S_Γ, where $\pi_p : \Gamma \to \mathrm{SL}_n(\mathfrak{f}_p)$ is the homomorphism induced by the residue map $\pi_p : \mathbb{Z} \to \mathfrak{f}_p$ and $\mathcal{G}_p = \mathcal{G} \times \mathrm{Spec}(\mathfrak{f}_p)$.
(4) $\prod_{p \notin S_\Gamma} \mathcal{G}(\mathbb{Z}_p)$ is a subgroup of the closure of Γ in $\prod_{p \notin S_0} \mathrm{SL}_n(\mathbb{Z}_p)$ (where $\mathbb{Z}_p$ is the ring of p-adic integers).

For a given $f \in \mathbb{Q}[\mathbb{G}]$, there is a finite set $S_\Gamma \subseteq S$ of primes such that $f \in \mathbb{Z}_S[\mathcal{G}]$ (we take the smallest such set). We say that p is a ramified prime with respect to

Γ and f if $f(\gamma) \in p\mathbb{Z}_S$ for any $\gamma \in \Gamma$. We denote the set of all the ramified primes with respect to Γ and f by $S_{\Gamma,f}$.

We also note that $f \in \mathbb{Q}[\mathbb{G}]$ can be lifted to a regular function $\tilde{f}$ on all the $n \times n$ matrices (we pick one such lift with smallest possible degree).

Theorem 5. *In the above setting, if $\mathbb{G}$ is perfect and generated by its unipotent subgroups, then there is a positive integer r depending on Γ, the degree of $\tilde{f}$, a lift of f to $\mathbb{A}^{N^2}$, and $\#S_{\Gamma,f}$ such that $\Gamma_{r,S_{\Gamma,f}}(f)$ is Zariski dense in $\mathbb{G}$.*

To establish Theorem 5, we follow the treatment given in the work of Bourgain, Gamburd, and Sarnak [BGS10] and combine it with a recent result of Salehi Golsefidy and Varjú [SV][1]. Theorem 5 enables us to get a fixed r that works for all the linear combinations of a given finite set of regular functions f_i, as soon as we have a uniform control on the set of associated ramified primes. In the second step, we get a uniform upper bound on the ramified primes with respect to Γ and all the coprime linear combinations of the f_i's.

Theorem 6. *In the above setting, let $\mathbb{G}$ be Zariski connected and perfect. Then for any finite set of primes S' and any given $f_1, \dots, f_m \in \mathbb{Q}[\mathbb{G}]$ which are linearly independent over $\mathbb{Q}$, there are a positive integer r and a finite set S of primes such that $\Gamma_{r,S}(f_{\mathbf{v},g})$ is Zariski dense in $\mathbb{G}$ for any primitive integer vector $\mathbf{v} = (v_1, \dots, v_m)$ and any $g \in \mathcal{G}(\mathbb{Z}_{S'})$, where $f_{\mathbf{v},g} = L_g(\sum_{i=1}^m v_i f_i)$.*

Using Theorem 6, we are able to finish the proof of Theorem 3.

We end the introduction by fixing some notation that will be used in the rest of article. Let Π be the set of all the primes. For any rational number q, let $\Pi(q)$ be the set of all the prime factors of q (with a positive or negative power). For a Zariski connected group $\mathbb{G}$, let $R(\mathbb{G})$ (resp. $R_u(\mathbb{G})$) be the radical (resp. the unipotent radical) of $\mathbb{G}$ and let $\mathbb{G}_{ss} := \mathbb{G}/R(\mathbb{G})$ be the semisimple factor of $\mathbb{G}$. If $\mathbb{G}$ is a Zariski connected, Levi-semisimple group, then $\mathbb{G} \simeq \mathbb{G}_{ss} \ltimes R_u(\mathbb{G})$. Let $\mathbb{Z}_*^m$ be the set of all the primitive m-tuples of integers. For any affine scheme $X = \mathrm{Spec}(A)$ and a regular function f on X, $V(f)$ denotes the closed subscheme of X defined by f, i.e., $V(f) := \{\mathfrak{p} \in \mathrm{Spec}(A) |\ f \in \mathfrak{p}\}$.

2. The unipotent case

In this section, we prove Theorem 4. We start with the abelian case.

Lemma 7. *Let $P(x) \in \mathbb{Z}[x]$; then there is a positive integer $r = r(\deg P)$ which depends only on $\deg P$ such that $P(n)$ has at most r prime factors outside $S_P = \gcd_{m\in\mathbb{Z}} P(m)$ for infinitely many integers n.*

Proof. This is a classical result of sieve theory [HR74]. □

Lemma 8. *For a given $P(x) = \sum_{i=0}^m a_i x^i \in \mathbb{Z}[x]$, one has*

$$S_P \subseteq [1, \deg P] \cup \Pi(\gcd_i\ a_i).$$

Proof. It is clear. □

[1]This work relies in part on a number of recent developments ([H08], [BG08], [BGT11],[PS], [V12]).

Lemma 9. *For $M \in \mathbb{Z}$ and $P_1(x), \dots, P_m(x) \in \mathbb{Z}[x]$, there are integers a and b such that*

$$\bigcup_{i=1}^{m} \Pi(\gcd(P_i(aj+b), M)) \subseteq \bigcup_{i=1}^{k} S_{P_i},$$

for any integer j.

Proof. For a given prime p which is not in $\bigcup_{i=1}^{k} S_{P_i}$, by the definition, for some i and b_p, $P_i(pj+b_p)$ is coprime to p for any integer j. One can complete the argument by the Chinese remainder theorem. □

In the following lemma, we prove a stronger version of Theorem 4 when $\mathbb{U} = \mathbb{G}_a^d$.

Lemma 10. *Let $P, P_{ij} \in \mathbb{Z}[x_1, \dots, x_d]$ for $1 \le i \le m$ and $1 \le j \le m'$. Assume that, for any $1 \le i \le m$, $\gcd_{j=1}^{m'}(P_{ij}) = 1$. Then there are a positive integer r, a finite set S of primes, and a Zariski dense subset X of $\mathbb{Z}^d$ such that for any $\mathbf{x} \in X$:*

(1) *$P(\mathbf{x})$ has at most r prime factors outside S.*
(2) *$\bigcup_{i=1}^{m} \Pi(\gcd_{j=1}^{m'}(P_{ij}(\mathbf{x}))) \subseteq S$.*

Proof. We proceed by induction on d, the number of variables. For $d = 1$ and any i, there are integer polynomials Q_{ij} such that $\sum_{j=1}^{m'} Q_{ij}(x)P_{ij}(x) = m_i \in \mathbb{Z}$. Hence for any $x \in \mathbb{Z}$, $\gcd_{j=1}^{m'}(P_{ij}(x))$ divides m_i, and, by Lemma 7, we are done.

For the induction step, without loss of generality, by increasing m if necessary, we may and will assume that the P_{ij}'s are irreducible polynomials. Viewing the P_{ij}'s as polynomials on x_d, for any i, we can find polynomials $Q_{ij}(x_1, \dots, x_d)$ such that $\sum_{j=1}^{m'} Q_{ij}P_{ij} = Q_i \in \mathbb{Z}[x_1, \dots, x_{d-1}]$. Let $P_{ij} = \sum_l H_{ij}^{(l)} x_d^l$, where $H_{ij}^{(l)} \in \mathbb{Z}[x_1, \dots, x_{d-1}]$. Since P_{ij} is irreducible, either P_{ij} is independent of x_d or $\gcd_l(H_{ij}^{(l)}) = 1$. We also write P as a polynomial in x_d:

$$P(x_1, \dots, x_d) = H(x_1, \dots, x_{d-1}) \sum H_i(x_1, \dots, x_{d-1}) x_d^i,$$

where $\gcd_i H_i = 1$. Now let's apply the induction hypothesis for the following polynomials:

(1) Let $H(x_1, \dots, x_{d-1})$ be the new P.
(2) Let $\{H_i\}$ be one of the sequences of the coprime polynomials.
(3) For a given i, either $\{P_{ij}\}_j$ if all of them are independent of x_d or $\{H_{ij}^{(l)}\}_l$ where P_{ij} depends on x_d.

Because of the way we chose the sequences of polynomials, certainly the g.c.d. of each sequence is 1, and we can use the induction hypothesis. So we get a positive number r, a finite set S of primes, and a Zariski dense subset X of $\mathbb{A}^{d-1}$, such that for any $\mathbf{x} = (x_1, \dots, x_{d-1}) \in X$:

(1) $H(\mathbf{x})$ has at most r prime factors in the ring of S-integers.
(2) $\Pi(\gcd_i(H_i(\mathbf{x}))) \subseteq S$.
(3) For a given i, either $\Pi(\gcd_j(P_{ij}(\mathbf{x}))) \subseteq S$ if all of $\{P_{ij}\}_j$ are independent of x_d or $\Pi(\gcd_l(H_{ij}^{(l)}(\mathbf{x}))) \subseteq S$ where P_{ij} depends on x_d.

Let us fix $\mathbf{x} \in X$ and set $M = \prod_i Q_i(\mathbf{x})$. For a given i, if $\{P_{ij}\}_j$ are independent of x_d, for all j, we already have obtained the condition on the g.c.d. of their value. So let us just focus on the i's for which there is a j such that P_{ij} depends on x_d. For

all such i and j, consider the single variable polynomials $\mathcal{P}_{ij}(x_d) = \sum_k H_{ij}^{(k)}(\mathbf{x})x_d^k$. Let us also introduce $\mathcal{P}(x_d) = \sum H_i(\mathbf{x})x_d^i$. By Lemma 8 and Lemma 9, there is an arithmetic progression $ax + b$, such that for any $x \in \mathbb{Z}$,

$$\Pi(\gcd(\mathcal{P}(ax+b), M)) \cup \bigcup_{i,j} \pi(\gcd(\mathcal{P}_{ij}(ax+b), M)) \subseteq [1, \deg p + \sum_{i,j} \deg p_{ij}] \cup S.$$

Let $\widetilde{S} = \Pi \cap ([1, \deg \mathcal{P} + \sum_{i,j} \deg \mathcal{P}_{ij}] \cup S)$. Thus, by this discussion and Lemma 8, we have that for any integer x and $\mathbf{x} \in X$,

$$S_{\mathcal{P}(ax+b)} \cup \bigcup_i \Pi(\gcd_j(P_{ij}(\mathbf{x}, ax+b))) \subseteq \widetilde{S}.$$

Now an application of the classical sieve on $\mathcal{P}(ax+b)$ and the induction hypothesis give us $\tilde{r}$ such that, for any $\mathbf{x} \in X$, we can find an infinite subset of integer numbers $V_{\mathbf{x}}$ with the following properties:

(1) $P(\mathbf{x}, x_d)$ has at most $\tilde{r}$ prime factors in the ring of $\widetilde{S}$-integers, for any $x_d \in V_{\mathbf{x}}$.
(2) $\bigcup_i \Pi(\gcd_j(P_{ij}(\mathbf{x}, x_d))) \subseteq \widetilde{S}$, for any $x_d \in V_{\mathbf{x}}$.

Hence $\tilde{r}$, $\widetilde{S}$, and $\bigsqcup_{\mathbf{x}\in X}\{\mathbf{x}\} \times V_{\mathbf{x}}$ satisfy our claim. □

Lemma 11. *A finitely generated subgroup of the group of unipotent upper-triangular rational matrices* $\mathrm{U}_n(\mathbb{Q})$ *is discrete in* $\mathrm{U}_n(\mathbb{R})$.

Proof. Let $d_N = \mathrm{diag}(N^{n-1}, N^{n-2}, \dots, 1)$. The claim is a clear consequence of the fact that

$$\mathrm{U}_n(\mathbb{Q}) = \bigcup_{N\in\mathbb{N}} d_N^{-1} \cdot \mathrm{U}_n(\mathbb{Z}) \cdot d_N,$$

and if N divides M,

$$d_N^{-1} \cdot \mathrm{U}_n(\mathbb{Z}) \cdot d_N \subseteq d_M^{-1} \cdot \mathrm{U}_n(\mathbb{Z}) \cdot d_M. \qquad \square$$

Lemma 12. *Let* $\mathbb{U}$ *be a unipotent* $\mathbb{Q}$*-group. If* Γ *is a finitely generated, Zariski dense subgroup of* $\mathbb{U}(\mathbb{Q})$*, then there is a lattice* Λ *in* $\mathfrak{u} = \mathrm{Lie}(\mathbb{U})(\mathbb{R})$ *such that* $\exp(\Lambda)$ *is a subset of* Γ.

Proof. By the Lie-Kolchin theorem, $\mathbb{U}$ can be embedded in U_n, for some n, as a $\mathbb{Q}$-group. Therefore, by Lemma 11, Γ is a closed subgroup of $U = \mathbb{U}(\mathbb{R})$. Hence by [Ra72, Theorem 2.12], it is a lattice in U. So Λ_0, the $\mathbb{Z}$-span of $\log\Gamma$, is a lattice in $\mathfrak{u}$, and $\widetilde{\Gamma} = \langle \exp(\Lambda) \rangle$ is a finite extension of Γ. In particular, for some m, $\exp(m\Lambda_0)$ is a subset of Γ, as we desired. □

Proof of Theorem 4. Since $\mathbb{U}$ is a unipotent group, $\mathrm{Lie}(\mathbb{U})$ can be identified with the underlying $\mathbb{Q}$-variety of $\mathbb{U}$ via the exponential map $\exp : \mathrm{Lie}(\mathbb{U}) \to \mathbb{U}$. Via this identification, we can and will view p and the p_i's as regular functions on $\mathrm{Lie}(\mathbb{U})$, i.e., polynomials in $d = \dim \mathbb{U}$ variables. By Lemma 12, we find a lattice Λ of $\mathrm{Lie}(\mathbb{U})(\mathbb{R})$ such that $\exp(\Lambda) \subseteq \Gamma$. Since the logarithmic map is defined over $\mathbb{Q}$, Λ is a subgroup of $\mathrm{Lie}(\mathbb{U})(\mathbb{Q})$. Hence we can identify $\mathrm{Lie}(\mathbb{U})(\mathbb{Q})$ with $\mathbb{Q}^d$ so that Λ gets identified with $\mathbb{Z}^d$. The proof is completed, using Lemma 10. □

3. The perfect case. I

The goal of this section is to prove Theorem 5. To do so, we essentially follow [BGS10]. However we have to be extra careful as we need to understand how r and S depend on f.

In this section, we will assume that the Zariski closure Γ is perfect and it is generated by its unipotent subgroups. This is equivalent to saying that $\mathbb{G} \simeq \mathbb{G}_{ss} \ltimes R_u(\mathbb{G})$ is perfect and $\mathbb{G}_{ss}$ is Zariski connected and simply connected.

Proposition 13. *In the above setting, let f be a non-zero element of $\mathbb{Q}[\mathbb{G}]$ and let $\tilde{f}$ be a lift of f to $\mathbb{A}^{n^2}_{\mathbb{Q}}$. Then there is a positive integer M which depends only on the degree of $\tilde{f}$ such that $V(f)$ has at most M geometric irreducible components.*

Proof. Let $g_i \in \mathbb{Q}[\mathbb{A}^{N^2}]$ be defining relations of $\mathbb{G}$. So $V(f)$ is isomorphic to

$$\operatorname{Spec}(\mathbb{Q}[x_1, \dots, x_{N^2}]/\langle \tilde{f}, g_1, \dots, g_k \rangle).$$

We also observe that the number of irreducible components of a subvariety of $\mathbb{A}^{N^2}$ is the same as the number of irreducible components of its closure in $\mathbb{P}^{N^2}$. On the other hand, by the general Bezout's theorem [Sch00], we have that

$$\sum_i \deg W_i \leq \deg \overline{V(\tilde{f})} \cdot \prod_i \deg \overline{V(g_i)},$$

where the W_i are the irreducible components of the projective closure of $V(f)$. This completes the proof. □

Lemma 14. *Let V be a closed subset of $\mathbb{A}^n_{\mathfrak{f}_p}$ defined over $\mathfrak{f}_p$. If $\mathfrak{f}$ is a non-trivial extension of $\mathfrak{f}_p$ and $\operatorname{Aut}(\mathfrak{f})$ acts simply transitively on the geometric irreducible components of V, then*

$$\#V(\mathfrak{f}_p) = O(p^{\dim V - 1}),$$

where the constant depends only on n, the geometric degree, and the geometric dimension of V.

Proof. By the assumption, $V = \bigcup_{\sigma \in \operatorname{Aut}(\mathfrak{f})} W^\sigma$ and $\dim(W \cap W^\sigma) \leq \dim V - 1$ when σ is not the identity. It is clear that $V' = \bigcap_{\sigma \in \operatorname{Aut}(\mathfrak{f})} W^\sigma$ is also defined over $\mathfrak{f}_p$. We claim that

$$V(\mathfrak{f}_p) = V'(\mathfrak{f}_p).$$

To show this, we note that any irreducible component is also affine. Let $\mathbf{x}_0 \in V(\mathfrak{f}_p)$. Then $\mathbf{x}_0 \in W^\sigma$ for some $\sigma \in \operatorname{Aut}(\mathfrak{f})$, i.e., $f(\mathbf{x}_0) = 0$ for any $f \in \mathfrak{f}[x_1, \dots, x_n]$ which vanishes on W^σ. Let $f = \sum_j \lambda_j f_j$ where $\{\lambda_j\}$ is an $\mathfrak{f}_p$-basis of $\mathfrak{f}$ and $f_j \in \mathfrak{f}_p[x_1, \dots, x_n]$. Thus $f_j(\mathbf{x}_0) \in \mathfrak{f}_p$. Since the λ_j's are linearly independent over $\mathfrak{f}_p$ and $\sum_j \lambda_j \mathfrak{f}_j(\mathbf{x}_0) = 0$, we have that $f_j(\mathbf{x}_0) = 0$ for any j. Hence $\sigma'(f)(\mathbf{x}_0) = 0$ for any $\sigma' \in \operatorname{Aut}(\mathfrak{f})$, which completes the proof of the claim. We can also control the degree of V' by the degree and the dimension of V. Hence, by [FHM94, Lemma 3.1], the lemma follows. □

If V is a closed subset of $\mathbb{A}^n_{\mathbb{Q}}$, by the definition there are polynomials $p_1, \dots, p_k \in \mathbb{Q}[x_1, \dots, x_n]$ such that $V = \{\mathfrak{p} \in \operatorname{Spec} \mathbb{Q}[x_1, \dots, x_n] | \ \langle p_1, \dots, p_k \rangle \subseteq \mathfrak{p}\}$. For a large enough prime p, we can look at the p_i's modulo p and get a new variety V_p over $\mathfrak{f}_p$. Changing the p_i's to another set of defining relations only changes finitely many V_p. Hence for almost all p, V_p just depends on V. We will abuse notation and use $V(\mathfrak{f}_p)$ instead of $V_p(\mathfrak{f}_p)$ in the following statements.

Proposition 15. *Let V be a closed subset of $\mathbb{A}^n_{\mathbb{Q}}$ all of whose geometric irreducible components are defined over k and let the group of automorphisms $\mathrm{Aut}(k)$ of k act simply transitively on the geometric irreducible components of V. Then for almost all p,*

$$\#V(\mathfrak{f}_p) = \begin{cases} O(p^{\dim V-1}) & \text{if } p \text{ does not split completely over } k, \\ \deg(k)\, p^{\dim V} + O(p^{\dim V-\frac{1}{2}}) & \text{otherwise,} \end{cases}$$

and the implied constants depend only on n, the degree of k, the geometric degree, and the geometric dimension of V.

Proof. Let W be an irreducible component of V; then, by the assumption, we have $V = \bigcup_{\sigma\in\mathrm{Aut}(k)} W^\sigma$, the W^σ's are distinct irreducible components of V, and

$$V_p = \bigcup_{\mathfrak{p}|p} \bigcup_{\sigma\in\mathrm{Aut}(\mathfrak{f}_\mathfrak{p})} W^\sigma_\mathfrak{p},$$

where $W_\mathfrak{p}$ is defined by defining relations of W modulo $\mathfrak{p}$ (it is well-defined for almost all $\mathfrak{p}$). Let $V_\mathfrak{p} = \bigcup_{\sigma\in\mathrm{Aut}(\mathfrak{f}_\mathfrak{p})} W^\sigma_\mathfrak{p}$. By Nöether-Bertini's theorem, $W_\mathfrak{p}$ is irreducible for almost all $\mathfrak{p}$. In particular,

$$\dim(V_{\mathfrak{p}_1} \cap V_{\mathfrak{p}_2}) \le \dim V - 1,$$

for $\mathfrak{p}_1 \neq \mathfrak{p}_2$ and the degree of this variety has an upper bound which only depends on the degree and the dimension of V. Hence, by [FHM94, Lemma 3.1],

$$\#V_p(\mathfrak{f}_p) = \sum_{\mathfrak{p}|p} \#V_\mathfrak{p}(\mathfrak{f}_p) + O(p^{\dim V-1}),$$

where the constant just depends on the degree and the dimension of V. By Lemma 14, $\#V_\mathfrak{p}(\mathfrak{f}_p) = O(p^{\dim V-1})$ unless p splits completely over k. If p splits completely over k, $V_\mathfrak{p}$ is an irreducible variety. Thus, by Lang-Weil [LW54], we have that

$$\#V_\mathfrak{p}(\mathfrak{f}_p) = p^{\dim V} + O(p^{\dim V-\frac{1}{2}}),$$

where the constant depends on n and the degree and the dimension of V, which completes the proof. □

Corollary 16. *Let V be a closed subset of $\mathbb{A}^n_{\mathbb{Q}}$. Then there are number fields k_i such that*

$$\#V(\mathfrak{f}_p) = \left(\sum_{p \text{ splits completely}/k_i} \deg(k_i) \right) p^{\dim V} + O(p^{\dim V-\frac{1}{2}}),$$

where the constant depends only on n, the geometric degree, and the geometric dimension of V. Moreover $\sum_i \deg k_i$ is at most the number of geometric irreducible components of V.

Proof. This is a direct corollary of Proposition 15 and [FHM94, Lemma 3.1]. □

Corollary 17. *In the above setting, there exists a positive integer M depending only on the degree of $\tilde{f}$ such that one can find number fields k_i where $\sum_i \deg k_i \le M$ and such that for almost all p,*

$$\#V(f)(\mathfrak{f}_p) = \left(\sum_{p \text{ splits completely}/k_i} \deg(k_i) \right) p^{\dim \mathbb{G}-1} + O(p^{\dim \mathbb{G}-\frac{3}{2}}).$$

Proof. This is a consequence of Proposition 13 and Corollary 16. □

Since we assumed that $\mathbb{G}$ is perfect and Zariski connected, we can find a free Zariski dense subgroup of Γ (e.g., see [SV]). So without loss of generality, we can and will assume that Γ is a free group.

Let us also recall that since Γ is finitely generated, it is a subgroup of $\mathrm{SL}_n(\mathbb{Z}_{S_0})$. Its Zariski closure in $(\mathbb{SL}_n)_{\mathbb{Z}_{S_0}}$ is denoted by $\mathcal{G}$. As we said in the introduction, whenever $\mathbb{G}$ is generated by its unipotent subgroups, the closure of Γ in $\prod_{p\notin S_\Gamma}\mathrm{SL}_n(\mathbb{Z}_p)$ is equal to $\prod_{p\notin S_\Gamma}\mathcal{G}(\mathbb{Z}_p)$.

Let $\pi_d:\Gamma\to\mathrm{SL}_n(\mathbb{Z}_{S_{\Gamma,f}}/d\mathbb{Z}_{S_{\Gamma,f}})$ be the homomorphism induced by the quotient (residue) map $\pi_d:\mathbb{Z}_{S_{\Gamma,f}}\to\mathbb{Z}_{S_{\Gamma,f}}/d\mathbb{Z}_{S_{\Gamma,f}}$ for any d which is not a unit in the ring of $S_{\Gamma,f}$-integers. If d is a unit in the ring of $S_{\Gamma,f}$ integers, we set π_d to be the trivial homomorphism. Let $\Gamma(d):=\ker(\pi_d)$. From the definition it is clear that if $\pi_d(\gamma_1)=\pi_d(\gamma_2)$, then $\pi_d(f(\gamma_1))=\pi_d(f(\gamma_2))$.

Lemma 18. *Let $N_f(d)=\#\{\pi_d(\gamma)\ s.t.\ \pi_d(f(\gamma))=0\}$. Then $N_f(d)$ is a multiplicative function for square-free integer numbers d.*

Proof. For any square-free integer d, let $d_{\Gamma,f}=\prod_{p|d,p\notin S_{\Gamma,f}}p$. Note that $\pi_d(\gamma)=\pi_{d_{\Gamma,f}}(\gamma)$ and $\mathbb{Z}_{S_{\Gamma,f}}/d\mathbb{Z}_{S_{\Gamma,f}}$ is isomorphic to $\mathbb{Z}/d_{\Gamma,f}\mathbb{Z}$. Thus $N_f(d)=N_f(d_{\Gamma,f})$.

On the other hand, we know that the closure of Γ in $\prod_{p\notin S_\Gamma}\mathrm{SL}_n(\mathbb{Z}_p)$ is equal to $\prod_{p\notin S_\Gamma}\mathcal{G}(\mathbb{Z}_p)$. Hence

$$\Gamma/\Gamma(d)\simeq\prod_{p|d_\Gamma}\Gamma/\Gamma(p)\simeq\prod_{p|d_\Gamma}\mathcal{G}_p(\mathfrak{f}_p), \tag{4}$$

where $d_\Gamma=\prod_{p|d,p\notin S_\Gamma}p$. Therefore $N_f(d)=\prod_{p|d_{\Gamma,f}}\#V(f)(\mathfrak{f}_p)$. □

In order to prove Theorem 5, we use the combinatorial sieve formulated in [BGS10]. However we need to adjust some of the definitions before we proceed as we are working with rational numbers instead of integers. Let $f_\Gamma:\Gamma\to\mathbb{Z}^+$ be the map

$$f_\Gamma(\gamma):=\prod_{p\notin S_{\Gamma,f}}|f(\gamma)|_p^{-1}=|f(\gamma)|\prod_{p\in S_{\Gamma,f}}|f(\gamma)|_p,$$

where $|\cdot|$ is the usual absolute value and $|\cdot|_p$ is the p-adic norm. Note that $f_\Gamma(\gamma)\mathbb{Z}_{S_{\Gamma,f}}=f(\gamma)\mathbb{Z}_{S_{\Gamma,f}}$. In particular, $\pi_d(f(\gamma))=0$ if and only if $\pi_d(f_\Gamma(\gamma))=0$.

Let Γ be freely generated by Ω, let $d_{\Omega^{\pm1}}(\cdot,\cdot)=d(\cdot,\cdot)$ be the relative word metric, let $l(\gamma)=d(I,\gamma)$, and let

$$a_n(L)=\#\{\gamma\in\Gamma|\ l(\gamma)\le L, f_\Gamma(\gamma)=n\}.$$

Let $\|\gamma\|_{S_{\Gamma,f}}=\max\{\|\gamma\|,\|\gamma\|_p|\ p\in S_{\Gamma,f}\}$, where $\|\gamma\|$ (resp. $\|\gamma\|_p$) is the operator norm of γ on $\mathbb{R}^n$ (resp. $\mathbb{Q}_p^n$). It is clear that, if $l(\gamma)\le L$, then $\|\gamma\|_{S_{\Gamma,f}}$ is at most C^L, where $C=\max\{\|\gamma\|_{S_{\Gamma,f}}|\ \gamma\in\Omega\}$. Hence

$$f_\Gamma(\gamma)\le C_f\cdot C^{\deg\tilde{f}(\#S_{\Gamma,f}+1)\cdot L}, \tag{5}$$

if $l(\gamma)\le L$. We also observe that if $a_n(L)\neq0$, then n has no prime factor in $S_{\Gamma,f}$.

Following the same computation as in [BGS10, pp. 576–579] and using the main result of Salehi Golsefidy and Varjú [SV] yield that, for any square-free d,

$$\sum_{d|n}a_n(L)=\beta(d)X+r(d,\{a_i\}), \tag{6}$$

where $X = \sum_n a_n(L)$, $|r(d, \{a_i\})| \ll N_f(d) X^\tau$, $\tau < 1$, is independent of the choice of the regular function f, and, if d has no prime factor in $S_{\Gamma,f}$, then

$$\beta(d) = \frac{N_f(d)}{\#\Gamma/\Gamma(d)}. \tag{7}$$

If d has a prime factor in $S_{\Gamma,f}$, then $\beta(d) = 0$.

Lemma 19. *In the above setting, β is multiplicative on the square-free numbers d. Moreover there exists c_1 a positive real number (which may also depend on f) such that $\beta(p) \leq 1 - \frac{1}{c_1}$.*

Proof. By (4) and (7) and the proof of Lemma 18, we have that

$$\beta(d) = \prod_{p|d} \frac{\#V(f)(\mathfrak{f}_p)}{\#\mathcal{G}_p(\mathfrak{f}_p)}$$

if d does not have a prime factor in $S_{\Gamma,f}$ and $\beta(d) = 0$ if d has a prime factor in $S_{\Gamma,f}$. Hence β is a multiplicative function for square-free integers and, for almost all p, by Corollary 17, we have that $\beta(p) \leq M/p$, where M just depends on the degree of $\tilde{f}$. We also notice that $\beta(p) < 1$ for any p, from which the lemma follows. □

Lemma 20. *In the above setting, for any positive integer number D and any positive number ε, we have*

$$\sum_{d \leq D} |r(d, \{a_i\})| \ll X^\tau D^{\dim \mathbb{G} + \varepsilon},$$

where the constant only depends on ε and the degree of $\tilde{f}$.

Proof. By the above discussion, we know that $|r(d, \{a_i\})| \ll N_f(d) X^\tau$. On the other hand,

$$N_f(d) = \prod_{p|d_{\Gamma,f}} N_f(p) \leq \prod_{p|d_{\Gamma,f}} C p^{\dim \mathbb{G} - 1},$$

where C only depends on the degree of $\tilde{f}$. Thus

$$N_f(d) \leq C' d^{\dim \mathbb{G} - 1 + \varepsilon},$$

where C' only depends on ε and the degree of $\tilde{f}$. Hence

$$\sum_{d \leq D} |r(d, \{a_i\})| \ll X^\tau D^{\dim \mathbb{G} + \varepsilon},$$

as we wished. □

Lemma 21. *In the above setting, there are constants T, c_f, and t_f such that:*

1. *T depends on the degree of $\tilde{f}$.*
2. *$t_f \leq T$.*
3. *$|\sum_{w \leq p \leq z} \beta(p) \log p - t_f \log \frac{z}{w}| \leq c_f$, for $\max S_{\Gamma,f} = p_0 < w \leq z$.*

Proof. By (7) and Corollary 17,

$$\begin{aligned} \sum_{p_0 \leq p \leq z} \beta(p) \log p = & \sum_{p_0 \leq p \leq z} \Big(\sum_{p \text{ splits completely}/k_i} \deg(k_i) \Big) \frac{\log p}{p} + O(1) \\ = & \sum_i \deg(k_i) \sum_{p_0 \leq p \leq z \,\&\, p \text{ splits completely}/k_i} \frac{\log p}{p} + O(1). \end{aligned}$$

where the constant and the k_i's depend on f and $\sum_i \deg(k_i)$ has an upper bound which only depends on $\deg \tilde{f}$. By Chebotarev's density theorem, we have

$$\sum_{p_0 \le p \le z \,\&\, \text{ splits completely}/k_i} \frac{\log p}{p} = \frac{1}{\deg k_i} \log z + O(1).$$

Hence

$$\sum_{p_0 \le p \le z} \beta(p) \log p = \sum_i \log z + O(1) = t_f \log z + O(1),$$

where $t_f \le T$ for some T which depends only on the degree of $\tilde{f}$. Note that the implied constants might depend on f but they do not depend on w and z. □

Proposition 22. *In the above setting, there is a positive number T depending on the degree of $\tilde{f}$ such that for $z = X^{(1-\tau)/9T(\dim \mathbb{G}+1)}$ and large enough L we have*

$$\frac{X}{(\log X)^{t_f}} \ll \sum_{\Pi(n) \cap [1,z] = \varnothing} a_n(L) \ll \frac{X}{(\log X)^{t_f}},$$

where $t_f \le T$ and the implied constants depend on f and Γ.

Proof. This is a direct consequence of the formulation of the statement of combinatorial sieve recounted in [BGS10], Lemma 19, Lemma 20, and Lemma 21. □

Corollary 23. *In the above setting, there are constants r and T such that:*

1. *r only depends on $\deg \tilde{f}$, $\#S_{\Gamma,f}$, and Γ.*
2. *T only depends on $\deg \tilde{f}$.*
3. *For large enough L (depending on f), we have*

$$\frac{X}{(\log X)^T} \ll \#\{\gamma \in \Gamma |\ l(\gamma) \le L,\ f_\Gamma(\gamma) \text{ has at most } r \text{ prime factors}\}.$$

Proof. If γ contributes to the sum in Proposition 22, then any prime factor of $f_\Gamma(\gamma)$ is larger than $X^{(1-\tau)/9T(\dim \mathbb{G}+1)}$. On the other hand, by (5), we have that $f_\Gamma(\gamma) \le C_f \cdot C^{\deg \tilde{f}(\#S_{\Gamma,f}+1)\cdot L}$. Thus the number of such factors is at most

$$\frac{9T(\log C_f + L(\#S_{\Gamma,f}+1)\deg \tilde{f} \cdot \log M_0)(\dim \mathbb{G}+1)}{(1-\tau)(L+1)\log \#\Omega}.$$

So, for large enough L, the number of prime factors is at most

$$r = \left\lfloor \frac{9(\#S_{\Gamma,f}+1)\deg \tilde{f} \cdot T \cdot (\dim \mathbb{G}+1) \cdot \log M_0}{(1-\tau)\log \#\Omega} \right\rfloor + 1.$$

□

Proof of Theorem 5. This is now a direct consequence of [BGS10, Proposition 3.2] and Corollary 23. □

4. The perfect case. II

In this section, we prove Theorem 6. We assume that the Zariski closure of Γ is perfect and Zariski connected.

Lemma 24. *It is enough to prove Theorem* 6 *when the semisimple part of $\mathbb{G}$ is simply connected.*

Proof. Since $\mathbb{G}$ is equal to its commutator subgroup, its Levi component is semisimple and, as it is also Zariski connected, $\mathbb{G} \simeq \mathbb{G}_{ss} \ltimes R_u(\mathbb{G})$ as $\mathbb{Q}$-groups (see [M55] or [PR94, Theorem 2.3]). Let $\tilde{\mathbb{G}}_{ss}$ be the simply connected covering of $\mathbb{G}_{ss}$ and let $\tilde{\mathbb{G}} = \tilde{\mathbb{G}}_{ss} \ltimes R_u(\mathbb{G})$. Thus we have the short exact sequence

$$1 \to \mu \to \tilde{\mathbb{G}} \xrightarrow{\iota} \mathbb{G} \to 1,$$

where μ is the center of $\tilde{\mathbb{G}}$. Let $\tilde{\Gamma} = \iota^{-1}(\Gamma)$ and $\Lambda = \tilde{\Gamma} \cap \tilde{\mathbb{G}}(\mathbb{Q})$. One has the long exact sequence

$$\mu(\mathbb{Q}) \to \tilde{\mathbb{G}}(\mathbb{Q}) \xrightarrow{\iota} \mathbb{G}(\mathbb{Q}) \to H^1(\mathbb{Q}, \mu).$$

Thus $\Gamma/\iota(\Lambda)$ is a finitely generated, torsion, abelian group, and so it is finite. As μ is also finite, $\tilde{\Gamma}/\Lambda$ is also finite. Therefore Λ and $\iota(\Lambda)$ are Zariski dense in $\tilde{\mathbb{G}}$ and $\mathbb{G}$, respectively, as $\tilde{\mathbb{G}}$ and $\mathbb{G}$ are Zariski connected. Moreover Λ is finitely generated as Γ is finitely generated and $\Gamma/\iota(\Lambda)$ and μ are finite.

Now let us take a $\mathbb{Q}$-embedding of $\tilde{\mathbb{G}}$ in $\mathbb{SL}_{N'}$ for some N'. It is clear that we can find a finite set $\tilde{S}$ of primes such that:

(1) $\Lambda \subseteq \mathrm{SL}_{N'}(\mathbb{Z}_{\tilde{S}})$ and $\Gamma \subseteq \mathrm{SL}_N(\mathbb{Z}_{\tilde{S}})$.
(2) ι can be extended to a map from $\tilde{\mathcal{G}}$ to $\mathcal{G} \times \mathrm{Spec}(\mathbb{Z}_{\tilde{S}})$, where $\tilde{\mathcal{G}}$ is the Zariski closure of Λ in $(\mathbb{SL}_{N'})_{\mathbb{Z}_{\tilde{S}}}$.

Let $f_i^* \in \mathbb{Q}[\tilde{\mathbb{G}}]$ be the pull back of f_i. Then the f_i^*'s are $\mathbb{Q}$-linearly independent. So if Theorem 6 holds for $\tilde{\mathbb{G}}$, then there are r and S such that $\Lambda_{r,S}(f^*_{\mathbf{v},1})$ is Zariski dense for any $\mathbf{v} \in \mathbb{Z}^m_*$. By the definition, this means that $\iota(\Lambda)_{r,S}(f_{\mathbf{v},1})$ is Zariski dense. By the above discussion, we have that $\Gamma_{r,S}(f_{\mathbf{v},1})$ is Zariski dense for any $\mathbf{v} \in \mathbb{Z}^m_*$.

We are assuming that $f \in \mathbb{Z}_S[\mathcal{G}]$ is not constant and that $\iota(\Lambda)_{r,S}(f)$ is Zariski dense for a positive integer r. We would like to show that after enlarging S, if necessary, we have that $\iota(\Lambda)_{r,S}(L_g(f))$ is also Zariski dense for any $g \in \mathcal{G}(\mathbb{Z}_{S'})$. Without loss of generality, let us assume that S contains both S' and $\tilde{S}$. Now let $f_g^* \in \mathbb{Z}_S[\tilde{\mathcal{G}}]$ be the pull back of $L_g(f)$. By a similar argument to the above, it is enough to show that after enlarging S we have that $\Lambda_{r,S}(f_g^*)$ is Zariski dense in $\tilde{\mathbb{G}}$ for any g. To see this, it is enough, by Theorem 5, to get a uniform bound on the degree of lifts of f_g^* and a uniform upper bound for their sets of ramified primes. The claim on the degree of these functions is clear. Now let p be a ramified prime of f_g^*. This means that for any $\lambda \in \Lambda$ we have that $f_g^*(\lambda) \in p\mathbb{Z}_S$. Hence $\pi_p(f(g^{-1}\iota(\lambda))) = 0$. Thus by [N87] we have that a coset of $\iota(\tilde{\mathcal{G}}_p(\mathfrak{f}_p))$ is a subset of $V(f)(\mathfrak{f}_p)$. This implies that

$$\#V(f)(\mathfrak{f}_p) \gg p^{\dim \mathbb{G}}, \tag{8}$$

where the implied constant just depends on $\mathbb{G}$. By Corollary 17, (8) cannot hold for large enough p unless it is a ramified prime of f. This completes the proof of Lemma 24. □

For the rest of this section, by Lemma 24, we can and will assume that the semisimple part of $\mathbb{G}$ is simply connected. Let us continue with a few elementary lemmas in commutative algebra.

Lemma 25. *Let A be a finitely generated integral domain of characteristic zero. Then there exists a finite set S of primes such that $A_S = A \otimes_{\mathbb{Z}} \mathbb{Z}_S$ is a free $\mathbb{Z}_S$-module. Moreover there are $\mathbb{Q}$-algebraically independent elements $x_1, \dots, x_d$ in A, such that A_S is a finitely generated $\mathbb{Z}_S[x_1, \dots, x_d]$-module.*

Proof. By the assumptions, $A_{\mathbb{Q}}$ is a finitely generated $\mathbb{Q}$-integral domain. By the Nöether normalization lemma, $A_{\mathbb{Q}}$ is an integral, and so a finite extension of a polynomial algebra $B_{\mathbb{Q}} = \mathbb{Q}[x_1, \dots, x_d]$. One can easily find a finite set of prime numbers S, such that A_S is a finite extension of $B_S = \mathbb{Z}_S[x_1, \dots, x_d]$, i.e., it is a finitely generated B_S-module. Let L (K, resp.) be the field of fractions of A_S (B_S, resp.). Since B_S is integrally closed and L/K is a separable extension, there exists $\{v_1, \dots, v_n\}$ a K-basis of L such that

$$A_S \subseteq B_S v_1 \oplus B_S v_2 \oplus \cdots \oplus B_S v_n$$

(see [AM69, Proposition 5.17]). Hence A_S is a $\mathbb{Z}_S$-submodule of a free module, and so it is a free $\mathbb{Z}_S$-module. □

Corollary 26. *Let A be as above. If $a_1, \dots, a_m$ are $\mathbb{Q}$-linearly independent elements of A, then there is a finite set S of primes such that the $a_i \pmod p$ are linearly independent over $\mathfrak{f}_p$, for any $p \in \Pi \setminus S$.*

Proof. This is a direct consequence of Lemma 25. □

Definition 27. For any $P(T) = \sum_i c_i T^i$ in the ring of polynomials with coefficients in $\mathbb{Q}[x_1, \dots, x_d]$, we define the height of P to be

$$H(P) = \max_i \{\deg c_i\}.$$

Lemma 28. *Let A_S be a finitely generated $\mathbb{Z}_S$-integral domain which is a finite extension of a polynomial ring $B_S = \mathbb{Z}_S[x_1, \dots, x_d]$. If $a_1, \dots, a_m$ are $\mathbb{Q}$-linearly independent elements of A, then there exists $D > 0$, depending on the a_i's, such that any integer combination of the a_i's satisfies a monic polynomial over B_S whose height is* at most *D.*

Proof. We prove the lemma for $m = 2$ and the general case can be deduced by induction. Let P_α and P_β be monic polynomials with coefficients in B_S which are satisfied by $\alpha = a_1$ and $\beta = a_2$, respectively. It is clear that, for any integer n, there is a monic polynomial $\mathcal{Q}(T) \in B_S[T]$ such that $\mathcal{Q}(nT) = n^{\deg P_\alpha} P_\alpha(T)$. In particular, $n\alpha$ satisfies a monic polynomial in $B_S[T]$ with height at most equal to $H(P_\alpha)$ and degree at most $\deg(P_\alpha)$. Thus it is enough to show that $\alpha + \beta$ satisfies a monic polynomial over B_S whose height is bounded by a function of $H(P_\alpha)$, $H(P_\beta)$, $\deg(P_\alpha)$, and $\deg(P_\beta)$.

Let $x - \alpha^{(1)}, \dots, x - \alpha^{(n_1)}$ and $x - \beta^{(1)}, \dots, x - \beta^{(n_2)}$ be the linear factors of $P_\alpha(x)$ and $P_\beta(x)$, respectively, in an extension of the field of fractions of A. So $\alpha + \beta$ satisfies

$$P_{\alpha+\beta}(x) = \prod_{i=1}^{n_1} \prod_{j=1}^{n_2} (x - \alpha^{(i)} - \beta^{(j)}).$$

On the other hand, consider the $n_1 + n_2 + 1$ variable polynomial

$$P(T, \alpha_1, \dots, \alpha_{n_1}, \beta_1, \dots, \beta_{n_2}) = \prod_{i=1}^{n_1} \prod_{j=1}^{n_2} (T - \alpha_i - \beta_j).$$

Since P is invariant under any permutation of the α_i's, there are linearly independent symmetric polynomials $\mathcal{S}_n$ in the α_i's and polynomials $\mathcal{Q}_n$ in T and the β_j's such that

$$P(T,\alpha_i,\beta_j)=\sum_n \mathcal{Q}_n(T,\beta_j)\mathcal{S}_n(\alpha_i) \quad \text{and} \quad \deg \mathcal{Q}_n+\deg \mathcal{S}_n\le n_1n_2.$$

As P is also invariant under any permutation of the β_j's, we have

$$P(T,\alpha_i,\beta_j)=\sum_{n,l} \mathcal{S}_n(\alpha_i)\mathcal{S}'_{nl}(\beta_j)\mathcal{Q}_{nl}(T) \quad \text{and} \quad \deg \mathcal{S}_k+\deg \mathcal{S}'_{nl}\le n_1n_2,$$

where the $\mathcal{S}'_{nl}$'s are symmetric polynomials in the β_j's. Thus

$$P_{\alpha+\beta}(x)=\sum_{n,l} \mathcal{S}_n(\alpha^{(i)})\mathcal{S}'_{nl}(\beta^{(j)})\mathcal{Q}_{nl}(x).$$

Moreover $\mathcal{S}_n(\alpha^{(i)}),\mathcal{S}'_{nl}(\beta^{(j)})\in\mathbb{Z}[x_1,\dots,x_d]$ and

$$\deg(\mathcal{S}_n(\alpha^{(i)})\mathcal{S}'_{nl}(\beta^{(j)}))\le D=D(H(P_\alpha),H(P_\beta),\deg(P_\alpha),\deg(P_\beta)),$$

which finishes the proof. □

Proposition 29. *Let $\mathbb{G}=\mathrm{Zcl}(\Gamma)$ be a Zariski connected perfect group such that its semisimple factor is simply connected. Let $f\in\mathbb{Q}[\mathbb{G}]$ be a non-zero function and let S' be a finite set of primes. Then there is a finite set S of primes such that*

$$\bigcup_{g\in\mathcal{G}(\mathbb{Z}_{S'})}\ \bigcup_{\mathbf{v}\in\mathbb{Z}_*^m} S_{\Gamma,f_{\mathbf{v},g}}\subseteq S.$$

Proof. Since $\mathbb{G}_{ss}$ is simply connected, by Nori's theorem [N87], the closure of Γ in $\prod_{p\in\Pi\setminus S_\Gamma}\mathrm{SL}_N(\mathbb{Z}_p)$ is equal to $\prod_{p\in\Pi\setminus S_\Gamma}\mathcal{G}(\mathbb{Z}_p)$. In particular, $\#\pi_p(\Gamma)=\#\mathcal{G}_p(\mathfrak{f}_p)=p^d+O(p^{d-\frac{1}{2}})$, for any $p\in\Pi\setminus S_\Gamma$, where $d=\dim\mathbb{G}$.

We also note that by a similar argument to that in Lemma 24, a large enough p is a ramified prime of $f_{\mathbf{v},g}$ if and only if it is a ramified prime of $f_{\mathbf{v},1}$. So it is enough to prove the proposition only for the $f_{\mathbf{v}}=f_{\mathbf{v},1}$'s.

On the other hand, by Corollary 26, there is a finite set S_1 of primes such that the f_i's modulo p are linearly independent over $\mathfrak{f}_p$. Also, by Lemma 25, there is a finite set S_2 of primes such that $\mathbb{Z}_{S_2}[\mathcal{G}]$ is a finite extension of a polynomial ring over $\mathbb{Z}_{S_3}$. Let $p\in S_{\Gamma,\sum_{i=1}^m v_if_i}\setminus(S_\Gamma\cup S_1\cup S_2)$, where $\mathbf{v}\in\mathbb{Z}_*^m$. It follows that $\phi(\sum_{i=1}^m v_if_i)=0$, for any homomorphism $\phi:\mathbb{Z}[\mathcal{G}]\to\mathfrak{f}_p$. Any such homomorphism can be extended to a homomorphism from $\mathbb{Z}[\mathcal{G}]\otimes\mathbb{Z}_{S_3}$ to $\mathfrak{f}_p$. Let $A=\mathbb{Z}[\mathcal{G}]$. Then we have that A_{S_3} is a finite extension of $B_{S_3}=\mathbb{Z}_{S_3}[x_1,\dots,x_d]$. Hence there is a positive number D_1 (independent of $\mathbf{v}$) such that at most D_1 homomorphisms $\phi:A_{S_3}\to\mathfrak{f}_p$ have the same restriction on B_{S_3}. In particular,

$$\#\{\phi':B_{S_3}\to\mathfrak{f}_p:\ \exists\phi\in\mathrm{Hom}(A_{S_3},\mathfrak{f}_p)\text{ s.t. }\phi'=\phi|_{B_{S_3}}\}\ge\frac{1}{2D_1}p^d. \tag{9}$$

On the other hand, by Lemma 28, there is a positive number D_2 depending only on the f_i's such that $f_{\mathbf{v}}=\sum_i v_if_i$ satisfies an equation of degree at most D_2

$$\sum_i c_i^{(\mathbf{v})}f_{\mathbf{v}}^i=0, \tag{10}$$

where $c_i^{(\mathbf{v})} \in B_{S_3}$ and $\deg c_i^{(\mathbf{v})} \le D_2$. Thus, for any $\phi \in \mathrm{Hom}(A_{S_3}, \mathfrak{f}_p)$, we have $\phi(f_{\mathbf{v}}) = 0$ as p is in $S_{\Gamma,f_{\mathbf{v}}} \setminus (S_1 \cup S_2 \cup S_\Gamma)$. Hence, by (10), $\phi(c_i^{(\mathbf{v})}) = 0$ for some i. Therefore, by (9), we have

$$\#V(\prod_i c_i^{(\mathbf{v})})(\mathfrak{f}_p) = \#\{\phi' \in \mathrm{Hom}(B_{S_3}, \mathfrak{f}_p) :\ \phi'(\prod_i c_i^{(\mathbf{v})}) = 0\} \ge \frac{1}{2D_1} p^d. \tag{11}$$

Notice that, since $p \notin S_2$, $f_{\mathbf{v}} (\mathrm{mod}\, p)$ is not zero and neither is $\prod_i c_i^{(\mathbf{v})} (\mathrm{mod}\, p)$. Thus (see [Sc74])

$$\#V(\prod_i c_i^{(\mathbf{v})})(\mathfrak{f}_p) \le \deg(\prod_i c_i^{(\mathbf{v})}) p^{d-1} \le D_2^{D_2} p^{d-1}. \tag{12}$$

Proposition 29 now follows from (11) and (12). □

Lemma 30. *In the above setting, for any $g \in \mathrm{SL}_N(\mathbb{Q})$ and $\mathbf{v} \in \mathbb{Z}^m$,*

$$\deg L_g(\sum_{i=1}^m v_i \tilde{f}_i) \le \max_i \deg \tilde{f}_i.$$

Proof. It is clear. □

Proof of Theorem 6. This is a direct consequence of Theorem 5, Proposition 29, and Lemma 30. □

5. The general case

In this section, we complete the proof of Theorem 3. To do so, first we reduce it to the case of Zariski connected groups and then carefully combine the perfect case with the unipotent case.

Lemma 31. *If Theorem* 3 *holds when $\mathbb{G}$ is a Zariski connected group, then it holds in general.*

Proof. Let $\Gamma^\circ = \Gamma \cap \mathbb{G}^\circ$, where $\mathbb{G}^\circ$ is the connected component of $\mathbb{G}$ containing the identity element. Since Γ is Zariski dense in $\mathbb{G}$, $\mathbb{G}/\mathbb{G}^\circ \simeq \Gamma/\Gamma^\circ$. Let $\{\gamma_i\}$ be a set of coset representatives of $\mathbb{G}^\circ$ in $\mathbb{G}$ chosen from Γ. Hence

$$Z(f) = \bigsqcup \gamma_i(\mathbb{G}^o \cap Z(L_{\gamma_i}(f))).$$

Let $\iota : \mathbb{Q}[\mathbb{G}] \to \mathbb{Q}[\mathbb{G}^\circ]$ be the homomorphism induced by the restriction map. Then by the assumption on the dimension of $Z(f)$, $\iota(L_{\gamma_i}(f))$ are non-zero, and clearly for any choice of finite sets of prime numbers S_i and positive integer numbers r_i,

$$\bigsqcup \gamma_i \Gamma^\circ_{S_i, r_i}(\iota(L_{\gamma_i}(f))) \subseteq \Gamma_{\cup S_i, \max r_i}(f),$$

finishing the proof of the lemma. □

From this point on we will assume that $\mathbb{G}$ is Zariski connected. Thus all of its derived subgroups are also connected. Let us recall that derived subgroups are defined inductively, $\mathbb{G}^{(0)} = \mathbb{G}$, and $\mathbb{G}^{(i+1)} = [\mathbb{G}^{(i)}, \mathbb{G}^{(i)}]$.

Lemma 32. (1) *Let $\mathbb{G}$ be Levi-semisimple. Then $\mathbb{G}^{(i)}$ is also Levi-semisimple, $\mathbb{G}/\mathbb{G}^{(i)}$ is unipotent, and $\mathbb{G}$ is homeomorphic to $\mathbb{G}/\mathbb{G}^{(i)} \times \mathbb{G}^{(i)}$, as a $\mathbb{Q}$-variety. In particular, if $\mathbb{G}$ is solvable and Levi-semisimple, then it is unipotent.*

(2) *$\Gamma^{(i)}$ is Zariski dense in $\mathbb{G}^{(i)}$, for any i.*

Proof. If $\mathbb{G}$ is Levi-semisimple, $\mathbb{G} \simeq \mathbb{G}_{ss} \ltimes R_u(\mathbb{G})$ as $\mathbb{Q}$-groups. Therefore for any i, $\mathbb{G}^{(i)} = \mathbb{G}_{ss} \ltimes \mathbb{U}_i$, for some $\mathbb{Q}$-subgroup $\mathbb{U}_i$ of $R_u(\mathbb{G})$. Using [Sp98, Theorem 14.2.6], $R_u(\mathbb{G})$ is homeomorphic to $R_u(\mathbb{G})/\mathbb{U}_i \times \mathbb{U}_i$, as a $\mathbb{Q}$-variety, and so $\mathbb{G}$ is homeomorphic to $\mathbb{G}/\mathbb{G}^{(i)} \times \mathbb{G}^{(i)}$ as a $\mathbb{Q}$-variety. The other parts are clear. □

Since $\mathbb{G}$ is connected, for some $i \leq \dim \mathbb{G}$, $\mathbb{G}^{(i)} = \mathbb{G}^{(i+1)}$. Let us call

$$\mathbb{H} = \mathbb{G}^{(\dim \mathbb{G})}$$

the perfect core of $\mathbb{G}$. Note that the perfect core might be trivial.

Proof of Theorem 3. By Lemma 32, $\mathbb{Q}[\mathbb{G}] \simeq \mathbb{Q}[\mathbb{H}] \otimes \mathbb{Q}[\mathbb{G}/\mathbb{H}]$ and $\mathbb{U} = \mathbb{G}/\mathbb{H}$ is a unipotent $\mathbb{Q}$-group. Let $\pi : \mathbb{G} \to \mathbb{G}/\mathbb{H}$ be the projection map and let $\phi : \mathbb{G}/\mathbb{H} \to \mathbb{G}$ be a $\mathbb{Q}$-section. Hence $\phi \circ \pi$ is a $\mathbb{Q}$-morphism from $\mathbb{G}$ to itself. Thus there is a finite set S' of primes such that

$$\phi \circ \pi(\Gamma) \subseteq \mathcal{G}(\mathbb{Z}_{S'}).$$

Let $\mathcal{H}$ be the Zariski closure of $\Gamma^{(\mathbb{H})} = \Gamma \cap \mathbb{H}$ in $(\mathbb{SL}_N)_{\mathbb{Z}_{S_0}}$. By Lemma 25, we can find a finite set S of primes and a $\mathbb{Z}_S$-basis of $\mathbb{Z}_{S_0}[\mathcal{H}] \otimes \mathbb{Z}_S$. So f is mapped to $\sum_{i=1}^m Q_i \otimes a_i$ for some $Q_i \in \mathbb{Q}[\mathbb{U}]$, which means that for any $g \in \mathbb{G}$ we have

$$f(g) = \sum_{i=1}^m Q_i(\pi(g)) a_i(\phi(\pi(g))^{-1} g) = \sum_{i=1}^m Q_i(\pi(g)) L_{\phi(\pi(g))}(a_i)(g).$$

Let $P = \gcd_i(Q_i)$ and $P_i = Q_i/P$. Applying Theorem 4 to $\pi(\Gamma)$, P, and the P_i's, we can find a positive integer r, a finite set S'' of prime numbers, and a Zariski dense subset X of $\pi(\Gamma)$ such that:

(1) $P(u)$ has at most r prime factors in the ring of S'-integers, for any $u \in X$.
(2) $\Pi(\gcd(P_1(u), \dots, P_m(u))) \subseteq S'$, for any $u \in X$.

By the definition, any $u \in X$ is equal to $\pi(\gamma_u)$ for some $\gamma_u \in \Gamma$. We can identify $\mathbb{G}$ with $\mathbb{U} \times \mathbb{H}$ as $\mathbb{Q}$-varieties via

$$(u, h) \mapsto \phi(u)h \qquad \text{and} \qquad g \mapsto (\pi(g), \phi(\pi(g))^{-1} g).$$

For any $u \in X$ and $\gamma_{\mathbb{H}} \in \Gamma^{(\mathbb{H})}$, we have that

$$\gamma_u \gamma_{\mathbb{H}} \mapsto (u, \phi(u)^{-1} \gamma_u \gamma_{\mathbb{H}}) \tag{13}$$

and

$$f(\gamma_u \gamma_{\mathbb{H}}) = \sum_{i=1}^m Q_i(u) L_{\gamma_u^{-1}\phi(u)}(a_i)(\gamma_{\mathbb{H}}). \tag{14}$$

On the other hand, by the above properties and Theorem 6, there are a positive integer r' and a finite set S''' of prime numbers such that, for any $u \in X$,

$$Y_u = \Gamma^{(\mathbb{H})}_{r',S'''} \left(P(u) \sum_{i=1}^m P_i(u) L_{\gamma_u^{-1}\phi(u)}(a_i) \right) = \Gamma^{(\mathbb{H})}_{r',S'''} \left(\sum_{i=1}^m Q_i(u) L_{\gamma_u^{-1}\phi(u)}(a_i) \right)$$

is Zariski dense in $\mathbb{H}$. Therefore $\phi(u)^{-1}\gamma_u Y_u$ is also Zariski dense in $\mathbb{H}$, for any $u \in X$, as $\gamma_u^{-1}\phi(u) \in \mathbb{H}$. Thus

$$\tilde{X} = \bigsqcup_{u \in X} \{u\} \times \phi(u)^{-1} \gamma_u Y_u$$

is Zariski dense in $\mathbb{U} \times \mathbb{H}$, and, by (13) and (14), we are done. □

6. Effectiveness of our arguments

In order to avoid adding unnecessary complications, we did not discuss the effectiveness of our argument in the course of the paper. In this section, we address four issues from which one can easily verify that our arguments are effective.

(1) Let Γ be the group generated by a finite subset S of $\mathrm{GL}_n(\mathbb{Q})$. Let $\mathbb{G}$ be the Zariski closure of Γ and assume that $\mathbb{G}$ is Zariski connected. Then in the course of our arguments (e.g., proof of Proposition 13), we need to be able to compute a presentation for $\mathbb{G}$, i.e., compute a finite subset F of $\mathbb{Q}[\mathbb{GL}_n]$ such that $\mathbb{Q}[\mathbb{G}] \simeq \mathbb{Q}[\mathbb{GL}_n]/\langle F\rangle$.

(2) Computing the irreducible components of a given affine variety and an effective version of the Nöether-Bertini theorem is needed in the proof of Proposition 15.

(3) We need to compute the spectral gap of the discrete Laplacian on the Cayley graphs of $\pi_q(\Gamma)$ with respect to $\pi_q(\Omega)$, where Ω is a symmetric finite generating set of Γ, if the connected component of the Zariski closure of Γ is perfect.

(4) An effective version of Nori's strong approximation theorem is needed in various parts of this article, e.g., in understanding the density of the sieve. We need a more or less equivalent formulation. To be precise, we need to say that $\pi_q(\Gamma) = \prod_{p|q} \mathbb{G}(\mathfrak{f}_p)$ if Γ is a Zariski dense subgroup of $\mathbb{G}$ and $\mathbb{G}$ is generated by its $\mathbb{Q}$-unipotent subgroups.

The first three items are dealt with in [SV]. [SV, Lemma 62] gives us the first item. In order to get the second item, first we use [BW93, Chapter 8.5] to compute the primary decomposition of the defining ideal of the variety, which gives us the irreducible components. Then we use [SV, Theorem 40] to get an effective version of the Nöether-Bertini theorem. In fact, [SV, Theorem 40] proves an effective version of [G69, Theorem 9.7.7(i) and Theorem 12.2.4(iii)] which is a generalization of the Nöether-Bertini theorem. The third item is the main result of [SV] and the authors of [SV] also show that their result is effective.

Let Γ be the group generated by a finite subset Ω of $\mathrm{SL}_n(\mathbb{Z}_{S_0})$. Let $\mathcal{G}$ be the Zariski closure of Γ in $(\mathbb{SL}_n)_{\mathbb{Z}_{S_0}}$ and let $\mathcal{G}_p = \mathcal{G} \times \mathrm{Spec}(\mathfrak{f}_p)$.

Theorem 33 (Effective version of Theorem 5.4 in [N87])**.** *In the above setting, assume that the generic fiber $\mathbb{G}$ of $\mathcal{G}$ is generated by $\mathbb{Q}$-unipotent subgroups. Then there is a recursively defined function f from finite subsets of $\mathrm{SL}_n(\mathbb{Q})$ to positive integers such that for any square-free integer q with prime factor at least $f(\Omega)$, we have*

$$\pi_q(\Gamma) = \prod_{p|q} \mathcal{G}_p(\mathfrak{f}_p),$$

where $\Gamma = \langle\Omega\rangle$ and p runs through the prime divisors of q.

Remark 34. (1) In [N87], it is said that (the non-effective version of) Theorem 33 can be deduced from [N87, Theorems A, B, and C] and the reader is referred to an unpublished manuscript. As we need the effective version of this result, we decided to write down a proof of this statement.

(2) In the appendix of [SV], the effective versions of [N87, Theorems A, B, and C] are given. Furthermore [SV, Theorem 40] provides an effective version of [N87, Theorem 5.1], when $\mathbb{G}$ is perfect.

Lemma 35. *Let $\{G_i\}_{i\in I}$ be a finite collection of finite groups such that G_i and $G_{i'}$ do not have a (non-trivial) common homomorphic image for $i \neq i'$. Let H be a subgroup of $G = \prod_i G_i$. If the projection $\pi_i(H)$ of H to G_i is onto, i.e., $\pi_i(H) = G_i$, then $H = G$.*

Proof. We proceed by induction on the order of G. Let $H_i = G_i \cap H$. Since $\pi_i(H) = G_i$, H_i is a normal subgroup of G_i. Let $G_i' := G_i/H_i$, $H' := H/\prod_i H_i$, and $G' := \prod_i G_i/H_i$. It is clear that $\pi_i(H') = G_i'$ for any i. If $H_i \neq 1$ for some i, then $|G| > |G'|$. Hence by the induction hypothesis we have that $H' = G'$, which implies that $H = G$ and we are done. So without loss of generality we can assume that

$$H \cap G_i = 1, \tag{15}$$

for any i. For a fixed i_0, let H'_{i_0} be the projection of H to $\prod_{i\neq i_0} G_i$. It is clear that $\pi_i(H'_{i_0}) = G_i$ for any $i \neq i_0$. Hence by the induction hypothesis we have that

$$\pi_{I\setminus\{i_0\}}(H) = \prod_{i\neq i_0} G_i, \tag{16}$$

where $\pi_{I\setminus\{i_0\}}$ is the projection to $\prod_{i\neq i_0} G_i$. By (15) and (16), we have that G_{i_0} is a homomorphic image of $\prod_{i\neq i_0} G_i$. Let N be the normal subgroup of $\prod_{i\neq i_0} G_i$ such that $(\prod_{i\neq i_0} G_i)/N \simeq G_{i_0}$. Then again by the induction hypothesis there is some $i_1 \neq i_0$ such that $\pi_{i_1}(N) \neq G_{i_1}$. Thus G_{i_0} and G_{i_1} have a (non-trivial) common homomorphic image, which is a contradiction. □

Proof of Theorem 33. Let $\mathcal{H} = \mathcal{D}^{(\dim \mathbb{G})}(\mathcal{G})$. Then the generic fiber $\mathbb{H}$ of $\mathcal{H}$ is the perfect core of $\mathbb{G}$ and $\mathcal{D}^{(\dim \mathbb{G})}(\Gamma) \subseteq \Gamma \cap \mathcal{H}(\mathbb{Z}_{S_0})$ is Zariski dense in $\mathcal{H}$. Since $\mathbb{H}$ is Zariski connected, by [SV, Lemma 62], we can find a finitely generated subgroup of $\mathcal{D}^{(\dim \mathbb{G})}(\Gamma)$ which is Zariski dense in $\mathbb{H}$. Hence by [SV, Theorem 40] we can compute p_0 such that for any $p > p_0$ we have

$$\pi_p(\mathcal{D}^{(\dim \mathbb{G})}(\Gamma)) = \mathcal{H}_p(\mathfrak{f}_p), \tag{17}$$

where $\mathcal{H}_p = \mathcal{H} \times_{\mathrm{Spec}(\mathbb{Z}_{S_0})} \mathrm{Spec}(\mathfrak{f}_p)$. On the other hand, $\mathbb{U} = \mathbb{G}/\mathbb{H}$ is a unipotent $\mathbb{Q}$-group and the image $\phi(\Gamma)$ of Γ to $\mathbb{U}$ is a Zariski dense group. We can compute an embedding of $\mathbb{U}$ to $(\mathbb{GL}_m)_{\mathbb{Q}}$ for some m. By enlarging S_0, if necessary, we can compute the Zariski closure $\mathcal{U}$ of $\pi(\Gamma)$ in $(\mathbb{GL}_m)_{\mathbb{Z}_{S_0}}$ and extend ϕ to a $\mathbb{Z}_{S_0}$-homomorphism from $\mathcal{H}$ to $\mathcal{U}$. Using the logarithmic and exponential maps, we can effectively enlarge p_0, if necessary, to make sure that

$$\pi_p(\phi(\Gamma)) = \mathcal{U}_p(\mathfrak{f}_p), \tag{18}$$

where $\mathcal{U}_p = \mathcal{U} \times_{\mathrm{Spec}(\mathbb{Z}_{S_0})} \mathrm{Spec}(\mathfrak{f}_p)$ and $p > p_0$. Hence by (17) and (18) we have that $\pi_p(\Gamma) = \mathcal{G}_p(\mathfrak{f}_p)$, for any $p > p_0$. By [SV, Lemma 64] we know the composition factors of $\mathcal{G}_p(\mathfrak{f}_p)$. In particular, if p and p' are primes larger than 7, then $\mathcal{G}_p(\mathfrak{f}_p)$ and $\mathcal{G}_{p'}(\mathfrak{f}_{p'})$ do not have a (non-trivial) common homomorphic image. Thus Lemma 35 finishes the proof. □

Appendix A. Heuristics

Finding primes or almost primes in very sparse sequences of integers is notoriously difficult and the most believable speculations are based on probabilistic reasoning. Such an argument for Fermat primes $F_n = 2^{2^n} + 1$ suggest that their number is finite [HW79, p. 15]. Similar arguments have been carried out for other

sequences such as Fibonacci numbers [BLMS05]. Here we pursue such probabilistic heuristics for tori.

Let $\Gamma \subseteq \mathrm{GL}_n(\mathbb{Q})$ be a (finitely generated) torus. That is to say, it is conjugate to a group of diagonal matrices; there is $g \in \mathrm{GL}_n(K)$, K a number field, such that

$$g^{-1}\Gamma g \subseteq \mathbb{D}(K) = \{\mathrm{diag}(a_1, \dots, a_n) |\ a_i \in K^\times\}, \tag{19}$$

where

$$\mathrm{diag}(a_1, \dots, a_n) = \begin{bmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{bmatrix}.$$

The heuristics will show that there is an $f \in \mathbb{Q}[\mathbb{A}^{n^2}]$ for which not only does (Γ, f) not saturate, but $\Gamma_{r,S}(f)$ is finite for every r and S. To this end, we can assume that $g^{-1}\Gamma g$ is a subgroup of the S-units of K for some finite set of places (with $\varepsilon \to \mathrm{diag}(\sigma_1(\varepsilon), \dots, \sigma_n(\varepsilon))$ and the σ_i's the embeddings of K). For simplicity we assume that S is empty and since the torsion is finite, we can ignore it for our purposes. That is, Γ is a free abelian group of rank $t \geq 1$ with generators $\gamma_1, \dots, \gamma_t$ and $\Gamma \subseteq \mathrm{GL}_n(\mathbb{Z})$. For $x \in \mathrm{GL}_n(\mathbb{Q})$ let $F(x) = \mathrm{Tr}(x^t x) \in \mathbb{Q}[\mathbb{A}^{n^2}]$ be its Hilbert-Schmidt norm. It is clear from the discreteness property of the log of unit maps and (19) that for $\mathbf{m} = (m_1, \dots, m_t)$ in $\mathbb{Z}^t$

$$A_2^{|\mathbf{m}|} \ll F(\gamma_1^{m_1} \cdots \gamma_t^{m_t}) \ll A_1^{|\mathbf{m}|}, \tag{20}$$

where $A_1 > A_2 > 1$ and the implied constants are independent of $\mathbf{m}$. Fix $\nu > t$ and set

$$f(x) := f_1(x) f_2(x) \cdots f_\nu(x), \tag{21}$$

where

$$f_j(x) = F(x) + j, \qquad j = 1, 2, \dots, \nu.$$

The heuristic argument is that for each $m \in \mathbb{Z}^t$, $F(\gamma_1^{m_1} \cdots \gamma_t^{m_t})$ is a "random" integer in the range (20) and that the $f_j(x)$ for $j = 1, 2, \dots, \nu$ are independent as far as the number of their prime factors. Actually there may be some small forced prime factors of f but these will only enhance the reasoning below. Now let r be a large integer and for $\mathbf{m} \in \mathbb{Z}^t$ let $p(\mathbf{m}, r)$ be the probability that an integer in the range (20) has at most r-prime factors. According to the prime number theorem

$$p(\mathbf{m}, r) \ll \frac{[\log(|\mathbf{m}| + 1)]^{r-1}}{|\mathbf{m}| + 1} \tag{22}$$

(again the implied constants being independent of $\mathbf{m}$).

Hence assuming that the number of prime factors of the f_j, $j = 1, \dots, \nu$, are independent and that these values are "random", we see that $p_f(\mathbf{m}, r)$, the probability that $f(\gamma_1^{m_1} \cdots \gamma_t^{m_t})$ has at most r-prime factors, satisfies

$$p_f(\mathbf{m}, r) \ll \frac{[\log(|\mathbf{m}| + 1)]^{\nu(r-1)}}{(|\mathbf{m}| + 1)^\nu}. \tag{23}$$

Hence since $\nu > t$,

$$\sum_{\mathbf{m} \in \mathbb{Z}^t} p_f(\mathbf{m}, r) < \infty. \tag{24}$$

By the Borel-Cantelli lemma it follows that the probability that there are infinitely many $\mathbf{m}$'s for which $f(\gamma_1^{m_1} \dots \gamma_t^{m_t})$ has at most r-prime factors is zero. That is, for any r we should expect that $\Gamma_r(f)$ is finite!

For a general $\Gamma \subseteq \mathrm{GL}_n(\mathbb{Z})$ (or finitely generated in $\mathrm{GL}_n(\mathbb{Q})$) if $\mathbb{G} = \mathrm{Zcl}(\Gamma)$ is not Levi-semisimple, then there is an onto $\mathbb{Q}$-homomorphism $\phi : \mathbb{G}^\circ \to \mathbb{T}$, where $\mathbb{T}$ is a non-trivial $\mathbb{Q}$-torus. Hence $\Lambda = \phi(\Gamma)$ is a finitely generated subgroup of $\mathbb{T}(\mathbb{Q})$. Thus one can use the heuristics above to show there is an $f \in \mathbb{Q}[\mathbb{T}]$ such that $\Lambda_r(f)$ is finite for any r. In particular, as in the proof of Theorem 3, $\Gamma_r(f)$ cannot be Zariski dense in $\mathbb{G}$ for any r. The conclusion is that if we accept the probabilistic heuristics, then the condition that $\mathbb{G}$ be Levi-semisimple in Theorem 1 is necessary if we allow all f's.

References

[AM69] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969. MR0242802 (39 #4129)

[BW93] Thomas Becker and Volker Weispfenning, *Gröbner bases*, Graduate Texts in Mathematics, vol. 141, Springer-Verlag, New York, 1993. A computational approach to commutative algebra; In cooperation with Heinz Kredel. MR1213453 (95e:13018)

[BG08] Jean Bourgain and Alex Gamburd, *Uniform expansion bounds for Cayley graphs of* $\mathrm{SL}_2(\mathbb{F}_p)$, Ann. of Math. (2) **167** (2008), no. 2, 625–642, DOI 10.4007/annals.2008.167.625. MR2415383 (2010b:20070)

[BGS10] Jean Bourgain, Alex Gamburd, and Peter Sarnak, *Affine linear sieve, expanders, and sum-product*, Invent. Math. **179** (2010), no. 3, 559–644, DOI 10.1007/s00222-009-0225-3. MR2587341 (2011d:11018)

[BGT11] Emmanuel Breuillard, Ben Green, and Terence Tao, *Approximate subgroups of linear groups*, Geom. Funct. Anal. **21** (2011), no. 4, 774–819, DOI 10.1007/s00039-011-0122-y. MR2827010

[BLMS05] Yann Bugeaud, Florian Luca, Maurice Mignotte, and Samir Siksek, *On Fibonacci numbers with few prime divisors*, Proc. Japan Acad. Ser. A Math. Sci. **81** (2005), no. 2, 17–20. MR2126070 (2005k:11020)

[Ch73] Jing Run Chen, *On the representation of a larger even integer as the sum of a prime and the product of at most two primes*, Sci. Sinica **16** (1973), 157–176. MR0434997 (55 #7959)

[FHM94] Michael D. Fried, Dan Haran, and Moshe Jarden, *Effective counting of the points of definable sets over finite fields*, Israel J. Math. **85** (1994), no. 1-3, 103–133, DOI 10.1007/BF02758639. MR1264342 (95k:12016)

[G69] A. Grothendieck, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III*, Inst. Hautes Études Sci. Publ. Math. **28** (1966), 255. MR0217086 (36 #178)

[HR74] H. Halberstam and H.-E. Richert, *Sieve methods*, Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London-New York, 1974. London Mathematical Society Monographs, No. 4. MR0424730 (54 #12689)

[HW79] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th ed., The Clarendon Press Oxford University Press, New York, 1979. MR568909 (81i:10002)

[H08] H. A. Helfgott, *Growth and generation in* $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, Ann. of Math. (2) **167** (2008), no. 2, 601–623, DOI 10.4007/annals.2008.167.601. MR2415382 (2009i:20094)

[LW54] Serge Lang and André Weil, *Number of points of varieties in finite fields*, Amer. J. Math. **76** (1954), 819–827. MR0065218 (16,398d)

[M55] G. D. Mostow, *Self-adjoint groups*, Ann. of Math. (2) **62** (1955), 44–55. MR0069830 (16,1088a)

[NS10] Amos Nevo and Peter Sarnak, *Prime and almost prime integral points on principal homogeneous spaces*, Acta Math. **205** (2010), no. 2, 361–402, DOI 10.1007/s11511-010-0057-4. MR2746350 (2011m:22040)

[N87] Madhav V. Nori, *On subgroups of* $\mathrm{GL}_n(\mathbf{F}_p)$, Invent. Math. **88** (1987), no. 2, 257–275, DOI 10.1007/BF01388909. MR880952 (88d:20068)

[PR94] Vladimir Platonov and Andrei Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139, Academic Press Inc., Boston, MA, 1994. Translated from the 1991 Russian original by Rachel Rowen. MR1278263 (95b:11039)

[PS] L. Pyber and E. Szabó, *Growth in finite simple groups of Lie type of bounded rank,* preprint.

[Ra72] M. S. Raghunathan, *Discrete subgroups of Lie groups*, Springer-Verlag, New York, 1972. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 68. MR0507234 (58 #22394a)

[SV] Alireza Salehi Golsefidy and Péter P. Varjú, *Expansion in perfect groups*, Geom. Funct. Anal. **22** (2012), no. 6, 1832–1891, DOI 10.1007/s00039-012-0190-7. MR3000503

[Sch00] A. Schinzel, *Polynomials with special regard to reducibility*, Encyclopedia of Mathematics and its Applications, vol. 77, Cambridge University Press, Cambridge, 2000. With an appendix by Umberto Zannier. MR1770638 (2001h:11135)

[Sc74] Wolfgang M. Schmidt, *A lower bound for the number of solutions of equations over finite fields*, J. Number Theory **6** (1974), 448–480. Collection of articles dedicated to K. Mahler on the occasion of his seventieth birthday. MR0360598 (50 #13045)

[Sp98] T. A. Springer, *Linear algebraic groups*, 2nd ed., Progress in Mathematics, vol. 9, Birkhäuser Boston Inc., Boston, MA, 1998. MR1642713 (99h:20075)

[V12] Péter P. Varjú, *Expansion in* $SL_d(\mathcal{O}_K/I)$*, I square-free*, J. Eur. Math. Soc. (JEMS) **14** (2012), no. 1, 273–305, DOI 10.4171/JEMS/302. MR2862040

Department of Mathematics, University of California, San Diego, California 92093-0112

E-mail address: golsefidy@ucsd.edu

Department of Mathematics, Princeton University, Princeton, New Jersey 08544-1000

E-mail address: sarnak@math.princeton.edu