J. Group Theory **17** (2014), 525–539
DOI 10.1515/jgt-2014-0001

Homogeneous number of free generators

Menny Aka, Tsachik Gelander and Gregory A. Soĭfer

Communicated by Miklós Abért

Abstract. We address two questions of Simon Thomas. First, we show that for any $n \geq 3$ one can find a four-generated free subgroup of $\mathrm{SL}_n(\mathbb{Z})$ which is profinitely dense. More generally, we show that an arithmetic group Γ that admits the congruence subgroup property has a profinitely-dense free subgroup with an explicit bound on its rank. Next, we show that the set of profinitely-dense, locally-free subgroups of such an arithmetic group Γ is uncountable.

1 Introduction

Let G be a simply-connected semisimple algebraic group defined over $\mathbb{Q}$ with a fixed embedding to GL_n. Let Γ be an arithmetic subgroup of $G(\bar{\mathbb{Q}})$, i.e., a group commensurable to $G(\mathbb{Z}) := G(\bar{\mathbb{Q}}) \cap \mathrm{GL}_n(\mathbb{Z})$. Assume moreover that $G(\mathbb{R})$ is non-compact. The aim of this paper is to show the following:

Theorem 1.1. *Assume that G admits the congruence subgroup property (see Section 3.2), and let $d(\widehat{\Gamma})$ be the minimal number of generators of the profinite completion of Γ (see Section 3.1). Then there exists a free subgroup $F \subset \Gamma$, on at most $2 + d(\widehat{\Gamma})$ generators, which is profinitely dense, i.e., maps onto any finite quotient of Γ.*

Let $\alpha(\Gamma)$ be the minimal rank of a profinitely dense free subgroup of Γ. Theorem 1.1 claims that $\alpha(\Gamma) \leq d(\widehat{\Gamma}) + 2 \leq d(\Gamma) + 2$. In [13] it is proved that Γ as above admits a profinitely-dense free subgroup of finite rank. Consequently Simon Thomas asked whether one can find a uniform bound on $\alpha(\mathrm{SL}_n(\mathbb{Z}))$, $n \geq 3$. It is known that $\mathrm{SL}_n(\mathbb{Z})$ is generated by two elements for all $n \geq 2$ (see [15]) and that $\mathrm{SL}_n(\mathbb{Z})$ (see Section 3.2) admits the Congruence Subgroup Property for $n \geq 3$.

We acknowledge the support of the ERC grant 226135, the ERC grant 203418, the ISEF foundation, the Ilan and Asaf Ramon memorial foundation, the "Hoffman Leadership and Responsibility" fellowship program, the ISF grant 1003/11, the BSF grant 2010295, the SFB grant 701 "Spektrale Strukturen und Topologische Methoden in der Mathematik", the Emmy Noether Research Institute for Mathematics Bar-Ilan University, the Israel Science Foundation under ISF grant 657/09 and the Max Planck Institute for Mathematics, Bonn.

Thus Theorem 1.1 implies that for any $n \geq 3$ there exists a free profinitely-dense subgroup of $\mathrm{SL_n}(\mathbb{Z})$ with rank ≤ 4. In particular, given a family $\{\Gamma_n\}$ of such arithmetic groups, a uniform bound on $d(\Gamma_n)$ will provide a uniform bound on $\alpha(\Gamma_n)$. It is an interesting question whether $\alpha(\mathrm{SL_n}(\mathbb{Z})) = 2$ for all n. We note that there are arithmetically-defined families such that $\alpha(\Gamma_n)$ is not uniformly bounded. For example, let

$$\Delta_n := \mathrm{SL_n}(\mathbb{Z})$$

and for a rational prime p let

$$\Delta_n(p) := \{\gamma \in \Delta_n : \gamma \equiv I \pmod{p}\}.$$

It is shown in [4, Theorem 1.1] that the finite quotient $\Delta_n(p)/\Delta_n(p^2)$ is a vector space over $\mathbb{F}_p$ of dimension $n^2 - 1$ so any profinitely-dense and free subgroup has as least $n^2 - 1$ generators. That is $\alpha(\Delta_n(p)) \geq n^2 - 1$ and, in particular, is not uniformly bounded.

We remark that although it is shown in [3] that the profinite completion $\widehat{\Gamma}$ of any non-virtually solvable subgroup Γ has a free dense subgroup of rank $d(\Gamma)$, it is in general impossible to find a free group inside Γ. For example, Fuchsian groups are LERF [12] (i.e., every finitely-generated subgroup is the intersection of the finite-index subgroups that contain it), hence cannot admit a finitely-generated profinitely-dense proper subgroup.

We also address another question of Simon Thomas. Let $\mathfrak{U}$ be the set of locally-free subgroups of Γ containing a profinitely-dense finitely-generated subgroup.

Theorem 1.2. *The set $\mathfrak{U}_m$ of maximal elements of $\mathfrak{U}$ is uncountable.*

In essence, these theorems can be proved using techniques and results of [3,6]. The advantage of the following scheme of proof is in being elementary, using simple tools from ergodic theory.

Following Tits [14], in order to find free subgroups we use dynamics on projective spaces and we review relevant definitions and properties in Section 2. Tits' original result allows us to find a Zariski-dense free subgroup $\langle h_1, h_2\rangle$ of Γ of rank 2. Assuming the Congruence Subgroup Property, the closure of $\langle h_1, h_2\rangle$ in the profinite topology is of the form $\widehat{\Gamma'}$ for a finite-index subgroup $\Gamma' < \Gamma$, as we explain in Section 3. In order to find a profinitely-dense free subgroup, we will find so-called "ping-pong" partners to h_1 and h_2 that will belong to specified cosets of Γ' in Γ. We will need to add at most $d(\widehat{\Gamma})$ elements in order to construct a profinitely-dense free subgroup. This will be done in two steps. The first step is to find elements in cosets with prescribed dynamics on the projective space. In this step we establish the main new technique of this paper; we use the mixing property of the action of G on the homogeneous space G/Γ. This is done in

Section 4 where we also recall the necessary notions from Ergodic Theory. The second step is to use, with necessary modifications, the mechanism of rooted free systems (which originates in [6]) in order to inductively add "ping-pong" partners with desirable properties. This is done in Section 5. Using all the above ingredients we conclude the proofs of Theorems 1.1 and 1.2 in Section 6.

2 Dynamics on projective spaces

2.1 Proximal and hyperbolic elements

Let V be a vector space of dimension n over a local field K, $\mathbb{P}(V)$ be the associated projective space and $v \mapsto [v]$ be the associated projection map. The group $\mathrm{GL}(V)$ acts naturally on $\mathbb{P}(V)$ by $g[v] = [gv]$. An element $g \in \mathrm{GL}(V)$ is called *hyperbolic* if it is semisimple and admits a unique (counting multiplicities) eigenvalue of maximal absolute value and minimal absolute value. We denote by $\mathfrak{H}(G)$ the set of hyperbolic elements of G.

For $g \in \mathfrak{H}(G)$, let $\{v_1, \dots, v_n\}$ be a basis of eigenvectors such that v_1 corresponds to the unique maximal eigenvalue of g and v_n corresponds to the unique minimal eigenvalue of g. Note that although g is not necessarily diagonalizable over K, $\mathrm{span}(v_1, \dots, v_{n-1})$ and $\mathrm{span}(v_2, \dots, v_n)$ are defined over K. Indeed, this follows since there is a unique extension of the norm on K to any algebraic extension of K. (See e.g. [7, Proposition 6.4].)

We denote the following subsets of $\mathbb{P}(V)$ by

$$\begin{aligned} A^+(g) &= [v_1], & A^-(g) &= [v_n], \\ B^+(g) &= [\mathrm{span}(v_2, \dots, v_n)], & B^-(g) &= [\mathrm{span}(v_1, \dots, v_{n-1})], \\ A^\pm(g) &= A^+(g) \cup A^-(g), & B^\pm(g) &= B^+(g) \cup B^-(g). \end{aligned}$$

Note that

$$A^\pm(g) \subset B^\pm(g).$$

For further use we record some basic properties:

$$hA^+(g) = A^+(hgh^{-1})$$

and likewise for A^-, B^+, B^-. Also

$$A^\pm(g) = A^\pm(g^n), \quad B^\pm(g) = B^\pm(g^n) \quad \text{for all } g \in \mathfrak{H}(G) \tag{2.1}$$

and

$$A^+(g^{-1}) = A^-(g) \quad \text{for all } g \in \mathfrak{H}(G). \tag{2.2}$$

2.2 Distance on projective spaces

In order to study separation properties of projective transformations, we consider the following, so-called *standard metric* on $\mathbb{P}(V)$. For any $[v], [w] \in \mathbb{P}(V)$ let

$$d(a,b) = \frac{\|v \wedge w\|}{\|v\|\|w\|}.$$

See [2, Section 3] for the choices of the above norms and related properties. The reader should check that d is well-defined and that d induces the topology on $\mathbb{P}(V)$ that is inherited from the local field K. For any two sets $A, B \subset \mathbb{P}(V)$ we set $d(A,B) = \min\{d(a,b) : a \in A,\ b \in B\}$. We also need the following notion of distance between sets. For any two sets $A, B \subset \mathbb{P}(V)$ we define the Hausdorff distance by

$$d_h(A,B) = \max\Big\{\sup_{a\in A}\inf_{b\in B} d(a,b), \sup_{b\in B}\inf_{a\in A} d(a,b)\Big\}.$$

The only property of the Hausdorff distance that we are going to use is the following: Let $a \in \mathbb{P}(V)$, $B, C \subset \mathbb{P}(V)$. Then, $d(a,C) \le d(a,B) + d_h(B,C)$.

2.3 Transversality

We call two elements $g, h \in \mathfrak{H}(G)$ *transverse*, denoted by $g \perp h$, if they have the property that $A^{\pm}(g) \subset \mathbb{P} \setminus B^{\pm}(h)$ and $A^{\pm}(h) \subset \mathbb{P} \setminus B^{\pm}(g)$. If, moreover, $d(A^{\pm}(g), B^{\pm}(h)) > \epsilon$ and $d(A^{\pm}(h), B^{\pm}(g)) > \epsilon$, they are called *$\epsilon$-transverse*. Clearly any finite set of transverse elements is ϵ-transverse for some $\epsilon > 0$.

3 Profinite completions and the congruence subgroup property

3.1 Basic properties

For background on profinite groups the reader can consult the book of Ribes and Zalesskii [11]. For completeness we record here the definition of the profinite completion of a group. We write $A <_{\mathrm{fi}} B$ to mean that A is a finite-index subgroup of B. Let Γ be a finitely-generated group. The profinite topology on Γ is defined by taking as a fundamental system of neighborhoods of the identity the collection of all normal subgroups N of Γ such that Γ/N is finite. One can easily show that a subgroup H is open in Γ if, and only if, $H <_{\mathrm{fi}} \Gamma$. We can complete Γ with respect to this topology to get

$$\widehat{\Gamma} := \varprojlim\{\Gamma/N : N \lhd_{\mathrm{fi}} \Gamma\};$$

this is the profinite completion of Γ. There is a natural homomorphism $i : \Gamma \to \widehat{\Gamma}$ given by

$$i(\gamma) = \varprojlim(\gamma N).$$

A subgroup $\Lambda < \Gamma$ is profinitely dense in Γ if, and only if, $i(\Lambda)$ is dense in $\widehat{\Gamma}$. This, in turn, is equivalent to the property that Λ is mapped onto every finite quotient of Γ. The minimal number of elements of $\widehat{\Gamma}$ needed to generate a dense subgroup of $\widehat{\Gamma}$ is denoted by $d(\widehat{\Gamma})$.

Lemma 3.1. *Let Γ be a residually-finite group. There is a one-to-one correspondence between the set $\mathcal{X}$ of all cosets of finite-index subgroup of Γ and the set $\mathcal{Y}$ of all cosets of open subgroups of $\widehat{\Gamma}$, given by*

$$X \mapsto \mathrm{cl}(X) \quad (X \in \mathcal{X}),$$
$$Y \mapsto Y \cap \Gamma \quad (Y \in \mathcal{Y}),$$

where $\mathrm{cl}(X)$ *denotes the closure of X in $\widehat{\Gamma}$. Moreover, this correspondence maps normal subgroups to normal subgroups.*

Proof. See [5, Window: profinite groups, Proposition 16.4.3] for a proof of a correspondence between finite-index subgroups of Γ and the set $\mathcal{Y}$ of all open subgroups of $\widehat{\Gamma}$. The natural generalization to cosets is immediate. □

3.2 The congruence subgroup property

We give here a brief survey; for proofs of the assertions below the reader can consult [9].

For arithmetic groups, which are by definition commensurable to groups of the form $G(\mathcal{O}_k)$, we can give another interesting topology which is weaker than the profinite topology. As stated in the beginning, G is a simply-connected semisimple algebraic group defined over a number field k and equipped with an implicit k-embedding into GL_n. For any non-zero ideal I of $\mathcal{O}_k$ let K_I be the kernel of the map

$$G(\mathcal{O}_k) \to G(\mathcal{O}_k/I). \tag{3.1}$$

The completion of $G(\mathcal{O}_k)$, with respect to the topology in which these kernels form a system of neighborhoods of the identity, is called the congruence completion. We denote this completion by $\overline{G(\mathcal{O}_k)}$. Under the assumption we made on G, the Strong Approximation Theorem holds for G. This means that the maps in (3.1) are surjective for all but finitely many ideals I. (See [8, Theorem 7.12]). Using this, one can show that $\overline{G(\mathcal{O}_{k,S})}$ is naturally isomorphic to the open compact subgroup $\prod_{v \in V^f} G(\mathcal{O}_v)$ of $G(\mathbb{A}_{k,f})$ where V^f denotes the finite valuations of k

and $\mathbb{A}_{k,f}$ denotes the ring of finite Adeles. (See [8, Section 1.2].) As the profinite topology is stronger, we have the short exact sequence

$$1 \to C(G) \to \widehat{G(\mathcal{O}_k)} \to \overline{G(\mathcal{O}_k)} \to 1$$

and $C(G)$ is called the congruence kernel of G. If $C(G)$ is finite, we say that G admits the congruence subgroup property.

Finally, if Γ is commensurable to $G(\mathcal{O}_k)$, then the completion of Γ with respect to the family $\{K_I \cap \Gamma\}_{I \lhd \mathcal{O}_k}$ is called the congruence completion of Γ and is denoted by $\overline{\Gamma}$. One has a similar short exact sequence

$$1 \to C(\Gamma) \to \widehat{\Gamma} \to \overline{\Gamma} \to 1,$$

and one says that Γ has the congruence subgroup property if $|C(\Gamma)| < \infty$.

Assuming Γ has the congruence subgroup property, the closure $\overline{\Lambda} < \widehat{\Gamma}$ of a subgroup $\Lambda < \Gamma$ has finite-index if, and only if, for all but finitely many $I \lhd \mathcal{O}_k$, Λ maps onto $\Gamma/(K_I \cap \Gamma)$. As stated above, by [8, 16] every Zariski dense subgroup of $G(\bar{k})$ satisfy the last condition.

4 Elements in cosets with prescribed dynamics

In [14, Theorem 3], Tits constructs a strongly-irreducible representation (i.e., no finite union of proper subspaces is invariant) $\rho : G(k) \to \mathrm{GL}_d(K)$ for some $d \in \mathbb{N}$ and some local field K. From now on, we identify G (also topologically) with its image under ρ. We let $\mathbb{P} = \mathbb{P}(K^d)$ and for $p \in \mathbb{P}$ we write

$$gp := \rho(g)p.$$

We begin with several lemmata:

Lemma 4.1. *Let $g_0 \in \mathfrak{H}(G)$, and for $j = +, -$ set*

$$X_1^j(\epsilon) = \{g \in \mathfrak{H}(G) : d(A^j(g_0), A^j(g)) < \epsilon\},$$
$$X_2^j(\epsilon) = \{g \in \mathfrak{H}(G) : d_h(B^j(g_0), B^j(g)) < \epsilon\}.$$

Then there exists an $\epsilon > 0$ such that, for any $i = 1, 2$, $j = +, -$ and $h \in X_i^j(\epsilon)$, there exist a symmetric neighborhood of the identity $W \subset G$ and $N \in \mathbb{N}$ such that, for all $n > N$, we have $W h^n W \subset X_i^j(\epsilon)$.

Proof. We start with $i = 1$ and $j = +$. We first choose ϵ such that $B(A^+(g_0), \epsilon)$ (the ball of radius ϵ) and $\bigcup_{g \in X_1^+(\epsilon)} B^+(g)$ are disjoint and denote $X_1^+ = X_1^+(\epsilon)$. Let $h \in X_1^+$ be an arbitrary element. We can choose $U \subset B(A^+(g_0), \epsilon)$ a neighborhood of the subset $A^+(g_0)$, and W a neighborhood of the identity in G, such

that $WU = \{wu : w \in W, u \in U\} \subset B(A^+(g_0), \epsilon)$ and $A^+(h) \in U$. By choosing W even smaller we can also find $U' \subset U$ such that the following are satisfied:

- $A^+(h) \in U'$,
- $WU' = \{wu : w \in W, u \in U'\} \subset U$,
- $WU \subset \mathbb{P} \setminus B^+(h)$,
- for all n, $Wh^nW \subset \mathfrak{H}(G)$.

Then there exists an $N \in \mathbb{N}$ such that $h^n(WU) \subset U'$ for all $n > N$ and it follows that $(Wh^nW)U \subset U$. Therefore any element $\tilde{h} \in Wh^nW$, with $n > N$, has a fixed point inside U which is necessarily $A^+(\tilde{h})$. Thus $A^+(\tilde{h}) \in U$ so, by the choice of U, we have $d(A^+(\tilde{h}), A^+(g_0)) < \epsilon$, which implies that $Wh^nW \subset X_1^+$ for all $n > N$. Using equation (2.2), a proof along the exact same lines shows the case $i = 1$, $j = -$.

For the case $i = 2$, one can use duality of hyperplanes and points in the projective space and proceed with the same proof as above. Alternatively, we can apply the same proof with the natural action on $\mathbb{P}(\bigwedge^{d-1} K^d)$ where hyperplanes of the form $B^+(h)$ for some $h \in \mathfrak{H}(G)$ correspond to points. □

Lemma 4.2. *Let $g_1, \ldots, g_n$ be hyperbolic elements of G. There exists an element $g \in \mathfrak{H}(G)$ with $g \perp g_i$ for all $i = 1, \ldots, n$.*

Proof. Let

$$U^+ := \{g \in G : gA^+(g_1) \notin B^\pm(g_j) \text{ for all } j = 1, \ldots, n\}.$$

We claim that U^+ is a non-empty Zariski open set. Assume not, then the union $\bigcup_{i=1}^n B^\pm(g_i)$ will contain an invariant set which is a union of proper subspaces, which contradicts our assumption. Similarly,

$$U^- := \{g \in G : g^{-1}A^-(g_j) \notin B^\pm(g_1) \text{ for all } j = 1, \ldots, n\}$$

is a non-empty Zariski open set. As G is Zariski connected, $U = U^+ \cap U^-$ is non-empty open set, and moreover, for any $g \in U$ we have $A^\pm(gg_1g^{-1}) \notin B^\pm(g_j)$ for all $j = 1, \ldots, n$. A similar argument shows that there exists a non-empty open $V \subset G$ such that for any $g \in V$ we have

$$g^{-1}A^\pm(g_j) \notin B^\pm(g_1) \iff A^\pm(g_j) \notin B^\pm(gg_1g^{-1}).$$

Thus any element of the form gg_1g^{-1} for some $g \in U \cap V$ is transverse to all g_j, as needed. □

The aim of this section is to find such an element g in a given coset of G/Λ where Λ is a lattice in G. To this end, we begin by "approximating" the transverse element we get from Lemma 4.2.

Lemma 4.3. *Given $\epsilon > 0$, assume that $\{g_1, \dots, g_s, g\}$ is a set of pairwise ϵ-transverse hyperbolic elements. There exist an integer $N = N(g, \epsilon)$ and a symmetric neighborhood $W = W(g, \epsilon)$ of the identity in G such that if $n > N$, then, for any $h \in Wg^nW$, $\{g_1, \dots, g_s, h\}$ is a set of pairwise $\frac{\epsilon}{2}$-transverse hyperbolic elements.*

Proof. We first claim that any $h \in \mathfrak{H}(G)$ with

$$\begin{aligned} d(A^+(h), A^+(g)) < \frac{\epsilon}{2}, \quad d(A^-(h), A^-(g)) < \frac{\epsilon}{2}, \\ d_h(B^+(h), B^+(g)) < \frac{\epsilon}{2}, \quad d_h(B^-(h), B^-(g)) < \frac{\epsilon}{2} \end{aligned} \tag{4.1}$$

is $\frac{\epsilon}{2}$-transverse to any element which is ϵ-transverse to g. Indeed, suppose that g' is ϵ-transverse to g. Then we have, for example,

$$\begin{aligned} \epsilon < d(A^+(g), B^{\pm}(g')) \le d(A^+(g), A^+(h)) + d(A^+(h), B^{\pm}(g')), \\ \epsilon < d(A^{\pm}(g'), B^+(h)) \le d(A^+(g'), B^+(h)) + d_h(B^+(h), B^+(g)), \end{aligned}$$

so, using (4.1), we see that g' and h are $\frac{\epsilon}{2}$-transverse.

It follows readily from Lemma 4.1 that there exists a symmetric neighborhood W of the identity of G and $N = N(g, \epsilon) \in \mathbb{N}$ such that, for large enough $n > N$, any $h \in Wg^nW$ is hyperbolic and satisfies (4.1). □

Before proceeding to the main proposition of this section we recall some notions from Ergodic Theory. By the Borel Harish-Chandra Theorem (see [8, Section 4.6]), arithmetic subgroups are lattices. By definition, Λ is a lattice in G if Λ is discrete and G/Λ carry a finite G-invariant measure which we denote by μ. The action of G on G/Λ allows us to use techniques from Ergodic Theory. In particular, for semisimple groups G as in our case, we have the vanishing Theorem of Howe–Moore (see [1, Chapter III] and the references therein). It states that, for any $g \in G$ with the property that for any compact subset $K \subset G$ there exists an M such that $g^n \notin K$ for all $n > M$, we have

$$\lim_{n \to \infty} \mu(A \cap g^n B) \to \mu(A)\mu(B) \tag{4.2}$$

for any two measurable sets $A, B \subset G/\Lambda$.

Proposition 4.4. *Let Λ be a lattice in G, $\{g_1, \dots, g_s\}$ be a set of pairwise transverse hyperbolic elements, and $x \in G$. Then there exists an element $h \in x\Lambda$ such that $\{g_1, \dots, g_s, h\}$ is a set of pairwise transverse hyperbolic elements.*

Proof. Using Lemma 4.2 we find some $g \in \mathfrak{H}(G)$ such that $\{g_1, \dots, g_s, g\}$ is a set of pairwise ϵ_0-transverse hyperbolic elements for some $\epsilon_0 > 0$. In order to finish the proof we only need to find $h \in x\Lambda$ which also satisfies $h \in Wg^nW$ for

some $n > N$, where $W = W(g, \epsilon_0)$ and $N = N(g, \epsilon_0)$ are supplied by Lemma 4.3. To this end we consider the homogeneous space G/Λ equipped with the unique left invariant probability measure μ on G/Λ. As $g \in \mathfrak{H}(G)$, for any compact subset $K \subset G$, there exists an M such that $g^n \notin K$ for all $n > M$. Therefore, by the Howe–Moore Theorem stated above, we have that

$$\lim_{n\to\infty} \mu(g^n W\Lambda \cap Wx\Lambda) = \mu(W\Lambda)\mu(Wx\Lambda) > 0$$

so, for large enough n, and, in particular, for some $n > N$, $g^n W\Lambda \cap Wx\Lambda \neq \emptyset$. This yields some $w_1, w_2 \in W$ and $\gamma \in \Lambda$ with the property that $g^n w_1 = w_2 x\gamma$ so $h := x\gamma = w_2^{-1} g^n w_1$, as desired. □

5 Free g_0-rooted systems

Definition 5.1. Given $g_0 \in \mathfrak{H}(G)$, a tuple $\{g_i\}_{i=1}^s \subset \mathfrak{H}(G)$ is called a g_0-rooted free system if there exist open sets $\{X_i\}_{i=0}^s$ of $\mathbb{P}$ satisfying:

(1) $\{X_i\}_{i=0}^s$ are pairwise disjoint,

(2) $A^{\pm}(g_i) \subseteq X_i \subset \overline{X_i} \subset \mathbb{P} \setminus B^{\pm}(g_0)$ for all $i = 1, \ldots, s$,

(3) $A^{\pm}(g_0) \subseteq X_0 \subset \overline{X_0} \subset \mathbb{P} \setminus \bigcup_{i=1}^s B^{\pm}(g_i)$,

(4) $g_i^{\pm}(\overline{X_j}) \subset X_i$ for any $i, j \in \{0, \ldots, s\}$.

Note that by the so-called Ping-Pong Lemma [14, Proposition 1.1], the elements $g_0, \ldots, g_s$ are independent; $(\{g_i\}_{i=1}^s, g_0)$ is clearly free. The following lemma exemplifies how one can use g_0-rooted systems in order to enlarge a given independent set of elements.

Lemma 5.2. *Assume we are given a g_0-rooted free system $\{g_1, \ldots, g_s\}$, a subset $F \subset G$, and an element $h \in F \cap \mathfrak{H}(G)$ such that*

- *the set $M_1 = \{n : g_0^n h g_0^{-n} \in F\}$ is infinite,*
- *the sets $M_{2,l} = \{n : g_0^l h^n g_0^{-l} \in F\}$ are infinite whenever $l \in M_1$,*
- *$h \perp g_i$ for $i = 0, \ldots, s$.*

Then there exist $k, n_0, n_1 \in \mathbb{N}$ such that $g_{s+1} := g_0^{n_0} h^{n_1} g_0^{-n_0}$ is an element of F and $\{g_1, \ldots, g_s, g_{s+1}\}$ is a g_0^k-rooted free system.

Proof. Let $\{X_i\}_{i=0}^s$ be the sets showing that $\{g_1, \ldots, g_s\}$ is a g_0-rooted free system and let $h_n := g_0^n h g_0^{-n}$. As $g_0 \perp h$, there exists an $N_1 \in \mathbb{N}$ such that, for any $n > N_1$, the following holds:

$$A^{\pm}(h_n) = g_0^n(A^{\pm}(h)) \subset X_0 \tag{5.1}$$

and, for any $i = 1, \dots, s$, we have $g_0^{-n}\overline{X_i} \subset \mathbb{P} \setminus B^{\pm}(h)$, which is equivalent to

$$\overline{X_i} \subset \mathbb{P} \setminus g_0^n B^{\pm}(h) = \mathbb{P} \setminus B^{\pm}(h_n). \tag{5.2}$$

This shows that $g_1, \dots, g_s, h_n$ are pairwise transverse for all $n > N_1$. Furthermore, it is easy to see that g_0 and h_n are transverse for any $n \in \mathbb{N}$. By assumption there is an arbitrarily large $n \in \mathbb{N}$ for which $h_n \in F$ so we can choose $n_0 > N_1$ such that $h_{n_0} \in F$.

We now define open subsets

$$\{Y_i\}_{i=0}^{s+1} \tag{5.3}$$

which will show that for some n_1, $\{g_1, \dots, g_s, h_{n_0}^{n_1}\}$ is g_0^k-rooted system (n_1 and k will be defined in a moment). Let $Y_i = X_i$ for $i = 1, \dots, s$ and let Y_{s+1} be an open subset of $\mathbb{P}$ such that $Y_{s+1} \subset \overline{X_0}$ and

$$A^{\pm}(h_{n_0}) \subset Y_{s+1} \subset \overline{Y_{s+1}} \subset \mathbb{P} \setminus B^{\pm}(g_0). \tag{5.4}$$

Furthermore, we let Y_0 be an open subset of $\mathbb{P}$ such that

$$A^{\pm}(g_0) \subset Y_0 \subset \overline{Y_0} \subset X_0 \quad \text{and} \quad \overline{Y_0} \subset \mathbb{P} \setminus B^{\pm}(h_{n_0}). \tag{5.5}$$

Such sets exist since we have seen that $g_0, \dots, g_s, h_{n_0}$ are pairwise transverse; this also implies that there exists an N_2 such that, for any integer n with $|n| > N_2$, we have that

$$h_{n_0}^n(Y_i) \subset Y_{s+1} \quad \text{for } i = 0, \dots, s. \tag{5.6}$$

Finally, by assumption, the set

$$M := \{n \in \mathbb{N} : h_{n_0}^n \in F\} \tag{5.7}$$

is infinite. Let $g_{s+1} = h_{n_0}^{n_1}$ for some $n_1 \in M$ with $n_1 > N_2$. The above transversality also implies that there exists a $k \in \mathbb{N}$ such that

$$g_0^k \left(\bigcup_{i=0}^{s+1} Y_i \right) \subset Y_0. \tag{5.8}$$

We end the proof by showing that $\{g_1, \dots, g_s, g_{s+1}\}$ is a g_0^k-rooted system, using the sets $\{Y_i\}_{i=0}^{s+1}$. Condition (1) is satisfied by the choice of the sets $\{Y_i\}_{i=0}^{s+1}$. Using (2.1), we see that (5.4) and the fact that $X_i = Y_i$ for $i = 1, \dots, s$, imply condition (2). Similarly, (5.5) implies condition (3). Lastly, (5.6) implies condition (4) for $i = s + 1$, and (5.8) does it for $i = 0$. □

The following two propositions are the main ingredients in the proofs of our main theorems.

Proposition 5.3. *Let $\Gamma_1 \lhd_{\mathrm{fi}} \Gamma$, $x \in \Gamma$ and let $\{g_1, \dots, g_s\}$ be a g_0-rooted free system for $g_0 \in \Gamma$. Then there exist a $k \in \mathbb{N}$ and a hyperbolic element $g_{s+1} \in x\Gamma_1$ such that $\{g_1, \dots, g_s, g_{s+1}\}$ is a g_0^k-rooted free system.*

Proof. By Proposition 4.4 we can find hyperbolic $h \in x\Gamma_1$ such that $g_1, \dots, g_s, h$ are pairwise transverse. Moreover, as $g_0 \in \Gamma$ and $\Gamma_1 \lhd_{\mathrm{fi}} \Gamma$, the set

$$M_1 = \{n : g_0^n h g_0^{-n} \in x\Gamma_1\}$$

is infinite and so are the sets

$$M_{2,l} = \{n : g_0^l h^n g_0^{-l} \in x\Gamma_1\}$$

whenever $l \in M_1$. Thus, applying Lemma 5.2 with $F = x\Gamma_1$, we find a $k \in \mathbb{N}$ and a hyperbolic element $g_{s+1} \in x\Gamma_1$ such that $\{g_1, \dots, g_s, g_{s+1}\}$ is a g_0^k-rooted free system, as claimed. □

Proposition 5.4. *Let $H < \Gamma$ be a profinitely-dense subgroup and let $\{g_1, \dots, g_s\}$ be a g_0-rooted free system with $\{g_i\}_{i=0}^s \subset \Gamma$. Then there exists a hyperbolic element $g_{s+1} \notin H$ such that $\{g_1, \dots, g_s, g_{s+1}\}$ is a $\tilde{g_0}$-rooted free system for some $\tilde{g_0} \in \mathfrak{H}(G) \cap \Gamma$ (typically $\tilde{g_0} = g_0^k$ for some $k \in \mathbb{N}$).*

Proof. Consider first the case where $g_0 \in H$. By [6, Proposition 3] we know that H is Zariski dense since it is profinitely dense. It follows from [6, Lemma 8] that there exists an element $\tilde{h} \in \mathfrak{H}(G)$ with $\tilde{h} \in \Gamma \setminus H$. Now

$$W = \{w \in G : (w\tilde{h}w^{-1}) \perp g_i \text{ for all } i \in \{0, \dots, s\}\}$$

is Zariski open; indeed

$$W = \bigcap_{i=1}^{s} \{w : (wA^{\pm}(\tilde{h})) \cap B^{\pm}(g_i) = \emptyset\} \cap \bigcap_{i=1}^{s} \{w : B^{\pm}(\tilde{h}) \cap w^{-1}A^{\pm}(g_i) = \emptyset\}$$

and each one of the sets in the intersection is clearly a Zariski open set. As H is Zariski dense, we can find some element $w \in H \cap W$. Let $h = w\tilde{h}w^{-1}$. Clearly, $h \in \mathfrak{H}(G)$, $h \in \Gamma \setminus H$ and the elements of $\{g_1, \dots, g_s, h\}$ are pairwise transverse. Moreover, as $g_0 \in H$, it follows that the set $M_1 = \{n : g_0^n h g_0^{-n} \in \Gamma \setminus H\} = \mathbb{N}$ and the sets $M_{2,l} = \{n : g_0^l h^n g_0^{-l} \in \Gamma \setminus H\}$ are infinite whenever $l \in M_1$. Thus, applying Lemma 5.2 with $F = \Gamma \setminus H$, we find a $k \in \mathbb{N}$ and a hyperbolic element $g_{s+1} \in \Gamma \setminus H$ such that $\{g_1, \dots, g_s, g_{s+1}\}$ is a g_0^k-rooted free system, which concludes the case when $g_0 \in H$.

Now assume $g_0 \notin H$. Let $\{X_i\}_{i=0}^s$ be the sets showing that $\{g_1, \dots, g_s\}$ is a g_0-rooted free system and set

$$d = \min_{1 \le i \le s} d(B^{\pm}(g_0, \overline{X_i})).$$

Let

$$U_1 = \{g \in G : g \in \mathfrak{H}(G), g \perp g_0\},$$

$$U_2 = \left\{g \in G : A^{\pm}(g) \subset X_0, d_h(B^{\pm}(g_0), B^{\pm}(g)) < \frac{d}{4}\right\}$$

and $U = U_1 \cap U_2$. We now consider two possibilities: if $U \cap H \neq \emptyset$, it is easy to see that there exist $h_0 \in U \cap H$ and $k \in \mathbb{N}$ such that $\{g_1, \dots, g_s\}$ is a h_0^k-rooted free system. Thus this possibility reduces to the first case with g_0 interchanged with $h_0^k \in H$.

Therefore we can assume that $U \cap H = \emptyset$. Note that, by Lemma 4.1, for any element $g \in U$ there exist W and $N_0 \in \mathbb{N}$ such that $Wg^nW \subset U$ for all $n > N$. As $g \in \mathfrak{H}(G)$, for any compact subset $K \subset G$, there exists an M such that $g^n \notin K$ for all $n > M$. Therefore, by the Howe–Moore Theorem stated above, we have that

$$\lim_{n\to\infty} \mu(g^n W\Gamma \cap W\Gamma) = \mu(W\Gamma)\mu(W\Gamma) > 0,$$

so, for large enough n, and, in particular, for some $n > N_0$, $g^n W\Gamma \cap W\Gamma \neq \emptyset$. This yields some $w_1, w_2 \in W$ and $\gamma \in \Gamma$ with the property that $g^n w_1 = w_2\gamma$ so $h := \gamma = w_2^{-1} g^n w_1 \in \Gamma \cap U$ as desired. By the definition of U, the elements of $\{g_1, \dots, g_s, h\}$ are pairwise transverse, and all of them are transverse to g_0. To show that they form a g_0-rooted free system, we can follow the proof of Lemma 5.2 from equation (5.3) onwards, interchanging h_{n_0} with h everywhere, and noting that (5.7) is also true in our situation as the set $M = \{n : h^n \notin H\}$ is infinite since $h \notin H$ by the assumption that $U \cap H = \emptyset$. □

6 Proof of Theorems 1.1 and 1.2

Proof of Theorem 1.1. We first claim that there exist two elements $h_1, h_2, g_0 \in \Gamma$ such that $\{h_1, h_2\}$ is a g_0-rooted free system and $\langle h_1, h_2\rangle$ is Zariski dense in G. By [14, Theorem 3] we can find $f_1, f_2 \in \Gamma$ such that $\langle f_1, f_2\rangle$ is free and Zariski dense in G. We can assume that $\overline{\langle f_1\rangle}^{\mathrm{Zar}}$ and $\overline{\langle f_2\rangle}^{\mathrm{Zar}}$ are connected tori. Indeed, by [10, Definition 6.10 and Theorem 6.11] there exists a finite-index subgroup $\Gamma_0 < \Gamma$ such that the eigenvalues of any semisimple element of Γ_0 are not a (non-trivial) root of unity. This implies that the Zariski closure of any hyperbolic element of Γ_0 is a connected torus. Using [14, Theorem 3] for Γ_0, we can assume that $f_1, f_2 \in \Gamma_0$ and that $\langle f_1, f_2\rangle$ is free and Zariski dense in G. It now follows that the same is true for f_1^k, f_2^k for any $k \in \mathbb{N}$. Indeed, as

$$\overline{\langle f_1^k\rangle}^{\mathrm{Zar}}, \overline{\langle f_2^k\rangle}^{\mathrm{Zar}} \subset \overline{\langle f_1^k, f_2^k\rangle}^{\mathrm{Zar}},$$

it suffices to show that $f_i \in \overline{\langle f_i^k\rangle}^{\mathrm{Zar}}$, $i = 1, 2$. As $f_i \in \Gamma_0$ is hyperbolic, $\overline{\langle f_i\rangle}^{\mathrm{Zar}}$ is

connected. Therefore, the finite-index closed subgroup $\overline{\langle f_i^k \rangle}^{\mathrm{Zar}}$ is in fact equal to $\overline{\langle f_i \rangle}^{\mathrm{Zar}}$, showing that

$$f_i \in \overline{\langle f_i^k \rangle}^{\mathrm{Zar}}.$$

Now, by Proposition 4.4, we can find $f_0 \in \Gamma$ such that $\{f_0, f_1, f_2\}$ are pairwise transverse. Therefore there exists a $k \in \mathbb{N}$ such that $\{f_1^k, f_2^k\}$ is f_0^k-free rooted system. Thus the claim is proved by letting

$$g_0 := f_0^k, \quad h_1 := f_1^k, \quad h_2 := f_2^k.$$

As explained at the end of Section 3.2, since Γ admits the Congruence Subgroup Property and $\langle h_1, h_2 \rangle$ is Zariski dense, the closure of $\langle h_1, h_2 \rangle$ is of finite index in $\widehat{\Gamma}$. By Lemma 3.1 there exists a $\Gamma_1 \lhd_{\mathrm{fi}} \Gamma$ such that

$$\widehat{\Gamma_1} \subset \overline{\langle h_1, h_2 \rangle}.$$

Let $y_1, \ldots, y_m$ be elements of $\widehat{\Gamma}$ which generate of $\widehat{\Gamma}/\widehat{\Gamma_1}$ with $m \leq d(\widehat{\Gamma})$. By Lemma 3.1, there exist $x_1, \ldots, x_m$ with

$$x_i \Gamma_1 = y_i \widehat{\Gamma_1} \cap \Gamma.$$

Then, using Proposition 5.3 inductively, we find $\{g_i\}_{i=1}^m \in \Gamma$ such that $g_i \in x_i \Gamma_1$ and $\{h_1, h_2, g_1, \ldots, g_m\}$ is a g_0^k-rooted free system for some $k \in \mathbb{N}$. Therefore the image of Γ_1 in $\widehat{\Gamma}$ together with $\{g_1, \ldots, g_m\}$ generate $\widehat{\Gamma}$ (topologically). This shows that $\langle h_1, h_2, g_1, \ldots, g_m \rangle$ is profinitely dense and is free of rank $m + 2$, as asserted. □

Proof of Theorem 1.2. Assume, by a way of contradiction, that $\mathfrak{U}_{\mathfrak{m}}$ is countable and let $\{U_i\}_{i=1}^{\infty}$ be some enumeration of it. Let $\{F_i\}_{i=1}^{\infty}$ be an enumeration of all the cosets of finite-index subgroups of Γ. Let $g_0 \in \Gamma$ be some hyperbolic element. Using Proposition 5.3 (with the empty g_0-rooted free system) we can find $g_1 \in F_1$ and $g_{0,1} \in \mathfrak{H}(G) \cap \Gamma$ such that $\{g_1\}$ is a $g_{0,1}$-rooted free system. Similarly, using Proposition 5.4, we can find g_2 and $g_{0,2} \in \mathfrak{H}(G) \cap \Gamma$ such that $g_2 \notin U_1$ and $\{g_1, g_2\}$ is a $g_{0,2}$-rooted free system. Continuing in this fashion and using Propositions 5.3 and 5.4 alternately, we find sequences $\{g_i\}_{i=1}^{\infty}, \{g_{0,i}\}_{i=1}^{\infty} \subset \mathfrak{H}(G) \cap \Gamma$ such that, for any $k \in \mathbb{N}$, $g_{2k} \notin U_k$, $g_{2k-1} \in F_k$ and, for any $l \in \mathbb{N}$, $\{g_1, \ldots, g_l\}$ is a $g_{0,l}$-rooted free system. Let $H = \langle \{g_i\}_{i=1}^{\infty} \rangle$; we claim that H is free and profinitely dense. Indeed, H is freely generated by $\{g_i\}_{i=1}^{\infty}$ since any finite subset of $\{g_i\}_{i=1}^{\infty}$ is contained in some free rooted system. It is profinitely dense as otherwise H would be contained in a finite-index subgroup Λ, which is impossible as H has elements in each coset of Λ in Γ. Therefore $H \subseteq U_i$ for some i. This is a contradiction as $g_{2i} \notin U_i$. □

Acknowledgments. We thank the anonymous referee for the careful reading of our manuscript and the valuable comments.

Bibliography

[1] M. Bachir Bekka and M. Mayer, *Ergodic Theory and Topological Dynamics of Group Actions on Homogeneous Spaces*, London Math. Soc. Lecture Note Ser. 269, Cambridge University Press, Cambridge, 2000.

[2] E. Breuillard and T. Gelander, On dense free subgroups of Lie groups, *J. Algebra* **261** (2003), 448–467.

[3] E. Breuillard and T. Gelander, A topological Tits alternative, *Ann. of Math. (2)* **166** (2007), 427–474.

[4] R. Lee and R. H. Szczarba, On the homology and cohomology of congruence subgroups, *Invent. Math.* **33** (1976), 15–53.

[5] A. Lubotzky and D. Segal, *Subgroup Growth*, Progr. Math. 212, Birkhäuser-Verlag, Basel, 2003.

[6] G. A. Margulis and G. A. Soĭfer, Maximal subgroups of infinite index in finitely generated linear groups, *J. Algebra* **69** (1981), 1–23.

[7] J. Neukirch, *Algebraic Number Theory*, Grundlehren Math. Wiss. 322, Springer-Verlag, Berlin, 1999.

[8] V. Platonov and A. Rapinchuk, *Algebraic Groups and Number Theory*, Pure Appl. Math. 139, Academic Press, Boston, 1994.

[9] G. Prasad and A. S. Rapinchuk, Developments on the congruence subgroup problem after the work of Bass, Milnor and Serre, preprint (2008), `http://arxiv-web3.library.cornell.edu/abs/0809.1622v1`.

[10] M. S. Raghunathan, *Discrete Subgroups of Lie Groups*, Ergeb. Math. Grenzgeb. 68, Springer-Verlag, New York, 1972.

[11] L. Ribes and P. Zalesskii, *Profinite Groups*, 2nd ed., Ergeb. Math. Grenzgeb. (3) 40, Springer-Verlag, Berlin, 2010.

[12] P. Scott, Subgroups of surface groups are almost geometric, *J. Lond. Math. Soc. (2)* **17** (1978), 555–565.

[13] G. A. Soifer and T. N. Venkataramana, Finitely generated profinitely dense free groups in higher rank semi-simple groups, *Transform. Groups* **5** (2000), 93–100.

[14] J. Tits, Free subgroups in linear groups, *J. Algebra* **20** (1972), 250–270.

[15] S. M. Trott, A pair of generators for the unimodular group, *Canad. Math. Bull.* **5** (1962), 245–252.

[16] B. Weisfeiler, Strong approximation for Zariski-dense subgroups of semisimple algebraic groups, *Ann. of Math. (2)* **120** (1984), 271–315.

Received May 4, 2012; revised December 10, 2013.

Author information

Menny Aka, Section de mathématiques, EPFL,
Station 8 - Bât. MA, CH-1015 Lausanne, Switzerland.
E-mail: mennyaka@gmail.com

Tsachik Gelander, Einstein Institute of Mathematics, Edmond J. Safra Campus,
Givat Ram, The Hebrew University of Jerusalem, 91904 Jerusalem, Israel.
E-mail: tsachik.gelander@gmail.com

Gregory A. Soĭfer, Department of Mathematics, Bar-Ilan University,
52900 Ramat-Gan, Israel.
E-mail: soifer@macs.biu.ac.il