CHEEGER CONSTANT AND ALGEBRAIC ENTROPY OF LINEAR GROUPS

EMMANUEL BREUILLARD AND TSACHIK GELANDER

Abstract. We prove a uniform version of the Tits alternative. As a consequence, we obtain uniform lower bounds for the Cheeger constant of Cayley graphs of finitely generated non virtually solvable linear groups in arbitrary characteristic. Also we show that the algebraic entropy of discrete subgroups of a given Lie group is uniformly bounded away from zero.

In this note, we summarize some results whose full proofs will appear in [5].

1. Free subgroups in linear groups

Let K be an arbitrary field and Γ a subgroup of $GL_d(K)$ generated by a finite subset Σ. Assume Σ is symmetric (i.e. $s \in \Sigma \Rightarrow s^{-1} \in \Sigma$), contains the identity e, and let $\mathcal{G} = \mathcal{G}(\Gamma, \Sigma)$ be the associated Cayley graph. The set Σ^n is the set of all products of at most n elements from Σ, i.e. the ball of radius n centered at the identity in $\mathcal{G}$. We introduce the following definition:

Definition 1.1. *Two elements in a group are said to be* ***independent*** *if they generate a non-commutative free subgroup. The* ***independence diameter*** *of a Cayley graph $\mathcal{G}(\Gamma, \Sigma)$ is the quantity $d_\Gamma(\Sigma) = \inf\{n \in \mathbb{N} : \Sigma^n$ contains two independent elements $\}$. Similarly, we define the independence diameter of the group Γ to be $d_\Gamma = \sup\{d_\Gamma(\Sigma) : \Sigma$ finite symmetric generating set with $e \in \Sigma\}$.*

The Tits alternative [11] asserts that either Γ is virtually solvable (i.e. contains a solvable subgroup of finite index) or Γ contains two independent elements, i.e. $d_\Gamma(\Sigma) < +\infty$ for every generating set Σ. The two events are mutually exclusive. Tits' proof provides no estimate as to how close to the identity in $\mathcal{G}$ the independent elements may be found. We obtain:

Theorem 1.1. *(Uniform Tits alternative) Let Γ be a finitely generated subgroup of $GL_n(K)$. Assume that Γ is not virtually solvable. Then $d_\Gamma < +\infty$.*

This result improves a theorem of A. Eskin, S. Mozes and H. Oh who proved in [7] the analogous statement when free subgroup is replaced by free semigroup. Although only linear groups in characteristic zero where

1991 *Mathematics Subject Classification.* Primary 05C38, 15A15; Secondary 05A15, 15A18.

Key words and phrases. Linear groups, growth, free subgroups.

considered in [7], our proof of Theorem 1.1 treats the general case. This relies on a general version of the Eskin-Mozes-Oh theorem which we proved together with Alireza Salehi-Golsefidy and will appear in [6]. As an important corollary and original motivation to their main result, the authors of [7] obtained that finitely generated linear groups in characteristic zero either are virtually nilpotent or have uniform exponential growth. Theorem 1.1 has a similar corollary which implies not just uniform exponential growth but a uniform estimate on the Cheeger constant of the Cayley graph. Before stating it, we recall the following definitions:

Definition 1.2. *For a group Γ generated by a finite symmetric set Σ, we define its* ***uniform ℓ^2-Kazhdan constant*** *$\kappa_\Gamma(\Sigma)$ to be the largest $\varepsilon \geq 0$ such that*

$$\max_{s\in\Sigma} \|s \cdot f - f\|_2 \geq \varepsilon \cdot \|f\|_2$$

for all $f \in \ell^2(\Gamma)$. Similarly, we let $\kappa_\Gamma = \inf\{\kappa_\Gamma(\Sigma) : \Sigma$ is a finite symmetric generating set$\}$.

It is easy to see that $\kappa_{F_k} > 0$ for the free group F_k (e.g. see [10]). Another related quantity is the uniform Cheeger constant defined as follows:

Definition 1.3. *For a group Γ generated by a finite symmetric set Σ, the Cheeger constant of the Cayley graph $\mathcal{G}(\Gamma, \Sigma)$ is defined by*

$$h_\Gamma(\Sigma) = \inf\{\frac{\#\partial A}{\#A} : A \subseteq \mathcal{G}(\Gamma, \Sigma)\}$$

where $\partial A = A \setminus \cap_{s\in\Sigma} sA$ is the inner boundary of a subset A. And the ***uniform Cheeger constant*** *of the group Γ is defined by $h_\Gamma = \inf\{h_\Gamma(\Sigma) :$ Σ is a finite symmetric generating set$\}$.*

The above quantities are easily seen to satisfy the following relations:

$$\sqrt{8 \cdot h_\Gamma} \geq \sqrt{2} \cdot \kappa_\Gamma \geq \frac{\kappa_{F_2}}{d_\Gamma}.$$

In [1] (see also [10]), a finitely generated group is called *uniformly non-amenable* if $h_\Gamma > 0$. We thus have:

Corollary 1.2. *Let Γ be a finitely generated subgroup of $GL_n(K)$. Assume Γ is not amenable. Then $\kappa_\Gamma > 0$ and Γ is uniformly non-amenable.*

One should compare this result to [8], where it is shown that many arithmetic groups do not have a uniform lower bound for the Kazhdan constant with respect to an arbitrary unitary representation.

Corollary 1.3. *Under the same assumptions on Γ, there is a constant $\varepsilon = \varepsilon(\Gamma) > 0$ such that if Σ is a finite symmetric generating subset of Γ, then*

$$\#\Sigma^n \geq \#\Sigma \cdot (1 + \varepsilon)^n$$

for all positive integers n.

As in Eskin, Mozes and Oh's original proof, the proof of Theorem 1.1 makes use of the theory of arithmetic groups. However, when proving Theorem 1.1, we first obtain along the way a clear and short proof of the result of Eskin, Mozes and Oh which is very geometric in nature and does not use arithmetic groups (see Section 3.1 below). Arithmeticity is really required when one wants to find a free group instead of just a free semi-group because it is then crucial to obtain elements of Γ that play ping-pong with good "separation properties". Several new ingredients are needed in the proof of Theorem 1.1 such as the Borel–Harish-Chandra theorem, the argument behind Kazhdan–Margulis theorem and some facts from the geometry of symmetric spaces and Bruhat-Tits buildings. We shall outline some of these arguments in Section 3.

The general case reduces to the arithmetic one by the following:

Lemma 1.4. *For any finitely generated non-virtually solvable linear group Γ there is a global field $\mathbb{K}$, a finite set of valuations S of $\mathbb{K}$, a simple $\mathbb{K}$ algebraic group $\mathbb{G}$, and a homomorphism $f : \Gamma \to \mathbb{G}(\mathbb{K})$ whose image is Zariski dense and lies in $\mathbb{G}(\mathcal{O}_{\mathbb{K}}(S))$.*

Note that f is not injective in general. Here $\mathcal{O}_{\mathbb{K}}(S)$ is the ring of S-integers in the number field $\mathbb{K}$, and $\mathbb{G}(\mathcal{O}_{\mathbb{K}}(S))$ is the set of elements in $\mathbb{G}(\mathbb{K})$ whose matrix elements lie in $\mathcal{O}_{\mathbb{K}}(S)$ under some fixed faithful $\mathbb{K}$-representation of $\mathbb{G}$ in $\mathbb{SL}_n$.

For arithmetic groups we obtain the following stronger result:

Theorem 1.5. *Let $\mathbb{K}$ be a number field, S a finite set of places of $\mathbb{K}$ containing all Archimedean ones, and let $\mathbb{G}$ be a simple $\mathbb{K}$-algebraic group. Then there exists a constant $m = m(\mathbb{K}, S, \mathbb{G}) \geq 1$ with the following property. For any symmetric set Σ in $\mathbb{G}(\mathcal{O}_{\mathbb{K}}(S))$ with $e \in \Sigma$, which generates a Zariski dense subgroup Γ of $\mathbb{G}$, $d_\Gamma(\Sigma) \leq m$.*

Finally, let us also remark that the main result of [3], i.e. the connected case of the topological Tits alternative, can be deduced easily from 1.5.

2. Algebraic entropy and discrete subgroups

If Γ is a group, let $\mathcal{C}$ be the set of all finite (not necessarily symmetric) subsets Σ containing e and generating Γ.

Definition 2.1. *Two elements in a group are said to be* ***positively independent*** *if they generate a free semigroup. The* ***diameter of positive independence*** *of set Σ containing e is the quantity $d^{pi}(\Sigma) = \inf\{n \in \mathbb{N} : \Sigma^n$ contains two positively independent elements$\}$. Similarly, the diameter of positive independence of the group Γ is defined by $d^{pi}_\Gamma = \sup\{d^{pi}(\Sigma) : \Sigma \in \mathcal{C}\}$.*

The next definition is more standard:

Definition 2.2. *Assume Γ is finitely generated. For Σ in $\mathcal{C}$ we can define the* ***algebraic entropy*** *of the pair (Γ, Σ) to be the quantity $S_\Gamma(\Sigma) =$*

$\lim \frac{1}{n} \log(\#\Sigma^n)$. *Similarly, the algebraic entropy of* Γ *is defined by* $S_\Gamma = \inf_{\Sigma \in \mathcal{C}} S_\Gamma(\Sigma)$.

It is easy to see that $S_\Gamma(\Sigma)$ is either positive for all Σ in $\mathcal{C}$ or 0 for all Σ simultaneously. Accordingly, the group Γ is said to have exponential or sub-exponential growth. If $S_\Gamma > 0$, then Γ is said to have *uniform exponential growth.* It is a consequence of Tits' proof of the Tits alternative and some additional simple argument for solvable groups that for a linear group $\Gamma \leq GL_n(K)$ generated by a finite set Σ, either $d^{pi}(\Sigma) < +\infty$ (and Γ has exponential growth) or Γ is virtually nilpotent, hence $d^{pi}(\Sigma) = +\infty$ and Γ actually has polynomial growth. The latter quantities are related by the following inequality:

$$S_\Gamma \geq \frac{\log 2}{d_\Gamma^{pi}}$$

A. Eskin, S. Mozes and H. Oh proved in [7] that if $\Gamma \leq GL_n(K)$ is finitely generated non-virtually nilpotent then $d_\Gamma^{pi} < \infty$, hence $S_\Gamma > 0$. In general, the constant d_Γ^{pi} depends strongly on Γ (see the paragraph concluding this section) however, for discrete subgroups of Lie groups, as well as for non-relatively compact subgroups over non-Archimedean local fields we have the following uniform result. Note further that Σ is not assumed to be symmetric in the following statement:

Theorem 2.1. *For every integer* $d \geq 1$*, there is a constant* $m = m(d) \geq 1$ *with the following property. Let* k *be a local field and* $\Sigma \subset GL_d(k)$ *a subset which generates a non-virtually nilpotent group. Assume further that either:*

- *the group* $\langle\Sigma\rangle$ *is discrete, or*
- *the field* k *is non-Archimedean and* $\langle\Sigma\rangle$ *is not relatively compact.*

Then $d^{pi}(\Sigma) \leq m(d)$.

This implies:

Corollary 2.2. *(Entropy Gap for Discrete Subgroups) For any integer* $d \geq 1$*, there is a constant* $s = s(d) > 0$ *such that*

$$S_\Gamma > s$$

for all non-virtually nilpotent finitely generated discrete subgroups Γ *of* $GL_d(\mathbb{R}) \times GL_d(k_1) \times ... \times GL_d(k_n)$ *for any* $n \geq 0$ *and any non-archimedean local fields* $k_1, ..., k_n$.

We also prove the following uniform statement for linear groups over general fields:

Theorem 2.3. *For any* n *there is* $m = m(n) \geq 1$*, such that if* $d \leq n$ *and* $\mathbb{K}$ *is an algebraic extension of degree* $[\mathbb{K} : \mathbb{F}] \leq n$ *over a purely transcendental extension* $\mathbb{F}$ *of the prime field* $\mathbb{K}_0$*, and* $\Sigma \subset GL_d(\mathbb{K})$ *generates a non-virtually nilpotent group, then* $d^{pi}(\Sigma) \leq m$.

The restrictions on $[K:F]$ and on the dimension d are really necessary. In fact, even for $d=2$, it is possible to find a sequence Σ_n of finite symmetric sets in $SL_2(\overline{\mathbb{Q}})$ such that each Σ_n generates a non virtually nilpotent group, although no pair of elements in Σ_n^n generates a free semigroup (see [2]). Similarly, R. Grigorchuk and P. de la Harpe have exhibited in [9] a sequence of finitely generated non-virtually solvable subgroups Γ_n in $SL_{k_n}(\mathbb{Z})$ such that $\liminf S_{\Gamma_n}=0$ and $k_n \to +\infty$.

3. Proofs

In this section we sketch the proofs of the above results. Let k be a local field.

3.1. **Proximal elements.** Like in Tits' original proof of his alternative, one basic ingredient in all the results above is the so-called *ping-pong lemma*. This ensures that if two projective transformations a and b are in a suitable geometric configuration when acting on the projective space $\mathbb{P}(k^d)$, then a and b generate a free semigroup, or a free group. To describe this geometric configuration, we need the following definition:

Definition 3.1. *An element $g \in PGL_d(k)$ is called ε-contracting, for some $\varepsilon > 0$, if there exists a projective hyperplane H, called a repelling hyperplane, and a projective point v called an attracting point such that $d(gp, v) \leq \varepsilon$ whenever $p \in \mathbb{P}(k^d)$ satisfies $d(p, H) \geq \varepsilon$. Moreover g is called (r, ε)-proximal, for $r > 2\varepsilon$, if it is ε-contracting for some H and v with $d(H, v) \geq r$. Finally, g is called ε-very contracting (resp. (ε, r)-very proximal) if both g and g^{-1} are ε-contracting (resp. (r, ε)-proximal).*

The distance $d([x],[y])$ on $\mathbb{P}(k^d)$ is the standard distance $d([x],[y]) = \frac{\|x \wedge y\|}{\|x\|\|y\|}$ where $\|\cdot\|$ is a Euclidean norm on k^n if k is $\mathbb{R}$ or $\mathbb{C}$ and the supermum norm if k is non-Archimedean. We refer the reader to [3] for elementary properties of such projective transformations. We then have:

Lemma 3.1. *(The ping-pong lemma) Assume that a and b are (r, ε)-very proximal transformations, for some $r > 2\varepsilon$, and the attracting points of a and a^{-1} (resp. b and b^{-1}) are at least r apart from the repelling hyperplanes of b and b^{-1} (resp. a and a^{-1}), then a and b generate a free group.*

Such elements a and b will be called *ping-pong players*. Observe that the conditions imposed on a and b imply that the attracting points of a and b *must* be at least $r - 2\varepsilon$ apart. This *separation property* is a crucial difficulty encountered when trying to find generators of a free group as opposed to generators of a mere free semigroup. Indeed, if one only needs a free semigroup, then no condition on the distance between the two attracting points is necessary as the following version of the ping-pong lemma for semigroups show:

Lemma 3.2. *(The ping lemma) Assume* $\varepsilon \le \frac{1}{3}$ *and* $r > 4\varepsilon^2$. *Let* a *be an* (r, ε^3)*-proximal transformation with attracting fixed point* v *and repelling hyperplane* H. *Let* b *be a projective transformation such that* $bv \neq v$, $d(bv, H) \ge \varepsilon$ *and such that the global Lipschitz constant of* b *on* $\mathbb{P}(k^d)$ *satisfies* $Lip(b) \le \frac{1}{\varepsilon}$. *Then* a *and* ba *generate a free semigroup.*

To exhibit ε-contracting elements, it is useful to look at the Cartan decomposition of $SL_d(k)$ since the ratio between the highest and second to highest component in the diagonal part of the decomposition determines the contraction properties of the transformation g on $\mathbb{P}(k^d)$ (see [3]). When g is a diagonal matrix, then this ratio coincides with the ratio between the highest eigenvalue of g to the second highest, and the attracting point of g will be the direction of the highest eigenvector. This situation prevails when g is only assumed to be *quasi-diagonal*, meaning that the size of its operator norm is comparable to its highest eigenvalue. This is the ideal situation, because the attracting points of g being eigendirections, we have control upon them. In general, elements in a generating set Σ need not be simultaneously quasi-diagonal, however the following crucial proposition says that up to conjugating Σ and looking at a bounded power Σ^{d^2} it is possible to bound the norm of elements in Σ by the maximal eigenvalue.

For $y \in SL_d(k)$, let $\Lambda_k(y) = \max\{|\lambda|_k : \lambda \text{ is an eigenvalue of } y\}$[1]. For a bounded set Ω in $SL_d(k)$, let $\Lambda_k(\Omega) = \sup\{\Lambda_k(y), y \in \Omega\}$ and

$$E_k(\Omega) = \inf_{h \in SL_d(k)} \{\|h\Omega h^{-1}\|\}$$

where $\|\Omega\| := \sup_{y\in\Omega} \|y\|$ and $\| \ \|$ is the operator norm. The quantity $E_k(\Omega)$ is comparable (up to bounded powers) with the minimal exponential displacement of the set Ω acting on the symmetric space or building associated to $SL_d(k)$. Clearly $\Lambda_k(\Omega) \le E_k(\Omega)$.

Proposition 3.3. *There is a constant* $c = c(d) > 0$ *such that for any compact subset* Ω *in* $SL_d(k)$ *with* $e \in \Omega$ *we have*

$$\Lambda_k(\Omega^{d^2}) \ge c \cdot E_k(\Omega) \tag{3.1}$$

Furthermore, if k *is not Archimedean, the same holds with* $c = 1$.

Proposition 3.3 is a strong version of Proposition 8.5 of [7], while its proof is significantly simpler and shorter.

3.2. **Generation of free semigroups and a proof of the Eskin-Mozes-Oh theorem.** The above Proposition is the main step towards producing a proximal element in Σ^{d^2}. Its proof is a rather simple contrapositive argument. Together with some elementary properties of projective transformations as studied in [3], it is essentially enough to prove the result of [7], namely that $d_\Gamma^{pi} < +\infty$ for all non virtually solvable finitely generated linear

[1] the eigenvalue λ may not be in k but in a finite extension of it, however the absolute value on k extends uniquely to any algebraic extension, thus the notion $|\lambda|_k$ is meaningful

groups Γ, hence also uniform exponential growth for such Γ's. The ping-pong pair is obtained as follows.

Taking the Zariski closure and after moding out by the solvable radical, we can assume that the group Γ generated by Σ is Zariski dense in some semisimple algebraic group lying in SL_d. By Selberg's lemma we can assume that Γ is torsion free. Using Lemma 3.4 below, we see that, up to taking a bounded power of Σ, we may assume that Σ contains a non trivial semisimple element. Then at least one eigenvalue of this element is not a root of unity, hence there exists a local field k such that $\Gamma \leq SL_d(k)$ and $\Lambda_k(\Sigma) > 1 + \delta$ where $\delta > 0$ depends only on Γ. Let $\alpha \in \Sigma^{d^2}$ be such that $\Lambda_k(\alpha) = \Lambda_k(\Sigma^{d^2})$. By Proposition 3.3, one can conjugate Σ inside $SL_d(k)$ so that $\Lambda_k(\alpha) \geq c \cdot \|\Sigma\|$. Up to considering a suitable wedge power representation $V_i = \Lambda^i k^d$, we may assume that $\Lambda_k(A)/\lambda_k(A) \geq \Lambda_k(A)^{1/d^2}$ where $\lambda_k(A)$ is the maximum modulus of the second highest eigenvalue and $A = \Lambda^i(\alpha)$. After this operation we have $\|\Sigma\| \leq \left(\frac{\Lambda_k(A)}{c}\right)^d$. Applying Lemma 3.5 below we can conjugate further Σ in $SL(V_i)$ and get that for all n large enough (so that $(1+\delta)^{n/2d^2} > 3$ say), A^n is a $(1, 1/\Lambda_k(A)^{n/2d^2})$-proximal transformation with attracting fixed point v and repelling hyperplane H and is such that $\Lambda_k(A) = \|A\|$, while $\|\Sigma\| \leq \left(\frac{3\Lambda_k(A)}{c}\right)^{3d \cdot \dim^2 V_i}$. Since Γ is Zariski dense, not all elements from Σ can fix v. Applying Lemma 3.4 again, we may find an element B in some bounded power of Σ such that none of the powers B^j for $j = 1, ..., \dim V_i$ fixes v. But, as can be seen from Cayley Hamilton's theorem for instance, at least one of the B^j's must send v at least ε away from H where ε is at least some fixed bounded power of $\|B\|$, hence of $\Lambda_k(A)$ because $\|B\| \leq \|\Sigma\| \leq \left(\frac{3\Lambda_k(A)}{c}\right)^{3d \cdot \dim^2 V_i}$. Hence A^n and $B^j A^n$ are ping-players (i.e. generate a free semigroup) as soon as n is larger than a fixed constant depending only on d, c and δ. We can apply the ping lemma 3.2. $\square$

In order to find non-torsion semisimple ping-pong players in a bounded ball Σ^m we have just used the following lemma from [7]:

Lemma 3.4. *([7]) Let $\mathbb{G}$ be a Zariski connected algebraic group. Given a closed algebraic subvariety $X \subset \mathbb{G}$, there is an integer $k = k(\mathbb{G}, X)$ such that for any subset $\Sigma \subset \mathbb{G}$ with $e \in \Sigma$ generating a Zariski dense subgroup of $\mathbb{G}$, the set Σ^k is not contained in X.*

Also we made use of the following simple lemma:

Lemma 3.5. *Suppose $A \in SL_d(k)$ satisfies $\Lambda_k(A) \geq 2\lambda_k(A)$ where $\lambda_k(A)$ is the modulus of the second highest eigenvalue of A. Then the top eigenvalue λ_1 belongs to k, $|\lambda_1| = \Lambda_k(A)$ and there exists $h \in SL_d(\overline{k})$ with $\|h\| \leq 3^d \|A\|^{d^2}$ such that the matrix $A' = hAh^{-1}$ is such that $A'e_1 = \lambda_1 e_1$ and $A'H = H$ where $H = \langle e_2, ..., e_d \rangle$ and $\left\| A'_{|H} \right\| \leq \lambda_k(A)$.*

To obtain the uniformity in Theorem 2.1 we make use of the classical Margulis lemma which can be stated as follows:

Lemma 3.6. *(The Margulis lemma) There is a constant $\varepsilon = \varepsilon(d) > 0$ such that for every finite set Σ in $SL_d(\mathbb{R})$, if Σ generates a non virtually nilpotent discrete subgroup, then $E_{\mathbb{R}}(\Sigma) \geq 1 + \varepsilon$.*

By another compactness argument we finally obtain:

Proposition 3.7. *For every $d \in \mathbb{N}^*$ there is a constant $C = C(d) > 0$ and an integer $N = N(d) > 0$ such that for any finite subset Σ in $SL_d(k)$ with $e \in \Sigma$ such that Σ generates a non-virtually solvable group, if $E_k(\Sigma) > C$, then $d^{pi}(\Sigma) \leq N$.*

In particular the constant s in Corollary 2.2 depends on the Margulis constant $\varepsilon(d)$ and on the constant $c(d)$ from Proposition 3.3.

The argument sketched above treats the case of non-virtually solvable linear groups. For virtually solvable non-virtually nilpotent linear groups we apply a different argument using one dimensional affine representations instead of projective representations, which is based on some tools developed in [[4] Section 10] and in [2].

3.3. **Separation properties, arithmeticity and free subgroups.** Here we give some hints on the proof of our main result, Theorem 1.5. For the sake of simplicity, let us restrict ourselves to the case of Zariski-dense subgroups of $SL_d(\mathbb{Z})$. In the last paragraph of this section, we shall give some indications about the general case.

The main difficulty comes from the fact that in order to generate a free group rather than just a free semigroup, one should construct a very proximal element rather than just a proximal one. To do that, one needs both a good control on the norms of the generators and good separation properties. For the latter we shall need arithmeticity.

Proposition 3.3 supplies us, for each given Σ, with a conjugating element h in $SL_d(\mathbb{R})$ such that the norm of $h\Sigma h^{-1}$ is bounded in terms of $\Lambda(\Sigma)$. However, conjugating by h we "loose the arithmeticity". The first part of the proof of Theorem 1.5 consists in replacing the conjugating element h by some $\gamma \in SL_d(\mathbb{Z})$:

Proposition 3.8. *There are positive constants $c_1 = c_1(d)$ and $r_1 = r_1(d)$ such that for any subset Σ in $SL_d(\mathbb{Z})$ that generates a Zariski-dense subgroup of $SL_d(\mathbb{R})$ there exists $\gamma \in SL_d(\mathbb{Z})$ such that*

$$\left\|\gamma\Sigma\gamma^{-1}\right\| \leq c_1 \cdot E(\Sigma)^{r_1}$$

The proof of Proposition 3.8 relies on the following quantitative variant of Kazhdan–Margulis theorem[2] which was suggested to us by G.A. Margulis:

[2]Note that Kazhdan-Margulis theorem (which states merely the existence of unipotents) is trivial in our case because our lattice is arithmetic, however we need the quantitative estimate.

Lemma 3.9. *There are positive constants k_0, l_0 such that for any $h \in SL_d(\mathbb{R})$ the group $hSL_d(\mathbb{Z})h^{-1} \leq G$ contains a non-trivial unipotent u with*

$$\|u - 1\| \leq l_0 \cdot \|\pi(g)\|^{-k_0}$$

where $\pi : G \to SL_d(\mathbb{R})/SL_d(\mathbb{Z})$ is the canonical projection and $\|\pi(g)\| = \min_{\gamma \in SL_d(\mathbb{Z})} \|g\gamma\|$.

The main part of the proof of Theorem 1.5 relies on the construction of a very proximal element in a bounded power of $\gamma\Sigma\gamma^{-1}$ acting on the projective space of a corresponding wedge power. This is done in three steps, in the first we construct a proximal element, in the second a very contracting one and in the third a very proximal one.

Note that, using Lemma 3.4, we can find a semisimple torsion free element inside a bounded power Σ^{k_1} for some constant k_1. The eigenvalues of this element are algebraic integers of bounded degree, hence $\Lambda(\Sigma^{k_1}) \geq 1 + \varepsilon_1$ for some constant $\epsilon_1 > 0$. Combining this observation with Proposition 3.8 we may therefore assume $\|\Sigma\| \leq \Lambda(\Sigma)^{r_2}$ for some constant $r_2 = r_2(d) > 0$, after changing Σ into $\gamma\Sigma^N\gamma^{-1}$ for some power $N = N(d)$.

We now find $\alpha \in \Sigma$ such that $\Lambda(\alpha) = \Lambda(\Sigma)$ and make Γ act on the (irreducible) wedge power representation $V_i = \Lambda^i\mathbb{C}^d$, where i is chosen so that $\Lambda(A)/\lambda(A) \geq \Lambda(\Sigma)^{1/d}$ and $\lambda(A)$ is the maximum modulus of the second highest eigenvalue and $A = \Lambda^i(\alpha)$. Changing Σ into its image under this representation, we get

$$\|\Sigma\| \leq \Lambda(A)^{r_3}$$

for some other constant $r_3 = r_3(d) > 0$. This produces the desired proximal element, hence concludes Step 1.

In order to find a very contracting element in a bounded power of Σ we need to find an element B with good separation properties with respect to A, namely a B that sends one eigenvector of A far from some hyperplane spanned by $d-1$ eigenvectors of A.

Part of the problem is to make the word "far" more explicit. The condition that a matrix sends a vector outside a given hyperplane (with no condition on how far) is an algebraic one and is easily fulfilled thanks to Lemma 3.4. If the matrix has integer coefficients, as it will be the case thanks to Proposition 3.8 above, then it is possible to estimate this gap in terms of the norm of the matrix and the arithmetic complexity of the rationally defined hyperplane. This is the content of Lemma 3.10 below. For a vector $u \in \overline{\mathbb{Q}}^d \subset \mathbb{C}^d$ we denote $\|u\|_m = \max\{\|\sigma(u)\|, \sigma \in Gal(\overline{\mathbb{Q}}, \mathbb{Q})\}$.

Lemma 3.10. *Let $u_1, ..., u_d$ be d vectors in $\overline{\mathbb{Q}}^d$ whose coordinates are algebraic integers of degree at most $n \geq 1$, and let $M := \max_i \|u_i\|_m$. If H is the hyperplane spanned by $u_2, ..., u_d$ and $B \in SL_d(\mathbb{Z})$, then either $Bu_1 \in H$, or*

$$d([Bu_1], [H]) \geq \frac{1}{\|B\|^{n^d} M^{2dn^d}}$$

By Lemma 3.4 we can find B (in a bounded power of Σ) which is in "general position" with respect to the eigenvectors of A. We then prove:

Proposition 3.11. *There is $N = N(d)$ such that the following holds. Given $q \in \mathbb{N}$, there is a constant $m_0 > 0$ and there is $B \in \Sigma^N$ such that the element $A^{m_0} B A^{-m_0}$ is $\Lambda(A)^{-q}$-very contracting, with both attracting points lying at a distance at most $\Lambda(A)^{-q}$ from $\overline{v}$ – the eigendirection corresponding to the maximal eigenvalue of A.*

The proof of Lemma 3.11 relies on the following characterization of contracting elements in terms of their Lipschitz constants.

Lemma 3.12 (See Lemma 3.4, Lemma 3.5 and Proposition 3.3 in [4])**.** *Let $\epsilon \in (0, \frac{1}{4}]$, $r \in (0, 1]$. Let $g \in SL_n(\mathbb{R})$ and let $k_g a_g k'_g$ be a KAK expression for g where $a_g = diag(a_1(g), a_2(g), \dots, a_n(g))$, $a_i(g) \geq a_{i+1}(g) > 0$.*

1. *If $a_2(g)/a_1(g) \leq \epsilon$ then g is ϵ/r^2-Lipschitz outside the r-neighborhood of the repelling hyperplane span$\{{k'}_g^{-1}(e_i)\}_{i=1}^n$.*
2. *If the restriction of g to some open neighborhood $O \subset \mathbb{P}^{n-1}(\mathbb{R})$ is ϵ-Lipschitz, then $a_2(g)/a_1(g) \leq \epsilon/2$.*
3. *If $a_2(g)/a_2(g) \leq \epsilon^2$ then g is ϵ-contracting, and vice versa, if g is ϵ-contracting, then $a_2(g)/a_2(g) \leq 4\epsilon^2$.*

The third step is then to obtain a very proximal element by multiplying the very contracting one $A^{m_0} B A^{-m_0}$ by some bounded word in the generators. We want to"separate" the repelling hyperplanes from the attracting points. Note that we do not have any information on the position of the repelling hyperplanes of $A^{m_0} B A^{-m_0}$, but we do have a good estimate on the position of its attracting points. We find the right multiplying element using a simple argument based on the pigeon-hole principle, and the fact that if d arithmetically defined vectors are linearly independent in $\mathbb{C}^d$ then we can bound from below their maximal distance to an arbitrary hyperplane in terms of their arithmetic complexities and norms.

In the last part of the proof of Theorem 1.1, we conjugate our very proximal element by a suitable bounded word in the generators and obtain a second very proximal element which plays ping-pong with the first one. The argument for finding the appropriate conjugating element is quite similar to the argument for making the very contracting element a very proximal one.

Let us now say some words about the general case, i.e. when Γ is Zariski-dense in $\mathbb{G}(\mathcal{O}_{\mathbb{K}}(S))$. By the Borel–Harish-Chandra theorem, $\mathbb{G}(\mathcal{O}_{\mathbb{K}}(S))$ is an arithmetic lattice in some semisimple Lie group $G \leq \prod_{v \in S} SL_d(\mathbb{K}_v)$ over a product of local fields. The absolute value on each $\mathbb{K}_v$ extends uniquely to any algebraic extension. For $g = (g_v)_{v \in S}$ we define $\|g\| = \max \|g_v\|_v$ and $\Lambda(g) = \max(\Lambda_{\mathbb{K}_v}(g_v))$. We obtain the general version of Proposition 3.8 from Proposition 3.3 in two steps. The fist step consists in replacing the conjugating element $h \in \prod_{v \in S} SL_d(\mathbb{K}_v)$ by some element $g \in G$. To do that we exploit theorems of Mostow and Landvogt about totally geodesic embeddings of symmetric spaces, and some simple geometric argument using orthogonal projections on convex subsets in CAT(0) spaces. In a second step, we replace the element g by some element $\gamma \in \mathbb{G}((\mathcal{O}_{\mathbb{K}}(S))$. This step is quite simple in the case where $\mathbb{G}$ is anisotropic, i.e. when $G/\mathbb{G}(\mathcal{O}_{\mathbb{K}}(S))$ is compact, because then we can pick γ at a bounded distance from g. In the isotropic case we use a generalized version of Lemma 3.9.

The rest of the proof goes along the same lines sketched above. The guiding idea is that the distance between arithmetically defined geometric objects is either 0 or can be bound from below in terms of their arithmetic complexity.

Remark 3.1. *Let us note that the uniform bound for the independence diameter that our proof gives for a subgroup of an arithmetic lattice* $\Delta = \mathbb{G}(\mathcal{O}_{\mathbb{K}}(S)) \leq G$ *does strongly depend on* Δ *and not just on the ambient Lie group* G*. In case* Δ *is a uniform lattice, it depends on the the diameter and the injectivity radius of the associated locally symmetric manifold* $K\backslash G/\Gamma$*. However, for non-uniform arithmetic lattices* $\Delta \leq G$ *we do obtain a uniform constant depending only on* G*.*

References

[1] G.N. Arzhantseva, J. Burillo, M. Lustig, L. Reeves, H. Short, E. Ventura, *Uniform non-amenability*, Advances in Math., (2005).

[2] E. Breuillard, *A note on exponential growth for solvable groups*, preprint.

[3] E. Breuillard, T. Gelander, *On dense free subgroups of Lie groups*, J. Algebra, **261** , no. 2, pp. 448–467, (2003).

[4] E. Breuillard, T. Gelander, *A topological Tits alternative*, to appear in the Annals of Math.

[5] E. Breuillard, T. Gelander, *A uniform Tits alternative*, in preperation,

[6] E. Breuillard, T. Gelander, A. Salehi-Golsefidy, *On uniform exponental growth in general characteristic*, an appendix to [5], in preparation.

[7] A. Eskin, M. Mozes, H. Oh, *On uniform exponential growth for linear groups in characteristic zero*, Invent. Math. **160**, no. 1, pp. 1–30, (2005).

[8] T. Gelander, A. Zuk, *Dependence of Kazhdan constants on generating subsets*, Israel J. Math. 129 (2002), 93–98.

[9] R. Grigorchuk, P. de la Harpe, *Limit behaviour of exponential growth rates for finitely generated groups*, in Essays on geometry and related topics, Vol. 1, 2, 351–370, Monogr. Enseign. Math., **38**, (2001).

[10] Y. Shalom, *Explicit Kazhdan constants for representations of semisimple and arithmetic groups*, Ann. Inst. Fourier, **50** (2000), no. 3, 833–863.

[11] J. Tits, *Free subgroups of Linear groups*, Journal of Algebra **20** (1972), 250-270.

E-mail address: `emmanuel.breuillard@math.univ-lille1.fr`

E-mail address: `tsachik.gelander@yale.edu`