Diophantine geometry and uniform growth of finite and infinite groups

Emmanuel Breuillard*

Abstract. We survey a number of recent results regarding the geometry and spectra of finite and infinite groups. In particular we discuss the uniform Tits alternative for infinite linear groups highlighting the inputs from diophantine geometry and the consequences for finite groups.

Mathematics Subject Classification (2010). Primary 22E40; Secondary 11G50.

Keywords. Diophantine geometry, heights, small points, Lehmer conjecture, exponential growth, amenability, Tits alternative, spectral gaps, approximate groups.

1. Uniform growth for infinite groups and Lehmer's conjecture

Let Γ be a finitely generated group and S a finite symmetric (i.e. $S = S^{-1}$) generating set containing the identity. The study of the *growth of* Γ is the study of the number of elements in the n-th fold product set $S^n = S \cdot \cdots \cdot S \subset \Gamma$ as a function of n. The set S^n is also the ball of radius n in the Cayley graph $Cay(\Gamma, S)$ of Γ relative to the generating set S, namely the graph with vertex set Γ in which two group elements x, y are linked by an (undirected) edge if $x = ys$ for some $s \in S \setminus \{1\}$. A simple way to quantify the growth of Γ with respect to S is to introduce the *exponential growth rate*

$$\rho_S := \lim_{n \to +\infty} |S^n|^{1/n} \tag{1.1}$$

The limit exists by sub-multiplicativity $|S^{n+m}| \leqslant |S^n| \cdot |S^m|$. Note that $\rho_S \leqslant |S^n|^{1/n}$ for each $n \geqslant 1$. The group Γ is said to be of exponential growth if $\rho_S > 1$. While ρ_S typically depends on S, the property that it is strictly bigger than 1 is easily seen to be independent of the choice of generating set S. Similarly one says that Γ has polynomial growth if there are constants $C, d > 0$ independent of n such that $|S^n| \leqslant Cn^d$ for all $n \geqslant 1$.

The growth of groups has been widely studied since the 1950's and the initial works of Svarc [92] and Milnor [77] who noticed that fundamental groups of neg-

*The author was partially supported by ERC Grant GADA 208091 and ANR-11-BS01-013, ANR-12-BS01-0011, ANR-13-BS01-0006.

atively curved compact manifolds have exponential growth. See [49, 50] and [75] for thorough recent expository texts. We begin with a quick historical review of some important developments regarding group growth:

- Milnor and Wolf [78] proved that nilpotent groups have polynomial growth and that solvable groups have either exponential growth or are virtually nilpotent (i.e. contain a nilpotent subgroup of finite index). See §5.1 below.

- Tits showed that linear groups, i.e. subgroups of $GL_n(K)$ over a (commutative) field K have exponential growth unless they are virtually nilpotent, a consequence of his famous alternative: any linear group either contains a non-abelian free group, or is virtually solvable [96].

- Gromov [52] famously proved that every finitely generated group with polynomial growth is virtually nilpotent.

- Grigorchuk [46], answering by the negative a question of Milnor, gave the first example of a group with *intermediate growth*, i.e. whose growth is neither polynomial nor exponential: the so-called *Girgorchuk group* (see [47]). Recently Bartholdi and Erschler [5], using ingenious variants of Grigorchuk's construction, built for each $\alpha \in (.77, 1)$ groups for which $e^{c_1 n^\alpha} \leqslant |S^n| \leqslant e^{c_2 n^\alpha}$ for some constants $c_1, c_2 > 0$. Interesting groups with oscillating behaviors also exist (see [59, 5, 29]).

- Kleiner [65] gave a new proof of Gromov's theorem using harmonic functions and arguments closely related to the work of Colding and Minicozzi [31] in differential geometry. These arguments were pushed further by Shalom and Tao [91] to show that if $|S^n| \leqslant n^{\varepsilon(\log\log n)^\varepsilon}$ for some small absolute constant $\varepsilon > 0$, then the group is virtually nilpotent.

- The Grigorchuk *gap conjecture* asserts that if $|S^n| \leqslant e^{n^\alpha}$ for some $\alpha < \frac{1}{2}$, then the group has polynomial growth and hence is virtually nilpotent ([49, 48]).

A finitely generated group is said to have *uniform exponential growth* if

$$\inf_S \rho_S > 1,$$

where S varies among all (finite symmetric) generating subsets of the group. Gromov [53, Remark 5.2.] asked in the early eighties whether every group with exponential growth has uniform exponential growth. The answer is no. The first example was given more than a decade later by J.S. Wilson [101]. He built a group Γ containing a non-abelian free subgroup, and hence having exponential growth, and subsets $S_n := \{1, a_n^{\pm 1}, b_n^{\pm 1}\}$ generating Γ such that $\rho_{S_n} \to 1$ as $n \to +\infty$. Wilson's group is a subgroup of the group of automorphisms of a rooted tree (as is Grigorchuk's group by the way). It is known however that hyperbolic groups [60], solvable groups [83], linear groups in characteristic zero [39] or positive characteristic [15] have uniform exponential growth when they have exponential growth.

Although non virtually nilpotent linear groups have uniform exponential growth, the exponential growth rate ρ_S can be arbitrarily close to 1 when S and the group are allowed to vary. This fact, observed by Grigorchuk and de la Harpe in [51], can be seen as a consequence of the existence of the Grigorchuk group of intermediate growth. Indeed consider the Grigorchuk group G, generated by the usual four generators a, b, c, d (see e.g. [49, p 21]) and list the relations of G as reduced words in four letters of non-decreasing length $(w_n)_{n\geqslant 1}$. Then $G = \langle a, b, c, d | w_1, w_2, \dots, w_n, \dots \rangle$ is a presentation of G. Truncate this presentation after the n-th relator: we get this way a finitely presented group G_n. Clearly G_n surjects onto G and converges to G in the topology of marked groups: this means in particular that a ball $B_G(1, R)$ of radius R centered at the identity in G will be in bijection with the same ball $B_{G_n}(1, R)$ in G_n provided n is large enough and R is fixed. Consequently:

$$\rho_{S,G_n} \leqslant |B_{G_n}(1, R)|^{1/R} = |B_G(1, R)|^{1/R} = e^{\varepsilon(R)},$$

where $\varepsilon(R)$ tends to 0 as R tends to infinity, because G has sub-exponential growth. Grigorchuk and de la Harpe [51, 7] establish that each G_n has a quotient Γ_n containing the direct product of a finite number (increasing with n) of copies of a non-abelian free group as a subgroup of finite index. In particular $\rho_{S,G_n} \geqslant \rho_{S,\Gamma_n} > 1$. Moreover the Γ_n are clearly linear, since they contain a linear group of finite index. In conclusion:

Fact 1: *There are linear groups of exponential growth $\Gamma_n \leqslant GL_{d_n}(\mathbb{Z})$ each generated by a set S_n of 4 matrices and their inverses such that ρ_{S_n} tends to 1 as n tends to infinity.*

As far as we know it is an open problem to show that such a phenomenon of slow exponential growth arises as well in the class of all Gromov hyperbolic groups. However we conjecture that this cannot happen for linear groups of bounded dimension:

Conjecture 1.1 (Growth conjecture). *Given $d \in \mathbb{N}$, there is $\varepsilon(d) > 0$ such that for every field K and every finite subset $S \subset GL_d(K)$, either $\rho_S = 1$ and $\langle S \rangle$ is virtually nilpotent, or*

$$\rho_S > 1 + \varepsilon(d).$$

The examples of Grigorchuk and de la Harpe described above imply that $\varepsilon(d)$ must tend to 0 as d tends to infinity. Besides, their examples contain a direct product of a large number of copies of the free group, hence cannot be linear in bounded dimension, i.e. $d_n \to +\infty$.

In [13] we observed the following:

Fact 2: *The Growth conjecture implies the Lehmer conjecture.*

Let us recall the Lehmer conjecture. Given an algebraic number x with minimal polynomial $\pi_x = a_d X^d + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$, write $\pi_x = a_d \prod_1^d (X - x_i)$ and define the Mahler measure of π_x as

$$M(\pi_x) := |a_d| \prod_{|x_i| \geqslant 1} |x_i|$$

Lehmer's conjecture (initially stated as a problem) asserts that $M(\pi_x)$ ought to be bounded away from 1 unless it is equal to 1. Kronecker's theorem tells us that $M(\pi_x) = 1$ if and only if x is a root of unity (i.e. π_x is a cyclotomic polynomial). Hence Lehmer's conjecture is the statement that there is some absolute $\varepsilon > 0$ such that

$$M(\pi_x) > 1 + \varepsilon,$$

for every algebraic number $x \in \overline{\mathbb{Q}}$, which is not a root of unity. The smallest known Mahler measure is the Mahler measure of the so-called Lehmer polynomial $X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1$, which is approximately 1.17628. Somewhat surprisingly this number coincides with the growth rate of the $(2, 3, 7)$ triangle group $\langle s, t, u | s^2 = t^2 = u^2 = 1, (st)^2 = (tu)^3 = (us)^7 = 1 \rangle$ which is also the discrete subgroup of isometries of the hyperbolic plane of smallest possible co-volume (see [41]).

Fact 2 above can be easily seen by considering the following set of matrices:

$$S_x := \{ \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}^{\pm 1}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{\pm 1}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \}. \tag{1.2}$$

A simple calculation (see [13, §7]), involving estimating the number of points of height at most n in the ring $\mathbb{Z}[x]$, $x \in \mathbb{C}$, shows that

$$M(\pi_x) \geqslant \rho_{S_x} \tag{1.3}$$

where ρ_{S_x} is the rate of exponential growth of S_x. There is no equality in general in (1.3) because $M(\pi_x)$ can be large, while $\rho_{S_x} \leqslant 3$ since there are only two generators and their inverses. But there is equality in some cases, for example when x is a Salem number in the interval $[1, 2]$. It can easily be shown that $\langle S_x \rangle$ is virtually nilpotent if and only if x is a root of unity. If x is transcendental then $\langle S_x \rangle$ is isomorphic to the wreath product $\mathbb{Z} wr \mathbb{Z}$ and thus ρ_{S_x} is bounded away from 1. If x is not an algebraic unit or has a Galois conjugate $\sigma(x)$ such that $|\sigma(x)| > 1 + \eta$, then it is straightforward to establish a lower bound on ρ_{S_x} of the form $1 + \varepsilon(\eta)$, where $\varepsilon > 0$ depends only on η (see [13]). However there are algebraic numbers all of whose conjugates are close to the unit circle.

Note that for every possible choice of x, the group $\langle S_x \rangle$ in this example is solvable of derived length 2. Somewhat surprisingly, it turns out that the solvable case is the most difficult one. Indeed we have shown the following:

Theorem 1.2 (Growth gap [18, 17]). *There is $\varepsilon = \varepsilon(d) > 0$ such that given any field K and any finite symmetric set S containing 1 in $GL_d(K)$ and generating a non virtually solvable subgroup,*

$$\rho_S > 1 + \varepsilon.$$

Again we see that $\varepsilon(d)$ must tend to 0 as d tends to infinity, because the examples given above of Grigorchuk and de la Harpe contain a free subgroup, hence are not virtually solvable.

Theorem 1.2 is deduced from a more general statement, the uniform Tits alternative, which we discuss further below. At the heart of its proof lies some diophantine geometry and the behavior of large Galois orbits of algebraic numbers of small height. Earlier results in this direction, in particular Eskin-Mozes-Oh [39] and its strengthening by Gelander and the author [15], were focusing on proving a uniform lower bound on ρ_S where the matrix entries of S were constrained within a certain fixed finitely generating ring (this is in particular the situation when S varies among the generating sets of a fixed finitely generated subgroup). The main novelty of Theorem 1.2 is the uniformity in the field of definition of the subgroup $\langle S\rangle$. Of course, this is where the interplay with number theory comes in.

It is not the first time that a connection between the exponential growth rate of groups and some properties of algebraic numbers is made. For example Cannon [30] observed that the exponential growth rate ρ_S of the fundamental group of a closed surface of genus $g \geqslant 2$ in its standard presentation as $\langle a_1, \dots, a_g, b_1, \dots, b_g | \prod_{i=1}^{g} [a_i, b_i] = 1\rangle$ is a Salem number, i.e. an algebraic number having only one conjugate outside of the closed unit disc and at least one on the unit circle. More generally it is known [42, Chp 9.] that Gromov hyperbolic groups such as fundamental groups of closed hyperbolic manifolds admit a rational growth series, and thus the associated growth rates are algebraic numbers. See also the nice survey [41].

We end this section with some suggestions for further research. It can be easily seen, thanks to Theorem 1.2 that the growth conjecture reduces to the case of $GL_2(\mathbb{C})$ and even to the subgroups $\langle S_x\rangle$ considered above. In light of this it would be interesting to determine whether the converse to Fact 2 above holds, i.e. whether the Growth and the Lehmer conjecture are equivalent. This seems highly plausible and very likely related to Bernoulli convolutions. Another interesting problem would be to verify that Theorem 1.2 extends to sub-semi-groups.

2. Uniform Tits alternative and uniform spectral gap estimates

The growth gap theorem (Theorem 1.2) above is a direct consequence of the following uniform Tits alternative:

Theorem 2.1 (Uniform Tits alternative [18, 17]). *Given $d \in \mathbb{N}$, there is $N = N(d) \in \mathbb{N}$ such that if K is a field and S is a finite subset of $GL_d(K)$ with $S = S^{-1}$ and $1 \in S$, then*

- *either $\langle S\rangle$ is virtually solvable,*

- *or S^N contains two generators of a non-abelian free subgroup.*

That Theorem 1.2 follows from this is clear, because $\rho_S \geqslant \rho_{S^N}^{1/N} \geqslant 3^{1/N}$, where we have the last inequality, because S^N contains a pair $\{a, b\}$ generating a free subgroup.

Recall that the Tits alternative ([96, 62] first conjectured by Bass and Serre) asserts that every finitely generated linear group admits a non-abelian free subgroup unless it is virtually solvable. It is an alternative, because the two cases are mutually exclusive: non-abelian free subgroups do not contain solvable subgroups of finite index.

The proof of J. Tits uses the dynamics of powers of linear transformations on projective space and the so-called *ping-pong lemma*, well-known to hyperbolic geometers since Fricke and Klein. See [14, 62] for expositions. Theorem 2.1 is thus a strengthening of the Tits alternative, in which the generating pair for the free subgroup is shown to arise already in a ball of universally bounded radius in the Cayley graph of the linear group $\langle S \rangle$.

Theorem 2.1 improves on an earlier result of Gelander and the author [15] in which the bound N was proven to be uniform as S varies among the generating sets of a fixed linear group. That was the same kind of uniformity as was obtained by Eskin-Mozes-Oh [39] for the rate of growth (as remarked in the situation of Theorem 1.2 above): it assumes that the matrix entries of S lie in a fixed finitely generated ring. The key point in Theorem 2.1 is the uniformity of N in the field K. This new uniformity is intimately linked to number theory and as we will see below to properties of a certain height (in the sense of Diophantine geometry) on the representation variety of the free group in GL_d over $\overline{\mathbb{Q}}$. It is also key to proving uniform spectral gap and diameter estimates for finite quotients such as $SL_d(\mathbb{F}_p)$ as shown in work of Gamburd and the author [19].

The Tits alternative [96] implies that finitely generated non virtually solvable linear groups are non-amenable, because they contain a free subgroup. In a similar way, Theorem 2.1 shows that this non-amenability is uniform when the generating set varies. The non-amenability of a group can be quantified in terms of so-called Kazhdan constants

$$\kappa(S, \pi) := \inf_{f \in \mathcal{H}_\pi, ||f||=1} \max_{s \in S} \{||\pi(s)f - f||\} \tag{2.1}$$

with respect to a set S and a unitary representation π with Hilbert space $\mathcal{H}_\pi$. A discrete group Γ is said to be *non-amenable* if

$$\kappa(S, \lambda_\Gamma) > 0$$

for some (hence all) finite subset S of Γ, where λ_Γ is the left regular representation of Γ, i.e. the unitary representation with Hilbert space $\ell^2(\Gamma)$ defined by

$$\lambda_\Gamma(g)f(x) = f(g^{-1}x).$$

We can now state some spectral corollaries of Theorem 2.1.

Corollary 2.2. *(uniform non-amenability) There is $\varepsilon = \varepsilon(d) > 0$ such that if K is a field and $S \subset GL_d(K)$ a finite subset, either $\langle S \rangle$ is virtually solvable, or $\kappa(S, \lambda_{\langle S \rangle}) > \varepsilon$.*

That a uniform Tits alternative would imply such a spectral bound was observed by Shalom in [90, Theorem 8.4] in the context of hyperbolic groups. We now discuss further similar spectral bounds, all inspired by [90] and [80]. A discrete group Γ is said to have Kazhdan property (T) if there is a finite subset S and a uniform $\varepsilon = \varepsilon_S > 0$ such that $\kappa(S, \pi) > \varepsilon$ for every unitary representation π of Γ without invariant vectors. Usually there is no uniform lower bound on ε_S independent of the choice of S among generating subsets of a fixed group with property (T) (although that remains an open problem from $\mathrm{SL}_3(\mathbb{Z})$). Gelander and Zuk [40] showed that no such lower bound exists in the case when Γ has a non-discrete image in a connected topological group.

However if we restrict the set of representations to those coming from the ambient group, one can sometimes obtain a uniform lower bound. Indeed Theorem 2.1 implies, via the well-known *tensor power trick* (see [79, 33]):

Corollary 2.3. *(Uniform Kazhdan constant) Given $d \in \mathbb{N}$ there is $\varepsilon = \varepsilon(d) > 0$ such that the following holds. If G is a real Lie group with $\dim(G) \leqslant d$ and π is a unitary representation of G which is strongly L^p, then for every finite subset $S \subset G$ generating a non-virtually solvable discrete subgroup*

$$\kappa(S, \pi) > \frac{\varepsilon}{\sqrt{p}}.$$

Recall that a unitary representation π is called strongly L^p if there is a dense subspace of vectors $\xi \in \mathcal{H}_\pi$ whose matrix coefficients $g \mapsto \langle \pi(g)\xi, \xi \rangle$ belong to $L^p(G)$ for each ξ. M. Cowling [32] proved that for every simple Lie group with property (T) (e.g. $G = SL_n(\mathbb{R})$, $n \geqslant 3$) there is some $p_0 > 0$ such that every unitary representation of G without non zero invariant vectors is strongly L^{p_0}. See [70, 82] for the value of $p_0(G)$. Hence in this case $\kappa(S, \pi)$ can be bounded from below independently of π.

We conclude this section with a natural suggestion for further research. That is to give good bounds on $\varepsilon(d)$ and $N(d)$ from Theorems 1.2 and 2.1. The proof of the uniform Tits alternative given in [16, 18, 17] is effective, except at one point (the constant in [16, Lemma 2.1(b)] and Lemma 3.7 below). However even this constant can be made effective although with a relatively poor bound. At any case it would be interesting to work out an explicit lower bound on $\varepsilon(d)$ in terms of d only and compare it to the upper bound given by the examples of Grigorchuk and de la Harpe described in the previous section.

3. Heights on character varieties of semi-simple groups

3.1. A reformulation in terms of first order logic. The uniform Tits alternative (Theorem 2.1 above) for subgroups of GL_d is uniform over all fields: the length of the two words giving rise to generators of a free subgroup is universally bounded in terms of d only. Fields of different characteristic have to be dealt with independently, but it turns out that if the field has characteristic $p > 0$, then the uniformity in Theorem 2.1 is much easier to establish, is uniform in p, and requires no significantly new ingredient than what was already known from the previous uniformity result by Gelander and the author [15]. So in what follows we will focus on the zero characteristic case. It turns out that proving that the bound $N(d)$ holds uniformly over all fields of characteristic zero is equivalent to proving it for the field of algebraic numbers $\overline{\mathbb{Q}}$. This can be seen in a number of ways. For example by specialization. One other way is to view the statement of Theorem 2.1 as a countable union of statements expressible in first order logic. Let us be more precise.

To begin with, the condition on the set S viewed as a k-tuple of elements in GL_d for $\langle S\rangle$ to be virtually solvable is an algebraic condition: it defines a certain closed algebraic subvariety of $(GL_d)^k$, which we denote by $\mathcal{V}_{sol}$. In fact virtually solvable subgroups of GL_d in characteristic zero admit a subgroup of bounded index (i.e. $< c(d)$) which is conjugate to a subgroup of the upper-triangular matrices. Hence $\langle S\rangle$ is virtually solvable if and only if a certain number of words with letters in S and bounded length have a common fixed point in the flag variety.

On the other hand, to say that no two words w_1, w_2 of length at most $N(d)$ can ever generate a free subgroup is equivalent to say that there is an integer n, such that for all possible choices of w_1, w_2 among words of length at most $N(d)$ with letters in S, one can always find a non-trivial word of length at most n in the free group, such that $w(w_1(S), w_2(S)) = 1$. Clearly this is a finite set of algebraic conditions on S viewed as a k-tuple in $(GL_d)^k$. Call this subvariety $\mathcal{W}_n$.

Theorem 2.1 is the statement that for each integer n, $\mathcal{W}_n$ is contained in $\mathcal{V}_{sol}$. This implication is in itself a statement of first order logic, because the algebraic varieties involved are defined over $\mathbb{Q}$. In particular if it holds for some algebraically closed field of characteristic zero, it holds for all of them, because any two algebraically closed field with the same characteristic have the same first order theory.

The discussion regarding $\mathcal{V}_{sol}$ shows that there is an integer n_0 depending on d only such that $\mathcal{V}_{sol}(\mathbb{C}) \subset \mathcal{W}_{n_0}(\mathbb{C})$. Now Theorem 2.1 tells us that this is an equality. So finally Theorem 2.1 can be reformulated as the statement that

$$\mathcal{V}_{sol} = \mathcal{W}_n$$

for each integer $n \geqslant n_0(d)$.

Note in passing that Theorem 2.1 cannot be deduced automatically by logical compactness from the original Tits alternative. The reason is that the condition

that two matrices generate a free subgroup is not expressible in first order logic: it is a countable union of first order logic statements. Indeed it is very hard in general to understand the locus of tuples, say in $(GL_d)^k$, which generate a free subgroup. Not much can be said on this set even in the case of GL_2.

Anyways, reducing (the characteristic zero case of) Theorem 2.1 to the field of algebraic numbers $\overline{\mathbb{Q}}$ allows to introduce the theory of heights and take advantage of known results in Diophantine geometry, in particular regarding the action of the Galois group. For this purpose, we introduced in [16] a certain conjugation invariant normalized height $\widehat{h}$ on $(GL_d)^k$, to be discussed below.

As we saw in Section 1, the uniform growth of linear groups is closely related to the properties of algebraic numbers of high degree and small height, in particular to the Lehmer conjecture. There the Lehmer conjecture was the obstacle to prove uniform growth. This situation can be reversed in the non solvable case, by first establishing a strong analogue of the Lehmer conjecture for this normalized height $\widehat{h}$. Let us first set up some notation.

3.2. A normalized height on reductive groups. In this paragraph we discuss the Height gap theorem (Theorem 3.4 below), which is the key ingredient for the uniformity in the field in the proof of the uniform Tits alternative.

Let $\mathbb{G}$ be a connected reductive algebraic group defined over a number field K (such as $\mathbb{G} = GL_d$). Let (ρ, W) be a faithful linear representation of $\mathbb{G}$. Let V_K be the set of places of K, i.e. equivalence classes of absolute values on K. Associated to each $v \in V_K$ is a local field K_v, the completion of K with respect to v, and an absolute value $|\cdot|_v$ defined on an algebraic closure $\overline{\mathbb{Q}}_v$ of K_v. Picking a basis of W, we can define a norm $||\cdot||_v$ on $W_{K_v} := W \otimes K_v$ for each $v \in V_K$ to be equal to

- the Euclidean norm $\sqrt{\sum_i |x_i|_v^2}$ if v is archimedean (i.e. $K_v = \mathbb{R}$ or $\mathbb{C}$),
- the sup norm $\max |x_i|_v$ if v is non archimedean.

Let S denote as before a finite subset of $\mathbb{G}(K)$. Set

$$h_\rho(S) := \frac{1}{[K:\mathbb{Q}]} \sum_{v \in V_K} n_v \log^+ ||\rho(S)||_v,$$

where n_v is the degree of the local extension $[K_v : \mathbb{Q}_v]$, $\log^+$ is short for $\max\{0, \log\}$, and

$$||\rho(S)||_v := \max\{||\rho(s)||_v, s \in S\},$$

where $||\rho(s)||_v$ is the operator norm of the endomorphism $\rho(s)$ of W_{K_v} associated to the norm $||\cdot||_v$.

Definition 3.3 (Normalized height). *We set*

$$\widehat{h}_\rho(S) := \lim_{n \to +\infty} \frac{1}{n} h_\rho(S^n),$$

where $S^n = S \cdot \cdots \cdot S$ is the n-fold product set.

While $h_\rho(S)$ depends on the particular choice of basis used to defined the Euclidean and sup-norm on W_{K_v}, the normalized height $\widehat{h}(S)$ does not depend on this choice.

The definition of the normalized height is modeled on the definition of the Néron-Tate height in the theory of abelian varieties. Here the normalization encodes the way the powers S^n grow in each valuation. In particular this height carries some important information on the subgroup $\langle S\rangle$ generated by S. Heights on subgroups of matrices generated by one element have been studied by Talamanca in [100]. Our height is a natural extension of Talamanca's height to the case when S has more than one element.

The limit in the definition of $\widehat{h}_\rho$ exists because of sub-additivity. Indeed it is straightforward to check that $h_\rho(S^{n+m}) \leqslant h_\rho(S^n) + h_\rho(S^m)$ for all integers $n, m \geqslant 1$.

Moreover the height h_ρ and normalized height $\widehat{h}_\rho$ do not depend on the choice of the number field K. Namely if we replace K by any finite extension K' of K, so that S is again defined over K', then the value of the heights for K and for K' are the same.

Example. Consider the set $S = S_x$, for $x \in \overline{\mathbb{Q}}^\times$, from (1.2) in Section 1 and let ρ be the natural 2-dimensional representation of GL_2. Then

$$\widehat{h}_\rho(S_x) = h(x),$$

where $h(x)$ is the classical absolute Weil height (see [12] for background) of the algebraic number x, namely

$$h(x) := \frac{1}{[\mathbb{Q}(x):\mathbb{Q}]} \sum_{v \in V_{\mathbb{Q}(x)}} n_v \log^+ |x|_v = \frac{1}{D}(\log |a_D| + \sum_{y \in Gal(\overline{\mathbb{Q}}|\mathbb{Q})\cdot x} \log^+ |y|) = \frac{1}{D} \log M(\pi_x),$$

where $M(\pi_x)$ is as before the Mahler measure of the minimal polynomial $\pi_x := a_D X^D + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ of x.

Example. Let $S = \{g\} \in \mathbb{G}(K)$ a singleton in $\mathbb{G} = GL_d$ with the natural d-dimensional representation ρ. Let $\lambda_1, \ldots, \lambda_d$ the eigenvalues of g. Then

$$\widehat{h}_\rho(S) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in V_K} n_v \log^+ \max_i \{|\lambda_i|_v\}.$$

In particular

$$\frac{1}{d}\widehat{h}_\rho(S) \leqslant \max_i \{h(\lambda_i)\} \leqslant \widehat{h}_\rho(S).$$

To get a better understanding of this height, let us record now its main properties. Below S is a finite subset of $\mathbb{G}(\overline{\mathbb{Q}})$.

Properties of $\widehat{h}_\rho(S)$:

(i) (linearity in powers) $\forall n \in \mathbb{N}$, $\widehat{h}_\rho(S^n) = n\widehat{h}_\rho(S)$,

(ii) (conjugation invariance) $\forall g \in \mathbb{G}(\overline{\mathbb{Q}})$, $\widehat{h}_\rho(gSg^{-1}) = \widehat{h}_\rho(S)$,

(iii) (height zero points) $\widehat{h}_\rho(S) = 0$ if and only if $\langle S \rangle$ is virtually unipotent.

(iv) (change of representation) given two faithful linear representations ρ_1, ρ_2 of $\mathbb{G}$ there are constants $C_1, C_2 > 0$ such that

$$C_1\widehat{h}_{\rho_2}(S) \leqslant \widehat{h}_{\rho_1}(S) \leqslant C_2\widehat{h}_{\rho_2}(S)$$

for all finite subsets $S \subset \mathbb{G}(\overline{\mathbb{Q}})$,

(v) (comparison between h and $\widehat{h}$) There is $C = C(\mathbb{G}, \rho) > 0$ such that for every finite subset $S \subset \mathbb{G}(\overline{\mathbb{Q}})$ generating a Zariski-dense subgroup of $\mathbb{G}$ assumed semisimple, one can find $g \in \mathbb{G}(\overline{\mathbb{Q}})$ such that

$$\widehat{h}_\rho(S) \leqslant h_\rho(gSg^{-1}) \leqslant C\widehat{h}_\rho(S).$$

By virtually unipotent in item (*iii*) we mean that $\langle S \rangle$ has a subgroup of finite index, which can be conjugated inside a unipotent subgroup of $\mathbb{G}$ (i.e. there is a basis of W where all matrices in this subgroup are upper-triangular with all eigenvalues equal to 1).

Item (*v*) suggests that the other natural way to build a conjugation invariant height on $\mathbb{G}$ leads in fact to a comparable quantity, at least if S is not degenerate. There is at least one more natural way to define a conjugation invariant height function on k-tuples of $\mathbb{G}$. One may consider the stable quotient $\mathbb{G}^k /\!\!/ \mathbb{G}$ in the sense of Geometric Invariant Theory, where the quotient is via the diagonal action of $\mathbb{G}$ on $\mathbb{G}^k$ by coordinate-wise conjugation. This algebraic variety, whose coordinate ring is the ring of invariants $\mathbb{C}[\mathbb{G}^k]^{\mathbb{G}}$, is also called the variety of $\mathbb{G}$-characters of the free group F_k on k letters. Then one may simply consider a height on this variety defined using the usual Weil height machine [67, 56]. This height will be comparable, up to additive and multiplicative constants, to our height $\widehat{h}(S)$.

One particularly nice way to parametrize $\mathbb{G}^k /\!\!/ \mathbb{G}$ is to consider the traces of short words in the k-tuple. Fricke and Klein showed in the 19th century that $\mathrm{tr}(a), \mathrm{tr}(b)$ and $\mathrm{tr}(ab)$ are coordinates on the character variety of the free group F_2 on $\mathrm{SL}_2(\mathbb{C})$, namely away from some singular locus, these 3 values determine the conjugacy class of the pair (a, b). More recently Procesi [85] extended this to $GL_d(\mathbb{C})$, showing that the coordinate ring of $\mathbb{G}^k /\!\!/ \mathbb{G}$, when $\mathbb{G} = GL_d(\mathbb{C})$ is generated by the traces $\mathrm{tr}(w(g_1, \ldots, g_k))$, where w ranges through all (positive) words in k letters whose length is bounded by a bound depending only on d.

Given an embedding $\rho : \mathbb{G} \to GL_d$, traces of words are no longer enough to tell apart non $\mathbb{G}$-conjugate tuples, but the induced natural morphism $\mathbb{G}^k /\!\!/ \mathbb{G} \to$

$GL_d^k /\!\!/ GL_d$, is a finite morphism: indeed if two generic k-tuples in $\mathbb{G}$ are conjugate in GL_d, they must be conjugate by an element of the normalizer of $\mathbb{G}$ in GL_d, because they generate a Zariski-dense subgroup of $\mathbb{G}$. This normalizer, when acting on $\mathbb{G}$, contains the inner automorphisms as a subgroup of finite index, see [98].

A consequence of Corollary 3.6 below is that there is $N \in \mathbb{N}$ and $C > 0$ depending only on the embedding ρ, such that for every finite subset $S \subset \mathbb{G}(\overline{\mathbb{Q}})$,

$$\frac{1}{C|S|^C}\widehat{h}_\rho(S) - C \leqslant \max_{|w|\leqslant N} h(\mathrm{tr}(\rho(w(S))) \leqslant C\widehat{h}_\rho(S)$$

So with this parametrization of $\mathbb{G}^k /\!\!/ \mathbb{G}$, $k = |S|$, we obtain a height function, which is comparable to our normalized height $\widehat{h}_\rho(S)$.

Our main theorem regarding $\widehat{h}_\rho$ is the following. It can be seen as an analogue for reductive groups of the Lehmer conjecture:

Theorem 3.4 (Height gap [16]). *There is $\varepsilon = \varepsilon(\mathbb{G}, \rho) > 0$ such that*

$$\widehat{h}_\rho(S) > \varepsilon$$

for every finite subset $S \subset \mathbb{G}(\overline{\mathbb{Q}})$ such that the subgroup $\langle S \rangle$ generated by S is not virtually solvable.

By way of contrast, one can see that the Lehmer conjecture itself is equivalent to the existence of some $\varepsilon_\rho > 0$ such that

$$\widehat{h}_\rho(S) > \frac{\varepsilon_\rho}{[K : \mathbb{Q}]} \tag{3.1}$$

for every number field K and all finite subsets $S \subset \mathbb{G}(K)$ generating a non-virtually unipotent subgroup, that is a subgroup whose elements have only roots of unity as eigenvalues (for those subsets $\widehat{h}_\rho(S) = 0$ by property (iii) above).

For example, if $\mathbb{G}$ is the multiplicative group $\mathbb{G}_m$, and $S := \{x\}$ a singleton, then $\widehat{h}(S) = h(x)$, the Weil height of x. Theorem 3.4 does not apply to this situation, because all subgroups of $\mathbb{G}_m$ are abelian, hence solvable.

Similarly the first example given above with $S_x \subset GL_2$ also shows that no such uniform lower bound can be expected when $\langle S \rangle$ is virtually solvable. There $\widehat{h}_\rho(S_x)$ was exactly the Weil height $h(x)$ of the algebraic number x, and hence could be very small (e.g. take $x = 2^{1/n}$). So the theorem claims in fact a uniform lower bound on the height, rather than on the height times the degree as the Lehmer conjecture asks. Uniform lower bounds on heights are related to the so-called *Bogomolov property* in Diophantine geometry. An algebraic extension F of $\mathbb{Q}$ of infinite degree is said to have the Bogomolov property if there is a uniform $\varepsilon > 0$ such that all elements of F with Weil height at most ε are in fact roots of unity (hence have zero Weil height). See [12, 1] for recent results about this property.

The proof of Theorem 3.4 makes use of some important facts borrowed from Diophantine geometry. Most importantly, Zhang's theorem [103], [12, Thm 4.2.] and Bilu's theorem [9], [12, Thm 4.3.1]. Zhang's theorem says that the points of very small height that lie on a proper algebraic subvariety of an algebraic torus $(\overline{\mathbb{Q}}^\times)^r$, must in fact lie in a finite union of even smaller dimensional subsets, unless the subvariety itself is a translate of a subtorus. In particular torsion points (and even points of small height!) cannot be Zariski-dense in a subvariety unless this subvariety is very special... For example, there are only finitely many points of height $< 1/100$ on the line $x + y = 1$, see [102] for optimal bounds. These lines of thought form by now a well-established branch of Diophantine geometry, encompassing such far-reaching statements as the Manin-Mumford conjecture, the Andre-Oort conjecture, etc.

This idea carries the key to the proof of the Height gap of Theorem 3.4, because too small a $\widehat{h}_\rho(S)$ would yield too many points of small height and contradict the Zariski-density of the group generated by S (after reduction to the case with the Zariski-closure of $\langle S\rangle$ is semisimple).

Zhang's theorem, as well as many other results in Diophantine geometry (starting with Szpiro-Ullmo-Zhang [93]) can be established via equidistribution methods. The prototype of these results is Bilu's theorem, according to which the Galois orbit of any algebraic number whose height is close to zero but non zero is almost equidistributed on the unit circle with its Lebesgue measure. In fact Zhang's theorem can be deduced from Bilu's, see [9]. Although we make use of Bilu's theorem in the proof of Theorem 3.4, it would be interesting to come up with a more direct argument proving an equidistribution result for the Galois orbit of S in the character variety $\mathbb{G}^k /\!\!/ \mathbb{G}$, before reaching a contradiction:

Problem. Give a proof of Theorem 3.4 via equidistribution.

3.5. Large eigenvalues. As the reader would have guessed by now, there is a relationship between our normalized height $\widehat{h}_\rho(S)$ and the Weil height of the eigenvalues of subgroup elements in $\langle S\rangle$. For example it is clear that if λ is an eigenvalue of $\rho(g)$ for some $g \in S^n$, then $|\lambda|_v \leqslant ||\rho(g)||_v \leqslant n||\rho(S)||_v$ for all $v \in V_K$ and so $h(\lambda) \leqslant n\widehat{h}_\rho(S)$. An important consequence of Theorem 3.4 and the analysis done in its proof is the following converse:

Corollary 3.6 (finding large eigenvalues). *There is a constant $C > 0$ depending only on $\mathbb{G}$ and ρ such that if $S \subset \mathbb{G}(\overline{\mathbb{Q}})$ is a finite set, then there is a positive integer $k \leqslant C$ and an element $g \in S^k$ such that for some eigenvalue λ of $\rho(g)$.*

$$h(\lambda) \geqslant \frac{1}{|S|^C}\widehat{h}_\rho(S)$$

In particular, there is a uniform $N_1 = N_1(d) > 0$ such that if two elements $a, b \in GL_d(\overline{\mathbb{Q}})$ generate a non-virtually solvable subgroup, then there is an element

g expressible as a word of length at most N_1 with letters in a and b and an eigenvalue λ of g with Weil height $h(\lambda) \geqslant 1$.

In the proof of the uniform Tits alternative, a crucial step consists in finding in S^N, for some bounded N, an element with a large eigenvalue. The above corollary does just that. The largeness of the eigenvalue is measured in terms of its height.

An important fact regarding the joint spectral radius of a bounded set of matrices is encapsulated in Lemma 3.7 below. It is used many times in order to produce a large eigenvalue, both in the proof of Theorem 3.4 and of Theorem 2.1.

Let K be a local field, that is either $\mathbb{R}$, $\mathbb{C}$, or a finite extension of the p-adic numbers, or (in characteristic p) of the field of Laurent series $\mathbb{F}_p((t))$. We choose an absolute value $|\cdot|$ on K and extend it (such an extension is unique) to an algebraic closure of K. Let S be a bounded subset of $d \times d$ matrices in $M_d(K)$, endowed with the operator norm $||\cdot||$ induced by the choice of some norm on K^d. Define the spectral radius of S to be

$$R(S) = \lim_{n \to +\infty} ||S^n||^{1/n},$$

where $||S^n||$ denotes the maximum of the (operator) norms of the elements in S^n. We also let $\Lambda(S)$ be the maximal eigenvalue:

$$\Lambda(S) := \max_{s \in S} \{|\lambda|; \lambda \in Spec\{s\}\},$$

where $Spec(s)$ is the set of eigenvalues of s. If $S = \{s\}$ is a singleton, the well-known spectral radius formula tells us that

$$R(\{s\}) = \Lambda(\{s\}).$$

Obviously $\Lambda(S) \leqslant R(S)$, for all S, but general $\Lambda(S) < R(S)$ if there are two or more matrices in S. However, somewhat surprisingly, we have the following converse inequality:

Lemma 3.7 (Spectral radius formula for several matrices). *There is $c = c(d) > 0$ such that for every bounded subset $S \subset M_d(K)$, there is an integer $k \leqslant d^2$ such that*

$$\Lambda(S^k)^{1/k} \geqslant c(d) \cdot R(S),$$

moreover $c(d) = 1$ if K is non-archimedean (i.e. K not $\mathbb{R}$ or $\mathbb{C}$).

In particular, if K is non-archimedean (for example a p-adic field), then $R(S) = \max_{k \leqslant d^2} \Lambda(S^k)^{1/k}$. This information is crucial, because it says that in order to find an element in a small power of S with a large eigenvalue, it is enough to have a good lower bound on $R(S)$. And since

$$\widehat{h}_\rho(S) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in V_K} n_v \log^+ R_{K_v}(S),$$

with the obvious notation, we understand now why the Height gap theorem 3.4 above is precisely what is needed in order to find an element with large eigenvalue.

We note in passing that this lemma produces an element in S^k, $k \leqslant d^2$, whose individual powers are already responsible for most of the growth of the full power set S^n. This feature is reminiscent of one of the key claims in the Gleason-Yamabe solution to Hilbert's fifth problem on the structure of locally compact groups. See the so-called Gleason-Yamabe lemmas [58, Thm II.13], [44, Lemma 5.4].

Problem. Find a good lower bound on $c(d)$ in terms of d.

3.8. A group theoretic consequence. The Grigorchuk group is one of the simplest example of a finitely generated infinite periodic group. Periodic means that every element has finite order. According to a classical theorem of Schur (see e.g. [89, 34]) every finitely generated periodic linear group is finite. A simple consequence of the Height gap theorem is that one can always quickly get out of torsion elements unless one belongs to a finite subgroup, namely we have a quantitative version of Schur's theorem ([18, Cor 3.6]):

Corollary 3.9 (Escaping torsion elements). *Let K be a field and S a finite subset of $GL_d(K)$. If the subgroup generated by S is infinite, then one can find a word of length at most $N_1(d)$ with letters in $S \cup S^{-1}$, which has infinite order. Here $N_1(d)$ is independent of S and K.*

To see the connection with the Height gap theorem, note that (in characteristic zero) unless $\langle S \rangle$ is virtually unipotent, $\widehat{h}_\rho(S) > 0$ and hence there is $g \in S^k$ and an eigenvalue λ of g such that $h(\lambda) > 0$ by Corollary 3.6, where k is bounded in terms of d only. In particular this g has infinite order. We also remark proving escape from elements of bounded torsion is easier. It follows from the Eskin-Mozes-Oh escape from subvarieties lemma, see [39, Lemma 3.2], or [24, Lemma 3.11], according to which for any proper subvariety $\mathcal{V}$ of the Zariski closure of $\langle S \rangle$, one can find a word of bounded length with letters in S lying outside the subvariety. However the length of the word can only be bounded by a function of the degree of $\mathcal{V}$, and in the case of $\mathcal{V} = \{g; g^e = 1\}$, this degree increases with e.

It is also worth pointing out that, as in the Growth gap theorem (Theorem 1.2), the constant $N_1(d)$ from the above statement must tend to infinity. The same examples of Grigorchuk and de la Harpe can be used to show, and this was done by Bartholdi and de Cornulier in [4], that for each n, there is a 3-generated infinite linear group all of whose elements lying in the word ball of radius n are of finite order.

3.10. Does the spectral gap imply a height gap ?. As we already mentioned, the uniform Tits alternative (Theorem 2.1) can be derived (see [18, 17]) from the Height gap theorem and the ping-pong techniques introduced by Tits in his original paper [96]. The uniform spectral gap estimate for non-amenable linear

groups, i.e. Corollary 2.2 is a simple consequence of Theorem 2.1. It is interesting to wonder whether one can also go backwards and prove the Height gap theorem assuming the uniform spectral gap for non-amenable linear groups. As it turns out, the uniform spectral gap is not quite enough to get the Height gap theorem as stated in Theorem 3.4. But one can recover the weak form of it discussed after the statement of Theorem 3.4 in (3.1), as follows.

Claim. For a finite (symmetric) subset S of $\mathbb{G}(K)$, K any number field,

$$\widehat{h}_\rho(S) \geqslant \frac{1}{C[K:\mathbb{Q}]} \log(r_S^{-1}),$$

where $C > 0$ is a constant depending only of $\mathbb{G}$ and ρ, and $r_S = ||\lambda_{\langle S\rangle}(\mu_S)||$ is the spectral radius of μ_S on the regular representation of $\langle S\rangle$.

To see the claim, set $\Phi_C(g) := e^{-C[K:\mathbb{Q}]h_\rho(g)}$ for some $C > 0$ and view it as a function defined on the group of adèles $G := \mathbb{G}(\mathbb{A}_K)$. We may assume that $\mathbb{G} = SL_d$ and ρ is the identity embedding. If C is large enough (depending on d only) a simple volume computation shows that Φ_C belongs to $L^2(G)$. Now, $h(xy) \leqslant h(x) + h(y)$, so $\Phi_C(xy) \geqslant \Phi_C(x)\Phi_C(y)$, from which one obtains $\forall g \in G$,

$$\langle \lambda_G(g)\Phi_C, \Phi_C\rangle_{L^2(G)} \geqslant \Phi_C(g^{-1})\langle \Phi_C, \Phi_C\rangle_{L^2(G)},$$

hence integrating over $\mu_S^{(n)}$, the n-th fold convolution power of the uniform probability measure supported on S,

$$\begin{aligned} ||\lambda_G(\mu_S^{(n)})|| &\geqslant \mathbb{E}_{\mu_S^{(n)}}\Phi_C(g^{-1}) = \mathbb{E}_{\mu_S^{(n)}}\Phi_C(g) \\ &\geqslant e^{-C[K:\mathbb{Q}]\mathbb{E}_{\mu_S^{(n)}}(h(g))} \geqslant e^{-C[K:\mathbb{Q}]h(S^n)}, \end{aligned}$$

where we applied the Jensen inequality to go from the first to the second line. The claim then follows by taking the n-th root and letting n tend to infinity. Note that $||\lambda_G(\mu_S))|| = r_S$, because $\langle S\rangle$ is a discrete subgroup of G ([6, F.1.11]). This argument is inspired from those in [99] and [80].

4. Uniform spectral gap and uniform diameter bounds for finite groups of Lie type

We now present some applications of the Height gap theorem to diameter bounds and spectral gaps for finite groups of Lie type.

4.1. Diameter bounds. Let G be a finite group and S a symmetric generating subset of G. The diameter $diam_S(G)$ is the least integer n such that every element of G can be written as a product of at most n elements from S. There is an extensive literature on diameter bounds for finite groups, from abelian groups to simple groups, including the Rubik's cube group, etc. One of the most celebrated conjecture is Babai's conjecture:

Conjecture 4.2 (Babai's conjecture). *For every finite simple group and every symmetric generating set S*

$$diam_S(G) \leqslant C(\log |G|)^C,$$

where $C > 0$ is an absolute constant (independent of G and S).

For example this conjecture is widely open in the special case of alternating groups $G = A_n$, the best bounds to date are due to Helfgott and Seress [55] and are in $\exp((\log\log |G|)^{O(1)})$ for these groups.

However Babai's conjecture was recently shown to hold for finite simple groups of Lie type and bounded rank. Such simple groups can also be described as those admitting a non trivial linear representation of bounded degree (over some, possibly finite, field).

Theorem 4.3 (Case of groups of Lie type). *If K is a field and $G \leqslant GL_d(K)$ a finite simple subgroup generated by a finite subset S, then*

$$diam_S(G) \leqslant C(\log |G|)^C,$$

where $C = C(d) > 0$ is a constant depending on d but otherwise independent of S, G and K.

Most approaches towards Babai's conjecture use the classification of finite simple groups. We will see in the next section a diameter bound, weaker than the one claimed by Babai's conjecture, but whose proof is independent of the classification.

The bound in the above theorem is a direct consequence of the following result applied repeatedly to the powers of a fixed generating set.

Theorem 4.4 (Product theorem). *If K is a field and $G \leqslant GL_d(K)$ a finite simple subgroup generated by a finite subset S, then*

$$|SSS| \geqslant \min\{|S|^{1+\varepsilon}, |G|\}$$

where $\varepsilon = \varepsilon(d) > 0$ is a constant depending on d but otherwise independent of S, G and K.

These results are due to Pyber and Szabó [86, 87] and, independently, to Green, Tao and the author [24], following work of Helfgott, who first solved Babai's conjecture for the family of groups $SL_2(\mathbb{F}_p)$ and $SL_3(\mathbb{F}_p)$, p prime. While Helfgott's arguments used clever ad hoc matrix computations coupled with techniques from additive combinatorics (the sum-product theorem), the proof of the general case is mainly based on algebraic geometry over finite fields. It can largely be seen as a derivative of the techniques introduced by Larsen and Pink [68] in their classification of finite subgroups of algebraic groups. See [22, 21] and [87] for a discussion of these arguments.

While this represents a significant advance compared to what was known prior to these developments, the polylogarithmic bound of Theorem 4.3 is most likely not optimal. Indeed we conjecture:

Conjecture 4.5 (Logarithmic diameter). *If K is a field and $G \leqslant GL_d(K)$ a finite simple subgroup generated by a finite symmetric set S, then*

$$diam_S(G) \leqslant C \log |G|,$$

where $C = C(d) > 0$ is a constant depending on d but otherwise independent of S, G and K.

The product theorem (Theorem 4.4 above) falls short of proving any exponential growth at any early stage, because iterating n times the bound $|SSS| \geqslant |S|^{1+\varepsilon}$ gives only subexponential growth in $\exp(Cn^\alpha)$ for some $\alpha < 1$. In particular it is not optimal for small n and not sufficient to get logarithmic diameter.

As it turns out, the uniform Tits alternative can be used precisely for this purpose of establishing exponential growth at an early stage. Coupled with Theorem 4.4 above, used at a later stage, it can say something towards this conjecture. Indeed the fact that the uniform Tits alternative holds over $\overline{\mathbb{Q}}$ allows for its reinterpretation in terms of a series of equality between *a priori* unrelated algebraic subvarieties as we pointed out in Paragraph 3.1. The equality between two algebraic varieties defined over $\mathbb{Z}$ implies their equality modulo p for every large enough prime. This will mean that unless the group G generated by S has a large solvable subgroup (of index bounded in terms of d only), one will be able to find two short words (of length L bounded in terms of d only) with letters in S admitting no relation of length $\leqslant \ell(p)$ for some function $\ell(p)$ tending to $+\infty$ as p gets large. In particular this will give at least $2^{\ell(p)}$ elements in $S^{L\ell(p)} \subset G$.

The question is how large can $\ell(p)$ be. Applying standard bounds on the *effective nullstellensatz* (e.g. those in [76]) one sees that $\ell(p)$ can be taken as large as $c(\log p)^\alpha$, where α is some positive exponent strictly less than one. This falls short of reaching the range where the product theorem can be applied successfully to get the desired logarithmic bound, as one would need to be able to have $\alpha = 1$. However one can instead play with several primes in order to turn the nullstellensatz bounds to one's advantage and obtain:

Theorem 4.6 (Uniform growth at almost all primes). *There is a constant $A = A(d) \geqslant 1$ such that, for every $\varepsilon > 0$, except perhaps for a (small yet possibly infinite) set of primes $\mathcal{P}_{\varepsilon-bad}$ satisfying $|\mathcal{P}_{\varepsilon-bad} \cap [1, X]| \leqslant X^{\varepsilon}$, for all $X \geqslant 1$, every symmetric subset $S \subset GL_d(\overline{\mathbb{F}_p})$ satisfies $|S^{\log p}| \geqslant p^{\varepsilon/A}$, unless the subgroup generated by S has a solvable subgroup of index at most A.*

Conjecturally the set of bad primes ought to be empty and uniform growth should take place at all primes. Recall that according to the prime number theorem, there are roughly $X/\log X$ primes less than X. So we see that uniform exponential growth does indeed take place at most primes. However we cannot say for which primes it does.

The proof of the above statement, already as outlined above, follows the same lines as the main argument in the paper by Gamburd and the author [19], which we will discuss in the next paragraph. With this we obtain:

Corollary 4.7 (diameter of perfect subgroups of $GL_d(\mathbb{F}_p)$). *Given $\varepsilon > 0$, if p is a prime not in $\mathcal{P}_{\varepsilon-bad}$, then for every perfect subgroup $G \leqslant GL_d(\mathbb{F}_p)$ generated by elements of order p*

$$\max_S diam_S G \leqslant \frac{C}{\varepsilon} \log p,$$

Here $C = C(d) > 0$ is a constant independent of p.

While this improves (at least for good primes) on the polylogarithmic bound given by Pyber and Szabó in Theorem 8 of [86], the proof uses their analog of the product theorem above for perfect groups combined with Theorem 4.6. Finite simple subgroups $GL_d(\mathbb{F}_p)$ are perfect and generated by their elements of order p (unless their order is prime to p, in which case they are bounded in size by a function of d only). In particular, we can reformulate this consequence in the following way:

Corollary 4.8 (Logarithmic diameter for almost all primes). *Conjecture 4.5 holds for simple subgroups of $GL_d(\mathbb{F}_p)$ for a density one set of primes.*

What if $G \leqslant GL_d(\mathbb{F}_p)$ is an arbitrary subgroup, not necessarily perfect or generated by elements of order p ? Well, in that case we can describe what happens regarding the diameter by studying the subgroup G_p of G generated of elements of order p. Clearly this is a characteristic subgroup of G. Moreover G/G_p has order prime to p, and there is a subgroup H_1 whose order is prime to p such that $G = H_1 G_p$ (indeed the Frattini argument shows that $G = G_p N_G(P)$, where P is the p-Sylow subgroup of G, and since $N_G(P)/P$ has prime to p order, it must be a semi-direct product $N_G(P) = H_1 P$, by the Schur-Zassenhauss theorem). But since $H_1 \leqslant GL_d(\mathbb{F}_p)$ is a subgroup whose order is prime to p, Jordan's theorem applies[1] and says that H_1 has an abelian normal subgroup whose index is bounded in terms of d only.

[1] Usually Jordan's theorem [57] is cited as a theorem about subgroups of $GL_d(\mathbb{C})$, but Jordan's original proof, unlike the more often quoted geometric argument due to Frobenius (see [34]), assumes only that all subgroups elements are semisimple and nothing on the field.

Now regarding G_p, one can always take the last term of the derived series of G_p, i.e. its iterated commutators $D^k = [D^{k-1}, D^{k-1}]$. This sequence must stabilise since we started with a finite group. The last term is then a perfect group generated by elements of order p. Denote by P_G this characteristic subgroup of G. By the discussion above, we see that G/P_G has a subgroup of bounded index (in terms of d only), which is solvable, and in fact of bounded derived length (actually Nori's theorem [81, Thm B] can be applied to prove that G_p has a subgroup of bounded index which is an algebraic subgroup over $\mathbb{F}_p$). We conclude that Corollary 4.7 helps estimating the diameter of an arbitrary subgroup of $GL_d(\mathbb{F}_p)$, by essentially reducing the question to the diameter of the virtually solvable quotient G/P_G. Diameters of abelian and solvable groups are typically much larger than those of simple or perfect groups. See e.g. [66] for a recent paper on the diameter of abelian groups.

Problem.(Function field analogues) Theorem 4.6 and its corollaries above say something interesting only when p is large. For a fixed p, it would be interesting to derive a statement of a similar flavor (from the characteristic p case of the uniform Tits alternative) for the quotient fields $\mathbb{F}_p[X]/(\pi)$, where π varies among the irreducible polynomials of $\mathbb{F}_p[X]$.

We finally note that it is plausible that an even stronger phenomenon than the logarithmic diameter bounds of Corollary 4.7 holds for finite simple groups of bounded rank. Namely it is likely that

$$diam_S(G) \leqslant C\frac{\log|G|}{\log|S|}$$

for every generating subset S. This means that we take into account the size of the generating set, whereas the previous statement does not distinguish between $|S|$ large or small. This kind of bound would be optimal.

Related statements occur in the work of Liebeck, Shalev, Nikolov [71] and others, where one allows to take arbitrary conjugates of S to compute the diameter (or rather *width*) of G. For example it is known, thanks to recent work of Gill, Pyber, Short and Szabó [43], that every element in a finite simple group of Lie type of rank at most d can be written as a product of only $C(d)\frac{\log|G|}{\log|S|}$ conjugates of elements from any subset $S \subset G$ (of size $\geqslant 2$). We refer the reader to the recent survey by Martin Liebeck [72] for many beautiful recent results in this direction.

We finally quote another result, proved by Green, Guralnick and the author [27], which provides further evidence towards Conjecture 4.5.

Theorem 4.9 (Logarithmic diameter for almost all generating sets). *If K is a field and $G \leqslant GL_d(K)$ a finite simple subgroup, then*

$$diam_{\{a^{\pm 1}, b^{\pm 1}\}}(G) \leqslant C\log|G|,$$

for all but a proportion $\leqslant 1/|G|^{\delta}$ *of all pairs* $\{a, b\} \subset G$*, where* $C, \delta > 0$ *are certain constants depending on* d *but otherwise independent of* S*,* G *and* K*.*

4.10. Uniform spectral gap bounds, Ellenberg's property $\widehat{\tau}$.

In what follows, we will say that the Cayley graph of a finite group G with finite symmetric generating set S is an ε-expander if

$$\kappa(S, \ell_0^2(G)) > \varepsilon,$$

where $\ell_0^2(G)$ is the regular representation of G on functions with zero average, and $\kappa(S, \ell_0^2(G))$ is the Kazhdan constant defined in (2.1). We refer the reader to the books [73], [88] and surveys [63], [61] for the background on expanders. Let us only mention that expander graphs with N vertices have logarithmic diameter (i.e. $O(\log N)$) and that the simple random walk on them equidistributes after logarithmically many steps.

As it turns out, the Height gap theorem and the uniform Tits alternative can also be used to prove uniform spectral gap estimates for Cayley graphs of finite simple groups of Lie type. A very general method, due to Bourgain and Gamburd, allows to establish spectral gaps for Cayley graphs of finite groups. We refer the reader to [61], [22] and [27] for an exposition of this method. An important requirement for the method to work is to be able to assert that the probability that the simple random walk on the Cayley graph of G hits any given subgroup decays exponentially fast at an initial stage (say for $c \log |G|$ steps). When $G = \mathrm{SL}_2(\mathbb{F}_p)$ and the Cayley graph has girth $\geqslant c \log p$, then this easily achieved as did Bourgain and Gamburd in their seminal paper [10]. Using the uniform Tits alternative, one can claim that this happens without any girth condition, at least at almost all primes p. We have:

Theorem 4.11 (Breuillard-Gamburd [19]). *For every* $\delta > 0$ *there is* $\varepsilon > 0$ *such that, given any* $X > 1$*, for all but at most* X^{δ} *primes* $p \leqslant X$*, all Cayley graphs of* $SL_2(\mathbb{F}_p)$ *are* ε*-expanders.*

We record here the following folklore conjecture, which implies Conjecture 4.5 above:

Conjecture 4.12. *Given* $d \geqslant 1$*, there is* $\varepsilon > 0$ *such that all Cayley graphs of all finite simple subgroups of* GL_d *over some field are* ε*-expanders.*

Although this conjecture seems out of reach at the moment even for $SL_2(\mathbb{F}_p)$'s and the entire family of primes p, the following looks more approachable:

Problem: Generalize Theorem 4.11 to higher rank finite simple groups of Lie type.

A related question is that of the spectral gap for finite subsets of compact groups. Following Jordan Ellenberg in [38] we will say that a topologically finitely

generated compact group G has *property* $\widehat{\tau}$ if for every finite subset S of G generating a dense subgroup

$$\kappa(S, L^2_0(G)) > 0,$$

where $L^2_0(G)$ is the regular representation of G on square integrable functions with zero average on G. The Kazhdan constant $\kappa(S, L^2_0(G))$ was defined above in (2.1).

The terminology echoes Lubotzky's property (τ), which is a property of a finitely generated group: property (τ) for a finitely generated group Γ means that for some (hence all) finite generating subsets S of Γ, one has

$$\kappa(S, L^2_0(\widehat{\Gamma})) > 0,$$

where $\widehat{\Gamma}$ is the profinite completion of Γ. We refer the reader to the forthcoming book [74] as well as [21] for more on property (τ).

Note that every finitely generated group with Kazhdan's property (T) has Lubotzky's property (τ). And there are also many other examples. However it surprisingly difficult to even exhibit one example of an infinite compact group G with Ellenberg's property $(\widehat{\tau})$. Using Theorem 4.11 it is possible to prove that certain infinite products $\prod_1^\infty \mathrm{SL}_2(\mathbb{F}_{p_i})$ for a sparse increasing sequence of primes have property $\widehat{\tau}$, thus giving the first examples of infinite compact groups with this property.

However difficult it appears to produce examples of compact groups with property $(\widehat{\tau})$, it is conjectured that this property is quite common and should hold in particular for all semisimple compact real Lie groups and the adèles groups $SL_n(\widehat{\mathbb{Z}})$. However it is not even known for $SU(2)$ and $SL_2(\mathbb{Z}_p)$ and these cases already appear to be very difficult (see [88, p.58] and [11]). See also Varju's paper [97, Corollary 4] for the current state of the art regarding spectral gap bounds for $SL_n(\widehat{Z})$ and other compact groups. For a connection between property $(\widehat{\tau})$ for certain Galois groups and Bogomolov's property for field extension, we refer the reader to Ellenberg's article [38] and to [37].

5. Approximate groups and polynomial growth

5.1. Polynomial growth. According to Gromov's theorem [52], a finitely generated group with polynomial growth is virtually nilpotent (i.e. has a nilpotent subgroup of finite index). The growth of virtually nilpotent groups is fairly well understood. In particular the exponent of polynomial growth is an integer given by the Bass-Guivarc'h formula ([2, 54])

$$d := \sum_{k \geqslant 1} k \cdot \mathrm{rank}(G^{(k)}/G^{(k+1)}),$$

where $\{G^{(k)}\}_k$ is the central descending series of $G = \langle S \rangle$. Pansu in his thesis [84] proved that there is even an asymptotics for the volume growth of the form

$$|S^n| = c(S)n^d + \varepsilon_n n^d,$$

where $\varepsilon_n \to 0$ and $c(S) > 0$ has a geometric interpretation as the normalized volume of the unit ball of the asymptotic cone of G. The estimation of the error term is more tricky:

Problem: Find good error terms for the above asymptotics.

While it is believed that $\varepsilon_n = O(\frac{1}{n})$, the best known estimate valid for arbitrary nilpotent groups is $\varepsilon_n = O(\frac{1}{n^\delta})$, where $\delta > 0$ depends only on the nilpotency class of G. See [28] for this estimate and more on this question.

5.2. Approximate groups. Approximate groups were introduced by Terence Tao in 2005 (see [94] and [95]) as a natural non-commutative generalization of a well studied object in additive number theory. Their study lies at the heart of the proofs of the product theorems mentioned above (Theorems 4.3 and 4.4).

Definition 5.3 (Approximate subgroup). *Let $K \geqslant 1$. A finite subset A of a group G is said to be a K-approximate subgroup of G if it is symmetric (i.e. $A = A^{-1}$) contains the identity and is such that*

$$AA \subset XA,$$

for some subset $X \subset G$ of cardinality at most K.

When $K = 1$, we recover the definition of a finite subgroup of G. When $K \geqslant 1$ however other type of sets arise, such as arithmetic progressions, e.g. $A = \{-N, \dots, N\}$ is a 2-approximate subgroup of $\mathbb{Z}$.

Approximate subgroups are interesting for the growth of groups because, if say $|S^{5n}| \leqslant K|S^n|$, then S^{2n} is a K-approximate subgroup, as a simple argument shows. For this reason, they already appear in disguise in Gromov's original proof of his polynomial growth theorem [52]. In [25] Green, Tao and the author, building on work of Hrushovski [64] gave a structure theorem for approximate subgroups:

Theorem 5.4 (Structure of approximate groups). *If A is a K-approximate subgroup of some group G, then there is a finite subgroup H contained in A^4 and a subgroup L containing H, such that L/H is nilpotent of nilpotency class at most C_1 and A is contained in fewer than C_2 left cosets of L. Here C_1, C_2 are positive constants depending on K only and not on G.*

From this result, one can easily deduce Gromov's polynomial growth theorem as well as several related statements, see [25]. See the surveys [21], [26] as well as Ben Green's article in these proceedings [45] for more on this topic.

5.5. Diameter bounds for arbitrary finite groups. A key feature of Theorem 5.4 is that it applies to any group, including finite groups. Among its consequences is a finite group analogue of Gromov's polynomial growth theorem (see [23]),

Theorem 5.6 (Diameter bound for a general finite groups). *Let $\varepsilon > 0$ and assume that G is a finite group with a symmetric generating set S such that*

$$diam_S(G) \geqslant |G|^{\varepsilon},$$

Then G has a subgroup of index C_ε which admits a nilpotent quotient of size at least $|G|^{\varepsilon/2}$ and nilpotency class at most C_ε. Here $C_\varepsilon > 0$ is a constant depending only on ε, and not on S nor G.

A consequence is that such groups have moderate growth in the sense of Diaconis and Saloff-Coste [36] and mixing time roughly $(diam_S(G))^2$. See also [69] for a related statement about groups with bounded doubling at all scales and [8] for an application to the identification of all Gromov-Hausdorff limits of such Cayley graphs. The following is an easy corollary:

Corollary 5.7 (Diameter bound for finite simple groups). *Given $\varepsilon > 0$, for all but perhaps finitely many finite simple groups G, the diameter of every Cayley graph of G is at most $|G|^{\varepsilon}$.*

A remarkable feature of this result is that its proof does not rely on the classification of finite simple groups! Of course much better bounds are available for finite simple groups of Lie type of bounded rank as mentioned earlier (see Theorem 4.3). For the alternating groups A_n much better bounds, in $\exp(O(\sqrt{\log |G|})$, have been known for a long time, see [3], and improved recently in [55]. It would be interesting to get non trivial bounds for all finite simple groups of Lie type also when the rank grows and see if one can improve the crude bound of Corollary 5.7.

Finally let us mention that, according to a well-known general inequality the spectral gap of a Cayley graph with fixed valency is bounded below by the square of the diameter (see [20, Prop. III.5] and [35, Cor 1.]). Hence a similar bound in $1/|G|^{\varepsilon}$ on the spectral gap of such Cayley graphs. Such crude bounds can already be useful in a number of applications, such as in [37].

Acknowledgements. I am very grateful to all my co-authors, present and past, for sharing their time and ideas with me, making my experience in research in mathematics so rewarding personally.

References

[1] Amoroso, F., David, S., Zannier, U., On fields with Property (B), *Proc. Amer. Math. Soc.* 142 (2014), no. 6, 1893–1910.

[2] Bass, H., The degree of polynomial growth of finitely generated nilpotent groups, *Proc. London Math. Soc.*, (3) 25 (1972), 603–614.

[3] Babai, L., Seress, ., On the diameter of Cayley graphs of the symmetric group, *J. Combin. Theory Ser. A*, 49(1):175-179, (1988).

[4] Bartholdi, L., de Cornulier, Y., Infinite groups with large balls of torsion elements and small entropy, *Arch. Math.* (Basel) 87 (2006), no. 2, 104-112.

[5] L. Bartholdi and A. Erschler, Groups of given intermediate word growth, *preprint 2011* arXiv1110.3650.

[6] B. Bekka, P. de la Harpe and A. Valette, *Kazhdan's property* (T) New Mathematical Monographs, 11. Cambridge University Press, Cambridge, 2008. xiv+472 pp.

[7] Benli, M. G., Grigorchuk, R., de la Harpe, P., Amenable groups without finitely presented amenable covers, *Bull. Math. Sci.* 3 (2013), no. 1, 73-131.

[8] Benjamini, I., Finucane, H., Tessera, R., On the scaling limit of finite vertex transitive graphs with large diameter, *preprint* arXiv:1203.5624

[9] Y. Bilu, Limit distribution of small points on algebraic tori, *Duke Math. J.*, 89 (1997), no. 3, 465–476.

[10] J. Bourgain, A. Gamburd, Uniform expansion bounds for Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$, *Ann. of Math.* **167** (2008), no. 2, 625–642.

[11] Bourgain, J., Gamburd, A., On the spectral gap for finitely-generated subgroups of $SU(2)$, *Invent. Math.* 171 (2008), no. 1, 83-121.

[12] Bombieri, E., Gubler, W., *Heights in Diophantine geometry*, New Mathematical Monographs, 4. Cambridge University Press, Cambridge, 2006. xvi+652

[13] E. Breuillard, On uniform exponential growth for solvable groups, *Pure Appl. Math. Q.* 3 (2007), no. 4, part 1, 949–967

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

[15] Breuillard, E., Gelander, T., Uniform independence for linear groups, *Invent. Math.* **173** (2008), no. 2, 225–263.

[16] E. Breuillard, A Height Gap Theorem for finite subsets of $\mathrm{GL}_d(\overline{\mathbb{Q}})$ and non amenable subgroups, *Ann. of Math.* (2) **174** (2011), no. 2, 1057–1110.

[17] Breuillard, E., Heights on SL_2 and free subgroups,in *Geometry, rigidity, and group actions*, 455-493, Chicago Lectures in Math., Univ. Chicago Press, Chicago, IL, (2011).

[18] Breuillard, E., A strong Tits alternative, *preprint*, arXiv:0804.1395.

[19] E. Breuillard, A. Gamburd, Strong uniform expansion in $\mathrm{SL}(2,p)$, *Geom. Funct. Anal.* **20** (2010), no. 5, 1201-1209.

[20] Breuillard, E., Expander graphs, property (τ) and approximate groups, *PCMI 12 Geometric Group Theory*, Lecture notes of a IAS-PCMI summer school held in Park City Utah in July 2012.

[21] Breuillard, E., A brief introduction to approximate groups, in *Thin Groups and Superstrong Approximation*, MSRI publication Breuillard and Oh eds., Cambridge Univ. Press (2014).

[22] Breuillard, E., Approximate groups and super-strong approximation, in *Group St. Andrews 2013*, to appear.

[23] Breuillard, E., Tointon, M., Nilprogressions and groups with moderate growth, *in preparation.*

[24] Breuillard, E., Green, B., Tao, T., Approximate subgroups of linear groups, *Geom. Funct. Anal.* 21 (2011), no. 4, 774-819.

[25] Breuillard, E., Green, B., Tao, T., The structure of approximate groups, *Publ. Math. IHES* **116**, Issue 1, pp 115–221, (2012),

[26] Breuillard, E., Green, B., Tao, T., Small soubling in groups, to appear in the Erdös centennial volume.

[27] Breuillard, E., Green, B., Guralnick, R., Tao, T., *Expansion in finite simple groups of Lie type*, to appear in J. Eur. Math. Soc.

[28] Breuillard, E., Le Donne, On the rate of convergence to the asymptotic cone for nilpotent groups and subFinsler geometry, *Proc. Nat. Acad. Sci.*, vol 110, no. 48, (2013).

[29] Brieussel, J., Behaviors of entropy on finitely generated groups, *Ann. Probab.* 41 (2013), no. 6, 4116–4161.

[30] Cannon, J. W., Wagreich, Ph., Growth functions of surface groups, *Math. Ann.* 293 (1992), no. 2, 239-257.

[31] Colding, T., Minicozzi, W. II, Harmonic functions on manifolds, *Ann. of Math.* (2) 146 (1997), no. 3, 725-747.

[32] Cowling, M., Sur les coefficients des reprsentations unitaires des groupes de Lie simples, in *Analyse harmonique sur les groupes de Lie* (Sém., Nancy-Strasbourg 1976-1978), II, pp. 132178, Lecture Notes in Math., 739, Springer, Berlin, (1979).

[33] Cowling, M., Haagerup, U., Howe, R. E., Almost L^2 matrix coefficients, *J. Reine Angew. Math.* 387 (1988), 97-110.

[34] C.W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Al- gebras*, (Interscience, New York) (1962).

[35] Diaconis, P., Saloff-Coste, L., Comparison techniques for random walk on finite groups, *Ann. Probab.* 21 (1993), no. 4, 2131-2156.

[36] Diaconis, P., Saloff-Coste, L., Moderate growth and random walk on finite groups, *Geom. Funct. Anal.* 4 (1994), no. 1, 1-36.

[37] Ellenberg, J., Hall, Ch., Kowalski, E., Expander graphs, gonality, and variation of Galois representations, *Duke Math. J.* 161 (2012), no. 7, 1233-1275.

[38] Ellenberg, J., Super strong approximation for monodromy groups, in *Thin Groups and Superstrong Approximation*, MSRI publication Breuillard and Oh eds., Cambridge Univ. Press (2014).

[39] Eskin, A., Mozes, S., and Oh, H., On uniform exponential growth for linear groups, *Invent. Math.* **160** (2005), no. 1, 1–30.

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

[41] Ghate, E., Hironaka, E., The arithmetic and geometry of Salem numbers, *Bull. Amer. Math. Soc.* (N.S.) 38 (2001), no. 3, 293-314.

[42] Ghys, E., de la Harpe, P., Sur les groupes hyperboliques d'après Mikhael Gromov (Bern, 1988), Progr. Math., 83, Birkhuser Boston, Boston, MA, (1990).

[43] Gill, N., Pyber, L., Short, I., Szabó, E., On the product decomposition conjecture for finite simple groups, *Groups Geom. Dyn.* 7 (2013), no. 4, 867-882.

[44] Goldbring, I., Van den Dries, L., Notes on Hilbert 5-th problem.

[45] Green, B., Approximate algebraic structure, *ICM Seoul 2014 Proceedings*.

[46] R. I. Grigorchuk, *Degrees of growth of finitely generated groups and the theory of invariant means*, Math. USSR-Izv. 25 (1985), no. 2, 259–300.

[47] R. I. Grigorchuk and I. Pak, *Groups of intermediate growth: an introduction*, Enseign. Math. (2) 54 (2008), no. 3-4, 251–272.

[48] Grigorchuk, R., On the Gap Conjecture concerning group growth, *Bull. Math. Sci.* 4 (2014), no. 1, 113-128.

[49] Grigorchuk, R., Milnor's Problem on the Growth of Groups and its Consequences, *preprint* arXiv:1111.0512

[50] Grigorchuk, R., de la Harpe, P., On problems related to growth, entropy, and spectrum in group theory, *J. Dynam. Control Systems* 3 (1997), no. 1, 51–89.

[51] Grigorchuk, R., de la Harpe, P., Limit behaviour of exponential growth rates for finitely generated groups, *Essays on geometry and related topics*, Vol. 1, 2, 351-70, Monogr. Enseign. Math., 38, Enseignement Math., Geneva, (2001).

[52] Gromov, M., *Groups of polynomial growth and expanding maps*, Inst. Hautes Études Sci. Publ. Math. No. 53 (1981), 53–73.

[53] Gromov, M., *Metric structures for Riemannian and non-Riemannian spaces*, based on original 1981 French original, Modern Birkhuser Classics, Birkhuser, (2007). xx+585 pp.

[54] Guivarc'h, Y., Croissance polynomiale et priodes des fonctions harmoniques, *Bull. Soc. Math. France*, 101 (1973), 333-379.

[55] Helfgott, H., Seress, ., On the diameter of permutation groups, *Ann. of Math.* (2) 179 (2014), no. 2, 611-658.

[56] Hindry, M., Silverman, J., *Diophantine geometry, an introduction*, Graduate Texts in Mathematics, 201. Springer-Verlag, New York, (2000).

[57] Jordan, C., Mémoire sur les équations différentielles linéaires à intégrale algébrique, *J. Reine Angew. Math.*, 84 (1878), 89–215.

[58] Kaplansky, I., *Lie algebras and locally compact groups*, The University of Chicago Press, Chicago, Ill.-London (1971) xi+148 pp.

[59] Kassabov, M., Pak, I., Groups of oscillating intermediate growth, *Ann. of Math.* (2) 177 (2013), no. 3, 1113-1145.

[60] Koubi, M., Croissance uniforme dans les groupes hyperboliques, *Ann. Inst. Fourier*, 48(5):1441–1453, (1998).

[61] Kowalski, E., lectures notes on expanders, http://www.math.ethz.ch/ kowalski/expanders.html

[62] P. de la Harpe, Free Groups in Linear Groups, *L'Enseignement Mathématique*, **29** (1983), 129-144.

[63] S. Hoory, N. Linial and A. Wigderson, Expander graphs and their applications, *Bull. Amer. Math. Soc.* (N.S.) **43** (2006), no. 4, 439–561.

[64] Hrushovski, E., Stable group theory and approximate subgroups, *J. Amer. Math. Soc.* 25 (2012), no. 1, 189-243.

[65] Kleiner, Br., A new proof of Gromov's theorem on groups of polynomial growth, *J. Amer. Math. Soc.*, 23 (2010), no. 3, 815-829.

[66] Klopsch, B., Lev, V. F., Generating abelian groups by addition only. *Forum Math.* 21 (2009), no. 1, 23-41.

[67] Lang, S., *Diophantine geometry*, Interscience Tracts in Pure and Applied Mathematics, No. 11, Interscience Publishers, New York-London (1962) x+ 170 pp.

[68] M. Larsen and R. Pink,*Finite subgroups of algebraic groups*, J. Amer. Math. Soc. 24 (2011), no. 4, 1105–1158.

[69] Lee, J., Makaychev, Y., Eigenvalue multiplicity and volume growth, *preprint* arXiv:0806.1745

[70] Li, J.S., The minimal decay of matrix coefficients for classical groups, in *Harmonic Analysis in China*, Math. Appl. 327, Kluwer, Dordrecht, 1995, 146-169.

[71] Liebeck, M. W., Nikolov, N., Shalev, A., A conjecture on product decompositions in simple groups, *Groups Geom. Dyn.* , 4(4):799812, (2010).

[72] Liebeck, M., Probabilistic and asymptotic aspects of finite simple groups, in *Probabilistic group theory, combinatorics, and computing*, 1-34, Lecture Notes in Math., 2070, Springer, London, (2013).

[73] Lubotzky, A., *Discrete groups, expanding graphs and invariant measures*, Progress in Mathematics, 125. Birkhuser Verlag, Basel, (1994). xii+195 pp.

[74] Lubotzky, A., Zuk, A., Property (τ), *book in preparation.*

[75] Mann, A., *How groups grow*, London Mathematical Society Lecture Note Series, 395. Cambridge University Press, (2012) x+199 pp.

[76] Masser, D., Wüstholz, G., Fields of large transcendence degree generated by values of elliptic functions, *Invent. Math.* 72 (1983), no. 3, 407-464.

[77] Milnor, J., A note on curvature and fundamental group, *J. Differential Geometry*, 2:1–7, (1968).

[78] Wolf, J., Growth of finitely generated solvable groups and curvature of Riemanniann manifolds, *J. Differential Geometry*, 2:421–446, 1968.

[79] Moore, C. C., Exponential decay of correlation coefficients for geodesic flows, in *Group representations, ergodic theory, operator algebras, and mathematical physics* (Berkeley, Calif., 1984), 163-181, MSRI Publ., 6, Springer, (1987).

[80] Nevo, A., The spectral theory of amenable actions and invariants of discrete groups, *Geom. Dedicata* 100 (2003), 187-218.

[81] Nori, M. V., On subgroups of $GL_n(\mathbb{F}_p)$, *Invent. math.*, **88** (1987), 257–275.

[82] Oh, H., Uniform pointwise bounds for matrix coefficients of unitary representations and applications to Kazhdan constants, *Duke Math. J.* 113 (2002), no. 1, 133-192.

[83] Osin, D., The entropy of solvable groups, *Ergodic Theory Dynam. Systems,* 23(3):907-918, (200)3

[84] P. Pansu, Croissance des boules et des géodésiques fermées dans les nilvariétés, *Ergodic Theory Dynam. Systems*, 3 (1983), no. 3, 415–445

[85] Procesi, C., The invariant theory of $n \times n$ matrices, *Advances in Math.* 19 (1976), no. 3, 306–381.

[86] L. Pyber, E. Szabó, *Growth in finite simple groups of Lie type*, preprint (2010) arXiv:1001.4556

[87] L. Pyber, E. Szabó, *Growth in linear groups*, in *Thin Groups and Superstrong Approximation*, MSRI publication Breuillard and Oh eds., Cambridge Univ. Press (2014).

[88] Sarnak, P., *Some applications of modular forms.*, Cambridge Tracts in Mathematics, 99, Cambridge University Press,(1990), x+111 pp.

[89] Schur I., Uber Gruppen periodischer Substitutionen, *Sitzber. Preuss. Akad. Wiss.* (1911), 619–627.

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

[91] Shalom, Y., Tao, T., A finitary version of Gromov's polynomial growth theorem, *Geom. Funct. Anal.* 20 (2010), no. 6, 1502-1547.

[92] Svarc, A., A volume invariant of covering, *Dokl. Akad. Nauj SSSR*, 105:32–34, (1955).

[93] Szpiro, L., Ullmo, E., Zhang, S., Équirépartition des petits points, *Invent. Math.* 127 (1997), no. 2, 337–347.

[94] Tao, T., Product set estimates for non-commutative groups, *Combinatorica*, 28(5):547-594, (2008).

[95] Tao, T., Vu, V., *Additive combinatorics*, ambridge Studies in Advanced Mathematics, 105. Cambridge University Press, (2006), xviii+512 pp.

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

[97] Varjù, P., Random walks in compact groups, *preprint* arXiv:1209.1745

[98] Vinberg, E. B., On invariants of a set of matrices., *J. Lie Theory* 6 (1996), no. 2, 249-269.

[99] Virtser, A., On the simplicity of the spectrum of characteristic Lyapunov exponents of the product of random matrices, *Theory Probabl. Appl.* 28 (1983), no. 1, 122-135.

[100] Talamanca, V., A Gelfand-Beurling type formula for heights on endomorphism rings, *J. Number Theory* 83 (2000), no. 1, 91-105.

[101] Wilson, J. S., On exponential growth and uniformly exponential growth for groups, *Invent. Math.*, 155(2):287–303, 2004.

[102] , Zagier, D., Algebraic numbers close to both 0 and 1, *Math. Comp.*, 61 (1993), no. 203, 485–491.

[103] Zhang, Sh., Small points and adelic metrics, *J. Algebraic Geom.* 4 (1995), no. 2, 281-300.

Laboratoire de Mathématiques
Bâtiment 425, Université Paris Sud 11
91405 Orsay
FRANCE

E-mail: emmanuel.breuillard@math.u-psud.fr