ON UNIFORM EXPONENTIAL GROWTH FOR SOLVABLE GROUPS

EMMANUEL BREUILLARD

Abstract. Using a theorem of J. Groves we give a ping-pong proof of Osin's uniform exponential growth for solvable groups. We discuss slow exponential growth and show that this phenomenon disappears as one passes to a finite index subgroup. Finally we make a connection between slow growth and the Lehmer conjecture.

Dedicated to G.A. Margulis on the occasion of his 60-th birthday.

1. Introduction

The main purpose of the present note is to give an alternative proof as well as a strengthening of the fact, proved by Alperin [1] (polycyclic case) and Osin [13, 14] that finitely generated solvable groups of exponential growth have uniform exponential growth. Our approach is quite different from the one taken up in those works and relies on a direct ping-pong argument.

Let Γ be a group generated by a finite subset Σ. Assume that 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 $\mathcal{G}$ for the word metric. Let $\mathcal{C}$ be the set of all such finite generating subsets Σ. We introduce the following definition:

Definition 1.1. *Two elements in a group are said to be* ***positively independent*** *if they freely generate a free semigroup. The* ***diameter of positive independence*** *of a Cayley graph $\mathcal{G}(\Gamma, \Sigma)$ is the quantity $d^+(\Sigma) = \inf\{n \in \mathbb{N},\ \Sigma^n$ contains two positively independent elements$\}$. Similarly, the diameter of positive independence of the group Γ is defined by $d^+_\Gamma = \sup\{d^+(\Sigma),\ \Sigma \in \mathcal{C}\}$.*

The next definition is more standard:

Definition 1.2. *Assume that 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.* If two elements

Date: January 5, 2006.

generate a free subsemigroup, there are exactly 2^n elements that can be written as positive words of length n in these two elements, hence the latter quantities are related by the following inequality:

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

In particular, if Γ has a finite positive independence diameter, i.e. $d_\Gamma^+ < +\infty$, then Γ has uniform exponential growth, i.e. $S_\Gamma > 0$. No converse is valid in general. As was proved by Osin in [15], the free Burnside groups of large odd exponent are uniformly non-amenable and in particular have uniform exponential growth. However, these groups obviously have an infinite diameter of positive independence.

In their seminal papers [12, 21] J. Milnor and J. Wolf proved that finitely generated groups that are finite extensions of a nilpotent group (i.e. virtually nilpotent groups) have polynomial growth (hence $S_\Gamma = 0$), while finitely generated solvable but non virtually nilpotent groups have exponential growth. Refining their methods, J. Rosenblatt showed subsequently in [19] that any finitely generated solvable group contains a free semigroup on two generators unless it is virtually nilpotent, and C. Chou [4] extended this dichotomy to the class of elementary amenable groups.

In the eighties, M. Gromov asked whether a group with exponential growth must have uniform exponential growth. Recently, J. Wilson [20] answered the question negatively by constructing several examples of finitely generated subgroups of the automorphism group of a rooted tree such that $S_\Gamma = 0$ although they contain a free subgroup and hence have exponential growth.

However, D. Osin [13, 14] (and independently R. Alperin [1] in the polycyclic case) proved that $S_\Gamma > 0$ for finitely generated solvable or even elementary amenable groups that are not virtually nilpotent. The class of elementary amenable groups is the smallest class of groups containing both abelian groups and finite groups and that is stable under subgroups, quotients, extensions and direct limit (see Chou [4]). Obviously any solvable group is elementary amenable. Although it is not explicitely stated in Osin's paper [14], reading between the lines of his proof one can fairly simply derive (see Section 6) the following stronger statement.

Theorem 1.3. *Let Γ be a finitely generated non virtually nilpotent elementary amenable group. Then Γ has finite positive independence diameter, i.e. $d_\Gamma^+ < +\infty$.*

The idea of proving the finiteness of d_Γ^+ in order to obtain uniform exponential growth has been used in many places in the past such as the work of Eskin-Mozes-Oh on non virtually solvable linear groups of characteristic zero [5], or for hyperbolic groups in Gromov's original monography [8]. Note finally that the existence of groups of intermediate growth shows that the above theorem cannot be extended to all amenable groups.

In this paper we want to address the following question: how large can d_Γ^+ be? The following theorem and corollary give an upper bound on d_Γ^+ for finitely generated solvable groups.

Theorem 1.4. *Let Γ be a finitely generated solvable group. Then one (and only one) of the following is true:*
(i) Γ is virtually nilpotent (i.e. it contains a nilpotent subgroup of finite index).
(ii) Γ has a finite index subgroup Γ_0 such that $d_{\Gamma_1}^+ \leq 3$ for any finite index subgroup $\Gamma_1 \leq \Gamma_0$.

It is easy to check that a subgroup Γ_0 of index n in a finitely generated group Γ, satisfies $d_\Gamma^+ \leq (2n+1) \cdot d_{\Gamma_0}^+$. Hence we obtain:

Corollary 1.5. *Let Γ be a finitely generated solvable group which is not virtually nilpotent. Then there is a number $C(\Gamma)$ such that $d_{\Gamma'}^+ \leq C(\Gamma)$ for every finite index subgroup Γ' of Γ.*

Hence within a given commensurability class of finitely generated non virtually nilpotent solvable groups, one can always find a group Γ with universally bounded growth, i.e. $S_\Gamma \geq \frac{\log 2}{3}$. In particular, slow exponential growth is a phenomenon that disappears completely as one passes to a suitable finite index subgroup.

The method used here to prove Theorem 1.4 is based on a direct ping-pong argument and hence differs radically from those of the above mentioned previous works [12, 21, 19, 13, 14]. Thanks to the following results that can be derived from the work of J. Groves, it is enough to prove Theorem 1.4 for metabelian groups (i.e. extensions of two abelian groups) and even for subgroups of affine transformations of a K-line. This on the other hand is fairly simple as explained in Section 3.

Theorem 1.6. *([7]) Let Γ be a non virtually nilpotent finitely generated solvable group all of whose proper quotients are virtually nilpotent. Then we have:*
(i) Γ is virtually metabelian.
(ii) If Γ is metabelian, then it embeds in the group of affine transformations of the K-line, for some field K.

For the convenience of the reader, we will provide a complete proof of Theorem 1.6 in Section 4 below. When proving (i), the polycyclic case is rather simple while the non polycyclic case is more delicate and relies on J. Groves' paper.

In [3], we show that a similar phenomenon as in Corollary 1.5 occurs for all finitely generated subgroups of the linear group GL_d. It would be interesting to study this also in the more general case of elementary amenable groups.

However, there is no uniform bound on d_Γ^+ itself in Theorem 1.4. As Osin pointed it out in [14], making use of a construction of Grigorchuk and de la Harpe [6], it is possible to construct, for every $\varepsilon > 0$, an elementary amenable group G_ε (and even solvable virtually metabelian, with polycyclic and non polycyclic examples, as Bartholdi and Cornulier recently verified in [2]) such that $0 < S_{G_\varepsilon} < \varepsilon$.

The sharp contrast between polycyclic and non polycyclic groups is well illustrated by the special case of metabelian groups. Indeed we have $d_\Gamma^+ \leq 3$ for every non polycyclic metabelian group (this can be derived both from Osin's method or ours, see Proposition 7.1) while the following example shows that there is no upper bound for d_Γ^+ in the class of polycyclic metabelian groups.

Theorem 1.7. *There exists a sequence $(G_n)_{n\geq 1}$ of metabelian polycyclic subgroups of $GL_2(\overline{\mathbb{Q}})$ such that $d_{G_n}^+ \geq n$ for all n.*

However this does not rule out the possibility that S_Γ may be bounded away from 0 by a universal bound for all metabelian groups that are not virtually nilpotent. Following Osin [14] (remark after Theorem 2.4) let us formulate this as a question:

Question 1.8. *Is it true that there exists an $\varepsilon_0 > 0$ such that $S_\Gamma \geq \varepsilon_0$ for all non virtually nilpotent finitely generated metabelian groups ?*

As any such group maps to the 2×2 matrices by Theorem 1.6 (ii), the question reduces to subgroups of $GL_2(\overline{\mathbb{Q}})$ and even to the 2-generated groups $\Gamma(x)$ defined in Section 7 below. It is interesting to observe that a positive answer to this question would imply the famous Lehmer conjecture from number theory, we explain this in Section 7.

Outline of the paper: In Section 2, we explain how to build two positively independent elements via the ping-pong argument. Section 3 is devoted to the proof of Theorem 1.4 in the particular case of subgroups of the affine group. In Section 4, we provide a complete proof of Theorem 1.6 along the lines of J. Groves' paper [7]. In Section 5, we complete the proof the Theorem 1.4. Section 6 deals with elementary amenable groups and we then prove Theorem 1.3. Finally in Section 7 we give examples of simple metabelian groups with arbitrarily large d_Γ^+, proving Theorem 1.7.

2. Ping-pong on the affine line

Let $\mathbb{A}$ be the algebraic group of affine transformations of the line $\{x \mapsto ax + b\}$, that is, if K is any field,

$$\mathbb{A}(K) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, a \in K^\times, b \in K \right\}$$

Elements from $\mathbb{A}(K)$ are of two types: they can either fix a point and hence be homotheties around that point (when $a \neq 1$), or fix none and be pure translations (when $a = 1$). We are now going to give a simple sufficient condition for two elements in $\mathbb{A}(k)$ to generate a free semigroup when the field k is a local field (i.e. $\mathbb{R}$, $\mathbb{C}$, a finite extension of $\mathbb{Q}_p$ or a field of Laurent series over a finite field). The construction of a free semigroup often relies on the ping-pong principle. This principle can take many different guises, one of which is illustrated by the following lemma:

Lemma 2.1. *(Ping-pong) Let k be an archimedean (resp. non-archimedean) local field. Let x and y be two affine transformations of the k-line such that x fixes $p \in k$ and y fixes $q \in k$. Assume moreover that x acts by multiplication by α around p while y acts by multiplication by β around q. Suppose that $|\alpha|$ and $|\beta|$ are $\leq \frac{1}{3}$ (resp. < 1). Then x and y generate a free semigroup.*

Proof. Let $d = |p-q|$ and let $B(p)$ and $B(q)$ be the open balls of radius $d/2$ (resp. d in the non-archimedean case) centered at p and at q. By definition they are disjoint and it follows from the assumption on α and β that x maps both of them into $B(p)$ while y maps both of them into $B(q)$. Now suppose that $w_1 = x^{n_1}y^{m_1} \cdot ... \cdot x^{n_k}y^{m_k}$ and $w_2 = x^{n'_1}y^{m'_1} \cdot ... \cdot x^{n'_l}y^{m'_l}$ are two non trivial words in x and y with non-negative powers. If they give rise to the same element of H, then they must be equal as abstract words, i.e. $k = l$, $n_i = n'_i$, $m_i = m'_i$ for all i's. Indeed multiplying by a negative power of x on the right hand side if necessary, we may assume that $n_1 = 0$ while $n'_1 > 0$, but then when acting on the affine line, w_1 would send q to a point in $B(q)$, while w_2 would send q to a point in $B(p)$, a contradiction. □

To play this game of ping-pong, we will need to be able to choose a suitable embedding of a finitely generated field K into an appropriate local field. This is done via the following easy and classical fact:

Lemma 2.2. *(see J. Tits [22]) Let K be a finitely generated field and $\alpha \in K$. If α^{-1} is not an algebraic integer (i.e. over $\mathbb{Z}$ if $char(K) = 0$ or over $\mathbb{F}_p$ if $char(K) = p$), then there exists an embedding $\sigma : K \hookrightarrow k$ into a non-archimedean local field k with absolute value $|\cdot|_k$ such that $|\sigma(\alpha)|_k < 1$. Moreover there exists a positive number $\varepsilon = \varepsilon(K) > 0$ such that if $\alpha \in K$ is an algebraic unit and satisfies $|\log|\sigma(\alpha)|_k| < \varepsilon$ for every embedding $\sigma : K \hookrightarrow k$ into an archimedean local field k, then α is a root of unity.*

Proof. Let $\beta = \alpha^{-1}$ and let K_0 be the prime field of K (i.e. $\mathbb{Q}$ if $char(K) = 0$ and $\mathbb{F}_p$ if $char(K) = p$). Suppose first that β is transcendental over K_0. Transcendental elements are dense in every local field, so if k is a non-archimedean local field containing K_0, then one can indeed find a transcendental element $\sigma(\beta)$ in k with $|\sigma(\beta)| > 1$. This gives rise to an embedding $\sigma : K_0(\beta) \to k$ which can always be extended to the whole of K up to changing k into a finite extension if necessary (K is finitely generated). Now if $K_0(\beta)$ is an algebraic extension and $|\beta| \leq 1$ for every non-archimedean absolute value $|\cdot|$ on $K_0(\beta)$, then β must be an algebraic integer.

Finally suppose α is an algebraic unit. Then its degree over K_0 is bounded by a constant depending only on K, namely by $[K : K_0(\zeta_1, ..., \zeta_r)] < +\infty$ where $K_0(\zeta_1, ..., \zeta_r)$ is a purely transcendental extension over which K is algebraic (by Noether's normalization theorem). However, there are only finitely many algebraic units of given degree all of whose conjugates are bounded. Moreover, Kronecker's theorem implies that if $|\delta| \leq 1$ for all conjugates δ of α, then α must be a root of unity. Hence the result. □

3. Proofs for subgroups of the affine group $\mathbb{A} = \{x \mapsto ax + b\}$

First consider a general finitely generated metabelian group Γ with the exact sequence

$$1 \to M \to \Gamma \xrightarrow{\pi} Q \to 1$$

where M and Q are abelian groups. The group Q acts on M by conjugation. If we denote by A the subring of $End(M)$ generated by Q, then M becomes an A-module. The following is classical:

Claim 1: M is finitely generated as an A-module.

Indeed let $\{x_1, ..., x_n\}$ be generators of Γ. Since Q is a finitely generated abelian group, it is finitely presented $Q = \langle y_1, ..., y_n | r_1, ..., r_m \rangle$ where $y_i = \pi(x_i)$. We then verify that M is generated as an A-module by the $r_i(x_1, ..., x_n)$'s and the x_i's that already belong to M. This proves the claim.

We are now going to prove Theorem 1.4 and Proposition 7.1 *with the additional assumption* that the group Γ is a subgroup of $\mathbb{A}(K)$ for some field K. In the next section, we will prove the general case by reducing to this one. We can take K to be the field generated by the matrix coefficients of the generators of Γ so that K will then be finitely generated. Let T be the subgroup of $\mathbb{A}(K)$ consisting of pure translations. We take $M = \Gamma \cap T$ and let π be the canonical projection map from $\mathbb{A}(K)$ to $K^\times$ so that Q is viewed as a multiplicative subgroup of $K^\times$.

3.1. Proof of Theorem 1.4 for subgroups of the affine line.

Suppose now that Γ is not virtually nilpotent. Then clearly Q does not lie within the group of roots of unity of K, because otherwise Q, being finitely generated, would be finite, and Γ would be virtually abelian. Now suppose that Q lies in the subgroup of $K^\times$ consisting of algebraic units. Then K must have characteristic zero and according to Lemma 2.2, there exists a positive ε depending only on the field K, hence only on the group Γ, such that, if $\alpha \in Q$ is not a root of unity then there exists an embedding of K into an archimedean local field k such that $|\log |\alpha|_k| > \varepsilon$. Let n_0 be an integer (depending only on Γ) such that $e^{-n_0\varepsilon} < \frac{1}{3}$. Then let $\Gamma_0 = \pi^{-1}(Q^{n_0})$. It is a subgroup of finite index in Γ, because $Q^{n_0} = \{b^{n_0}, b \in Q\}$ is a subgroup of finite index in the finitely generated abelian group Q. Let Γ_1 be a subgroup of finite index in Γ_0. We want to show that $d^+_{\Gamma_1} \leq 3$. Let $\{z_1, ..., z_n\}$ be generators of Γ_1. There must be at least one z_i, say z, such that $\pi(z)$ is not a root of unity. By definition of Γ_0, z is of the form $z_0^{n_0}a$ where $z_0 \in \Gamma$ and $a \in M$. Hence $\pi(z) = \pi(z_0)^{n_0}$ and $\pi(z_0)$ is not a root of unity either. By Lemma 2.2, there must exist an embedding of K into an archimedean local field k such that $|\log |\pi(z_0)|_k| > \varepsilon$. Up to changing z into z^{-1} if necessary, we may assume that $|\pi(z)|_k < \frac{1}{3}$. The element z is a non trivial homothety on the affine line of the local field k. It fixes a point $p \in k$. If all other z_i's fix the same point p then Γ_1 lies in the stabilizer of p, an abelian subgroup. Hence at least one of the z_i's, call it w, satisfies $wp \neq p$. Then the two affine transformations $x := z$ and $y := wzw^{-1}$ satisfy the hypothesis of Lemma 2.1 and hence generate a free semigroup. We are done.

Suppose now that Q does not lie inside the group of algebraic units of K. Then we show that in fact $d^+_{\Gamma_1} \leq 3$ for every finite index subgroup Γ_1 in Γ. Indeed, let $\{x_1, ..., x_n\}$ be generators of Γ_1. Then at least one of the x_i's, say x, is such that $\pi(x)$ is not an algebraic unit. Indeed $\pi(\Gamma_1)$ is of finite index in Q and if it were contained in the group of algebraic units of $K^\times$ then so would Q, because if α^n is a unit then α is a unit too. Up to changing x into x^{-1}, we may assume that $\pi(x)^{-1}$ is not an algebraic integer. Then, according to Lemma 2.2, there exists an embedding of K into a non-archimedean local field k such that $|\pi(x)|_k < 1$. The element x must be a non trivial homothety on the affine line of k. It fixes a point $p \in k$. Again, all other x_i's cannot fix the same point p. Hence at least one of the x_i's, call it w, satisfies $wp \neq p$. Then the two affine transformations x and $y := wxw^{-1}$ satisfy the hypothesis of Lemma 2.1. We are done.

This finishes the proof of Theorem 1.4 in the special case considered in the present section.

3.2. **Polycyclic versus non polycyclic in $\mathbb{A}(K)$.** Here we prove the following result that will be useful in the proof of Proposition 7.1.

Lemma 3.1. *Let K be a field and Γ be a finitely generated subgroup of $\mathbb{A}(K)$. Let $Q = \pi(\Gamma)$ be the image of Γ under the canonical projection homomorphism π from $\mathbb{A}(K)$ to $K^\times$. Then Γ is polycyclic (resp. virtually nilpotent) if and only if Q is contained in the subgroup of algebraic units of $K^\times$ (resp. the subgroup of roots of unity).*

Proof. Note that the Q action on M comes from the action of Γ by conjugation on the normal subgroup M, and when Q is viewed as a subgroup of $K^\times$ and M as an additive subgroup of K, then this action coincides with the action by multiplication. Also we may assume that K is finitely generated, since Γ is so. As observed in Lemma 2.2, the subfield of K consisting of algebraic elements over the prime field K_0 is a finite extension of K_0.

Suppose Γ is polycyclic and let $\alpha \in \pi(\Gamma)$. Since α is arbitrary, it is enough to show that α is an algebraic integer. Up to conjugating Γ inside $\mathbb{A}(K)$, we may assume that Γ contains the element $\gamma = \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$. Conjugation by γ acts on M by multiplication by α. Since Γ is polycyclic, M must be a finitely generated abelian group. By the Cayley-Hamilton theorem, α must satisfy a polynomial equation with coefficients in $\mathbb{Z}$. Hence α is an algebraic integer.

Conversely, from claim 1 above, there is a finite set $a_1, ..., a_n$ in M such that $M = Qa_1 + ... + Qa_n$. Let $\mathcal{O}_K$ be the ring of integers (over $\mathbb{Z}$) of K. Then we get that M lies inside $\mathcal{O}_K a_1 + ... + \mathcal{O}_K a_n$. However $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module, hence a finitely generated additive group. It follows that M itself is finitely generated and that Γ must be polycyclic contrary to the hypothesis made on Γ. We are done. The corresponding statement for virtually nilpotent groups is also straightforward and we omit the proof. □

4. Just non virtually nilpotent groups

In this section, we prove Theorem 1.6. A finitely generated solvable group is called just non virtually nilpotent (JNVN) if it is not virtually nilpotent but all of its proper quotients are virtually nilpotent. In [7], making use of ideas of P. Hall, J. Groves studied the structure of metanilpotent just non polycyclic groups (see also [18]). As it turns out, his methods apply with only minor changes to JNVN groups.

4.1. **JNVN groups are virtually metabelian.** We first make a few observations; we refer the reader to the textbook [17] for more details. Note that any subgroup and any quotient of a virtually nilpotent group is again virtually nilpotent. Also a finite index subgroup of a JNVN group is again JNVN. Further note that if N_1 and N_2 are two non trivial normal subgroup of a JNVN group G, then $N_1 \cap N_2 \neq \{1\}$ because $G/N_1 \cap N_2$ embeds in the product $G/N_1 \times G/N_2$ which is virtually nilpotent. Since finitely generated virtually nilpotent groups are *max-n*, i.e. have the maximal property on normal subgroups (any increasing sequence of normal subgroups stabilizes), so are the JNVN groups. Given a solvable group G, we denote by $Fit(G)$ the Fitting subgroup of G, i.e. the subgroup generated by all nilpotent normal subgroups of G. It is a basic fact that the subgroup generated by two normal nilpotent subgroups is again a normal nilpotent subgroup. Hence if G is max-n then $Fit(G)$ is itself nilpotent. When G is JNVN, we have more:

Lemma 4.1. *Let G be a JNVN group. Then $Fit(G)$ is abelian.*

Proof. Let N be a normal nilpotent subgroup of G. If $N' \neq \{1\}$ then N/N' is finitely generated (like any subgroup of a finitely generated virtually nilpotent group). Hence N itself is finitely generated (see [17] 5.2.17.). Therefore G, being an extension of two polycyclic groups is itself polycyclic. We now show that G must be virtually nilpotent, leading the desired contradiction. We can find a subgroup H containing N', with finite index in G, such that H/N' is nilpotent. Then H must act unipotently by conjugation on N/N', i.e.

$$(h_1 - 1) \cdot ... \cdot (h_n - 1)N/N' = \{1\} \tag{1}$$

for some n any any h_i's in H. As N acts trivially on N/N', (1) also holds for all h_i's in HN. Hence HN/N' is nilpotent. We can apply Hall's criterion for nilpotence (see [17] 5.2.10.) which says that HN too must be nilpotent. But HN has finite index in G so we are done. □

Furthermore:

Lemma 4.2. *$Fit(G)$ is either torsion free or is a torsion group of prime exponent p.*

Proof. Since G has max-n, the torsion subgroup of $Fit(G)$ has finite exponent, hence is a finite direct product of the p-torsion factors. But as we have mentioned above no two non trivial normal subgroups of G intersect trivially. Hence there must be at most one p-torsion factor, say T_p. Again $pFit(G)$ and T_p intersect trivially, hence either T_p is trivial and $Fit(G)$ is torsion free, or $pFit(G)$ is trivial and $Fit(G) = T_p$. □

It is a basic property of polycyclic groups due to Malcev that they contain a finite index subgroup whose derived group is nilpotent (see [17] Proposition 15.1.6.). Thus if G is JNVN and polycyclic, then it contains a finite index subgroup H with $H' \leq Fit(H)$, which means by Lemma 4.1 above that H is metabelian. So part (i) of Theorem 1.6 is proved in this case.

We now assume that G is JNVN and non polycyclic. Up to passing to a normal subgroup of finite index containing $Fit(G)$, we may assume that $G/Fit(G)$ is nilpotent (since the Fitting subgroup is a characteristic nilpotent subgroup, the two Fitting subgroups actually coincide). In this setting we are going to show that G is metabelian.

Let us denote by A the commutative ring equal to $\mathbb{Z}$ when $Fit(G)$ is torsion free and equal to $\mathbb{F}_p[T]$ when $Fit(G)$ is of exponent p. Let K be its field of fractions, i.e. $\mathbb{Q}$ or $\mathbb{F}_p(T)$ respectively. We make $Fit(G)$ into an A-module by letting T act via conjugation by some non trivial element $z \in G$ whose projection modulo $Fit(G)$ is of infinite order in the center of $G/Fit(G)$ (there always is such an element because $G/Fit(G)$ is an infinite finitely generated nilpotent group). The following lemma is crucial:

Lemma 4.3. *$Fit(G)$ is a torsion free A-module and $F_K := Fit(G) \otimes_A K$ is finite dimensional over K.*

Proof. We follow [7, Lemma 2]. We first show that $Fit(G)$ is torsion free as an A-module. This is clear if $A = \mathbb{Z}$. When $A = \mathbb{F}_p[T]$, the torsion elements in $Fit(G)$ form a subgroup that can be written as an increasing union of the (normal) subgroups killed by the the polynomial $T^{n!} - 1$ (any polynomial in $\mathbb{F}_p[T]$ divides $T^{n!} - 1$ for n large enough). As G has max-n, it follows that $Fit(G)$ is annihilated by some $T^{n!} - 1$. This means that $z^{n!}$ commutes with $Fit(G)$. Hence the subgroup generated by $Fit(G)$ and $z^{n!}$ is normal in G and abelian thus contradicting the definition of $Fit(G)$.

We now turn to the second half of the statement. It is a consequence of a result of P. Hall (see [17] 15.4.3.) saying that $Fit(G)$ contains a free A-module F_0 such that $Fit(G)/F_0$ is a torsion A-module with non trivial anihilator. Let $r \in A\backslash\{0\}$ in the anihilator of $Fit(G)/F_0$ and let $q \in A$ be relatively prime to r. Then clearly $qFit(G) \cap F_0 = qF_0$. Hence F_0/qF_0 embeds in $Fit(G)/qFit(G)$ hence is finitely generated (because $qFit(G)$ is a non trivial normal subgroup of G). Since F_0 is a free A-module, F_0 too must be finitely generated. Hence $F_0 \otimes_A K = Fit(G) \otimes_A K$ is finite dimensional over K. □

We are now ready to complete the proof of Theorem 1.6 (i). The group G acts by conjugation via its quotient $G/Fit(G)$ on $Fit(G)$ and this action extends to a K-linear action on $F_K := Fit(G) \otimes_A K$. On the other hand, for any nilpotent subgroup N of $\mathrm{GL}_n(K)$, its derived group N' acts unipotently on K^n, i.e. $(g_n - 1) \cdot ... \cdot (g_1 - 1) = 0$ for any $g_1, ..., g_n$ in N'. Therefore G' acts unipotently on F_K (here it is crucial that $\dim_K F_K < +\infty$). Hence $(g_n - 1) \cdot ... \cdot (g_1 - 1)f = 0$ in F_K for every g_i's in G' and every $f \in Fit(G)$. As $Fit(G)$ is a torsion free A-module, it embeds naturally in F_K and the previous equality actually holds in $Fit(G)$. Hence $[g_n, [g_{n-1}, [...[g_1, f]...]]]$ is trivial in $Fit(G)$. We conclude that G' is nilpotent and that $G' \leq Fit(G)$, that is $G/Fit(G)$ is abelian, so G is metabelian.

4.2. **Embeddings of metabelian groups into the affine group.** In this paragraph, we prove the second part of Theorem 1.6. More precisely, we show the following:

Proposition 4.1. *Let H be a finitely generated metabelian group. Then there is a field K and a homomorphism $\rho : H \to \mathbb{A}(K)$ with the following property. If H is not virtually nilpotent (resp. not polycyclic), then $\rho(H)$ too is not virtually nilpotent (resp. not polycyclic).*

Note that it is easy to see that every finitely generated metabelian group can be embedded in some $\mathbb{A}(R)$ where R is some commutative ring (Magnus embedding, see also [16]). The point here is to find a suitable quotient of R which is a field and preserves non virtually nilpotence. For the proof, we could again refer to further results in J. Groves' paper [7] after passing to a JNVN quotient. However, for the reader's convenience, we provide another, more constructive proof.

Proof. The finitely generated metabelian group H comes with the exact sequence

$$1 \to M \to H \to Q \to 1$$

where M and Q are abelian groups. The group Q acts on M by conjugation. If we denote by A the (commutative) subring of $End(M)$ generated by Q, then M becomes an A-module and we have the natural map $\alpha : H \to Aut(M)$ sending h to the conjugation by h on M. In *Claim 1* above we showed that M is a finitely generated A-module. Next we make the following observation:

Lemma 4.4. *Let $\{h_i\}_{1 \leq i \leq m}$ be a finite generating set for H, and let $z_i = \alpha(h_i) \in A$. Suppose that there are positive integers n_i and k_i such that $(z_i^{n_i} - 1)^{k_i} = 0$ in A for all $i = 1, ..., m$. Then H is virtually nilpotent.*

Proof. Indeed, if this were true, there would be $n \geq 1$ and $k \geq 1$ such that $(z_i^n - 1)^k = 0$ for all $i = 1, ..., m$. Now let Q_0 be the subgroup of Q generated by the $\pi(h_i^n)$ for $i = 1, ..., m$. It has finite index in Q and its pull-back $H_0 := \pi^{-1}(Q_0)$ has finite index in H. Clearly H_0 is the subgroup of H generated by M and the h_i^n's. Let $y_i = z_i^n$.

Then $[H_0, H_0] \subset M$ while

$$[H_0, M] = \langle (P_1 - 1)a | P_1 \in \mathcal{P}, a \in M \rangle$$

where $\mathcal{P}$ is the set of all monomials in $y_1, ..., y_m$, i.e. $P_1 = y_1^{k_1} \cdot ... \cdot y_m^{k_m}$ for some $k_i \geq 0$. Similarly with d commutators,

$$[H_0, [H_0 ... [H_0, M] ...] = \langle (P_d - 1) \cdot ... \cdot (P_1 - 1)a | P_1, ..., P_d \in \mathcal{P}, a \in M \rangle$$

Moreover for every $P \in \mathcal{P}$ there are elements $r_i \in A$ such that $P - 1 = \sum r_i(y_i - 1)$. Hence if $d > (k-1)m$ every product of the form $(P_d - 1) \cdot ... \cdot (P_1 - 1)$ can be written as a sum $\sum r_i'(y_i - 1)^k$ for some $r_i' \in A$, hence is always zero by the hypothesis on the y_i's. It follows that H_0 is nilpotent of order $d + 1$ at most. Hence H is virtually nilpotent. □

Similarly, it is (even more) straightforward to see that:

Lemma 4.5. *Keeping the notation of the previous lemma, suppose that there are polynomials $q_i \in \mathbb{Z}[X]$ with leading coefficient equal to 1 such that $q_i(z_i) = 0$ in A for all $i = 1, ..., m$. Then H is polycyclic.*

Let us go back to the proof of Proposition 4.1. According to the lemmas above, we can choose one of the z_i's, call it z, such that $(z^n - 1)^k \neq 0$ in A for all positive integers n and k. And if H is not polycyclic we may even assume that $q(z) \neq 0$ in A for all monic polynomials $q \in \mathbb{Z}[X]$.

Let S be the subset of A consisting of all products of factors of the form $\phi(z)$, where $\phi \in \mathbb{Z}[X]$ runs through the collection of all cyclotomic polynomials, i.e. $\{1, X-1, X+1, X^2+X+1, ...\}$. When H is not polycyclic we change the definition of S and consider instead the set of all $q(z)$ where $q \in \mathbb{Z}[X]$ is an arbitrary monic polynomial. Clearly S is a multiplicative subset of A and, according to the choice of z, S does not contain 0.

We can thus consider the localized ring $S^{-1}A$. Then $S^{-1}M$ is a non trivial finitely generated $S^{-1}A$-module. Let I be the annihilator of $S^{-1}M$, i.e. $I = \{r \in S^{-1}A, rS^{-1}M = 0\}$. Then I is a proper ideal if $S^{-1}A$. It is therefore contained in a maximal ideal P of $S^{-1}A$. We can now set $K = S^{-1}A/P$ and $M_0 = S^{-1}M/PS^{-1}M$.

K is a field and M_0 a finite dimensional K-vector space. Moreover, M_0 is non trivial. Indeed, suppose that $S^{-1}M = PS^{-1}M$. Then $(S^{-1}M)_P = P(S^{-1}M)_P$ as $(S^{-1}A)_P$-modules, where $(S^{-1}A)_P$ is the local ring associated to the prime ideal $P \subset S^{-1}A$. Moreover $(S^{-1}M)_P$ is a finitely generated $(S^{-1}A)_P$-module. Hence Nakayama's lemma applies and shows that $(S^{-1}N)_P = 0$. But this means that there must exists $r \in S^{-1}A$ with $r \notin P$ such that $rS^{-1}M = 0$ and contradicts the choice of P.

We are now in a position to define the desired linear representation. Let π be either one of the canonical maps $A \to K$ or $M \to M_0$. Let h_0 be an element of H such that $\alpha(h_0) = z$, and define the map $c : H \to M_0$ by

$$c(h) = \pi([h_0, h])$$

It is straightforward to check that for all h_1 and h_2 in H

$$c(h_1h_2) = \beta(h_1)c(h_2) + c(h_1)$$

where $\beta = \pi \circ \alpha$.

As $z - 1$ is invertible in $S^{-1}A$, we see that $c(M) = M_0$. Let $z_0 := \pi(z)$. Then, according to the choice to z, $z_0 \in K^\times$ is not a root of unity, and in the case when H is not polycyclic z_0 is even not an algebraic integer in K.

Let F_0 be a hyperplane in M_0 and let $\pi_0 : M_0 \to M_0/F_0 \simeq K$. Setting $\overline{c} = c \circ \pi_0$, we obtain the desired representation of H into the affine group $\mathbb{A}(K)$ defined by

$$\begin{aligned} \rho \quad &: \quad H \to \mathbb{A}(K) \\ h \quad &\mapsto \quad \begin{pmatrix} \beta(h) & \overline{c}(h) \\ 0 & 1 \end{pmatrix} \end{aligned}$$

And this homomorphism sends h_0 to $\begin{pmatrix} z_0 & 0 \\ 0 & 1 \end{pmatrix}$ where $z_0 \in K^\times$ is not a root of unity (resp. not an algebraic integer when H is non polycyclic), and $\rho(M)$ equals $\begin{pmatrix} 1 & K \\ 0 & 1 \end{pmatrix}$. By Lemma 3.1, any such subgroup of $\mathbb{A}(K)$ is not virtually nilpotent (resp. non polycyclic). We are done. $\square$

5. Proof of Theorem 1.4

To prove Theorem 1.4, it is enough to show that some quotient of Γ has the same property. Combining the proof of these results we gave in Section 3 for subgroups of $\mathbb{A}(K)$ with Theorem 1.6, we see that we are done if we make use of the following easy and standard fact:

Claim 2: Every finitely generated non virtually nilpotent group has a just non virtually nilpotent quotient.

Indeed, let G be such a group and let $\mathcal{N}$ be the set of all normal subgroups N of G, such that G/N is not virtually nilpotent. Suppose $N_1 \subset N_2 \subset ... \subset N_i \subset ...$ is an increasing chain of subgroups from $\mathcal{N}$. And let N be the union of all N_i's. Then N is indeed a normal subgroup of G. Now if G/N were virtually nilpotent, there would exist a subgroup of finite index G_0 in G, containing N, such that G_0/N is nilpotent. Like any finitely generated nilpotent group, G_0/N has a finite presentation $\langle x_1, ..., x_n | r_1, ..., r_m \rangle$. The finitely many relations r_i's belong to one of the N_i's, say N_{i_0}. Hence G_0/N_{i_0} appears as a quotient of G_0/N, hence is nilpotent, contradicting the assumption that G/N_{i_0} is not virtually nilpotent. It follows that we can apply Zorn's lemma and obtain a maximal element N in $\mathcal{N}$. Then clearly G/N is not virtually nilpotent, while any proper quotient of it is. qed.

6. Elementary amenable groups

In this section, we explain why Osin's work actually implies Theorem 1.3 and also Proposition 6.2 below.

We first discuss the following lemma:

Lemma 6.1. *Let Γ be a group generated by two elements x and y such that the normal subgroup $M = \langle x^n y x^{-n}, n \in \mathbb{Z}\rangle$ is not finitely generated. Then the elements x and yxy^{-1} generate a free semigroup.*

It is easy to prove this lemma directly by showing that equality between two different positive words in x and yxy^{-1} would force M to be generated by finitely many $x^n y x^{-n}$, we leave this exercise to the reader. A. Navas pointed out to me that this lemma/exercise is also stated (with its solution) in [11]. Also, as the referee pointed out to me, a careful analysis of Milnor's argument in [12] shows that it is in a way already contained there. However it is also possible to give a different (and more complicated!) proof using yet another ping-pong argument! And we now explain this idea.

Proof. Let $M_n = \left\langle x^k y x^{-k}, n \leq k\right\rangle$ and $M_n^- := \left\langle x^k y x^{-k}, n \geq k\right\rangle$. Suppose $y \in M_1 \cap M_{-1}^-$. Then M would be finitely generated. Indeed there exists $N \in \mathbb{N}$ such that $y \in \left\langle x^k y x^{-k}, 1 \leq k \leq N\right\rangle$. Hence all $x^k y x^{-k}$ for negative k also belong to $\langle x^i y x^{-i}, 1 \leq i \leq N\rangle$. Similarly all the $x^k y x^{-k}$ for positive k would belong to $\langle x^i y x^{-i}, -N' \leq i \leq -1\rangle$ for some $N_1 \in \mathbb{N}$. Therefore up to changing x into x^{-1} we may assume that $y \notin M_\infty = \cap_{n\in\mathbb{Z}} M_n$. Now Γ acts on M/M_∞ via the action $\gamma \cdot aM_\infty = x^n b a x^{-n} M_\infty$ where $\gamma = x^n b$ for some $n \in \mathbb{Z}$ and $b \in M$.

We define a valuation v on M by $v(a) = \sup\{n,\ a \in M_n\}$ – clearly $v(ab) \geq \min\{v(a), v(b)\}$ – and an ultrametric distance $d(x, y) = e^{-v(a^{-1}b)}$. This is a well defined distance on the quotient space M/M_∞. Let X be the completion of M/M_∞ for the distance d. Then the Γ-action extends to an action on X. Moreover M acts by isometries while x contracts distances by a factor e^{-1} and x^{-1} is e-Lipschitz. It is easy to check that the elements of Γ may be of three possible kinds: if $\gamma \notin M$ then γ has a unique fixed point on X and acts by contraction/dilatation by a facteur e^{-1} around it (the sequence $x_{n+1} = \gamma \cdot x_n$ is a Cauchy sequence), if $\gamma \in M$ then either γ has no fixed point and acts like a translation or it fixes a point and belongs to a conjugate of M_∞. Clearly x is of the first kind, fixes the coset M_∞, while y doesn't.

Just like in the non-archimedean case of Lemma 2.1, we see that x and yxy^{-1} are two contractions with different fixed points and play ping-pong on X. □

In [14] Osin also shows a strong uniformity statement about the growth of infinitely–generated–by–nilpotent groups. His argument actually gives the following bound for d_Γ^+.

Proposition 6.2. *Let Γ be a finitely generated group given by an extension*

$$1 \to M \to \Gamma \to N \to 1$$

where N is r-step nilpotent and M is not finitely generated. Then $d_{\Gamma}^{+} \leq 3^{2r+1}$.

Proof. In [14], Osin proves using commutator calculus and an intricate induction the remarkable fact that if S is a symmetric generating set for Γ and all subgroups of the form $\langle x^n y x^{-n}, n \in \mathbb{Z}\rangle$ where $x \in S^{(r)}$ and $y \in S^{(2r)}$ are finitely generated ($S^{(n)}$ denotes the finite set of all commutators of length at most n in the elements of S) then M too is finitely generated. See [14, Section 5 and Lemma 6.4.] The set $S^{(r)}$ lies in the ball of radius 3^r (rough estimate) for the word metric induced by S. Hence we can apply Lemma 6.1 to some choice of x and y. Then x and yxy^{-1} will lie in the ball of radius 3^{2r+1}. □

We now complete the proof of Theorem 1.3.

Proof of Theorem 1.3. Again as Osin observes in [14, Proposition 3.1.], if Γ is a finitely generated elementary amenable group which is just non virtually nilpotent, then either Γ is virtually polycyclic or Γ has a non trivial normal subgroup M which is not finitely generated. We can pass to a subgroup of finite index Γ_0, since $d_{\Gamma}^{+} \leq (2[\Gamma : \Gamma_0] + 1) \cdot d_{\Gamma_0}^{+}$. The polycyclic case was already treated in Theorem 1.4 and the other case follows directly from Proposition 6.2 above. □

7. Metabelian groups, a counter-example, and the Lehmer conjecture

As mentionned in the introduction we have the following:

Proposition 7.1. *Let Γ be a finitely generated metabelian group which is not polycyclic. Then* $d_{\Gamma}^{+} \leq 3$.

Proof. By *Claim 2* in Section 5 and Theorem 1.6 (ii) we can assume that Γ is a subgroup of $\mathbb{A}(K)$ for some field K. By Lemma 3.1, the quotient group Q does not lie in the group of algebraic units of K. Hence we are in the situation of 3.1 at the end of the proof of Theorem 1.4 for subgroups of $\mathbb{A}(K)$, hence $d_{\Gamma}^{+} \leq 3$. □

Next we prove Theorem 1.7 from the introduction, namely:

Theorem 7.2. *For every integer $n \geq 1$, there exists a 2-generated polycyclic subgroup G_n of the affine group $\mathbb{A}(\overline{\mathbb{Q}})$ such that $d_{G_n}^{+} \geq n$ and G_n is not virtually nilpotent.*

Proof. For $x \in \mathbb{C}$, let $\Gamma(x)$ be the subgroup of $\mathbb{A}(\mathbb{C})$ generated by the matrices $\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ that is the set of matrices of the form $\begin{pmatrix} x^n & P(x) \\ 0 & 1 \end{pmatrix}$ where $n \in \mathbb{Z}$ and $P \in \mathbb{Z}[X, \frac{1}{X}]$. Note that $\Gamma(x)$ is also generated by $A(x) = \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$ and $B(x) = \begin{pmatrix} x & 1 \\ 0 & 1 \end{pmatrix}$. We are going to exhibit a sequence of points $x_n \in \mathbb{C}$ such that $G_n := \Gamma(x_n)$ satisfies the requirement of the theorem, that is more precisely $d^{+}(\Sigma_n) \geq n$ where $\Sigma_n = \{A(x_n), B(x_n)\}$.

First, we make the following observation. Let a, b, a', b' be non trivial homotheties in $\mathbb{A}(\mathbb{C})$ with respective dilation ratio $x, y, x', y' \in \mathbb{C}^\times$. Assume that a and b have distinct fixed points and that so do a' and b'. Assume further that $x = x'$ and $y = y'$. Then the pair $\{a, b\}$ generates a free semigroup if and only if the pair $\{a', b'\}$ generates a free semigroup. Indeed we check easily that the two pairs are conjugate by a single element $\gamma \in \mathbb{A}(\mathbb{C})$, i.e. $a' = \gamma a \gamma^{-1}$ and $b' = \gamma b \gamma^{-1}$.

Second, we note that if a is a homothety with dilation ratio $x \in \mathbb{C}^\times$ and b is a translation then the pair $\{a, b\}$ never generates a free semigroup unless x is transcendental. Indeed, suppose x is algebraic over $\mathbb{Q}$, i.e. it is a root of a polynomial $\pi(X)$ of degree d with coefficients in $\mathbb{Z}$, then it is straightforward to check that the following non trivial relation is satisfied $b^{b_0}ab^{b_1}a...b^{b_d} = b^{a_0}ab^{a_1}a...b^{a_d}$, where $P(X) = a_0 + ... + a_d X^d$ and $Q(X) = b_0 + ... + b_d X^d$ are polynomials of degree d with non-negative integer coefficients such that $\pi = P - Q$.

From this it follows that whether or not two elements from $\Gamma(x)$ generate a free semigroup is a property that depends only on the respective dilation ratios of the two elements. And since in $\Gamma(x)$ all elements have a dilation ratio of the form x^n for some integer $n \in \mathbb{Z}$, we may define the subset $\mathcal{NF}(x)$ of $\mathbb{Z}^2$ to be the set of all couples $(n, m) \in \mathbb{Z}^2$ such that pairs of elements of $\Gamma(x)$ of ratio x^n and x^m respectively do not generate a free semigroup. The goal is now to find $x_n \in \mathbb{C}$ such that $\mathcal{NF}(x_n)$ contains all couples (p, q) with $|p|, |q| \leq n$.

Note that the matrices $A(x)$ and $B(x)$ satisfy $A(x)^4 = B(x)^2 A(x) B(x)$ if and only if $x^3 + x + 1 = 0$. Now let x_n be a root of the equation $X^{3n!} + X^{n!} + 1 = 0$. We can assume that $|x_n| < 1$. Hence $A(x_n^{n!})^4 = B(x_n^{n!})^2 A(x_n^{n!}) B(x_n^{n!})$. Note that for every $p \in \mathbb{Z}$, the element $B(x_n)^p$ does not fix 0 because x_n is not a root of unity. It follows that $B(x_n^p)$ is conjugate to $B(x_n)^p$ by a element of $\mathbb{A}(\mathbb{C})$ that fixes 0 (i.e. commutes with $A(x_n)$). Hence for all integers p and q with $|p|, |q| \leq n$ we have $A(x_n^q)^{\frac{4n!}{q}} = B(x_n^p)^{\frac{2n!}{p}} A(x_n^q)^{\frac{n!}{q}} B(x_n^p)^{\frac{n!}{p}}$. If follows that $A(x_n^q)$ and $B(x_n^p)$ do not generate a free semigroup (although they do not commute), therefore $(p, q) \in \mathcal{NF}(x_n)$. We are done. $\square$

Let us now come back to Question 1.8 from the introduction. Let us show that a positive answer to the question would imply the Lehmer conjecture from Number Theory. Recall that if $\pi \in \mathbb{Z}[X]$ is a monic polynomial, and $\pi = \prod_{1 \leq i \leq d}(X - \lambda_i)$ its factorization over $\mathbb{C}$, the Mahler measure of π is the number

$$m(\pi) = \prod_{1 \leq i \leq d} \max\{1, |\lambda_i|\}$$

A classical theorem of Kronecker says that $m(\pi) = 1$ if and only if all roots λ_i's are roots of unity. The Lehmer conjecture states that there exists a universal $\varepsilon_0 > 0$ such that if $m(\pi) > 1$ then $m(\pi) > 1 + \varepsilon_0$. Clearly, the conjecture reduces to the case when π is irreducible over $\mathbb{Q}$ and $\pi(0) = \pm 1$. Let x be a root of such a π and let us consider the group $\Gamma(x)$. The following claim is what we are aiming for:

Claim: $log(m(\pi)) \geq S_{\Gamma(x)}$

Let $\Sigma = \{1, A(x)^{\pm 1}, B(x)^{\pm 1}\}$. Any element w of Σ^n is of the form $\begin{pmatrix} x^k & P(x) \\ 0 & 1 \end{pmatrix}$ where $|k| \leq n$, $d^\circ P \leq n$, and $\|P\| \leq n$, where we have set $\|P\| = \sum |a_i|$ if $P = \sum a_i X^i$. Therefore $\#\Sigma^n \leq (2n+1) \cdot \#\{P(x), d^\circ P \leq n, \text{ and } \|P\| \leq n\}$. Let $P = \pi Q + R_P$ the Euclidean division of P by π. Let us give an upper bound on the number of possible remainders R_P for $P \in \mathbb{Z}[X]$ with $d^\circ P \leq n$, and $\|P\| \leq n$. For $k \geq 0$, let $Y_k = R_{X^k}$. Then it is clear that the coefficients of Y_k in the basis $1, X, ..., X^{d-1}$ satisfy a linear recurrence relation, i.e. $Y_k = M^k Y_0$ where M is the companion matrix of π. Let $(v_1, ..., v_d)$ be a basis of $\mathbb{C}_{d-1}[X]$ diagonalizing M (M has distinct eigenvalues, since π is irreducible). If $Y_0 = \Sigma_{1 \leq i \leq d} \alpha_i v_i$ is the expression of Y_0 in this basis, then $Y_k = \Sigma_{1 \leq i \leq d} \alpha_i \lambda_i^k v_i$ for every $k \geq 1$. Let $|\alpha| = \max_{1 \leq i \leq d}\{|\alpha_i|\}$ and $|\lambda| = \max_{1 \leq i \leq d}\{|\lambda_i|^{d-1}\}$.

Let $B_n = \left\{\sum_{1 \leq i \leq d} x_i v_i, |x_i| \leq n|\alpha| \cdot \max\{1, |\lambda_i|\}^n \text{ for each } i\right\}$ and $a_n(i) = n|\alpha| \cdot \max\{1, |\lambda_i|\}^n + \frac{d}{2}|\alpha| \cdot |\lambda|$ and $B'_n = \left\{\sum_{1 \leq i \leq d} x_i v_i \in \mathbb{C}[X], |x_i| \leq a_n(i) \text{ for each } i\right\}$. For each $P \in \mathbb{Z}[X]$ with $d^\circ P \leq n$, and $\|P\| \leq n$ we have $R_P \in B_n \cap \mathbb{Z}[X]$, and if $x \in B_n \cap \mathbb{Z}[X]$, then $x + \varepsilon \in B'_n$ for every $\varepsilon = \sum_{1 \leq i \leq d} \varepsilon_i X^{i-1}$ with $|\varepsilon_i| \leq \frac{1}{2}$. Therefore $\#\{R_P, P \in \mathbb{Z}[X], d^\circ P \leq n, \|P\| \leq n\} \leq vol(B'_n \cap V)$, where vol is the standard Lebesgue measure in $V = \mathbb{R}_{d-1}[X]$ in the basis $Y_0 = 1, Y_1 = X, ..., Y_{d-1} = X^{d-1}$. But if A_n is the endomorphism of $\mathbb{C}_{d-1}[X]$ such that $A_n(v_i) = v_i \cdot a_n(i)$ then $vol(B'_n \cap V) = vol(A_n(B' \cap O_n V)) = |\det_{(Y_0,...,Y_{d-1})}(A_n)| \cdot vol(B' \cap O_n V)$, where $B' = \left\{\sum_{1 \leq i \leq d} x_i v_i \in \mathbb{C}[X], |x_i| \leq 1\right\}$ and O_n is an orthogonal transformation such that $O_n V = A_n^{-1} V$. Hence

$$vol(B'_n \cap V) = \left(\prod_{1 \leq i \leq d} a_n(i)\right) \cdot |\det_{(v_1,...,v_d)}(Y_0, ..., Y_{d-1})| \cdot vol(B' \cap O_n V)$$

But $vol(B' \cap O_n V)$ converges to a non zero limit, as $O_n V$ converges in the grassmannian. Hence

$$\lim_{n \to +\infty} (vol(B'_n \cap V))^{\frac{1}{n}} = \lim_{n \to +\infty} \left(\prod_{1 \leq i \leq d} a_n(i)\right)^{\frac{1}{n}} = m(\pi)$$

Finally $\overline{\lim}_{n \to +\infty} (\#\Sigma^n)^{\frac{1}{n}} \leq m(\pi)$, which is what we wanted.

Acknowledgments 7.3. *I would like to thank Yves Guivarc'h for drawing my attention to his early work* [9]*, Yves de Cornulier for pointing out to me the references* [15], [16] *and* [18]*, Pierre de la Harpe and Andres Navas for their remarks on an earlier version of the paper.*

References

[1] R. Alperin, *Uniform exponential growth of polycyclic groups*, Geom. Dedicata **92** (2002), p. 105–113.

[2] L. Bartholdi, Y. de Cornulier, *Infinite groups with large balls of torsion elements and small entropy*, to appear in Archiv der Mathematik.
[3] E. Breuillard, T. Gelander, *A uniform Tits alternative*, preprint.
[4] C. Chou, *Elementary amenable groups*, Illinois J. Math. **24** (1980), no. 3, 396–407.
[5] A. Eskin, S. Mozes, H. Oh, *On uniform exponential growth for linear groups*, Invent. Math. **160** (2005), no. 1, 1–30.
[6] R. Grigorchuk, P. de la Harpe, *Limit behaviour of exponential growth rates for finitely generated groups*, Essays on geometry and related topics, Vol. 1, 2, 351–370, Monogr. Enseign. Math., **38**, Enseignement Math., (2001).
[7] J. Groves, *Soluble groups with every proper quotient polycyclic*, Illinois J. Math. **22** (1978), no. 1, 90–95.
[8] M. Gromov, *Hyperbolic groups. Essays in group theory*, 75–263, Math. Sci. Res. Inst. Publ., **8**, Springer, (1987).
[9] Y. Guivarc'h, *Générateurs des groupes résolubles*, Publications des Séminaires de Mathématiques de l'Université de Rennes (1968), Année 1967–1968, Exp. No. **1**, 17pp.
[10] P. de la Harpe, *Topics in Geometric Group Theory*, Chicago University Press, (2001).
[11] P. Lomgobardi, M. Maj, A.H. Rhemtulla, *Groups with no Free Subsemigroups*, Trans. Amer. Math. Soc., Vol **347**, No 4, (1995) p. 1419–1427.
[12] J. Milnor, *Growth of finitely generated solvable groups*, J. Diff. Geometry **2** (1968) p. 447-449.
[13] D. Osin, *The entropy of solvable groups*, Erg. Theory. Dyn. Sys. **23**, no. 3, (2003) p. 907–918.
[14] D. Osin, *Algebraic entropy of elementary amenable groups*, Geometriae Dedicata 107, (2004) p. 133–151.
[15] D. Osin, *Uniform non-amenability of free Burnside groups*, preprint arXiv math.GR/0404073.
[16] V. N. Remeslennikov, *Representation of finitely generated metabelian groups by matrices*, Algebra i Logika **8** (1969) p. 72–75.
[17] D. Robinson, *A course in the theory of groups*, Springer Verlag, GTM.
[18] D. Robinson, J. Wilson, *Soluble groups with many polycyclic quotients*, Proc. London Math. Soc. (3) **48** (1984), no. 2, p. 193–229.
[19] J. Rosenblatt, *Invariant measures and growth conditions*, Trans. Amer. Math. Soc. **193** (1974), p. 33–53.
[20] J. Wilson, *On exponential growth and uniformly exponential growth for groups*, Invent. Math. **155** (2004), no. 2, p. 287–303.
[21] J. Wolf, *Growth of finitely generated solvable groups and curvature of Riemanniann manifolds*, J. Differential Geometry, **2** (1968) p. 421–446.
[22] J. Tits, *Free subgroups in linear groups*, J. Algebra **20** (1972) p. 250-270.

Emmanuel Breuillard, CMLS, Ecole Polytechnique, 91128 Palaiseau, France
E-mail address: `emmanuel.breuillard@math.polytechnique.fr`