Uniform Exponential Growth for Linear Groups

Alex Eskin*, Shahar Mozes† and Hee Oh‡

August 23, 2001

1 Introduction

Let Γ be a finitely generated group. Given a finite set of generators S one has the corresponding Cayley graph $\mathcal{C}(\Gamma, S)$ and a word metric d_S on Γ. Let us denote by

$$B_S(n) = \{\gamma \in \Gamma \ : \ \mathrm{d}_S(\gamma, e) \leq n\},$$

the ball of radius n in the Cayley graph $\mathcal{C}(\Gamma, S)$.

Definition 1.1. We shall say that Γ has exponential growth if

$$\omega_S(\Gamma) \equiv \lim_{n\to\infty} |B_S(n)|^{1/n} > 1,$$

or equivalently, $\lim_{n\to\infty} \frac{1}{n} \log |B_S(n)| > 0$.

Note that if Γ has this property with respect to some generating set S, it has it with respect to an arbitrary set of generators.

Definition 1.2. We shall say that Γ has uniform exponential growth if

$$\inf_S \omega_S(\Gamma) > 1,$$

where the infimum is taken over all finite generating sets S of Γ. Equivalently Γ has uniform exponential growth if and only if there is some $c > 1$ so that for any generating set S and all $n \geq 0$ we have $|B_S(n)| \geq c^n$.

*Research partially supported by the Packard Foundation.
†Research partially supported by the BSF.
‡Research partially supported by NSF grant DMS0070544.

A central question concerning groups of exponential growth which goes back to the book [4] is whether a group Γ of exponential growth is necessarily also of uniform exponential growth. This was shown to be the case when the group Γ is hyperbolic by M. Koubi [5] (see also [2]) and in the case when Γ is solvable independently by D. Osin [8] and J. Wilson [11]. Recently R. Alperin and G. Noskov [1] have announced an affirmative answer for certain subgroups of $SL_2(\mathbb{C})$. For a general discussion of these questions see the survey [3]. Our main result is the following:

Theorem 1.3. *Let Γ be a finitely generated group which is linear over a field of characteristic 0. Then Γ has exponential growth if and only if it has uniform exponential growth.*

Recalling that a linear group is of exponential growth if and only if it is not virtually nilpotent (see [10], [7], [12]) we have an equivalent formulation:

Corollary 1.4. *If Γ is a finitely generated group which is linear over a field of characteristic 0, then either Γ has uniform exponential growth or it is virtually nilpotent.*

2 Basic Observations

Note that if a homomorphic image of a group has uniform exponential growth then so does the original group. Also if a finite index subgroup has uniform exponential growth, then so does the original group. Thus in view of the theorem of Osin and Wilson mentioned above, we may assume that the Zariski closure of Γ is connected and simple, both in the algebraic sense.

Specialization. Let E be the field of coefficients of Γ. Note that since Γ is finitely generated it follows that E is finitely generated. Using the fact (see [6]) that if a finitely generated subgroup Λ of $GL_n(\mathbb{C})$ is virtually solvable then there is a bound on the index of a solvable subgroup in Λ depending only on n, we deduce that there exists a "specialization" i.e. a field homomorphism $\sigma : E \to K$ inducing a homomorphism $\rho : GL_n(E) \to GL_n(K)$ where K is a finite extension of $\mathbb{Q}$ so that $\rho(\Gamma)$ is not virtually solvable. Hence we may assume that we have a finitely generated group Γ contained in $SL_n(K)$ with K a number field and having a simple connected Zariski closure. Since Γ is finitely generated, we may, after possibly replacing Γ by a finite index subgroup, assume that there is some finite set of places $\mathcal{S}$ of the field K (which includes all the archimedean ones) so that $\Gamma \subset SL_n(\mathcal{O}_K(\mathcal{S}))$, where $\mathcal{O}_K(\mathcal{S})$ denotes the ring of $\mathcal{S}$-integers in K. Thus the diagonal embedding of Γ in $\prod_{\nu\in\mathcal{S}} SL_n(K_\nu)$ is discrete, where K_ν denotes the completion of K with respect to the absolute value $|\cdot|_\nu$ associated with the place $\nu \in \mathcal{S}$. We choose, for each ν, an extension of the absolute value $|\cdot|_\nu$ to the algebraic closure of K.

Notation and terminology. Let us set the following convention of terminology which makes some of the statements in the sequel more transparent. We shall use the term "bounded" to mean "bounded with a bound depending only on the dimension of the linear representation, the number field K and the set of places $\mathcal{S}$. We shall use the notation $x \prec y$ or equivalently $y \succ x$ to mean that there exist bounded positive constants c_1 and c_2 such that $x < c_1 y^{c_2}$. This is used only when $y \geq 1$. For a matrix $A \in SL_n(\bar{K})$, we define $\|A\|_\nu = \max_{ij} |A_{ij}|_\nu$, and $\|A\| = \max_{\nu \in \mathcal{S}} \|A\|_\nu$.

The following lemma plays a basic role and is one of the reasons why we need to specialize so that the field of coefficients of Γ is a number field.

Lemma 2.1. *For every $A \in SL_n(\mathcal{O}_K(\mathcal{S}))$, let $\lambda_1, \ldots, \lambda_r$ be the distinct eigenvalues of A. Then*

$$\prod_{\nu \in \mathcal{S}} \prod_{i \neq j} |\lambda_i - \lambda_j|_\nu \geq 1 \tag{1}$$

Hence for any $i \neq j$ and any $\nu \in \mathcal{S}$ we have $\frac{1}{|\lambda_i - \lambda_j|_\nu} \prec \|A\|$.

Proof. The left hand side of (1) is the absolute value of a non-zero (rational) integer, and is therefore at least 1. □

In the course of the argument we shall need certain words of bounded length with respect to any generating set of the group Γ to be as regular as possible. We shall use the following:

Lemma 2.2. *Let H be the connected Zariski closure of Γ and let $Z \subsetneq H$ be any Zariski closed proper subset of H. Then there exists $N = N(Z, H) \geq 1$ such that for any finite generating set S of Γ, $B_S(N) \not\subset Z$.*

Lemma 2.2 is proved using the generalized Bezout theorem.

To show that our group Γ has uniform exponential growth we shall show that there is some bounded constant m so that given any finite generating set S there exists a pair of elements in the ball $B_S(m)$ generating a free semigroup. We recall the well-known result of J. Tits [10] which states that any non-virtually-solvable linear group contains two elements A and B which generate a free subgroup; the proof is based on the so called "ping-pong lemma". Our result may be viewed as a sort of quantitative version of Tits' theorem, in the sense that we obtain a uniform bound on the word length of the elements A and B; however our elements are only guaranteed to generate a free semigroup.

Showing that a pair of elements generates a free semigroup is based on the following version of the ping-pong lemma which is due to G. A. Margulis.

Definition 2.3 (Ping-Pong Pair). Let k be a local field. A pair of matrices $A, B \in SL_n(k)$ is a *ping-pong pair* if there exists a nonempty set $U \subset \mathbb{P}(k^n)$ such that:

$$BU \cap U = \emptyset$$

$$ABU \subset U, \qquad A^2BU \subset U$$

Lemma 2.4 (Margulis). *If A, B are a ping-pong pair then AB and A^2B generate a free semigroup.*

To apply this lemma we need an effective way of showing that certain elements form a ping-pong pair.

Lemma 2.5. *Let k be a local field with an absolute value $|\cdot|_\nu$. Suppose that $A, B \in SL_n(k)$ are matrices such that after conjugation of both by a common matrix we have:*

(L1) $A = \begin{pmatrix} a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & a_n \end{pmatrix}$ *with* $|a_1|_\nu \geq |a_2|_\nu \geq \cdot \geq |a_n|_\nu$ *and* $|a_1|_\nu \geq \max(2, 2|a_2|_\nu)$.

(L2) *There exist constants $c_2 > 0$, $d_2 > 0$ such that $\frac{1}{|B_{11}|_\nu} \leq c_2 \|A\|_\nu^{d_2}$, and $Be_1 \notin ke_1$.*

(L3) *There exist constants $c_3 > 0$, $d_3 > 0$ such that $\|B\|_\nu \leq c_3 \|A\|_\nu^{d_3}$.*

Then there exists a constant m, depending only on n, c_2, c_3, d_2 and d_3, such that A^m and B form a ping-pong pair.

3 The steps of the proof

Step 1. Using Lemma 2.2 one deduces that given any finite generating set S of Γ there is a pair of elements A, B of Γ belonging to a ball of bounded diameter in the Cayley graph $\mathcal{C}(\Gamma, S)$ so that any word of a certain very large but bounded length in A and B yields an H-regular element, where H denotes the Zariski closure of Γ. (By an

H-regular element we mean a semisimple element the dimension of whose centralizer is equal to the rank of H. Such elements exist in H by [9].) Moreover (using Lemma 2.2 for $\Gamma \times \Gamma < H \times H$) we may require also that no two of these bounded length words lie in a common parabolic subgroup of H. We shall actually require these regularity and genericity conditions also for all the corresponding words in $\rho_m(A)$ and $\rho_m(B)$ where ρ_m denotes the m'th wedge representation of SL_n, $1 \leq m \leq n$.

For the next two steps, it is convenient to use the diagonal embedding and consider A and B as elements of $G = \prod_{\nu \in \mathcal{S}} SL_n(\bar{K}_\nu)$. Also for a matrix $C = \prod_{\nu \in \mathcal{S}} C_\nu \in G$, we write $\|C\|_\nu = \max_{ij} |(C_\nu)_{ij}|_\nu$, and $\|C\| = \max_{\nu \in \mathcal{S}} \|C\|_\nu$.

Step 2. As A is semisimple we may conjugate both A and B by the same matrix in G so that A becomes diagonal. Conjugating by an appropriate element from the centralizer of A and possibly replacing B by some word of bounded length in A and B we may ensure that either:

$$\|B\| \prec \|A\|, \tag{2}$$

or, for some bounded m,

$$\|A\|^m \max_{\nu \in \mathcal{S}} |\operatorname{Tr} B|_\nu \succ \|B\|. \tag{3}$$

Step 3. We claim we can modify our choice of A and B and conjugate by a common matrix in G so that (2) holds and A is diagonal.

Indeed, suppose (2) does not hold. Then, in view of Step 2, (3) holds. Also since (2) does not hold, we may assume

$$\|A\|^m \leq \|B\|^{1/2}, \tag{4}$$

where m is as in (3). (Recall that A is diagonal and has determinant 1, hence $\|A\| \geq 1$.) Hence, in view of Lemma 2.1 and the semisimplicity of B, we can diagonalize $B \in G$ using a matrix $C \in G$ such that $\max\{\|C\|, \|C^{-1}\|\} \prec \|B\|$. Hence in view of (4),

$$\|CAC^{-1}\| \leq \|C\|\|A\|\|C^{-1}\| \prec \|B\|. \tag{5}$$

Since CBC^{-1} is diagonal, and in view of (3) and (4),

$$\|CBC^{-1}\| \succ \max_{\nu \in \mathcal{S}} |\operatorname{Tr} B|_\nu \succ \|A\|^{-m}\|B\| \geq \|B\|^{1/2} \tag{6}$$

Hence in view of (5) and (6), $\|CBC^{-1}\| \succ \|CAC^{-1}\|$. Hence if (2) fails we can conjugate A and B by C and interchange the roles of A and B.

Step 4. Let $\nu \in \mathcal{S}$ be such that $\|A\|_\nu$ is maximal. Let ρ_m be as in Step 1. From the discreteness of $SL_n(\mathcal{O}_K(\mathcal{S}))$, there exists m, $1 \le m \le n/2$ such that $\rho_m(A_\nu)$ satisfies (L1). Note that in view of (2) we have (L3) for the elements $\rho_m(A_\nu)$ and $\rho_m(B_\nu)$. Next we claim that by replacing $\rho_m(B_\nu)$ by a bounded word in $\rho_m(A_\nu)$ and $\rho_m(B_\nu)$ we can ensure that (L2) is satisfied. Thus we produced a ping-pong pair using words of bounded length in the given set of generators.

4 Construction of words with nice properties

Observe that in steps 2 and 4 above we need to produce words of bounded length so that the coefficients of the corresponding matrices satisfy certain properties. Let us describe first how this is achieved in the case where the Zariski closure of our group Γ is SL_n. The reason for this case being simpler than the general one is that in this case we may assume that the diagonalized matrix $\rho_m(A)$ has distinct eigenvalues. For the following, we fix $\nu \in \mathcal{S}$. Also let us for simplicity of notation speak about A and B rather than about $\rho_m(A)$ and $\rho_m(B)$, and write $|\cdot|$ and $\|\cdot\|$ rather than $|\cdot|_\nu$ and $\|\cdot\|_\nu$. For a constant $c > 0$ define an entry B_{ij} of B to be *large* when $|B_{ij}| > c\|B\|$. Let $\mathcal{E}(c)$ denote the algebra generated by all the elementary matrices E_{ij} corresponding to large entries of B. The following lemma is used twice, once in the proof of Step 2, with c being a small absolute constant, and once in the proof of Step 4, with $c = \|A\|^{-m}$, with m a large but bounded positive constant.

Lemma 4.1. *If $E_{ij} \in \mathcal{E}(c)$ then there exists a bounded word C in A and B so that $|C_{ij}| > p\|A\|^{-k}\|B\|^l$ where p, k and l are bounded positive constants.*

Rather than giving here the proof of the lemma let us give an example explaining the main idea. Assume that B_{12} and B_{21} are big entries. Then we claim that some word of the form BA^kB with $0 \le k \le n-1$ has big $(1,1)$ entry. Indeed we have

$$(BA^kB)_{11} = \sum_i B_{1i}B_{i1}a_i^k. \tag{7}$$

Note that $B_{12}B_{21}$ is a large term, but a priori, it may cancel with other terms. However, it may not happen for all $0 \le k \le n-1$, in view of Lemma 2.1. More formally, we may argue as follows: Written vectorially, (7) is

$$\begin{pmatrix} (BA^0B)_{11} \\ (BA^1B)_{11} \\ \vdots \\ (BA^{n-1}B)_{11} \end{pmatrix} = \begin{pmatrix} 1 & a_1 & a_1^2 & \dots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \dots & a_2^{n-1} \\ \vdots & & & & \\ 1 & a_n & a_n^2 & \dots & a_n^{n-1} \end{pmatrix} \begin{pmatrix} B_{11}^2 \\ B_{12}B_{21} \\ \vdots \\ B_{1n}B_{n1} \end{pmatrix}$$

Hence using the formula for the Vandermonde determinant and Lemma 2.1 we deduce that since we have $B_{12}B_{21}$ big we cannot have $(BA^kB)_{11}$ small for all $0 \leq k \leq n-1$.

Almost Algebras. In the general case, another technical device is needed. For matrices A and B, let $\langle A, B\rangle = \operatorname{tr} AB^t$, and let $\epsilon > 0$ be a small parameter. We say that matrices $A_1, \dots A_k$ form an *ϵ-almost-algebra* if for each $1 \leq i, j \leq k$, $\langle A_i, A_j\rangle = \delta_{ij}$, and A_iA_j is within ϵ of a linear combination of $A_1, \dots, A_k$.

For each $1 \leq m \leq n^2+2$, let us choose constants ϵ_m so that $\epsilon_{m+1} \ll \epsilon_m$, and $\epsilon_1 \ll \epsilon$. Now let $B_1, \dots B_m$ be matrices of norm at most 1. For each $1 \leq k \leq n^2+1$, let

$$f(k) = \inf\{m \in \mathbb{N} |\ \text{there exists a subspace } V_m \text{ of dimension } m \text{ such that all words in the } B_i \text{ of length at most } 2^k \text{ are within } \epsilon_k \text{ of } V_m.\ \}$$

By construction, the function f is increasing, and is bounded by n^2. Hence there exists a minimal k, $1 \leq k \leq n^2+1$ such that $f(k) = f(k+1)$. Then an orthonormal basis for $V_{f(k)}$ is an ϵ-almost-algebra. We call it the *almost-algebra generated by* $B_1, \dots, B_m$.

In the proof we use, as a replacement to $\mathcal{E}(c)$, the almost-algebra generated by the "blocks" of B, (i.e. the projections of B onto the eigenspaces of $\operatorname{Ad}(A)$). It is easy to see that the analog of Lemma 4.1 is satisfied. Also, in the appropriate sense, every almost algebra is near an algebra. This allows us to complete the proof.

References

[1] R. Alperin, G. Noskov. "Uniform Growth, Actions on Trees and GL_2." math.GR/0105083.

[2] T. Delzant. "Sous-groupes distingués et quotients des groupes hyperboliques." *Duke Math. J.* **83** (1996), pp. 661–682.

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

[4] M. Gromov. *Structures mtriques pour les varits riemanniennes.* (French) [Metric structures for Riemann manifolds] Edited by J. Lafontaine and P. Pansu. Textes Mathmatiques [Mathematical Texts], 1. CEDIC, Paris, 1981.

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

[6] A. Lubotzky, A. Mann. "On groups of polynomial subgroup growth." *Invent. Math.* **104** (1991), no. 3, pp. 521–533.

[7] J. Milnor. "Growth of finitely generated solvable groups." *J. of Diff. Geometry* **2** (1968), pp. 447–449.

[8] D. Osin. "The entropy of solvable groups." *Preprint* (2000).

[9] G. Prasad. "R-regular elements in Zariski-dense subgroups." *Quart. J. Math. Oxford Ser. (2)* **45** (1994), no. 180, 541–545.

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

[11] J. Wilson. *Preprint.*

[12] J. Wolf. "Growth of finitely generated solvable groups and curvature of Riemanniann manifolds." *J. of Diff. Geometry* **2** (1968), pp 421–446.

Department of Mathematics, University of Chicago, Chicago IL 60637, USA;
eskin@math.uchicago.edu

Institute of Mathematics, Hebrew University, Jerusalem 91904, ISRAEL;
mozes@math.huji.ac.il

Department of Mathematics, Princeton University, Princeton NJ, USA;
heeoh@math.princeton.edu