On Uniform Exponential Growth for Linear Groups

Alex Eskin[*], Shahar Mozes[†] and Hee Oh[‡]

August 6, 2004

1 Introduction

Let Γ be a finitely generated group. Given a finite set of generators S of Γ, the word length $l_S(\gamma)$ for an element $\gamma \in \Gamma$ is defined to be the smallest positive integer for which there exist $s_1, \cdots, s_n \in S \cup S^{-1}$ such that $\gamma = s_1 \cdots s_n$.

For each $n \in \mathbb{N}$, denote by $B_S(n)$ the set of elements in Γ whose word length with respect to S is at most n. It follows from the subadditive property of $l_S(\cdot)$ that $\lim_{n\to\infty} |B_S(n)|^{1/n}$ exists, which we denote by $\omega_S(\Gamma)$.

A finitely generated group Γ is said to be of exponential growth if $\omega_S(\Gamma) > 1$, of polynomial growth if for some $c > 0$ and $d \in \mathbb{N}$, $|B_S(n)| \leq c \cdot n^d$ for all $n \geq 1$ and of intermediate growth otherwise, for some finite generating set S of Γ. Observe that the growth type of Γ does not depend on the choice of generating set S.

If a finitely generated group Γ is linear, it is known that Γ is either of polynomial growth in which case Γ is virtually nilpotent, or of exponential growth otherwise ([Tit72], [Mil68], [Wol68]).

Definition 1.1. A finitely generated group Γ is said to have uniform exponential growth if

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

where the infimum is taken over all finite generating sets S of Γ.

[*]Research partially supported by the Packard Foundation and the BSF.
[†]Research partially supported by the BSF.
[‡]Research partially supported by NSF grant DMS0070544 and 0333397.

A main open problem concerning the growth property of a group is whether a group Γ of exponential growth is necessarily of uniform exponential growth, as first asked by Gromov (Remark 5.12 of [Gro81]).

This was answered affirmatively in the case when Γ is hyperbolic by M. Koubi [Kou98] (see also [Del96]) and in the case when Γ is solvable independently by D. Osin [Osi03] and J. Wilson [Wil00]. Recently R. Alperin and G. Noskov [AN] have announced an affirmative answer for certain subgroups of $\mathrm{SL}_2(\mathbb{C})$. For a general discussion of these questions see the survey [GdlH97].

While writing the final version of the paper we have learned from J. Wilson that he has recently constructed groups having exponential growth but not uniform exponential growth [Wil02].

Our main result is the following:

Theorem 1.2. *Let Γ be a finitely generated group which is linear over a field of characteristic 0 and not virtually solvable. Then there exists a positive integer n depending only on Γ such that for any finite generating set S of Γ, $B_S(n)$ contains two elements generating free semi subgroup.*

This immediately implies:

Theorem 1.3. *Let Γ be as above. Then Γ has uniform exponential growth.*

Combined with the results of Osin and Wilson mentioned above, our theorem implies the following:

Corollary 1.4. *Let Γ be a finitely generated subgroup of $\mathrm{GL}_n(\mathbb{C})$. The following are equivalent:*

- Γ *is not virtually nilpotent*
- Γ *is of uniform exponential growth.*
- Γ *is of exponential growth.*

Recall that for a compact Riemannian manifold M, the volume entropy $h_{\mathrm{vol}}(M)$ is given by

$$h_{\mathrm{vol}}(M) = \lim_{r\to\infty} \frac{\log V_x(r)}{r}$$

where $V_x(r)$ denotes the volume of the ball of radius r centered at (any) x in the universal cover $\tilde{M}$ with the induced metric.

One motivation for studying the notion of uniform exponential growth is the observation that if the fundamental group of a compact manifold M has uniform exponential growth then one has a positive lower bound on the volume entropy for any Riemannian metric on M of normalized diameter.

On the other hand, Manning showed that the topological entropy $h_{\text{top}}(M)$ (see [Ma79] for definition) of the geodesic flow on the unit tangent bundle of a compact Riemannian manifold M is bounded below by the volume entropy $h_{\text{vol}}(M)$ of M [Ma79].

Thus, we have the following:

Corollary 1.5. *Let M be a compact manifold such that $\pi_1(M)$ is linear over a field of characteristic 0 and not virtually nilpotent. Then*

$$\inf h_{\text{top}}(g) \geq \inf h_{\text{vol}}(g) > 0$$

where the infimum is taken over all Riemannian metric g on M with normalized diameter.

An announcement of our result has appeared in [EMO] with an account for a main strategy. The approach is outlined in §2. Sections §3-§7 are preparation for the proof of the main Theorem 1.3, which is given in §8. With the exception of Lemma 4.2, only the results labelled propositions are used in the sequel.

2 A version of the ping-pong lemma.

To show that a non virtually solvable subgroup $\Gamma < \mathrm{GL}_n(\mathbb{C})$ 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 (with respect to the word metric corresponding to the generating set S) $B_S(m)$ generating a free non-abelian semigroup. We recall the well-known result of J. Tits [Tit72] which states that any non-virtually-solvable linear group contains two elements A and B which generate a free non-abelian subgroup; the proof is based on the so called "ping-pong lemma". Theorem 1.2 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 2.1 (Ping-Pong Pair). Let V be a finite dimensional vector space. A pair of matrices $A, B \in \mathrm{SL}(V)$ is a *ping-pong pair* if there exists a nonempty subset $U \subset \mathbb{P}(V)$ such that

- $BU \cap U = \emptyset$;
- $ABU \subset U$ and $A^2BU \subset U$.

Lemma 2.2. *If a pair $A, B \in \mathrm{SL}(V)$ is a ping-pong pair then AB and A^2B generate a free semigroup.*

Proof. Suppose that the semigroup generated by AB and A^2B is not free. Then (after some cancellation) we could find a relation of the form $w_1 = w_2$, where w_1 and w_2 are words in AB and A^2B with w_1 starting with A^2B and w_2 starting with AB. But this is a contradiction since we have $A^{-1}w_1U \subset U$ and $A^{-1}w_2U \cap U = \emptyset$, and hence $A^{-1}w_1 \neq A^{-1}w_2$. $\square$

The above lemma clearly yields:

Proposition 2.3. *Let Γ be a finitely generated subgroup of $\mathrm{SL}(V)$. Suppose that there exists an integer $N \in \mathbb{N}$ such that for any finite generating subset S of Γ, $B_S(N)$ contains a ping-pong pair A and B. Then Γ has the uniform exponential growth property.*

Notation: Let k be a local field (with char $k = 0$) endowed with an absolute value $|\cdot|$ and V a k-vector space of dimension n. By fixing a basis, we identify V with k^n. We fix a norm $\|\cdot\|$ on V by

$$\|(x_1, \cdots, x_n)\| = \max\{|x_i| \mid 1 \leq i \leq n\}.$$

Define a distance d on the projective space $\mathbb{P}(V) = \mathbb{P}(k^n)$ by

$$d(x_1, x_2) = \{\inf \|v_1 - v_2\| \mid v_i \in x_i, \|v_i\| = 1 \text{ for each } i = 1, 2\}.$$

If X_1 and X_2 are closed subsets of $\mathbb{P}(V)$, we set $d(X_1, X_2)$ to be the Hausdorff distance between X_1 and X_2, that is,

$$d(X_1, X_2) = \sup\{d(x_i, X_j) \mid x_i \in X_i,\ \{i, j\} = \{1, 2\}\}$$

where $d(x_i, X_j) = \inf\{d(x_i, x_j) \mid x_j \in X_j\}$. We also set a norm on the space $M_n(k)$ of $n \times n$ matrices by

$$\|A\| = \max\{|A_{ij}| \mid 1 \leq i, j \leq n\}.$$

Before we state an effective way of showing that a pair of matrices is a ping-pong pair, we need the following simple lemma:

Lemma 2.4. *There exist a constant $C > 0$ and a positive integer l, depending only on n, such that*

$$d(Bx, By) \leq C \cdot \|B\|^l \cdot d(x, y)$$

for any $B \in \mathrm{SL}(V)$ and for any $x, y \in \mathbb{P}(V)$.

Proof: We first claim that there exists a positive constant C' and a positive integer m such that for any $B \in \mathrm{SL}(V)$,

$$C' \cdot \|B\|^{-m} \leq \inf\{\|Bv\| \mid v \in V, \|v\| = 1\}.$$

Since any matrix in $\mathrm{SL}(V)$ can be brought into a diagonal form by multiplying orthogonal matrices from both sides, we may assume that B is a diagonal matrix; and then the claim is clear since $\det B = 1$.

Now let v and w be unit vectors in V such that $v \in x$ and $w \in y$. Then

$$\|\frac{Bv}{\|Bv\|} - \frac{Bw}{\|Bw\|}\| \leq \frac{\|B\| \cdot \|v - w\|}{\inf\{\|Bv\| \mid v \in V, \|v\| = 1\}} \leq \frac{1}{C'}\|B\|^{m+1} \cdot \|v - w\|.$$

Hence,

$$d(Bx, By) \leq \frac{1}{C'} \cdot \|B\|^{m+1} \cdot d(x, y).$$

$\square$

Let $e_1, \dots e_n \in k^n$ denote the standard basis, and let $\bar{e}_1, \dots, \bar{e}_n \in \mathbb{P}(k^n)$ denote the corresponding points in projective space.

Proposition 2.5. *Let $c_1, c_2, c_3, \kappa_1, \kappa_2$, and κ_3 be fixed positive constants. Suppose that $A, B \in \mathrm{SL}_n(k)$ are matrices such that*

(L1) $A = \mathrm{diag}(a_1, \cdots, a_n)$ *with* $|a_1| \geq |a_2| \geq \cdots \geq |a_n|$ *and*

$$\frac{|a_1|}{|a_2|} \geq \max(2, c_1\|A\|^{\kappa_1})$$

for some constants $c_1 > 0$ and $\kappa_1 > 0$;

(L2) $\|A\| \geq c_2\|B\|^{1/\kappa_2}$ *for some constants $c_2 > 0$ and $\kappa_2 \geq 1$.*

(L3) $|B_{11}| \geq c_3\|A\|^{-\kappa_3}$ *and* $Be_1 \notin ke_1$ *for some constants* $c_3 > 0$ *and* $\kappa_3 \geq 0$*;*

Then there exists a constant $m \in \mathbb{N}$ *(depending only on* $n, c_1, c_2, c_3, \kappa_1, \kappa_2$*,* κ_3 *and the field* k*) such that* A^m *and* B *form a ping-pong pair.*

Proof: Denote by W the projective hyperplane spanned by $e_2, \cdots, e_n$. Let $c_B = C \cdot \|B\|^l$ be as in Lemma 2.4.

Case 1: $d(\bar{e}_1, B\bar{e}_1) \leq \frac{1}{2} \cdot d(\bar{e}_1, W) = \frac{1}{2}$.

Set
$$\delta = \frac{d(\bar{e}_1, B\bar{e}_1)}{4(c_B+1)}$$
and $U = \mathbb{B}(\bar{e}_1, \delta)$, i.e., the open ball of radius δ with the center $\bar{e}_1$ in $\mathbb{P}(k^n)$. To show that $BU \cap U = \emptyset$, assume the contrary, i.e., there exists $v \in BU \cap U$. Let $u \in U$ such that $Bu = v$. Then

$$d(B\bar{e}_1, \bar{e}_1) \leq d(B\bar{e}_1, Bu) + d(v, \bar{e}_1) \leq c_B d(\bar{e}_1, u) + d(v, \bar{e}_1) < \delta(c_B+1) < d(B\bar{e}_1, \bar{e}_1).$$

This contradiction proves the claim that $BU \cap U = \emptyset$.

Note that for any $z \in BU$,

$$d(\bar{e}_1, z) \leq d(\bar{e}_1, B\bar{e}_1) + d(B\bar{e}_1, B(B^{-1}z)) \leq d(\bar{e}_1, B\bar{e}_1) + c_B \cdot \delta \leq \tfrac{5}{4} d(\bar{e}_1, B\bar{e}_1), \quad (1)$$

and hence $BU \subset \mathbb{B}(\bar{e}_1, \frac{5}{4}d(\bar{e}_1, B\bar{e}_1)) \subset \mathbb{B}(\bar{e}_1, \frac{5}{8})$. Now consider the "stereographic projection" map
$$\pi : \mathbb{B}(\bar{e}_1, \tfrac{5}{8}) \to \{x \in k^n \mid x_1 = 1\}$$
defined by $(x_1, \cdots, x_n) \mapsto (1, \frac{x_2}{x_1}, \cdots, \frac{x_n}{x_1})$. Clearly $\pi(A^m x) = A^m \pi(x)$. Note that there is a constant $L \geq 1$ depending only on n, such that for all $x \in \mathbb{B}(\bar{e}_1, \frac{5}{8})$,

$$L^{-1}\|\pi(x) - e_1\| \leq d(x, \bar{e}_1) \leq L\|\pi(x) - e_1\|. \quad (2)$$

Also note that for any $x \in \mathbb{P} \setminus W$ and any $m \in \mathbb{N}$,

$$\|A^m \pi(x) - e_1\| \leq \left|\frac{a_2}{a_1}\right|^m \|\pi(x) - e_1\|. \quad (3)$$

In view of (L1) and (L2), since $\|A\| = |a_1|$, and $c_B \leq c \cdot \|A\|^\kappa$ for $c, \kappa > 0$ depending only on $n, c_1, c_2, \kappa_1, \kappa_2$, there exists $r_0 \geq 1$ (depending only on $n, c_1, c_2, \kappa_1, \kappa_2$) such that for any $m \geq r_0$,
$$\left|\frac{a_2}{a_1}\right|^m \leq \frac{1}{20L^2 \max(c_B, 2)}. \quad (4)$$

Hence for any $z \in BU$ and any $m \geq r_0$,

$$d(A^m z, \bar{e}_1) \leq L\|A^m\pi(z) - \bar{e}_1\| \leq L\left|\frac{a_2}{a_1}\right|^m \|\pi(z) - \bar{e}_1\| \leq L^2\left|\frac{a_2}{a_1}\right|^m d(z, \bar{e}_1)$$
$$\leq L^2\frac{5|a_2|^m}{4|a_1|^m} d(\bar{e}_1, B\bar{e}_1) \leq \frac{1}{4}\cdot\frac{c_B+1}{\max(c_B,2)}\delta \leq \frac{1}{2}\delta,$$

using (1), (4), and the definition of δ. Hence for any $m \geq r_0$, $A^m(B(U)) \subset U$.

Case 2: $d(\bar{e}_1, B\bar{e}_1) > \frac{1}{2}\cdot d(\bar{e}_1, W) = \frac{1}{2}$.

From (L2) and (L3), we have

$$\frac{|B_{11}|}{\|B\|} \geq c_2 c_3^{-\kappa_3}\|A\|^{-\kappa_2-\kappa_3}$$

and hence there exist constants $c_4 > 0$ and $\kappa_4 > 0$ (depending only on n, c_2, c_3, κ_2 and κ_3) such that $d(B\bar{e}_1, W) \geq c_4\|A\|^{-\kappa_4}$. Clearly we may assume $c_4 < 1$. Set

$$\delta = \frac{c_4}{4\cdot\|A\|^{\kappa_4}\cdot(c_B+1)}$$

and $U = \mathbb{B}(\bar{e}_1, \delta)$. Assume that there exists $v \in BU \cap U$ and let $u \in U$ such that $Bu = v$. Then

$$d(B\bar{e}_1, \bar{e}_1) \leq d(B\bar{e}_1, Bu) + d(v, \bar{e}_1) \leq c_B\cdot d(\bar{e}_1, u) + d(v, \bar{e}_1)$$
$$< \delta(c_B+1) = \frac{c_4}{4\|A\|^{\kappa_4}} < d(B\bar{e}_1, \bar{e}_1),$$

since $c_4 < 1$, $\kappa_4 \geq 0$, $\|A\| \geq 1$, and $d(\bar{e}_1, B\bar{e}_1) \geq \frac{1}{2}$. This contradiction proves that $BU \cap U = \emptyset$.

Note that for any $z \in BU$,

$$d(z, W) \geq d(B\bar{e}_1, W) - c_B\delta \geq \frac{c_4}{\|A\|^{\kappa_4}} - \frac{c_B c_4}{4\|A\|^{\kappa_4}\cdot(c_B+1)} \geq \frac{3c_4}{4\|A\|^{\kappa_4}}$$

Hence

$$BU \subset X := \{z \in \mathbb{P}(k^n) \ : \ d(z, \bar{e}_1) \leq 1 - \frac{3c_4}{4\|A\|^{\kappa_4}}\}.$$

Let π be the stereographic projection from X to $\{x \in V \mid x_1 = 1\}$ defined in the same way as in Case 1. Note that (2) holds with $L \leq 4d\cdot\frac{\|A\|^{\kappa_4}}{3c_4}$ for some constant $d > 0$ depending only on n.

Hence for any $z \in BU \subset X$ and any $m \in \mathbb{N}$,

$$d(A^m z, \bar{e}_1) \leq L^2 \left|\frac{a_2}{a_1}\right|^m d(z, \bar{e}_1)$$
$$\leq L^2 \left|\frac{a_2}{a_1}\right|^m \leq d^2 \left(\frac{4\|A\|^{\kappa_4}}{3c_4}\right)^2 \left|\frac{a_2}{a_1}\right|^m = d^2 \left(\frac{4\|A\|^{\kappa_4}}{3c_4}\right)^2 \left(\frac{4\|A\|^{\kappa_4}(c_B+1)}{c_4}\right) \left|\frac{a_2}{a_1}\right|^m \delta.$$

Hence using (L2), there exist constants $c_5 > 0$ and $\kappa_5 > 0$ depending only on $n, c_1, c_2, c_3, \kappa_1, \kappa_2, \kappa_3$ such that for any $m \in \mathbb{N}$

$$d(A^m z, \bar{e}_1) \leq c_5 \|A\|^{\kappa_5} \left|\frac{a_2}{a_1}\right|^m \delta.$$

Thus, for some integer $r_0 \in \mathbb{N}$ (depending only on $n, c_1, c_2, c_3, \kappa_1, \kappa_2, \kappa_3$), $A^m(BU) \subset U$ for all $m \geq r_0$. □

Remark: The strategy of the proof of Theorem 1.2 is to try to find words W_1 and W_2 of a length which is bounded independently of the generating set, and a matrix g such that $A = gW_1g^{-1}$ and $B = gW_2g^{-1}$ satisfy the conditions of Proposition 2.5.

3 Getting out of Zariski closed subsets

Theorem 3.1 (Generalized Bezout Theorem). *Let $X_1, \ldots, X_s$ be pure-dimensional varieties over $\mathbb{C}$ and let $Z_1, \ldots, Z_t$ be the irreducible components of $X_1 \cap \cdots \cap X_s$. Then*

$$\sum_{i=1}^{t} \deg Z_i \leq \prod_{j=1}^{s} \deg X_j$$

(see: [Sch00, p. 519])

The aim of this section is to show the following proposition using the generalized Bezout theorem:

Proposition 3.2. *Let $\Gamma \subset \mathrm{GL}_n(\mathbb{C})$ be any finitely generated subgroup and let H denote the Zariski closure of Γ, which is assumed to be Zariski-connected. For any proper subvariety X of H, there exists $N \geq 1$ (depending on X) such that for any finite generating set S of Γ, we have*

$$B_S(N) \not\subset X.$$

The rest of this section is devoted to the proof of Proposition 3.2. Let $Y = \cup_{i=1}^n Y_i \subset H$ be an algebraic variety where Y_i, $1 \le i \le n$ are the irreducible components of Y. Set $\mathrm{d}(Y) = \max_i \dim(Y_i)$. Denote by $\mathrm{irr}(Y)$ the number of irreducible components of Y, by $\mathrm{irr}_{\mathrm{md}}(Y)$ the number of irreducible components of Y of the maximal dimension $\mathrm{d}(Y)$ and by $\mathrm{mdeg}(Y)$ the maximal degree of an irreducible component of Y.

Let S be any given finite generating set of Γ in what follows.

Lemma 3.3. *If* $\mathrm{irr}_{\mathrm{md}}(Y) = 1$ *then there exists an element* $s \in S$ *such that the variety* $Z = Y \cap sY$ *satisfies* $\mathrm{d}(Z) < \mathrm{d}(Y)$.

Proof. Without loss of generality we may assume that Y_1 is the unique irreducible component of maximal dimension. If for every $s \in S$ we have $sY_1 = Y_1$ then it would follow that Y_1 is invariant under the group generated by S. However as this subgroup is Zariski dense and Y_1 is a proper closed subvariety it follows that this is impossible; hence there is some $s \in S$ such that $sY_1 \neq Y_1$. It follows that $\mathrm{d}(sY \cap Y) < \mathrm{d}(Y)$.

Lemma 3.4. *Given* Y *as above there exists an* $s \in S$ *such that for* $Z = Y \cap sY$ *either* $\mathrm{d}(Z) < \mathrm{d}(Y)$ *or* $\mathrm{irr}_{\mathrm{md}}(Z) < \mathrm{irr}_{\mathrm{md}}(Y)$.

Proof. Consider the set $\mathcal{M}$ of all maximal dimension irreducible components of Y. If every element of S would have mapped this set into itself it would have been $\langle S \rangle$-invariant and this would contradict the assumption that $\Gamma = \langle S \rangle$ is Zariski dense whereas Y is a Zariski closed proper subset. Hence there is some $s \in S$ so that for some element $Y_i \in \mathcal{M}$ $sY_i \notin \mathcal{M}$ and it follows that for $Z = Y \cap sY$ either $\mathrm{d}(Z) < \mathrm{d}(Y)$ or $\mathrm{irr}_{\mathrm{md}}(Z) < \mathrm{irr}_{\mathrm{md}}(Y)$. $\square$

Lemma 3.5. *Let* Y *be a proper subvariety of* H. *Then there exists an integer* $m \in \mathbb{N}$ *(depending only on* $\mathrm{irr}(Y)$ *and* $\mathrm{mdeg}(Y)$*) and a sequence of* m *elements* $s_0, s_1, \cdots, s_{m-1}$ *of* S *so that if we define the following sequence of varieties* $V_0 = Y$, $V_{i+1} = V_i \cap s_i V_i$, $0 \le i \le m-1$, *then* V_m *satisfies* $\mathrm{d}(V_m) < \mathrm{d}(Y)$. *Moreover* $\mathrm{irr}(V_m)$ *as well as* $\mathrm{mdeg}(V_m)$ *are also bounded above by constants depending only on* $\mathrm{irr}(Y)$ *and* $\mathrm{mdeg}(Y)$.

Proof. We shall be applying Theorem 3.1 to the intersections of pairs of irreducible varieties. Namely, let $W = \cup_{i=1}^n W_i$ be the decomposition of a Zariski closed variety W into irreducible components. Then we have $\tilde{W} = W \cap sW = \cup_{i,j=1}^n W_i \cap W_j$. Thus given $n = \mathrm{irr}(W)$ and $\mathrm{mdeg}(W)$ we have an estimate both on $\mathrm{irr}(\tilde{W})$ as well as on

$\mathrm{mdeg}(\tilde{W})$. Combining this observation with Lemmas 3.3 and 3.4 one can deduce Lemma 3.5. $\square$

Proof of Proposition 3.2. By repeated application of Lemma 3.5 at most $\mathrm{d}(X)+1$ times we find elements $w_1, w_2, \ldots, w_t \in B_S(n)$, where $n \geq 2$ is bounded above by some bound depending only on $\mathrm{irr}(X)$ and $\mathrm{mdeg}(X)$, so that $\cap_{i=1}^{t} w_i X = \emptyset$.

Observe that this implies that $B_S(n) \not\subset X$. Indeed if $B_S(n)$ were contained in X, then it would follow that $e \in \cap_{i=1}^{t} w_i X$, as $B_S(n) = B_S(n)^{-1}$ and hence $w_i^{-1} \in B_S(n)$ for each $1 \leq i \leq t$. $\square$

4 Specialization

Note that if a homomorphic image of a finitely generated group has uniform exponential growth then so does the original group. Also if Γ' is a subgroup of Γ with index d, then for any finite generating set S of Γ, $B_S(2d-1)$ contains a generating set for Γ' (see [ShaWa92]).

Thus in view of the theorem of Osin and Wilson mentioned in the introduction, we may assume in proving Theorem 1.2 that the Zariski closure of Γ is connected and simple, both in the algebraic sense.

Specialization. Let E be the ring generated by the coefficients of Γ. Note that since Γ is finitely generated it follows that E is finitely generated. Using the fact (see [LM91]) that if a finitely generated subgroup Λ of $\mathrm{GL}_n(\mathbb{C})$ is virtually solvable then there is an upper bound (say M) on the index of a solvable subgroup in Λ depending only on n, we deduce that there exists a "specialization" i.e. there exists an appropriate number field K and a ring homomorphism $\sigma : E \to K$ inducing a homomorphism $\rho : \mathrm{GL}_n(E) \to \mathrm{GL}_n(K)$ so that $\rho(\Gamma)$ is not virtually solvable. Indeed let $\Gamma_0 = \bigcap_{|\Gamma/\Lambda| \leq M} \Lambda$ and choose a number field K and a ring homomorphism $\sigma : E \to K$ so that the image of the finite index subgroup Γ_0 under the induced homomorphism ρ is not solvable. The existence of such K and σ can be deduced as follows: For a solvable subgroup H of $\mathrm{SL}(n, \mathbb{C})$ one has that the commutator group $H' = [H, H]$ is nilpotent of degree at most $n-1$. On the other hand, since the group Γ_0 is not solvable, its n-th commutator subgroup Γ_n is not trivial. Choose a non-trivial element $g \in \Gamma_n$ and observe that there is a number field K and a ring homomorphism $\sigma : E \to K$ so that under the induced homomorphism ρ, the image of g is non-trivial (see [GS79] where a much stronger assertion is proved). It follows that the image of Γ_0 under ρ is not solvable. The image $\rho(\Gamma) < \mathrm{GL}_n(K)$ cannot be virtually solvable since if it were it would follow that the image of Γ_0 would be solvable.

Hence we may assume that we have a finitely generated group Γ contained in $\mathrm{SL}_n(K)$ with K a number field and having a connected Zariski closure which is simple.

Notational Conventions. Let K be a number field. Denote by $\mathcal{V}_K$ the equivalence classes of all valuations of K. For each $\nu \in \mathcal{V}_K$, we denote by K_ν the local field which is a completion of K with respect to ν and $|\cdot|_\nu$ be the absolute value on K_ν given by ν. For any finite set of valuations $\mathcal{S}$ containing all the archimedean valuations, we denote by $\mathcal{O}_K(\mathcal{S})$ the ring of $\mathcal{S}$-integral elements in K, that is,

$$\mathcal{O}_K(\mathcal{S}) = \{x \in K \mid |x|_\nu \leq 1 \text{ for each } \nu \notin \mathcal{S}\}$$

Since Γ is finitely generated, we may, after possibly replacing Γ by a finite index subgroup, assume that $\Gamma \subset \mathrm{SL}_n(\mathcal{O}_K(\mathcal{S}))$, where $\mathcal{S} \subset \mathcal{V}_K$ consists of all archimedean valuations as well as the valuations ν such that Γ is unbounded in $\mathrm{GL}_n(K_\nu)$. Thus the diagonal embedding of Γ in $\prod_{\nu\in\mathcal{S}} \mathrm{SL}_n(K_\nu)$ is discrete.

It follows that if Γ is infinite, then the image of Γ in $\prod_{\nu\in\mathcal{S}} \mathrm{SL}_n(K_\nu)$ is unbounded under the diagonal embedding.

Summarizing the above discussion we have:

Proposition 4.1. *It suffices to prove Theorem 1.2 for any finitely generated subgroup $\Gamma \subset \mathrm{SL}_n(\mathcal{O}_K(\mathcal{S}))$ whose image in $\prod_{\nu\in\mathcal{S}} \mathrm{SL}_n(K_\nu)$ is unbounded under the diagonal embedding, where K is a number field, $\mathcal{S}$ a finite set of valuations containing all archimedean valuations and the Zariski closure H of Γ is connected and simple.*

Notational Convention. A positive constant depending only on n, K, H and $\mathcal{S}$ will be referred to in the rest of the paper as a *bounded* constant.

Remark. For any group Γ as in Proposition 4.1 the lower bound on the rate of exponential growth actually depends only on n, K, H and $\mathcal{S}$.

We choose, for each $\nu \in \mathcal{S}$, an extension of the absolute value $|\cdot|_\nu$ to the algebraic closure $\bar{K}$ of K and denote by $\bar{K}_\nu$ the completion of $\bar{K}$ with respect to the valuation ν. For any $A \in \mathrm{SL}_n(\mathcal{O}_K(\mathcal{S}))$, we set

$$\Lambda(A) := \max\{|\lambda|_\nu \mid \lambda : \text{an eigenvalue of } A,\ \nu \in \mathcal{S}\}.$$

For $x = (x_\nu)_{\nu\in\mathcal{S}} \in \prod_{\nu\in\mathcal{S}} \bar{K}_\nu$ and $A = (A_\nu)_{\nu\in\mathcal{S}} \in \prod_{\nu\in\mathcal{S}} \mathrm{SL}_n(\bar{K}_\nu)$, we set

$$|x| = \max_{\nu\in\mathcal{S}} |x_\nu|_\nu \quad \text{and} \quad \|A\| = \max_{\nu\in\mathcal{S}} \|A_\nu\|_\nu.$$

For $A \in \mathrm{SL}_n(\mathcal{O}_K(\mathcal{S}))$, the notation $\|A\|$ is understood via the identification of $\mathrm{SL}_n(\mathcal{O}_K(\mathcal{S}))$ with its diagonal embedding into $\prod_{\nu\in\mathcal{S}} \mathrm{SL}_n(\bar{K}_\nu)$,

The following simple lemma plays a key role in the proof. It is the main reason we specialize so that $\Gamma \subset \mathrm{SL}_n(\mathcal{O}_K(\mathcal{S}))$.

Lemma 4.2. *Suppose $A \in \mathrm{SL}_n(\mathcal{O}_K(\mathcal{S})))$. Then*

(a) *If $\lambda_1, \cdots, \lambda_m$ is the set of all distinct eigenvalues of A, then*

$$\prod_{\nu\in\mathcal{S}} \prod_{1\le i<j\le m} |\lambda_i - \lambda_j|_\nu \ge 1.$$

(b) *For each $\nu \in \mathcal{S}$,*

$$\prod_{1\le i<j\le m} |\lambda_i - \lambda_j|_\nu \ge C \cdot \Lambda(A)^{-N},$$

for some positive constants C and N depending only on n and $\mathcal{S}$.

Proof: First note that $x := \prod_{1\le i<j\le m}(\lambda_i - \lambda_j) \in K$, since $\prod_{1\le i<j\le m}(\lambda_i - \lambda_j)$ is stable under the Galois group Gal $(\hat{K}/K)$ where $\hat{K}$ is the splitting field of the characteristic polynomial of A. If $\nu \notin \mathcal{S}$, $A \in \mathrm{SL}_n(\mathcal{O}_\nu)$ where $\mathcal{O}_\nu$ denotes the valuation ring of K_ν; hence $|\lambda_i - \lambda_j|_\nu \le 1$ for each $1 \le i \ne j \le m$. It follows that $\prod_{\nu\notin\mathcal{S}} |x|_\nu \le 1$. On the other hand, by the product formula, we have $\prod_{\nu\in\mathcal{V}_K} |x|_\nu = 1$. Hence $\prod_{\nu\in\mathcal{S}} |x|_\nu \ge 1$.

To show (b), in view of (a) it suffices to note that

$$|\lambda_i - \lambda_j|_\nu \le 2\Lambda(A)$$

for each $1 \le i < j \le n$. □

5 The Main Proposition

Motivation. In the sequel we would like given two matrices to produce words of bounded length whose entries satisfy certain conditions. Fix a valuation $\nu \in \mathcal{V}_K$ and rescale the given matrices so that their norms are less than 1. Given N and ϵ, there always exists a subspace $V = V(N, \epsilon, \nu) \subset M_n(K_\nu)$ of minimal dimension such that every word of length at most N, is within ϵ of V. (It is possible that $V = M_n(K_\nu)$). Roughly, the assertion of the main proposition (see Proposition 5.1 below) is that with the appropriate choice of constants we can choose V to be an *algebra* (i.e. is closed under matrix multiplication). This implies strong restrictions on V, some of which we will discuss in §6.

The group $T(A,\nu)$. Let $A = \mathrm{diag}(\lambda_1, \lambda_2, \dots, \lambda_n)$ be a diagonal matrix, and let $K' \supset K$ be the field generated by the elements of A over K. We assume $n! \geq [K' : K]$. Let $\nu \in \mathcal{S}$ be a valuation. Let $T = T(A,\nu) < \mathrm{SL}_n(K'_\nu)$ to be the subgroup of the diagonal defined by $T = \{\mathrm{diag}(t_1, t_2, \dots, t_n) \in \mathrm{SL}_n(K'_\nu) \ : \ t_i = t_j \text{ whenever } \lambda_i = \lambda_j\}$. Note that any element which commutes with A commutes with all of T as well. We remark that since there are only finitely many extension fields of degree at most $n!$ of K_ν (cf. [Kob84] chapter III) there are only finitely many possibilities for T independent of the specific element A.

The T-blocks of B. Let W_{ij} be the eigenspaces for both right and left action of T on $M_n(K'_\nu)$, so that for $C_{ij} \in W_{ij}$, $S^k C_{ij} S^l = \lambda_i^k \lambda_j^l C_{ij}$ for any $S = \mathrm{diag}(\lambda_1, \cdots, \lambda_n)$ in T. In particular, if T is the whole diagonal subgroup of SL_n, then each W_{ij} is spanned by the elementary matrix E_{ij}. As another example if $T = \{\mathrm{diag}(t,t,t^{-2}) \ : \ t \in K'_\nu\}$ then

$$W_{11} = \begin{pmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad W_{12} = \begin{pmatrix} 0 & 0 & * \\ 0 & 0 & * \\ 0 & 0 & 0 \end{pmatrix} \quad W_{21} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ * & * & 0 \end{pmatrix} \text{ and } W_{22} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & * \end{pmatrix}$$

Note that by the choice of T, W_{ij} with respect to T is the same as those with respect to the single element A.

For a matrix $B \in \mathrm{SL}_n(K'_\nu)$, define $B_{ij} = \mathrm{pr}_{W_{ij}}(B)/\|B\|_\nu$, where pr denotes orthogonal projection of $M_n(K'_\nu)$ onto W_{ij}. We call the B_{ij} the *blocks of* B with respect to the torus T. Observe that $B_{ij}B_{st} = 0$ unless $j = s$; hence any nonzero word in the T-blocks of B is of the form $B_{i_1 i_2} B_{i_2 i_3} \cdots B_{i_r i_{r+1}}$ for some $1 \leq i_1, \cdots, i_{r+1} \leq m$ (here m is equal to the number of different eigen-values of A and in particular $m \leq n$). In the rest of this paper the notation B_{ij} always denotes the blocks of B with respect to some torus of the diagonal subgroup which will be specified whenever used. For an $n \times n$ matrix X, the notation X^T means its transpose as usual.

We can now state

Proposition 5.1 (Main Proposition). *Let $K' \supset K$ be a field extension with $[K' : K] \leq n!$. Let $A \in \mathrm{SL}_n(K')$ be a diagonal element which is conjugate to an element of $\mathrm{SL}_n(\mathcal{O}_K(S))$ and let $T = T(A,\nu)$. For each $\nu \in \mathcal{S}$, let $B \in \mathrm{SL}_n(K'_\nu)$. For any $\epsilon > 0$, there exists a subalgebra $\mathcal{E}_\nu(\epsilon) \subset M_n(K'_\nu)$ normalized by T such that*

(a) *for any word w in the blocks of B (with respect to ν) of length at most 2^{2n^2},*

$$d_\nu(w, \mathcal{E}_\nu(\epsilon)) < \epsilon,$$

where $d_\nu(w,V) = \inf_{v\in V} \|w-v\|_\nu$.

(b) *for any* $\theta \in M_n(K'_\nu)$, *there exists a word* $W_\nu(\epsilon)$ *in* A *and* B *of length at most* 2^{2n^2} *such that*

$$|\langle \theta, W_\nu(\epsilon)\rangle|_\nu \geq c \cdot \Lambda(A)^{-r_1} \cdot \|B\|_\nu \cdot \left(\sup_{X\in\mathcal{E}_\nu(\epsilon)\setminus\{0\}} \frac{|\langle\theta, X\rangle|_\nu}{\|X\|_\nu} - 2\epsilon\|\theta\|_\nu \right),$$

where the inner product $\langle\cdot,\cdot\rangle$ *is given by* $\langle X, Y\rangle = \operatorname{Tr} XY^T$, r_1 *is a positive constant depending only on* n, K *and* $\mathcal{S}$, *and* c *is a positive constant depending only on* n, K, $\mathcal{S}$ *and* ϵ.

Remarks. If θ is almost orthogonal to $\mathcal{E}_\nu(\epsilon)$ the statement (b) is vacuous.

In the course of the proof we will first prove an alternative version of assertion (b), namely,

(b') *for any* $\theta \in M_n(K'_\nu)$, *there exists a word* $W_\nu(\epsilon)$ *in the blocks of* B *of length at most* 2^{n^2+2} *such that*

$$|\langle \theta, W_\nu(\epsilon)\rangle|_\nu \geq c \cdot \Lambda(A)^{-r_1} \cdot \|B\|_\nu \cdot \left(\sup_{X\in\mathcal{E}_\nu(\epsilon)\setminus\{0\}} \frac{|\langle\theta, X\rangle|_\nu}{\|X\|_\nu} - 2\epsilon\|\theta\| \right),$$

where r_1 *is a positive constant depending only on* n, K *and* $\mathcal{S}$, *and* c *is a positive constant depending only on* n, K, $\mathcal{S}$ *and* ϵ.

The assertion (b') is essentially the statement that $\mathcal{E}_\nu(\epsilon)$ viewed as a subspace is of minimal dimension among all subspaces satisfying (a). Indeed, if there is an element $v \in \mathcal{E}_\nu(\epsilon)$ which is almost orthogonal to all the words in the blocks of B of length at most 2^{n^2+2}, then we can choose $\theta = v$ (and $X = v$), contradicting (b').

The rest of this section consists of the proof of Proposition 5.1. The proof relies on a concept of an *almost-algebra*. Roughly, an almost-algebra is a subspace of $M_n(K'_\nu)$ which is "almost" closed under matrix multiplication. In §5.1 we make a precise definition and show that any almost-algebra is close to an algebra. In §5.2 we show how to obtain an almost-algebra which will lie close to the words generated by any given finite collection of elements (which in our case will be the blocks of B). This almost-algebra will then be close to an algebra V which will satisfy the conditions (a) and (b') of Proposition 5.1. It will also be normalized by T, since all the blocks of B are normalized by T. Finally, in §5.3, we show how to get the condition (b) from (b'). This is done by a direct argument using the Vandermonde determinant.

5.1 Almost algebras

Let k be a local field (with char $k = 0$) endowed with an absolute value $|\cdot|$. For $A \in M_n(k)$, we set $\|A\| = |\langle A, A\rangle|^{1/2}$, where the inner product $\langle\cdot,\cdot\rangle$ was defined in Proposition 5.1. Since this norm is equivalent to the one defined in Section 2 (in fact they coincide when k is non-archimedean), we do not need to distinguish them for our purpose. Let $d(A, B) = \|A - B\|$ denote the associated distance function on $M_n(k)$. Considering the canonical projection $\pi : M_n(k) - \{0\} \to \mathbb{P}(M_n(k))$, for subspaces V_1 and V_2 of $M_n(k)$, we define $d(V_1, V_2)$ to be the Hausdorff distance between $\pi(V_1 - \{0\})$ and $\pi(V_2 - \{0\})$.

For a subset $\Lambda \subset \mathrm{GL}_n(k)$, we say that a subspace V of $M_n(k)$ is normalized by Λ if $AVA^{-1} = V$ for all $A \in \Lambda$.

For $\epsilon > 0$, we say that a subspace V of $M_n(k)$ is an *ϵ-almost subalgebra* if

$$\sup_{X,Y\in V\setminus\{0\}} \frac{d(XY, V)}{\|X\|\cdot\|Y\|} < \epsilon,$$

where, as usual, the distance between a vector z and a subspace V is given as $\inf_{v\in V} \|z - v\|$.

Lemma 5.2. *If there exists an orthonormal basis $\{A_1, \ldots, A_m\}$ of a subspace $V \subset M_n(k)$ such that $d(A_iA_j, V) < \epsilon$ for all $1 \le i, j \le m$, then V is an $n^4 \cdot \epsilon$-almost subalgebra of $M_n(k)$.*

Proof. Consider arbitrary elements $X, Y \in V$. Then for some $x_i, y_i \in k$, we have $X = \sum_{i=1}^m x_iA_i$ and $Y = \sum_{i=1}^m y_iA_i$. Let $C_{ij} \in V$ such that $d(A_iA_j, V) = d(A_iA_j, C_{ij})$. Note that $\|XY - \sum_{ij} x_iy_jC_{ij}\| \le \sum_{1\le i,j\le m} |x_iy_j|\cdot\|A_iA_j - C_{ij}\| \le m^2\|X\|\cdot\|Y\|\epsilon$. Since $m \le n^2$, V is an $n^4 \cdot \epsilon$-almost subalgebra. □

Theorem 5.3 (Almost algebras are close to algebras). *There exists an increasing function $h : \mathbb{R}^+ \to \mathbb{R}^+$, depending only on n, with $h(\epsilon) \to 0$ as $\epsilon \to 0$ such that for any ϵ-almost-subalgebra $V \subset M_n(k)$ there exists a subalgebra $\mathcal{E}_\epsilon \subset M_n(k)$ such that $d(V, \mathcal{E}_\epsilon) < h(\epsilon)$. Moreover if V is normalized by a subset $\mathcal{T}$ of $\mathrm{SL}_n(k)$, we may take $\mathcal{E}_\epsilon$ to be normalized by $\mathcal{T}$ as well.*

Proof. (This proof was suggested to us by G. Margulis.) For a subspace V of $M_n(k)$, define $\eta(V) = 1$ if there is no subalgebra of $M_n(k)$ of dimension same as that of V; otherwise set $\eta(V)$ to be

$$\inf\{d(V, \mathcal{E}_0) : \mathcal{E}_0 \text{ is a subalgebra of } M_n(k) \text{ with } \dim \mathcal{E}_0 = \dim V\}.$$

For any $\epsilon > 0$, define

$$h(\epsilon) = \sup\{\eta(V) : V \text{ is an } \epsilon\text{-almost-algebra in } M_n(k)\}.$$

Clearly h is an increasing function on $\mathbb{R}^+$. We only need to show that $h(\epsilon) \to 0$ as $\epsilon \to 0$. Suppose not. Then there exist $\delta > 0$, a sequence $\epsilon_n \to 0$ and a sequence V_n of ϵ_n-almost-subalgebras such that for any n, $\eta(V_n) > \delta$. But by the compactness of the Grassmannian variety of $M_n(k)$, there is a subsequence of $\{V_n\}$ which converges to V. It is then easy to see that V must be an algebra and hence $\eta(V_n) \to 0$, which yields a contradiction. In the case when V is normalized by $\mathcal{T}$, we modify the definition of $\eta(V)$ so that we take the infimum only over those subalgebras which are normalized by $\mathcal{T}$. Then it is easy to see that the resulting subalgebra V is also normalized by $\mathcal{T}$. $\square$

5.2 Almost algebras generated by a finite set.

Lemma 5.4. *Let T be a torus in $\mathrm{SL}_n(k)$, i.e., a commutative subgroup consisting of semisimple elements. Consider matrices $B_1, \ldots, B_m \in M_n(k)$ such that for each $1 \le i \le m$, $\|B_i\| \le 1$ and AB_iA^{-1} is a scalar multiple of B_i for each $A \in T$. Then for any $\epsilon > 0$, there exists a subalgebra $\mathcal{E}_\epsilon \subset M_n(k)$ normalized by T such that*

- *for any word w in $B_1, \cdots, B_m$ of length at most 2^{n^2+2},*
$$d(w, \mathcal{E}_\epsilon) \le \epsilon;$$
- *for any $\theta \in M_n(k)$, there exists a word w in $B_1, \cdots, B_m$ of length at most 2^{n^2+2} such that*
$$|\langle \theta, w\rangle| \ge c \cdot \left(\sup_{X \in \mathcal{E}_\epsilon \setminus \{0\}} \frac{|\langle \theta, X\rangle|}{\|X\|} - 2\epsilon\|\theta\| \right), \tag{5}$$
where c is a positive constant depending only on n and ϵ.

Proof. Let $\epsilon_0 = \epsilon$. For each $0 \le r \le n^2+1$, let us choose constants $\epsilon_r > 0$ as big as possible so that $\epsilon_{r+1} \le \epsilon\epsilon_r^{2n^2}/(3n^4 2^{2n^2})$, $\epsilon_{r+1} \le \epsilon\epsilon_r^{n^2}/(n^2 2^{n^2+1})$, and $h(3n^4 2^{2n^2}\epsilon_r^{-2n^2}\epsilon_{r+1}) \le \epsilon_r/(3n^2)$. In the following proof, a word means a word in $B_1, \cdots, B_m$. For each $1 \le r \le n^2+1$, let

$$f(r) = \inf\{j \in \mathbb{N} |\ \text{there exists a subspace } V_r \subset M_n(k) \text{ of dimension } j \text{ normalized by } T \text{ and such that } d(V_r, w) \le \epsilon_r \text{ for any word } w \text{ of length at most } 2^r.\ \}$$

If $f(1) = 0$, then $\|B_i\| < \epsilon_0$ for each $1 \leq i \leq m$, and hence it suffices to take $\mathcal{E}_\epsilon = \{0\}$ to prove the claim. Suppose that $f(1) \geq 1$. By construction, the function f is increasing, and is bounded by n^2. Hence there exists a minimal integer $1 \leq r \leq n^2+1$ such that $f(r) = f(r+1)$. Fix a subspace $V_{r+1} \subset M_n(k)$ of dimension $f(r)$ such that $d(V_{r+1}, w) \leq \epsilon_{r+1}$ for any word w of length at most 2^{r+1}.

Claim 5.5. *The subspace V_{r+1} is an $3n^4 2^{2n^2} \epsilon_r^{-2n^2} \epsilon_{r+1}$-almost subalgebra of $M_n(k)$ normalized by T, and for every $\theta \in M_n(k)$, there exists a word w of length at most 2^r such that*

$$|\langle \theta, w \rangle| \geq \frac{\epsilon \epsilon_r^{n^2}}{n^2 2^{n^2+1}} \cdot \left(\sup_{v \in V_{r+1} \setminus \{0\}} \frac{|\langle \theta, v \rangle|}{\|v\|} - \epsilon \|\theta\| \right). \tag{6}$$

Proof of claim. For a subspace W of $M_n(k)$, the notation pr_W means the projection map of $M_n(k)$ to W. For simplicity, let $p = \mathrm{pr}_{V_{r+1}}$. By the definition of f, for any word w of length at most 2^{r+1}, we have

$$\|p(w) - w\| < \epsilon_{r+1}.$$

We now pick words $w_1, \ldots w_{f(r)}$ of length at most 2^r inductively as follows: w_1 is a word of length at most 2^r of maximal norm, and for each $2 \leq j \leq f(r)$, denoting by W_{j-1} the subspace spanned by $\{w_1, \ldots, w_{j-1}\}$, let w_j be a word such that the norm $\|\mathrm{pr}_{W_{j-1}^\perp}(w_j)\|$ is maximal among all words of length at most 2^r. Clearly each W_{j-1} is normalized by T.

Note that for each $1 \leq j \leq f(r)$, $\|\mathrm{pr}_{W_{j-1}^\perp}(w_j)\| > \epsilon_r$, since, otherwise, all the words of length at most 2^r would be within ϵ_r-distance to the subspace W_{j-1} where $j-1 = \dim W_{j-1} < f(r)$, contradicting the definition of f. Let $W'_j \subset V_{r+1}$ denote the subspace spanned by the projections $p(w_1), \cdots, p(w_j)$.

Then

$$\begin{aligned} \|\mathrm{pr}_{(W'_{j-1})^\perp}(p(w_j))\| &= d(p(w_j), W'_{j-1}) \\ &\geq d(w_j, W'_{j-1}) - d(w_j, p(w_j)) \geq \epsilon_r - \epsilon_{r+1} \geq \frac{\epsilon_r}{2} \end{aligned}$$

Hence the vectors $p(w_j)$, $1 \leq j \leq f(r)$, form a basis for V_{r+1}, and the determinant of the matrix, say Q, whose rows are the vectors $p(w_j)$ is at least $\epsilon_r^{n^2}/2^{n^2}$ (cf. Lemma 7.5). Thus if $X = \sum_{j=1}^{f(r)} x_j p(w_j)$ for some $x_j \in k$, then

$$\max_j |x_j| \leq \det(Q)^{-1} \|X\| \leq 2^{n^2} \epsilon_r^{-n^2} \|X\|, \tag{7}$$

using $\|p(w_j)\| \leq \|w_j\| \leq 1$ for each $1 \leq j \leq f(r)$. On the other hand,

$$d(w_i w_j, V_{r+1}) < \epsilon_{r+1}; \quad \text{hence} \quad d(p(w_i)p(w_j), V_{r+1}) < 3\epsilon_{r+1}.$$

Thus for any $X_1 = \sum_j c_{1j} p(w_j)$ and $X_2 = \sum_j c_{2j} p(w_j)$ in V_{r+1} of unit norm, we have

$$\begin{aligned} d(X_1 X_2, V_{r+1}) \leq & \sum_{1 \leq i,j \leq f(r)} c_{1i} c_{2j} d(p(w_i)p(w_j), V_{r+1}) \\ & \qquad \leq f(r)^2 2^{2n^2} \epsilon_r^{-2n^2} 3\epsilon_{r+1} \leq 3n^4 2^{2n^2} \epsilon_r^{-2n^2} \epsilon_{r+1}. \end{aligned}$$

It follows that V_{r+1} is an $3n^4 2^{2n^2} \epsilon_r^{-2n^2} \epsilon_{r+1}$-almost-subalgebra of $M_n(k)$.

Let $\tilde{\theta}$ denote the orthogonal projection of θ to V_{r+1}. Then, since θ and $\tilde{\theta}$ differ by an element of $V_{r+1}^{\perp}$, we have $\langle \theta, v \rangle = \langle \tilde{\theta}, v \rangle$ for all $v \in V_{r+1}$. Hence

$$\sup_{v \in V_{r+1} \setminus \{0\}} \frac{|\langle \theta, v \rangle|}{\|v\|} = \|\tilde{\theta}\|.$$

If $\|\tilde{\theta}\| \leq \epsilon \|\theta\|$, then there is nothing to prove. Hence, we may assume that $\|\tilde{\theta}\| \geq \epsilon \|\theta\|$. We may write $\tilde{\theta} = \sum x_j p(w_j)$. Taking inner product with $\tilde{\theta}$ we obtain,

$$\|\tilde{\theta}\|^2 = \sum x_j \langle p(w_j), \tilde{\theta} \rangle.$$

Hence there is a j such that $|x_j \langle p(w_j), \tilde{\theta} \rangle| \geq \frac{1}{n^2} \|\tilde{\theta}\|^2$. Then, in view of (7), we have

$$|\langle p(w_j), \tilde{\theta} \rangle| \geq \frac{\epsilon_r^{n^2}}{n^2 2^{n^2}} \|\tilde{\theta}\|.$$

Hence

$$\begin{aligned} |\langle \theta, w_j \rangle| \geq |\langle \theta, p(w_j) \rangle| - |\langle \theta, w_j - p(w_j) \rangle| \geq & \frac{\epsilon_r^{n^2}}{n^2 2^{n^2}} \|\tilde{\theta}\| - \epsilon_{r+1} \|\theta\| \\ & \geq \frac{\epsilon_r^{n^2}}{n^2 2^{n^2}} \|\tilde{\theta}\| - \frac{\epsilon_{r+1}}{\epsilon} \|\tilde{\theta}\| \geq \frac{\epsilon_r^{n^2}}{n^2 2^{n^2+1}} \|\tilde{\theta}\| \end{aligned}$$

where the last inequality is justified on the choice of ϵ_r made in the beginning of the proof.

This proves the claim. □

Proof of Lemma 5.4. Note that by the choice of ϵ_r, $\epsilon \leq 3n^4 2^{2n^2} \epsilon_r^{-2n^2} \epsilon_{r+1}$. Hence by Theorem 5.3, there exists an algebra $\mathcal{E}_\epsilon$ such that

$$d(V_{r+1}, \mathcal{E}_\epsilon) < h(3n^4 2^{2n^2} \epsilon_r^{-2n^2} \epsilon_{r+1}) < \epsilon_r / (3n^2) \leq \epsilon.$$

Now, (5) follows from (6). □

5.3 Proof of Proposition 5.1

Proposition 5.1 (a) and (b') follow from Lemma 5.4. To complete the proof we need to show how to deduce (b) from (b').

Fix $\epsilon > 0$. Consider the subalgebra $\mathcal{E}_\epsilon \subset M_n(K'_\nu)$ and N_ϵ as in Lemma 5.4. Let $\theta \in M_n(k)$, as observed before we may assume that $\|\tilde{\theta}\| \geq \epsilon\|\theta\|$, where $\tilde{\theta}$ denotes the orthogonal projection of θ into $\mathcal{E}_\epsilon$. (Otherwise (b) is vacuous).

Then for some $2 \leq r \leq 2^{n^2+2}+1$, there exists an r-tuple $(i_1, \cdots, i_r)$ of positive integers with $1 \leq i_j \leq m$ for each $1 \leq j \leq r$ such that

$$|\langle \theta, B_{i_1 i_2} B_{i_2 i_3} \dots B_{i_{r-1} i_r} \rangle| \geq c \cdot \sup_{X \in \mathcal{E}_\epsilon \setminus \{0\}} \frac{|\langle \theta, X \rangle|_\nu}{\|X\|_\nu}.$$

Note that for any positive integers $0 \leq k_1, \cdots, k_r \leq m-1$,

$$\operatorname{Tr}(\theta^T A^{k_1} B A^{k_2} B \dots B A^{k_r}) = \|B\|_\nu^{r-1} \cdot \sum_{I=(i_1,\dots,i_r)} \lambda_{i_1}^{k_1} \dots \lambda_{i_r}^{k_r} \operatorname{Tr}(\theta^T_{i_r i_1} B_{i_1 i_2} B_{i_2 i_3} \dots B_{i_{r-1} i_r}) \tag{8}$$

where the sum is taken over all the r-tuples $I = (i_1, \cdots, i_r)$ such that $1 \leq i_j \leq m$ for all $1 \leq j \leq r$.

Let $(\theta^T B)_I$ denote $\operatorname{Tr}(\theta^T_{i_r i_1} B_{i_1 i_2} B_{i_2 i_3} \dots B_{i_{r-1} i_r})$, that is

$$(\theta^T B)_I = \langle \theta, B_{i_1 i_2} B_{i_2 i_3} \dots B_{i_{r-1} i_r} \rangle.$$

For each multi-index $L = (l_1, \cdots, l_r)$ and $I = (i_1, \cdots, i_r)$ where $0 \leq l_j \leq m-1$ and $1 \leq i_j \leq m$ for each $1 \leq j \leq r$, let

$$D_{IL} = \lambda_I^L = \lambda_{i_1}^{l_1} \dots \lambda_{i_m}^{l_m}$$

and

$$C(L) = \operatorname{Tr} \theta^T A^{l_1} B A^{l_2} B \dots B A^{l_m}.$$

Thus (8) can be rewritten as

$$C(L) = \|B\|_\nu^{m-1} \sum_I D_{IL} (\theta^T B)_I$$

If we set the $m \times m$-matrix

$$X = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \lambda_1 & \lambda_2 & \dots & \lambda_m \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1^{m-1} & \lambda_2^{m-1} & \dots & \lambda_m^{m-1} \end{pmatrix}$$

then the $m^r \times m^r$-matrix D whose IL entry is $D_{IL} = \lambda_I^L$ coincides with the Kronecker tensor product $\otimes^r X$. Since $\det X = \prod_{1\le i<j\le m}(\lambda_i - \lambda_j)$, $\det D = \prod_{1\le i<j\le n}(\lambda_i - \lambda_j)^{rm^{r-1}}$.

In view of Lemma 4.2, $\|D^{-1}\|_\nu \le C\Lambda(A)^M$, where C and M are positive constants depending only on n, m, L and $\mathcal{S}$ (note that the dependency on r is resolved to that on N, but N is again dependent only on n, m, L and $\mathcal{S}$.)

Therefore

$$\|B\|_\nu^{r-1} \cdot \max_I |(\theta^T B)_I|_\nu \le C \cdot \Lambda(A)^M \cdot \max_L |C(L)|_\nu.$$

Hence

$$\max_L |C(L)|_\nu \ge \epsilon \cdot \frac{c}{C} \cdot \Lambda(A)^{-M} \cdot \|B\|_\nu^{r-1} \cdot \sup_{X\in\mathcal{E}_\epsilon\setminus\{0\}} \frac{|\langle\theta, X\rangle|}{\|X\|},$$

where K ranges over the multi indices $(l_1, \cdots, l_r)$ with $0 \le l_j \le m-1$ for all $1 \le j \le r$. Note that $r-1 \ge 1$, since $r \ge 2$. Noting that $C(L) = \mathrm{Tr}(\theta^T A^{l_1} B A^{l_2} B \cdots B A^{l_r})$ and that the word $A^{l_1} B A^{l_2} \cdots B A^{l_r}$ is of length less than $m(2^{n^2+2}+1)$ for any L, set $\mathcal{E}_\nu(\epsilon) = \mathcal{E}_\epsilon$. Since $m(2^{n^2+2}+1) \le 2^{2n^2}$, the claim is proved. □

6 Algebras

In view of §5, we need a result on the subalgebras of $M_n(k)$, where k is a local field. Denote by $\mathcal{D}$ the diagonal subgroup of $\mathrm{SL}_n(k)$. In this section, we fix a subtorus T of $\mathcal{D}$.

We say that an algebra is *unipotent* if it is nilpotent and its exponentiation is a unipotent group. Note that if an algebra is not unipotent, then it contains an element of non-zero trace. On the other hand, for any unipotent algebra, there exists an element $\alpha \in \mathrm{SL}_n(k)$ such that conjugation by α contracts each element in the algebra by a given factor. The following proposition is a quantitative version of the combination of these assertions.

Proposition 6.1. *For any $0 < \eta < 1$ there exist constants $d_1 > 0$ and $d_2 > 0$ (depending only on η and n) such that for any subalgebra $\mathcal{E}$ of $M_n(k)$ normalized by T, one of the following holds:*

(1) *There exists $X \in \mathcal{E}$ with $|\mathrm{Tr}\, X| > d_1\|X\|$.*

(2) *There exists $g \in \mathrm{SL}_n(k)$ in the centralizer of T with $\max(\|g\|, \|g^{-1}\|) \le d_2$ such that for all $X \in \mathcal{E}$, $\|gXg^{-1}\| \le \eta\|X\|$.*

The rest of the section consists of the proof of Proposition 6.1.

Let $\mathcal{E}$ be a subalgebra of $M_n(k)$ normalized by T and let $m = \dim \mathcal{E}$. Let $\mathcal{G}$ denote the Grassmanian of m-dimensional subspaces of $M_n(k)$. Let $\mathcal{R} \subset \mathcal{G}$ denote the subset consisting of subalgebras which are normalized by T. It is easy to see that $\mathcal{R}$ is closed in $\mathcal{G}$. Denote by $\mathcal{R}^u$ the subset of $\mathcal{R}$ consisting of unipotent algebras. Then $\mathcal{R}^u$ is also a closed subset of $\mathcal{G}$. Note that for a subalgebra $\mathcal{E} \in \mathcal{R}$, $\mathcal{E}$ belongs to $\mathcal{R}^u$ if and only if $\operatorname{Tr} X = 0$ for all $X \in \mathcal{E}$.

Lemma 6.2. *Suppose $\delta > 0$. Let $\mathcal{E}$ be a subalgebra of $M_n(k)$ normalized by T. Then at least one of the following holds:*

(a) *For some constant $d > 0$ depending only on T and δ, there exists an element $X \in \mathcal{E}$ such that $|\operatorname{Tr} X| > d \cdot \|X\|$.*

(b) $d(\mathcal{E}, \mathcal{R}^u) < \delta$.

Proof: Let $\mathcal{F} \subset \mathcal{R}$ denote the complement of the open δ-neighborhood of $\mathcal{R}^u$ in $\mathcal{R}$. Then $\mathcal{F}$ is a compact subset of $\mathcal{G}$. Note that for each $E_0 \in \mathcal{F}$, there exists $X \in E_0$ with $|\operatorname{Tr} X| > 0$. Then, by compactness of $\mathcal{F}$, there is a constant $d > 0$ depending on δ and on T such that

$$\inf_{\mathcal{E}_0 \in \mathcal{F}} \sup_{X \in \mathcal{E}_0 \setminus \{0\}} \frac{|\operatorname{Tr} X|}{\|X\|} > d.$$

□

Lemma 6.3. *For any unipotent subalgebra $\mathcal{E}_0$ of $M_n(k)$ and a diagonal subalgebra $\tilde{T}$ normalizing $\mathcal{E}_0$, there exists $g \in \mathrm{SL}_n(k)$ such that $\|g\|, \|g^{-1}\| \leq 1$, $g\mathcal{E}_0 g^{-1}$ is contained in the upper triangular subalgebra and $g\tilde{T}g^{-1}$ is contained in the diagonal subalgebra of $M_n(k)$.*

Proof: Let $e_1, \cdots, e_n$ denote the standard basis in k^n. Let $0 = V_0 \subset V_1 \subset \cdots \subset V_r = k^n$ be the flag associated with $\mathcal{E}_0$. (I.e., $\mathcal{E}_0 V_i \subset V_{i-1}$ with $V_{-1} = 0$). Let $k^n = E_1 \oplus \cdots \oplus E_s$ be the decomposition of k^n into the eigenspaces of $\tilde{T}$ corresponding to the distinct eigenvalues. Then since $\tilde{T}$ normalizes $\mathcal{E}_0$ we have

$$V_i = \oplus_{j=1}^{s} (V_i \cap E_j) \quad \text{for each } i. \tag{9}$$

For each $1 \leq j \leq s$, consider the flag F_j in E_j given by

$$0 \subset E_j \cap V_1 \subset \cdots \subset E_j \cap V_r = E_j.$$

Let L_j be a flag in E_j of same type as F_j compatible with the basis $E_j \cap \{e_1, \dots, e_n\}$. There exists an element $h \in \mathrm{SL}_n(k)$ such that $\|h\| \le 1$, $\|h^{-1}\| \le 1$, $hE_j = E_j$ and $hL_j = F_j$ for each j. Observe that by (9) the basis $he_1, he_2, \dots, he_n$ is compatible with the flag $0 = V_0 \subset V_1 \subset \cdots \subset V_r = k^n$. I.e., there is a permutation matrix w such that the basis $f_1 = whe_1, f_2 = whe_2, \dots, f_n = whe_n$ is such that for each $1 \le i \le r$ $V_i = Span\{f_1, f_2, \dots, f_{\dim V_i}\}$. With respect to this basis $\mathcal{E}_0$ is upper triangular and $\tilde{T}$ is diagonal. The element $g = wh$ satisfies the assertions. $\square$

Lemma 6.4. *For any $0 < \eta_1 < 1$, there exists a constant $d_3 > 0$ (depending only on n and η_1) such that for any unipotent algebra $\mathcal{E}_0$ normalized by T, there exists an element $\alpha \in \mathrm{SL}_n(k)$ which commutes with T such that* $\max(\|\alpha\|, \|\alpha\|^{-1}) \le d_3$ *and*

$$\|\alpha X \alpha^{-1}\| \le \eta_1 \|X\| \quad \textit{for all } X \in \mathcal{E}_0.$$

Proof: Let $\tilde{T}$ denote the linear span of T over k. Since $\mathcal{E}_0$ is normalized by $\tilde{T}$, by the previous lemma, for some $g \in \mathrm{SL}_n(k)$ such that $\|g\| \le 1$, $\|g^{-1}\| \le 1$, $g\mathcal{E}_0 g^{-1}$ is contained in the upper triangular subalgebra and $gTg^{-1} \subset \mathcal{D}$. Now we can find an element $\beta \in \mathcal{D}$ which contracts each element in the strictly upper triangular subalgebra by the factor of η_1, and the norm of β is bounded by a constant depending only on n and η_1. Now for all $X \in \mathcal{E}_0$, $\|g^{-1}\beta g X g^{-1}\beta^{-1} g\| \le \eta_1 \cdot \|X\|$. Set $\alpha = g^{-1}\beta g$. Since $gTg^{-1} \subset \mathcal{D}$ and $\mathcal{D}$ is commutative, $g^{-1}\mathcal{D}g$ centralizes T. Since $\alpha \in g^{-1}\mathcal{D}g$, we finish the proof. $\square$

Proof of Proposition 6.1. Let $\eta_1 = \eta/2$, and let d_3 be as in Lemma 6.4. Pick $\delta = \eta/(3d_3^2)$. Let $d_1 > 0$ be such that Lemma 6.2 holds with d_1 instead of d. Now suppose (1) of Proposition 6.1 does not hold. Then (b) of Lemma 6.2 holds, hence there exists a unipotent algebra $\mathcal{E}_0$ normalized by T such that $d(\mathcal{E}, \mathcal{E}_0) < \delta$. Let α in the centralizer of T be as in Lemma 6.4. Now for any $X \in \mathcal{E}$ with $\|X\| = 1$, there exists $X_0 \in \mathcal{E}_0$ with $\|X_0\| = 1$ and $\|X - X_0\| \le \delta$. Then,

$$\begin{aligned}
\|\alpha X \alpha^{-1}\| &\le \|\alpha X_0 \alpha^{-1}\| + \|\alpha(X - X_0)\alpha^{-1}\| \\
&\le \eta_1 \|X_0\| + \|\alpha\|\|\alpha\|^{-1}\|X - X_0\| \\
&\le \eta_1 + d_3^2 \delta \\
&< \eta.
\end{aligned}$$

Thus (2) of Proposition 6.1 holds. $\square$

7 Properties of $\mathrm{SL}_n(\mathcal{O}_K(\mathcal{S}))$

In this section we prove some simple consequences of Lemma 4.2. We continue to use the same notation K, $\mathcal{S}$, $\Lambda(\cdot)$ etc. as in §4.

7.1 A lower bound for the maximum eigenvalue of a semisimple element.

The aim of this subsection is to show:

Proposition 7.1. *There exists an $\eta > 0$ depending only on n, K and $\mathcal{S}$ such that $\Lambda(A) \geq 1 + \eta$ for any semisimple element $A \in \mathrm{SL}_n(\mathcal{O}_K(\mathcal{S}))$ of infinite order.*

Set $\mathcal{S}_\infty$ to be the subset of $\mathcal{S}$ consisting of all archimedean valuations in $\mathcal{S}$.

Lemma 7.2. *Let $G = \prod_{\nu \in \mathcal{S}_\infty} \mathrm{SL}_n(\bar{K}_\nu)$. Then there exists an ϵ-neighborhood $\mathcal{O}$ of the identity in G such that if $(h_\nu B h_\nu^{-1})_{\nu \in \mathcal{S}_\infty} \in \mathcal{O}$ for some $h_\nu \in \mathrm{GL}_n(\bar{K}_\nu)$ and the characteristic polynomial of B has coefficients in the set $\mathcal{O}_K$ of algebraic integers, then B is unipotent.*

Proof: Clearly the map ϕ sending $(g_\nu) \in G$ to $(f_\nu(X))$ for f_ν being the characteristic polynomial of g_ν is a continuous map from G to $\prod_\nu \bar{K}_\nu[X]$. Note that the diagonal embedding of $\mathcal{O}_K[X]$ is discrete in $\prod_\nu \bar{K}_\nu[X]$. Hence there exists a neighborhood V of $\phi(e)$ such that the only element of V intersecting the diagonal embedding of $\mathcal{O}_K[X]$ is $\phi(e)$. Noting that $\phi((g_\nu)) = \phi(e)$ implies that each g_ν is unipotent, it suffices to set $\mathcal{O}$ to be $\phi^{-1}(V)$. $\square$

Lemma 7.3. *For any $\delta > 0$, and for any diagonal matrix diag$(b_1 e^{2\pi\theta_1 i}, \cdots, b_n e^{2\pi\theta_n i}) \in \mathrm{SL}_n(\mathbb{C})$ where b_l are positive reals and $0 \leq \theta_l \leq 1$ for all $1 \leq l \leq n$, there exists $1 \leq d \leq \frac{1}{\delta^{2n}}$ such that for all $1 \leq l \leq n$, $d\theta_l \leq \delta$ mod 2π.*

Proof: Let R_m be the subdivision of $[0,1]$, identified with $\mathbb{R}/\mathbb{Z}$, into $m = \frac{1}{\delta}$ subintervals of equal length δ. Consider the box $[0,1]^n \times [0,1]^n$ and $R_m \times R_m$, which are m^{2n} subsets of size δ^{2n} in $[0,1]^{2n}$. Letting $\theta = (\theta_1, \cdots, \theta_n)$, consider $l \cdot \theta$ for $1 \leq l \leq m^{2n+1}$. Then by pigeon-hole principle, for some $1 \leq l_1 < l_2 \leq m^{2n+1}$, $l_1 \cdot \theta$ and $l_2 \cdot \theta$ must be in the same box in $R_m \times R_m$. Hence the size of $(l_2 - l_1) \cdot \theta$ is at most δ. Since $1 \leq l_2 - l_1 \leq m^{2n}$, this proves the claim. $\square$

For each $\nu \in \mathcal{S}$, set $\Lambda_\nu(A) = \max\{|\lambda|_\nu : \lambda : \text{ an eigenvalue of } A\}$.

Proof of Proposition 7.1: Let ϵ be as in Lemma 7.2 and d be as in Lemma 7.3 with respect to $\frac{\epsilon}{4}$. Let $K' \supset K$ be the splitting field of the characteristic polynomial of A. Since for each $\nu \in \mathcal{S}_\infty$, $K'_\nu \subset \mathbb{C}$ and $\mathcal{S}_\infty$ is finite, we may assume, after replacing A by a suitable power of A with a bounded exponent depending on d and $|\mathcal{S}_\infty|$, that the arguments of each eigenvalue of A is at most ϵ mod 2π. Note that since A is of infinite order, any power of A is non-trivial. Suppose that for some non-archimedean $\nu \in \mathcal{S}$, $\Lambda_\nu(A) > 1$. Then in fact, $\Lambda_\nu(A) \geq \pi^{1/n!}$ for π being the uniformizer of the field K_ν, since $[K'_\nu : K_\nu] \leq n!$. Now suppose that $\Lambda_\nu(A) = 1$ for all non-archimedean $\nu \in \mathcal{S}$. It follows that all eigenvalues of A are contained in the maximal compact ring $\mathcal{O}'_\nu$ of K'_ν. Let f denote the characteristic polynomial of A. Since the coefficients of f are contained in $K \cap \mathcal{O}'_\nu \subset \mathcal{O}_\nu$ for all non-archimedean $\nu \in \mathcal{S}$, f in fact belongs to $\mathcal{O}_K[X]$. By applying Lemma 7.2, we now have an archimedean valuation $\nu \in \mathcal{S}$ and a constant $\epsilon > 0$ depending only on n, $\mathcal{S}$ such that $|\lambda - 1|_\nu \geq \epsilon$ for some eigenvalue of A. Since the argument of λ is less than $\frac{\epsilon}{4}$, it follows that $|\lambda - 1|_\nu \geq 1 + \eta$ for some η depending on ϵ. $\square$

7.2 Effective Diagonalization

In this subsection, we prove the following:

Proposition 7.4. *Fix $\nu \in \mathcal{S}$. Let K'_ν be a finite extension of K_ν and $C_\nu \in \mathrm{SL}_n(K'_\nu)$ be a semisimple element which is conjugate to some matrix $C \in \mathrm{SL}_n(\mathcal{O}_K(\mathcal{S}))$ over $\mathrm{GL}_n(K'_\nu)$. Then there exists a matrix X_ν whose columns consist of linearly independent unit eigenvectors of C_ν (so that $X_\nu^{-1} C_\nu X_\nu$ is diagonal) and*

$$\|X_\nu^{-1}\|_\nu \leq D_1 \cdot \Lambda(C)^{M_1} \cdot \|C_\nu\|_\nu^{M_2}$$

where D_1, M_1 and M_2 are positive constants depending only on n and $\mathcal{S}$.

The proof relies on the following standard lemma:

Lemma 7.5. *Let k be local field with an absolute value $|\cdot|$. Let $n \geq 1$ and $v_1, \cdots, v_n$ be linearly independent unit vectors in k^n. For any $c > 0$ and $1 \leq j \leq n$, consider the following conditions:*

1. $\mathrm{I(c)} : |\det(\mathrm{v_1, \cdots, v_n})| \geq \mathrm{c}$
2. $\mathrm{II_j(c)}$*: for any $1 \leq i \leq j$ and any permutation σ on $\{1, \cdots, j\}$,*

$$\| \mathrm{pr}_{(V^\sigma_{i+1})^\perp}(v_{\sigma(i)})\| \geq c$$

where V_i^σ denotes the subspace spanned by $v_{\sigma(i)}, \cdots, v_{\sigma(j)}$ for $1 \le i \le j$ and $V_{j+1} = \{0\}$.

3. $\mathrm{III_j(c)}$*: for any $a_1, \cdots, a_j \in k$,*

$$\|\sum_{i=1}^{j} a_i v_i\| \ge c \max_{1\le i\le j} |a_i|$$

Then we have $\mathrm{I(c)} \Rightarrow \mathrm{II_n(c)}$*,* $\mathrm{II_j(c)} \Rightarrow \mathrm{III_j(c)}$ *and* $\mathrm{II_n(c)} \Rightarrow \mathrm{I(c^n)}$*.*

Proof: Note that $\det(v_1, \cdots, v_n) = \prod_{i=1}^n \| \mathrm{pr}_{(V_{i+1}^\sigma)^\perp}(v_{\sigma(i)})\|$. Since $\| \mathrm{pr}_{(V_{i+1}^\sigma)^\perp}(v_{\sigma(i)})\| \le 1$ for each $1 \le i \le n$, we obtain that $\| \mathrm{pr}_{(V_{i+1}^\sigma)^\perp}(v_{\sigma(i)})\| \ge c$ under assuming I(c). Now assume $\mathrm{II_j(c)}$. Let W_i denotes the subspace of k^n spanned by $v_1, \cdots, v_{i-1}, v_{i+1}, \cdots, v_j$. Note that for each $1 \le i \le j$,

$$\|\sum_{i=1}^{j} a_i v_i\|^2 = \| \mathrm{pr}_{W_i}(\sum_{i=1}^{j} a_i v_i)\|^2 + \| \mathrm{pr}_{W_i^\perp}(\sum_{i=1}^{j} a_i v_i)\|^2 \ge |a_i|^2 \cdot \| \mathrm{pr}_{W_i^\perp}(v_i)\|^2.$$

Since $\| \mathrm{pr}_{W_i^\perp}(v_i)\| \ge c$ by $\mathrm{II_j(c)}$ and $1 \le i \le j$ is arbitrary, we have

$$\|\sum_{i=1}^{j} a_i v_i\| \ge c \cdot \max_{1\le i\le j} |a_i|.$$

The implication $\mathrm{II_n(c)} \Rightarrow \mathrm{I(c^n)}$ is clear. □

Proof of Proposition 7.4. Let $\gamma_1, \cdots, \gamma_n$ denote the eigenvalues of C_ν, and let $v_1, \ldots, v_n$ denote corresponding unit eigenvectors, so that $C_\nu v_i = \gamma_i v_i$. We assume that if $\gamma_i = \gamma_j$ then v_i and v_j are orthogonal. Let X_ν be a matrix whose columns consist of the v_i's. Note that $\|X_\nu^{-1}\|_\nu \le \frac{M}{|\det\,(X_\nu)|_\nu}$ for some constant M depending only on n.

Then by Lemma 4.2, for each $\gamma_i \ne \gamma_j$,

$$|\gamma_i - \gamma_j|_\nu \ge d \cdot \Lambda(C)^{-N}$$

for some bounded positive constants d and N. We may clearly assume that $d \le 1$. By Lemma 7.5, it suffices to show that

$$\| \mathrm{pr}_{(V_{i+1}^I)^\perp}(v_i)\|_\nu \ge (\tfrac{d}{2})^{n-i} \cdot \Lambda(C)^{-(n-i)N} \|C_\nu\|_\nu^{-(n-i)} \quad \text{for each } 1 \le i \le n$$

(here I denotes the identity permutation). We proceed by induction on i. For $i = n$, it is clear. Assume that for $k+1 \leq i \leq n$,

$$\begin{aligned}\|\operatorname{pr}_{(V^I_{i+1})^\perp}(v_i)\|_\nu &\geq (\tfrac{d}{2})^{n-i} \cdot \Lambda(C)^{-(n-i)N} \|C_\nu\|_\nu^{-(n-i)} \\ &\geq (\tfrac{d}{2})^{n-k-1} \cdot \Lambda(C)^{-(n-k-1)N} \|C_\nu\|_\nu^{-(n-k-1)}.\end{aligned}$$

Hence by Lemma 7.5, for any $x_{k+1}, \cdots, x_n \in K_\nu$, we have

$$\|(\sum_{i=k+1}^n x_i v_i)\|_\nu \geq (\tfrac{d}{2})^{n-k-1} \cdot \Lambda(C)^{-(n-k-1)N} \|C_\nu\|_\nu^{-(n-k-1)} \max_{k+1 \leq i \leq n} |x_i|_\nu.$$

Write

$$v_k = \operatorname{pr}_{(V^I_{k+1})^\perp}(v_k) + \sum_{i=k+1}^n a_i v_i, \tag{10}$$

where $a_i \in K_\nu$. Now by applying C_ν to both sides of (10) we obtain

$$\begin{aligned}\|C_\nu\|_\nu \cdot \|\operatorname{pr}_{(V^I_{k+1})^\perp}(v_k)\|_\nu &\geq \|C_\nu \operatorname{pr}_{(V^I_{k+1})^\perp}(v_k)\|_\nu \\ &= \|\gamma_k \operatorname{pr}_{(V^I_{k+1})^\perp}(v_k) + \sum_{k+1 \leq i \leq n, \gamma_i \neq \gamma_k} a_i(\gamma_k - \gamma_i) v_i\|_\nu \\ &\geq \|\sum_{k+1 \leq i \leq n, \gamma_i \neq \gamma_k} a_i(\gamma_k - \gamma_i) v_i\|_\nu \\ &\geq d \cdot (\tfrac{d}{2})^{n-k-1} \cdot \Lambda(C)^{-N} \Lambda(C)^{-(n-k-1)N} \|C_\nu\|_\nu^{-(n-k-1)} \max_{k+1 \leq i \leq n} |a_i|_\nu.\end{aligned}$$

On the other hand, from (10) we have

$$n \cdot \max_{1 \leq i \leq n} |a_i|_\nu \geq 1 - \|\operatorname{pr}_{(V^I_{k+1})^\perp}(v_k)\|_\nu.$$

Since $d \leq 1$, $\Lambda(C) \geq 1$ and $\|C_\nu\| \geq 1$, we have

$$1 + \tfrac{1}{n} \cdot d \cdot (\tfrac{d}{2})^{n-k-1} \cdot \Lambda(C)^{-(n-k)N} \|C_\nu\|_\nu^{-(n-k-1)} \leq 2.$$

We deduce that

$$\begin{aligned}\|\operatorname{pr}_{(V^I_{k+1})^\perp}(v_k)\|_\nu &\geq \tfrac{1}{2} d \cdot (\tfrac{d}{2})^{n-k-1} \cdot \Lambda(C)^{-(n-k)N} \|C_\nu\|_\nu^{-(n-k)} \\ &= (\tfrac{d}{2})^{n-k} \cdot \Lambda(C)^{-(n-k)N} \|C_\nu\|_\nu^{-(n-k)}.\end{aligned}$$

This proves the claim. $\square$

8 The steps of the proof

Preliminary Reductions. Let Γ be an infinite finitely generated subgroup of $\mathrm{GL}_n(\mathbb{C})$ which is not-virtually solvable. By Proposition 4.1 we may assume that $\Gamma \subset \mathrm{SL}_n(\mathcal{O}_K(\mathcal{S}))$ where K is a number field, $\mathcal{S}$ is a set of valuations containing the archimedean ones, Γ is unbounded in $\prod_{\nu\in\mathcal{S}} \mathrm{SL}_n(K_\nu)$ via the diagonal embedding and the Zariski closure H of Γ in $\mathrm{GL}_n(\mathbb{C})$ is connected and simple.

Furthermore, in view of the Selberg Lemma [Sel60] we may assume that Γ is torsion free.

An element $g \in H$ is called H-regular if the multiplicity of the eigenvalue 1 of $Ad(g)$ is minimum possible in H where Ad denotes the adjoint representation of H.

It is well known that the set of all H-regular elements is a Zariski dense open subset in H and each H-regular element is semisimple and hence diagonalizable over $\mathrm{GL}_n(K')$ for some finite extension field K' of K (cf [Bo, 12.2]).

In the following, let S be an arbitrary finite generating set of Γ.

8.1 Step 1.

For each $1 \le i \le n-1$, ρ_i denotes the i-th wedge product representation of SL_n and set $l_i = \dim(\rho_i)$.

The following proposition will provide us with two elements of Γ denoted A and B. In Steps 2-4, will construct long words in A and B.

Proposition 8.1. *For any $N_0 \in \mathbb{N}$, there exists a bounded constant M_1 such that $B_S(M_1)$ contains H-regular elements A and B with the property that for each $1 \le i \le n-1$,*

1. *all words in $\rho_i(A)$ and $\rho_i(B)$ of length at most N_0 are $\rho_i(H)$-regular.*
2. *no pair of the above elements lies in a common parabolic subgroup of SL_{l_i} not containing $\rho_i(H)$ unless they, as words in a free group, commute.*

Proof: Let Q_i be the subset of $H \times H$ consisting of the pairs (g_1, g_2) such that all words in $\rho_i(g_1)$ and $\rho_i(g_2)$ of length at most N_0 are $\rho_i(H)$-regular and none of those two words lie in a common parabolic subgroup of SL_{l_i} not containing $\rho_i(H)$ unless they, as words in a free group, commute. Since each Q_i contains a Zariski open subset in $H \times H$, so does $Q := \cap_{i=1}^{n-1} Q_i$.

Since $\Gamma \times \Gamma$ is Zariski dense in $H \times H$, by Proposition 3.2, there exists a bounded constant M_1 such that $B_{S\times S}(M_1) \cap Q \neq \emptyset$ for any finite generating set S of Γ. Hence $B_S(M_1)$ contains A, B desired as above. $\square$

8.2 Step 2.

In the following sections, we let A, B be elements of Γ as in Proposition 8.1 for $N_0 = 2^{n^2+3}$.

Our aim in this section is to prove the following proposition:

Proposition 8.2. *For some positive bounded constants C_1, and r_1 there exists a word B' in A and B of length at most 2^{n^2+2} which involves B non-trivially, and for each $\nu \in \mathcal{S}$ there exists $x_\nu \in \mathrm{SL}_n(K'_\nu)$ (where K'_ν is the splitting field of the characteristic polynomial of A) such that $x_\nu A x_\nu^{-1}$ is diagonal, and we have*

$$\Lambda(B') \geq C_1 \cdot \Lambda(A)^{-r_1} \max_{\nu\in\mathcal{S}} \|x_\nu B x_\nu^{-1}\|_\nu.$$

Remarks. Note that since $x_\nu A x_\nu^{-1}$ is diagonal, $\|x_\nu A x_\nu^{-1}\| = \Lambda(A)$. Hence,

$$\|x_\nu B' x_\nu^{-1}\|_\nu \leq \Lambda(A)^{N_1} \|x_\nu B x_\nu^{-1}\|_\nu^{N_1}$$

for $N_1 = 2^{n^2+2}$. Hence, the assertion of Proposition 8.2 is roughly that it is possible to replace B by a word B' in A and B of bounded length such that after common conjugation A becomes diagonal, and B' has the property that its biggest eigenvalue becomes comparable to the norm.

We now begin the proof of Proposition 8.2. We identify the *Weyl group* of SL_n with the set of permutation matrices.

There exists $\hat{g} \in \mathrm{GL}_n(K')$ so that $\hat{g} A \hat{g}^{-1}$ is diagonal. Fix any $\nu \in \mathcal{S}$. There exists an element $g_\nu \in \mathrm{GL}_n(K')$ such that the eigenvalues of the diagonal matrix $g_\nu A g_\nu^{-1}$ are non-increasing, i.e.,

$$g_\nu A g_\nu^{-1} = \mathrm{diag}(\lambda_1 I_{n_1}, \cdots, \lambda_m I_{n_m})$$

where $|\lambda_1|_\nu \geq \cdots \geq |\lambda_m|_\nu$ and $\sum_i n_i = n$.

Set

$$A_\nu := g_\nu A g_\nu^{-1} \quad \text{and} \quad \hat{B}_\nu := g_\nu B g_\nu^{-1}.$$

Let $T_\nu = T(A_\nu, \nu)$. Note that given Γ and ν there are only finitely many possibilities for T_ν independently of A and B. Hence any constant which a priori depends on T in fact depends only on Γ (i.e. is bounded in the sense of the introduction to §8).

Definition 8.3. Let $A, B \in \mathrm{SL}_n(K'_\nu)$ with A diagonal. Let $Z(T) \subset \mathrm{SL}_n(K'_\nu)$ denote the centralizer of $T = T(A, \nu)$. We say that B is *balanced* with respect to A if

$$\|B\|_\nu \leq 2 \inf_{x \in Z(T)} \|xBx^{-1}\|_\nu.$$

Let $h_\nu \in Z(T)$ be such that $h_\nu \hat{B}_\nu h_\nu^{-1}$ is balanced with respect to A_ν. Set

$$B_\nu := h_\nu \hat{B}_\nu h_\nu^{-1}.$$

Note that $A_\nu = h_\nu A_\nu h_\nu^{-1}$ and

$$\Lambda(A) = \max\{|\lambda_i|_\nu \mid 1 \leq i \leq m,\ \nu \in \mathcal{S}\} \geq 1$$

since $\det A = 1$.

Lemma 8.4. *There exists a word $\tilde{B}_\nu$ in A_ν and B_ν of length at most 2^{n^2+2} (which involves B_ν non-trivially) such that*

$$|\operatorname{Tr}(\tilde{B}_\nu)|_\nu \geq C \cdot \|A_\nu\|_\nu^{-r_1} \|B_\nu\|_\nu \tag{11}$$

where C and r_1 are bounded positive constants.

Proof: Fix $0 < \eta < 1/32$. Let d_1 and d_2 be as in Proposition 6.1 with respect to η. Let $0 < \epsilon < d_1/2$ be such that $d_2^2 \epsilon < 1/32$ and $\eta\epsilon < 1/32$. Let $\mathcal{E}_\nu(\epsilon)$ be a subalgebra of $M_n(K'_\nu)$ as in Proposition 5.1 with A and B replaced by A_ν and B_ν respectively.

We now claim that alternative (2) of Proposition 6.1 cannot hold for $\mathcal{E} = \mathcal{E}_\nu(\epsilon)$. Indeed, let g be as in Proposition 6.1 (2). By assertion (a) of Proposition 5.1 there exists $B^* \in \mathcal{E}_\nu(\epsilon)$ such that $\|B_\nu - B^*\|_\nu \leq \epsilon \|B_\nu\|_\nu$. Then

$$\begin{aligned}
\|gB_\nu g^{-1}\|_\nu &\leq \|gB^* g^{-1}\|_\nu + \|g(B_\nu - B^*)g^{-1}\|_\nu \\
&\leq \eta \|B^*\|_\nu + \|g\|_\nu \|g^{-1}\|_\nu \|B_\nu - B^*\|_\nu \\
&\leq \eta \|B^*\|_\nu + d_2^2 \epsilon \|B_\nu\|_\nu \\
&\leq \eta(1+\epsilon)\|B_\nu\|_\nu + d_2^2 \epsilon \|B_\nu\|_\nu \\
&\leq (1/4)\|B_\nu\|_\nu
\end{aligned}$$

Since g centralizes A_ν, this contradicts the fact that B_ν is balanced with respect to A_ν. Therefore assertion (1) of Proposition 6.1 holds. Now we apply Proposition 5.1 with $\theta = I$ (the identity matrix). Since $\epsilon < d_1/2$, (11) follows from part (b) of Proposition 5.1. $\square$

In this subsection we have constructed A_ν and B_ν in $\mathrm{SL}_n(K'_\nu)$ for some finite extension field K'_ν of K_ν for each $\nu \in \mathcal{S}$ such that $[K'_\nu : K_\nu]$ is bounded by a constant depending only on n.

Let $\nu_1 \in \mathcal{S}$ be such that

$$\|B_{\nu_1}\|_{\nu_1} = \max_{\nu \in \mathcal{S}} \|B_\nu\|_\nu.$$

Let $\tilde{B}$ be as in Lemma 8.4 with respect to the valuation ν_1. By construction of $\tilde{B}$, clearly there exists $B' \in \mathrm{SL}_n(\mathcal{O}_K(\mathcal{S}))$ such that for each $\nu \in \mathcal{S}$,

$$\tilde{B} = x_\nu B' x_\nu^{-1} \tag{12}$$

where $x_\nu = h_\nu g_\nu$. Since $\Lambda(B') \geq \frac{1}{n}|\operatorname{Tr}(\tilde{B}_{\nu_1})|_{\nu_1}$, we have completed the proof of Proposition 8.2. □

8.3 Step 3

In this subsection, our goal is the following:

Proposition 8.5. *There exist bounded constants m_1, c and M such that for any given finite generating set S of $\Gamma \subset \mathrm{SL}_n(\mathcal{O}_K(\mathcal{S}))$ there exist two H-regular elements $A, B \in B_S(m_1)$ not lying in a common parabolic, such that for each $\nu \in \mathcal{S}$, there exists a finite extension field K'_ν of K_ν and an element $y_\nu \in \mathrm{GL}_n(K'_\nu)$ such that each $A_\nu := y_\nu A y_\nu^{-1}$ is diagonal and*

$$\Lambda(A) = \max_{\nu \in \mathcal{S}} \|A_\nu\|_\nu \geq c \cdot \max_{\nu \in \mathcal{S}} \|B_\nu\|_\nu^{1/M} \tag{13}$$

Note that B' is H-regular by Proposition 8.1. Set $X_\nu \in \mathrm{GL}_n(\bar{K})$ to be a matrix whose columns are unit eigenvectors of $\tilde{B}$ satisfying

$$\|X_\nu^{-1}\|_\nu \leq D \cdot \Lambda(B')^{M_1} \|\tilde{B}\|_\nu^{M_2}$$

for each $\nu \in \mathcal{S}$ as in Proposition 7.4.

Lemma 8.6. *We have*

$$\max_{\nu \in \mathcal{S}} \|A_\nu\|_\nu \geq \max_{\nu \in \mathcal{S}} \|B_\nu\|_\nu^{1/M}, \text{ or}$$

$$\max_{\nu \in \mathcal{S}} \|X_\nu^{-1} \tilde{B} X_\nu\|_\nu \geq D' \cdot \max_{\nu \in \mathcal{S}} \|X_\nu^{-1} A_\nu X_\nu\|_\nu^{1/M'}$$

where M, D' and M' are bounded constants.

Proof: Set $N_1 = 2^{n^2+2}$. Let M be a positive integer bigger than $r_1 + 1$ where r_1 is as in Proposition 8.2. If $\Lambda(A) \geq \|B_{\nu_1}\|^{1/M}$, then there is nothing to prove. Suppose that $\Lambda(A) \leq \|B_{\nu_1}\|^{1/M}$. Consider $X_\nu^{-1}\tilde{B}X_\nu$ and $X_\nu^{-1}A_\nu X_\nu$. Note that

$$\max_{\nu \in \mathcal{S}} \|X_\nu^{-1}\tilde{B}X_\nu\|_\nu = \Lambda(B').$$

By applying Proposition 8.2 and by the assumption, we have

$$\max_{\nu \in \mathcal{S}} \|X_\nu^{-1}\tilde{B}X_\nu\|_\nu \geq C_1 \cdot \Lambda(A)^{-r_1}\|B_{\nu_1}\|_{\nu_1} \geq C_1 \cdot \|B_{\nu_1}\|_{\nu_1}^{-r_1/M+1}.$$

On the other hand, Proposition 7.4 with notations M_1, M_2 and D_1 there implies for each $\nu \in \mathcal{S}$,

$$\begin{aligned} \max_{\nu \in \mathcal{S}} \|X_\nu^{-1}A_\nu X_\nu\|_\nu &\leq \max_{\nu \in \mathcal{S}} \|X_\nu^{-1}\|_\nu \cdot \|A_\nu\|_\nu \leq D_1 \cdot \Lambda(B')^{M_1}\|B_\nu\|_\nu{}^{M_2}\Lambda(A) \\ &\leq D_1 \cdot \Lambda(A)^{M_1N_1+1} \cdot \|B_{\nu_1}\|_{\nu_1}^{N_1M_1+M_2} \leq D_1 \cdot C_1^{M_1} \cdot \|B_{\nu_1}\|_{\nu_1}^{(M_1N_1+1)/M+N_1M_1+M_2} \end{aligned}$$

by the assumption. Since $-r_1/M + 1 > 0$, we can find bounded constants M' and D' such that

$$\max_{\nu \in \mathcal{S}} \|X_\nu^{-1}\tilde{B}_\nu X_\nu\|_\nu \geq D' \cdot \max_{\nu \in \mathcal{S}} \|X_\nu^{-1}A_\nu X_\nu\|_\nu^{1/M'}.$$

□

Proof of Proposition 8.5. If the first inequality in Lemma 8.6 does not hold, we simply need to replace A_ν by $X_\nu^{-1}B_\nu X_\nu$ and B_ν by $X_\nu^{-1}A_\nu X_\nu$.

8.4 Step 4.

In this subsection we aim to satisfy the remaining conditions of Proposition 2.5. Note that (L2) is already satisfied in view of Proposition 8.5. It remains to satisfy (L1) and (L3).

Let $\nu_0 \in \mathcal{S}$ be such that $\|A_{\nu_0}\|_{\nu_0} = \max_{\nu \in \mathcal{S}} \|A_\nu\|_\nu$, which is equal to $\Lambda(A)$.

Using Proposition 7.1 (note that Γ is assumed to be torsion-free), we may assume that $\|A_{\nu_0}\|_{\nu_0} \geq 4^{n-1}$, after taking a suitable power by a bounded exponent. By conjugating Γ by a Weyl element, we may also assume that the diagonal entries of A_{ν_0} are in decreasing order with respect to the absolute value $|\cdot|_{\nu_0}$. For the sake of simplicity, we omit the subscript ν_0 in the notation $|\cdot|_{\nu_0}$ for the rest of this section.

We now need the following easy lemma:

Lemma 8.7. *For any* $\mathrm{diag}(\alpha_1, \cdots, \alpha_n) \in \mathrm{SL}_n(K'_{\nu_0})$ *where* $|\alpha_i| \geq |\alpha_{i+1}|$ *for each* $1 \leq i \leq n-1$*, we have*

$$\left(\max_i \frac{|\alpha_i|}{|\alpha_{i+1}|}\right) \geq \tfrac{1}{2}|\alpha_1|^{1/(n-1)}.$$

Proof: Suppose that $|\alpha_i| \leq \frac{1}{2}|\alpha_1|^{1/(n-1)}|\alpha_{i+1}|$ for each $1 \leq i \leq n-1$. It follows that, using $\prod_i |\alpha_i| = 1$, $|\alpha_1| \prod_{1\leq i\leq n-1} |\alpha_i| \leq \frac{1}{2^{n-1}}|\alpha_1|$. Hence $\prod_{1\leq i\leq n-1} |\alpha_i| \leq \frac{1}{2^{n-1}}$, or equivalently $|\alpha_n| \geq 2^{n-1}$, which contradicts the assumption that α_i is in norm decreasing order. □

Write $A_{\nu_0} := \mathrm{diag}(\lambda_1, \cdots, \lambda_n)$. Let $1 \leq i \leq n-1$ be the smallest integer such that

$$\left|\frac{\lambda_i}{\lambda_{i+1}}\right| \geq \tfrac{1}{2}|\lambda_1|^{1/(n-1)} \geq 2.$$

By taking the i-th wedge product of ρ_i, we obtain that a bounded power of $\rho_i(A_{\nu_0})$ and $\rho_i(B_{\nu_0})$ satisfies (L1). Without loss of generality, we may assume that $\rho_i(A_{\nu_0})$ satisfies (L1). Note that the elements $\rho_i(A_{\nu_0})$ and $\rho_i(B_{\nu_0})$ satisfies (L2) by (13) and the choice of ν_0 and i.

Proposition 8.8. *Let k be a local field with an absolute value $|\cdot|$. Then for any matrix D in $\mathrm{SL}_m(k)$, the $(1,1)$-entry $(D^q)_{11}$ of the power D^q for some $1 \leq q \leq m$ satisfies*

$$|(D^q)_{11}| \geq c\|D^q\|^s$$

for some constants $s > -\infty$ and $c > 0$ depending only on n.

Assuming Proposition 8.8, we have $\rho_i(\hat{B}_{\nu_0})$ and $\rho_i(A_{\nu_0})$ satisfies (L3). Indeed it is easy to see that they also satisfy (L1) and (L2) from the fact that A_{ν_0} and B_{ν_0} satisfy those. Hence we produced a ping-pong pair using words of bounded length in the given set of generators. This completes the proof of the main theorem.

Proof of Proposition 8.8. Let $\chi_D(x) = \sum_{i=0}^m \alpha_i x^i$ be the characteristic polynomial of D. Note that $\alpha_0 = 1$. We then have $\chi_D(D) = 0$. Hence if we write $D^q = ((D^q)_{ij})$, then $\sum_{i=0}^m \alpha_i (D^i)_{11} = 0$ and hence $\sum_{i=1}^m \alpha_i (D^i)_{11} = -1$. Hence for some $1 \leq q \leq m$,

$$|\alpha_q (D^q)_{11}| \geq 1/m$$

which implies that $|(D^q)_{11}| \geq \frac{1}{m}\|D\|^{-q}$. This proves the proposition.

References

[AN] Roger Alperin and Gennady A. Noskov, *Uniform growth, actions on trees and GL_2*, math.GR/0105083.

[Bo] Armand Borel, *Linear algebraic groups*, 2nd ed. math. Springer-Verlag

[Dan94] Vladimir I. Danilov, *Algebraic varieties and schemes*, Algebraic geometry, I, Springer, Berlin, 1994, pp. 167–297. MR 95f:14001

[Del96] Thomas Delzant, *Sous-groupes distingués et quotients des groupes hyperboliques*, Duke Math. J. **83** (1996), no. 3, 661–682. MR 97d:20041

[DeLaH00] Pierre de la Harpe, *Topics in Geometric Group Theory*, Chicago Lec. Math., 2000

[EMO] Alex Eskin, Shahar Mozes, and Hee Oh, *Uniform exponential growth of Linear Groups*, IMRN **31** (2002) 1675-1683.

[Ful98] William Fulton, *Intersection theory*, second ed., Springer-Verlag, Berlin, 1998. MR 99d:14003

[GdlH97] Rostislav I. Grigorchuk and Pierre de la Harpe, *On problems related to growth, entropy, and spectrum in group theory*, J. Dynam. Control Systems **3** (1997), no. 1, 51–89. MR 98d:20039

[Gro81] Mikhael Gromov, *Structures métriques pour les variétés riemanniennes*, CEDIC, Paris, 1981, Edited by J. Lafontaine and P. Pansu. MR 85e:53051

[GS79] Firtz Grunewald and Daniel Segal, *Remarks on injective specializations*, J. Algebra **61** (1979), 538–547.

[Kob84] Neal Koblitz *p-adic Numbers, p-adic Analysis and Zeta Functions*, GTM 58, Springer-Verlag New York (1984).

[Kou98] Malik Koubi, *Croissance uniforme dans les groupes hyperboliques*, Ann. Inst. Fourier (Grenoble) **48** (1998), no. 5, 1441–1453. MR 99m:20080

[LM91] Alexander Lubotzky and Avinoam Mann, *On groups of polynomial subgroup growth*, Invent. Math. **104** (1991), no. 3, 521–533. MR 92d:20038

[Ma79] Anthony Manning, *Topological entropy for geodesic flows*, Ann. Math. **110** (1979), 567–573.

[Mil68] John Milnor, *Growth of finitely generated solvable groups*, J. Differential Geometry **2** (1968), 447–449. MR 39 #6212

[Osi03] Dennis Osin, *The entropy of solvable groups*, Ergodic Theory and Dynamical Systems **23** (2003), 907–918.

[ShaWa92] Peter Shalen and Philip Wagreich, *Growth rates, $\mathbb{Z}_p$-homology, and volumes of hyperbolic* 3*-manifolds*, Trans. Amer. Math. Soc. **331** (1992), 895–917.

[Sch00] Andrzej Schinzel, *Polynomials with special regard to reducibility*, Cambridge University Press, Cambridge, 2000, With an appendix by Umberto Zannier.

[Sel60] Atle Selberg, *On discontinuous groups in higher-dimensional symmetric spaces*, Contributions to function theory (internat. Colloq. Function Theory, Bombay, 1960) pp. 147–164, Tata Institute of Fundamental Research, Bombay.

[Tit72] Jacques Tits, *Free subgroups in linear groups*, J. Algebra **20** (1972), 250–270. MR 44 #4105

[Wil00] John Wilson, Preprint, 2000.

[Wil02] John Wilson, *On exponential growth and uniformly exponential growth for groups*, Inventiones. **155**, (2004), 287–303

[Wol68] Joseph A. Wolf, *Growth of finitely generated solvable groups and curvature of Riemanniann manifolds*, J. Differential Geometry **2** (1968), 421–446. MR 40 #1939

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
Institute for Advanced Study, Einstein Drive, Princeton, NJ, USA
Current address: Mathematicc 253-37, Caltech, Pasadena, CA 91125;
heeoh@its.caltech.edu