A spectral gap theorem in simple Lie groups

Yves Benoist and Nicolas de Saxcé*

Abstract

We establish the spectral gap property for dense subgroups generated by algebraic elements in any compact simple Lie group, generalizing earlier results of Bourgain and Gamburd for unitary groups.

1 Introduction

The purpose of the paper is to study the spectral gap property for measures on a compact simple Lie group G. If μ is a Borel probability measure on G, we say that μ has a *spectral gap* if the spectral radius of the corresponding operator on $L_0^2(G)$ – the space of mean-zero square integrable functions on G – is strictly less than 1. We also say that μ is *almost Diophantine* if it satisfies, for some positive constants C_1 and c_2, for n large enough and for any proper closed subgroup H,

$$\mu^{*n}(\{x \in G \,|\, d(x,H) \leq e^{-C_1 n}\}) \leq e^{-c_2 n}.$$

Using the discretized Product Theorem proved in [11] and the techniques developped by Bourgain and Gamburd in [3] for the group $SU(2)$, we prove the following theorem.

Theorem 1.1. *Let G be a connected compact simple Lie group and μ be a Borel probability measure on G. Then μ has a spectral gap if and only if it is almost Diophantine.*

A measure μ on the compact simple Lie group G is called *adapted* if its support generates a dense subgroup of G. It is not known whether every adapted probability measure on the compact simple Lie group G is almost Diophantine, but it is natural to conjecture a affirmative answer to this question. In this direction, Bourgain and Gamburd proved that if μ is an adapted probability measure on $SU(d)$ supported on elements with algebraic entries, then μ has a spectral gap. We generalize their result to an arbitrary simple group, and prove the following, using the theory of random matrix products over arbitrary local fields, as exposed in [2].

*N.S. is supported by ERC AdG Grant 267259

Theorem 1.2. *Let G be a connected compact simple Lie group and $\mathcal{U}$ a fixed basis for its Lie algebra. Let μ be an adapted probability measure on G and assume that for any g in the support of μ, the matrix of $\operatorname{Ad} g$ in the basis $\mathcal{U}$ has algebraic entries. Then μ is almost Diophantine, and therefore has a spectral gap.*

The plan of the paper is simple: in Section 2, we prove Theorem 1.1, in Section 3, we prove Theorem 1.2.

For us, a compact simple Lie group will be a compact real Lie group whose Lie algebra is simple. We will also make use of some classical notation:

- The Landau notation: $O(\epsilon)$ stands for a quantity bounded in absolute value by $C\epsilon$, for some constant C (generally depending on the ambient group G).
- The Vinogradov notation: we write $x \ll y$ if, $x \leq Cy$ for some constant C (again, possibly depending on the ambient group). We will also write $x \simeq y$ if $x \ll y$ and $x \gg y$, and similarly. For two real valued functions φ and ψ on G, we write $\varphi \ll \psi$ if there exists an absolute constant C such that for all x in G, $\varphi(x) \leq C \cdot \psi(x)$.

2 The spectral gap property

Let G be a connected compact simple Lie group. If μ is a Borel probability measure on G, we define an averaging operator T_μ on the space $L^2_0(G)$ of mean-zero square-integrable functions by the formula

$$T_\mu f(x) = \int_G f(xg)\, d\mu(g), \quad \forall f \in L^2_0(G).$$

Definition 2.1. We say that a probability measure μ on G has a *spectral gap* if the spectral radius of the averaging operator T_μ on the space $L^2_0(G)$ is strictly less than one.

The purpose of this section is to relate the spectral gap property to the following Diophantine property of measures.

Definition 2.2. We say that a probability measure μ on G is *almost Diophantine* if there exist positive constants C_1 and c_2 such that for n large enough, for any proper closed connected subgroup H,

$$\mu^{*n}(H^{(e^{-C_1 n})}) \leq e^{-c_2 n}. \tag{1}$$

where $H^{(\rho)}$ denotes the neighborhood of size ρ of the closed subgroup H: $H^{(\rho)} = \{x \in G \,|\, d(x,H) \leq \rho\}$.

With this definition, we have the following theorem.

Theorem 2.3 (Spectral gap for almost Diophantine measures)**.** *Let G be a connected compact simple Lie group. A Borel probability measure μ on G has a spectral gap if and only if it is almost Diophantine.*

Remark 1. The spectral radius of the averaging operator T_μ on $L^2_0(G)$ is less than one if and only if the spectral radius of $T_\mu T_{\check{\mu}} = T_{\mu*\check{\mu}}$ is less than one. This shows that it will be enough to prove the Theorem 2.3 in the case μ is symmetric.

We start by proving the trivial implication: if μ has a spectral gap, then it must be almost Diophantine.

Spectral gap $\Longrightarrow$ Almost Diophantine. Suppose μ has a spectral gap, and let $c > 0$ such that the spectral radius of T_μ satisfies $RS(T_\mu) \leq e^{-c}$. Let d be the dimension of G and let H be a maximal proper closed subgroup of G of dimension p. For $\delta > 0$, we can bound the L^2-norm of the indicator function of the 2δ-neighborhood of H:

$$\|\mathbb{1}_{H^{(2\delta)}}\|_2 \ll \delta^{\frac{d-p}{2}}.$$

Therefore, for n larger than $\frac{d-p}{2c}\log\frac{1}{\delta}$, we have

$$\|T_\mu^n \mathbb{1}_{H^{(2\delta)}}\|_2 \ll \delta^{d-p}.$$

Making the left-hand side explicit, we find

$$\sqrt{\int_G \mu^{*n}(xH^{(2\delta)})^2\,dx} \ll \delta^{d-p}$$

and this implies,

$$\mu^{*n}(H^{(\delta)}) \ll \delta^{\frac{d-p}{2}}.$$

Choosing $C_1 \leq \frac{2c}{d-p}$ and $c_2 = c$, and letting $\delta = e^{-C_1 n}$, this shows that μ is almost Diophantine. □

To prove the converse implication in Theorem 2.3, we use the strategy developped by Bourgain and Gamburd. If A is a subset of a metric space, for $\delta > 0$, we denote by $N(A,\delta)$ the minimal cardinality of a covering of A by balls of radius δ. We have the following Product Theorem [11, Theorem 3.9].

Theorem 2.4. *Let G be a simple Lie group of dimension d. There exists a neighborhood U of the identity in G such that the following holds.*
Given $\alpha \in (0,d)$ and $\kappa > 0$, there exists $\epsilon_0 = \epsilon_0(\alpha,\kappa) > 0$ and $\tau = \tau(\alpha,\kappa) > 0$ such that, for $\delta > 0$ sufficiently small, if $A \subset U$ is a set satisfying

1. *$N(A,\delta) \leq \delta^{-d+\alpha-\epsilon_0}$,*
2. *for all $\rho \geq \delta$, $N(A,\rho) \geq \rho^{-\kappa}\delta^{\epsilon_0}$,*
3. *$N(AAA,\delta) \leq \delta^{-\epsilon_0}N(A,\delta)$,*

then A is included in a neighborhood of size δ^τ of a proper closed connected subgroup of G.

We will use Theorem 2.4 to derive a flattening statement for measures. For $\delta > 0$, we let

$$P_\delta = \frac{\mathbb{1}_{B(1,\delta)}}{|B(1,\delta)|},$$

(where $|\cdot|$ is the volume associated to the Haar probability measure on G) and if μ is a probability measure on G, we denote by μ_δ the function approximating μ at scale δ:

$$\mu_\delta = \mu * P_\delta.$$

Lemma 2.5 (L^2-flattening)**.** *Let G be a connected compact simple Lie group. Given $\alpha, \kappa > 0$, there exists $\epsilon > 0$ such that the following holds for any $\delta > 0$ small enough.*
Suppose μ is a symmetric Borel probability measure on G such that one has

1. $\|\mu_\delta\|_2^2 \geq \delta^{-\alpha}$,
2. *for any $\rho \geq \delta$ and any closed connected subgroup H, $\mu*\mu(H^{(\rho)}) \leq \delta^{-\epsilon}\rho^\kappa$.*

Then,

$$\|\mu_\delta * \mu_\delta\|_2 \leq \delta^\epsilon \|\mu_\delta\|_2.$$

The proof goes by approximating the measure μ_δ by dyadic level sets. We say that a collection of sets $\{X_i\}_{i\in I}$ is *essentially disjoint* if for some constant C depending only on the ambient group G, any intersection of more than C distinct sets X_i is empty. We will use the following lemma.

Lemma 2.6. *Let G be a compact Lie group, μ a Borel probability measure on G and $\delta > 0$. There exist subsets A_i, $0 \leq i \ll \log\frac{1}{\delta}$ such that*

1. $\mu_\delta \ll \sum_i 2^i \mathbb{1}_{A_i} \ll \mu_{4\delta}$
2. *Each A_i is an essentially disjoint union of balls of radius δ.*

Proof. A proof in the case $G = SU(2)$ is given in [8] and also applies in this more general setting, mutatis mutandis. □

To derive Lemma 2.5, we will also use the non-commutative Balog-Szemerédi-Gowers Lemma, due to Tao. If A and B are two subsets of a metric group G, we define the *multiplicative energy* of A and B at scale δ by

$$E_\delta(A,B) = N(\{(a,b,a',b') \in A\times B\times A\times B \,|\, d(ab,a'b') \leq \delta\},\delta).$$

(See [12] for elementary properties.) We have the following important theorem (see Tao [12, Theorem 6.10]).

Theorem 2.7 (Non-commutative Balog-Szemerédi-Gowers Lemma)**.** *Let G be a compact Lie group with a Riemannian metric. There exists a constant $C > 0$ depending only on G such that the following holds for any $\delta > 0$ and any $K \geq 2$. Suppose that A and B are non-empty subsets of G such that*

$$E_\delta(A,B) \geq \frac{1}{K} N(A,\delta)^{\frac{3}{2}} N(B,\delta)^{\frac{3}{2}}.$$

Then there exists a K^C-approximate subgroup H and elements x, y in G such that

- $N(H, \delta) \le K^C \cdot N(A, \delta)^{\frac{1}{2}} N(B, \delta)^{\frac{1}{2}}$
- $N(A \cap xH, \delta) \ge K^{-C} \cdot N(A, \delta)$
- $N(B \cap Hy, \delta) \ge K^{-C} \cdot N(B, \delta)$.

Recall that a subset H of G is called a K-*approximate subgroup* if it is symmetric and there exists a finite symmetric set $X \subset H^2$ of cardinality at most K such that $HH \subset XH$. We are now ready to prove Lemma 2.5.

Proof of Lemma 2.5. Write

$$\mu_\delta \ll \sum_i 2^i \mathbb{1}_{A_i} \ll \mu_{4\delta}$$

as in Lemma 2.6. Note that for all i, one has

$$2^i |A_i|^{\frac{1}{2}} = \|2^i \mathbb{1}_{A_i}\|_2 \ll \|\mu_{4\delta}\|_2 \simeq \|\mu_\delta\|_2,$$

and

$$2^i |A_i| \simeq 2^i \delta^d N(A_i, \delta) \ll 1.$$

Assume for a contradiction that for some $\epsilon > 0$,

$$\|\mu_\delta * \mu_\delta\|_2 \ge \delta^\epsilon \|\mu_\delta\|_2,$$

with $\delta > 0$ arbitrarily small. This gives,

$$\begin{aligned}\delta^\epsilon \|\mu_\delta\|_2 &\ll \|\sum_{i,j} 2^i \mathbb{1}_{A_i} * 2^j \mathbb{1}_{A_j}\|_2 \\ &\le \sum_{i,j} \|2^i \mathbb{1}_{A_i} * 2^j \mathbb{1}_{A_j}\|_2,\end{aligned}$$

and as the sum on the right-hand side contains at most $O((\log \delta)^2)$ terms, we must have, for some i and j,

$$\|2^i \mathbb{1}_{A_i} * 2^j \mathbb{1}_{A_j}\|_2 \gg \frac{\delta^\epsilon}{(\log \delta)^2} \|\mu_\delta\|_2 \ge \delta^{O(\epsilon)} \|\mu_\delta\|_2.$$

Therefore,

$$\delta^{O(\epsilon)} \|\mu_\delta\|_2 \le \|2^i \mathbb{1}_{A_i} * 2^j \mathbb{1}_{A_j}\|_2 \le \|2^i \mathbb{1}_{A_i}\|_1 \|2^j \mathbb{1}_{A_j}\|_2 \ll 2^i |A_i| \|\mu_\delta\|_2. \quad (2)$$

This implies,

$$2^i |A_i| = \delta^{O(\epsilon)} \quad \text{and similarly} \quad 2^j |A_j| = \delta^{O(\epsilon)}. \quad (3)$$

So we have the following lower bound on the multiplicative energy of A_i and A_j:

$$\begin{aligned}E_\delta(A_i, A_j) &\gg \delta^{-3d} \|\mathbb{1}_{A_i} * \mathbb{1}_{A_j}\|_2^2 \\ &\ge \delta^{-3d + O(\epsilon)} 2^{-2i-2j} \|\mu_\delta\|_2^2 \\ &\ge \delta^{-3d + O(\epsilon)} 2^{-i-j} |A_i|^{\frac{1}{2}} |A_j|^{\frac{1}{2}} = \delta^{O(\epsilon)} N(A_i, \delta)^{\frac{3}{2}} N(A_j, \delta)^{\frac{3}{2}}.\end{aligned}$$

By Theorem 2.7, there exists a $\delta^{-O(\epsilon)}$-approximate subgroup $\tilde{H}$ and elements x, y in G such that

$$N(\tilde{H},\delta) \leq \delta^{-O(\epsilon)} N(A_i,\delta)^{\frac{1}{2}} N(A_j,\delta)^{\frac{1}{2}}, \tag{4}$$

$$N(x\tilde{H}\cap A_i,\delta) \geq \delta^{O(\epsilon)} N(A_i,\delta) \quad \text{and} \quad N(\tilde{H}y\cap A_j,\delta) \geq \delta^{O(\epsilon)} N(A_j,\delta). \tag{5}$$

We may replace $\tilde{H}$ by its δ-neighborhood, and then, $\mu_\delta(x\tilde{H}) \geq \delta^{O(\epsilon)}$. Let U be a neighborhood of the identity in G as in Theorem 2.4, let $r > 0$ be such that $B(1, 2r) \subset U$, and cover $x\tilde{H}$ by $O(1)$ balls of radius r. One of these balls B must satisfy $\mu_\delta(x\tilde{H} \cap B) \geq \delta^{O(\epsilon)}$ and thus,

$$\mu_\delta * \mu_\delta(\tilde{H}^2 \cap U) \geq \mu_\delta(\tilde{H}x^{-1} \cap B^{-1})\mu_\delta(x\tilde{H}\cap B) \geq \delta^{O(\epsilon)}.$$

On the other hand, by (2) and (3),

$$\delta^{O(\epsilon)}\|\mu_\delta\|_2 \leq \|2^i \mathbb{1}_{A_i}\|_1 \|2^j \mathbb{1}_{A_j}\|_2 \leq \|2^j \mathbb{1}_{A_j}\|_2 \leq \delta^{-O(\epsilon)} 2^{j/2},$$

so that $2^j \geq \delta^{-\alpha+O(\epsilon)}$ and similarly $2^i \geq \delta^{-\alpha+O(\epsilon)}$. This implies

$$N(A_j,\delta) \leq \delta^{-d+\alpha+O(\epsilon)} \quad \text{and similarly} \quad N(A_i,\delta) \leq \delta^{-d+\alpha-O(\epsilon)}.$$

The set $\tilde{H}$ is a $\delta^{-O(\epsilon)}$-approximate subgroup, so $N(\tilde{H}^2,\delta) \leq \delta^{-O(\epsilon)}N(\tilde{H},\delta)$. Recalling Inequality (4), we find

$$N(\tilde{H}^2 \cap U,\delta) \leq N(\tilde{H}^2,\delta) \leq \delta^{-d+\alpha-O(\epsilon)}.$$

On the other hand, $\mu_\delta * \mu_\delta(\tilde{H}^2 \cap U) \geq \delta^{O(\epsilon)}$ so the second assumption on μ_δ forces, for any $\rho \geq \delta$ (note that any ball of radius ρ is included in the ρ-neighborhood of some proper closed connected subgroup),

$$N(\tilde{H}^2 \cap U,\rho) \geq \rho^{-\kappa}\delta^{O(\epsilon)}.$$

Thus, provided we have chosen $\epsilon > 0$ small enough, the set $\tilde{H}^2 \cap U$ satisfies the assumptions of Theorem 2.4, and so must be included in the δ^τ-neighborhood of a proper closed connected subgroup H of G, contradicting the assumption $\mu * \mu(H^{(\delta^\tau)}) \leq \delta^{-\epsilon}\delta^{\kappa\tau}$. □

The idea is now to apply repeatedly that Flattening Lemma to obtain:

Lemma 2.8. *Let μ be a symmetric almost Diophantine measure on a connected compact simple Lie group G. There exists a constant $C_0 = C_0(\mu)$ such that for any $\delta = e^{-C_0 n} > 0$ small enough,*

$$\|(\mu^{*C_0 \log\frac{1}{\delta}})_\delta\|_2 \leq \delta^{-\frac{1}{4}}.$$

Remark 2. The constant $\frac{1}{4}$ could be replaced in this lemma by any fixed positive constant α. Of course, C_0 would then depend on α.

Proof. We first check that a suitable power $\nu = \mu^{c \log \frac{1}{\delta}}$ satisfies the second condition of Lemma 2.5. Since μ is almost Diophantine, taking $n = \frac{1}{C_1} \log \frac{1}{\delta}$ in Equation (1) shows that when $\delta < \delta_0$, for any proper closed connected subgroup H,

$$\mu^{*\frac{1}{C_1} \log \frac{1}{\delta}}(H^{(\delta)}) \leq \delta^{\frac{c_2}{C_1}}.$$

If xH is a left coset of a closed subgroup H and m any symmetric measure, we have

$$m(xH^{(\delta)})^2 \leq m * m(H^{(2\delta)}).$$

Therefore, denoting $c = \frac{1}{4C_1}$ and $\kappa = \frac{c_2}{3C_1}$, we have, for all $\delta < \delta_0$, for any left coset xH of a proper closed connected subgroup,

$$\mu^{*2c \log \frac{1}{\delta}}(xH^{(\delta)}) \leq \delta^{\kappa}.$$

Now, if H is a closed subgroup and m and m' are any two probability measures on G, we have

$$m * m'(H^{(\delta)}) \leq \sup_{x \in G} m'(xH^{(\delta)}).$$

Therefore, if $\delta < \rho < \delta_0$, we have, for any proper closed connected subgroup H,

$$\mu^{*2c \log \frac{1}{\delta}}(H^{(\rho)}) \leq \max_x \mu^{*2c \log \frac{1}{\rho}}(xH^{(\rho)}) \leq \rho^{\kappa}.$$

In other terms, for $\delta > 0$ small enough, the measure $\nu := \mu^{*c \log \frac{1}{\delta}}$ satisfies the second condition of Lemma 2.5.
We now apply Lemma 2.5 repeatedly, starting with the measure ν. If $\|\nu_\delta\|_2 \leq \delta^{-\frac{1}{4}}$, then we have what we want. Otherwise, Lemma 2.5 applied to ν_δ with $\alpha = \frac{1}{2}$ shows that

$$\|(\nu * \nu)_\delta\|_2 \ll \|\nu_\delta * \nu_\delta\|_2 \leq \delta^{\epsilon} \|\nu_\delta\|_2.$$

We then repeat the same procedure, replacing ν by $\nu * \nu$, and so on (note that the computations made above for ν also show that all the convolution powers of ν will satisfy the second condition of Lemma 2.5). After at most $\frac{d}{\epsilon}$ iterations, the procedure must stop, i.e. we must have,

$$\|(\mu^{*C_0 \log \frac{1}{\delta}})_\delta\|_2 = \|(\nu^{*2^{\frac{d}{\epsilon}}})_\delta\|_2 \leq \delta^{-\frac{1}{4}}.$$

□

The end of the proof of Theorem 2.3 relies on the high-multiplicity of irreducible representations in the regular representation $L^2(G)$. Recall that the irreducible representations of G are in bijection with dominant analytically integral weights (see e.g. [7]). We denote by π_λ the irreducible representation of G with highest weight λ. If μ is a finite Borel measure on G, the Fourier coefficient of μ at λ is

$$\hat{\mu}(\lambda) = \int_G \pi_\lambda(g)\, d\mu(g).$$

By Lemma 2.8, all we need to show is the following.

Lemma 2.9. *Let μ be a Borel probability measure on a compact semisimple Lie group G such that for some constant C, for all $\delta = e^{-Cn} > 0$ small enough (n a positive integer),*

$$\|(\mu^{*C\log\frac{1}{\delta}})_\delta\|_2 \le \delta^{-\frac{1}{4}}.$$

Then μ has a spectral gap in $L^2(G)$.

Proof. Since the representation V_λ occurs in $L^2(G)$ with multiplicity $\dim V_\lambda$, the Parseval Formula for $(\mu^{*C\log\frac{1}{\delta}})_\delta$ gives

$$\|(\mu^{*C\log\frac{1}{\delta}})_\delta\|_2^2 = \sum_\lambda (\dim V_\lambda)\|\hat{\mu}(\lambda)^{C\log\frac{1}{\delta}}\hat{P}_\delta(\lambda)\|_{HS}^2, \tag{6}$$

where $\|\cdot\|_{HS}$ is the Hilbert-Schmidt norm. Moreover, it is easily seen that we may bound the distance (in operator norm) from $\hat{P}_\delta(\lambda)$ to the identity (see for instance [10, Lemme 3.1]): for some constant $c > 0$ depending only on G, we have, whenever $\|\lambda\| \le c\delta^{-1}$,

$$\|\hat{P}_\delta(\lambda) - Id_{V_\lambda}\|_{op} \le \frac{1}{2}.$$

Therefore for any λ such that $\|\lambda\| \le c\delta^{-1}$, using (6) and the assumption of the lemma,

$$\delta^{-\frac{1}{2}} \ge \frac{1}{2}(\dim V_\lambda)\|\hat{\mu}(\lambda)^{C\log\frac{1}{\delta}}\|_{op}^2. \tag{7}$$

Now, as a consequence of the Weyl dimension Formula, we have, for some constant c depending only on G, for any representation V_λ with highest weight λ [10, Lemme 3.2],

$$\dim V_\lambda \ge c\|\lambda\|.$$

Taking λ with $e^{-C}c\delta^{-1} \le \|\lambda\| \le c\delta^{-1}$ in the above equation (7), we find

$$\|\hat{\mu}(\lambda)^{C\log\frac{1}{\delta}}\|_{op}^2 \ll \delta^{\frac{1}{2}}.$$

However, the spectral radius of an operator T satisfies, for any integer,

$$RS(T) \le \|T^n\|_{op}^{\frac{1}{n}},$$

so that for some absolute constant K, we have

$$\begin{aligned} RS(\hat{\mu}(\lambda)) &\le (K\delta^{\frac{1}{4}})^{\frac{1}{C\log\frac{1}{\delta}}} \\ &= e^{-\frac{1}{4C}}K^{\frac{1}{C\log\frac{1}{\delta}}} \end{aligned}$$

which is bounded away from 1 as long as δ is sufficiently small, i.e. as long as λ is sufficiently large. As the spectral radius of T_μ in $L_0^2(G)$ is equal to the supremum of all $RS(\hat{\mu}(\lambda))$ for $\lambda \ne 0$, this finishes the proof. □

3 Measures supported on algebraic elements

In this section, we fix a basis for the Lie algebra $\mathfrak{g}$. We say that an element $g \in G$ is *algebraic* if the entries of the matrix of $\mathrm{Ad}\, g$ in that fixed basis are algebraic numbers. Recall that a probability measure on G is called *adapted* if its support generates a dense subgroup of G. We want to prove the following.

Theorem 3.1. *Let G be a connected compact simple Lie group. If μ is an adapted probability measure on G whose support consists of algebraic elements, then μ has a spectral gap.*

Remark 3. We have already explained in Remark 1 that it is enough to prove such a theorem for a symmetric measure μ. Moreover, if μ is symmetric, under the assumptions of the theorem, we may always find a symmetric finitely supported adapted measure ν that is absolutely continuous with respect to μ. It is readily seen that if ν has a spectral gap, then so has μ, so we may assume in the proof of Theorem 3.1 that μ is finitely supported.

The proof has two parts. First, we show that, given a proper closed subgroup H, the probability $\mu^{*n}(H)$ decays exponentially, with a rate that does not depend on H. Then, we show that when the support of μ consists of algebraic elements, the measure μ is almost Diophantine. This second part is based on an application of the effective arithmetic Nullstellensatz, and relies crucially on the algebraic assumption on the elements of the support of μ.

3.1 Transience of closed subgroups

We want to prove the following.

Proposition 3.2. *Let μ be an adapted finitely supported symmetric probability measure on a connected compact simple Lie group G. Then, there exists a constant $\kappa = \kappa(\mu)$ such that for $n \geq n_0$, for any proper closed subgroup $H < G$,*

$$\mu^{*n}(H) \leq e^{-\kappa n}.$$

The proposition is based on the following lemma.

Lemma 3.3. *Let $\Gamma = \langle S \rangle$ be a finitely generated dense subgroup in G. There exists a finite collection of vector spaces $\mathcal{S}_i$, $1 \leq i \leq s$, over local fields K_i, such that the following holds:*

- *for each $i \in \{1, \dots, s\}$, the group Γ acts proximally and strongly irreducibly on $\mathcal{S}_i$;*
- *for any proper closed subgroup $H < G$ such that $\Gamma \cap H$ is infinite, there exists an $i \in \{1, \dots, s\}$ for which $\Gamma \cap H$ stabilizes a proper linear subspace of $\mathcal{S}_i$.*

Let us explain how this lemma implies Proposition 3.2, when combined with the following important result of random matrix products theory [2, Proposition 12.3] (see also [5, Theorem 4.4]).

Theorem 3.4. *Let K be a local field and $\mathcal{S}$ be a finite dimensional vector space over K. Suppose μ is a measure on $GL(\mathcal{S})$ such that the semigroup Γ generated by the support of μ acts proximally on $\mathcal{S}$. Then, there exists a constant $\kappa = \kappa(\mu)$ such that for any integer n large enough, for any vector $v \in \mathcal{S}$ and any hyperplane $V < \mathcal{S}$,*

$$\mu^{*n}(\{g \in GL(\mathcal{S}) \,|\, g \cdot v \in V\}) \leq e^{-\kappa n}.$$

Proof of Proposition 3.2. Let Γ be the group generated by the support of μ. Given a proper closed connected subgroup H of G, we distinguish two cases.
<u>First case:</u> $\Gamma \cap H$ is finite.
By Selberg's Lemma, Γ contains a torsion free subgroup of finite index N_0. Hence the cardinality of $\Gamma \cap H$ is bounded by N_0 and the uniform exponential decay of $\mu^{*n}(H) = \mu^{*n}(\Gamma \cap H)$ is a direct consequence of Kesten's Theorem [6, Corollary 3] since Γ is not amenable.
<u>Second case:</u> $\Gamma \cap H$ is infinite.
Let $\mathcal{S}_i$, $1 \leq i \leq s$, be the vector spaces given by Lemma 3.3. For each i, the measure μ may be viewed as a measure on $GL(\mathcal{S}_i)$. Choose $\kappa > 0$ such that the conclusion of Theorem 3.4 holds for each $\mathcal{S}_i$.
Choose i such that $\Gamma \cap H$ stabilizes a proper subspace L of $\mathcal{S}_i$. We then have, for n large enough,

$$\mu^{*n}(\{g \in \Gamma \,|\, g \cdot L = L\}) \leq e^{-\kappa n},$$

so that

$$\mu^{*n}(H) = \mu^{*n}(H \cap \Gamma) \leq e^{-\kappa n}.$$

□

Before turning to the proof of Lemma 3.3, let us recall the setting. The group Γ is a dense finitely generated free subgroup of the connected compact simple group G, and k is the field generated by the coefficients of the elements $\mathrm{Ad}\, g$, for g in Γ. As Γ is dense in G, we may view G as the group of real points of an algebraic group $\mathbf{G}$ defined over k. Whenever K is a field containing k, we will denote by $\mathbf{G}(K)$ the group of K-points of $\mathbf{G}$. Similarly, if V is a linear representation of $\mathbf{G}$ defined over K, we will write $V(K)$ for the associated K-vector space, on which $\mathbf{G}(K)$ acts.
In the case when Γ acts proximally on the adjoint representation $\mathfrak{g}(K)$, for some local field K containing k, the proof of Lemma 3.3 is substantially simpler. This is the content of the next lemma.

Lemma 3.5. *Assume that Γ acts proximally on $\mathfrak{g}(K)$, for some local field K containing k. Then,*

- *the group Γ acts proximally and strongly irreducibly on $\mathfrak{g}(K)$;*
- *for any proper closed subgroup $H < G$ such that $\Gamma \cap H$ is infinite, $\Gamma \cap H$ stabilizes a proper linear subspace of $\mathfrak{g}(K)$.*

Proof. By assumption, Γ acts proximally on $\mathfrak{g}(K)$. As Γ is dense in G, it is Zariski dense in $\mathbf{G}(K)$, and therefore Γ acts strongly irreducibly on $\mathfrak{g}(K)$.
Now if H is a proper closed infinite subgroup of G such that $\Gamma \cap H$ is infinite, then $\Gamma \cap H$ stabilizes the (complex) Lie algebra of the Zariski closure of $\Gamma \cap H$. This is a proper subspace $L < \mathfrak{g}_{\mathbb{C}}$ defined over k (and hence, over K), so that $\Gamma \cap H$ stabilizes a proper subspace of $\mathfrak{g}(K)$. ☐

Let $\Delta \subset E$ (E a Euclidean space of dimension $\operatorname{rk} G$) be the root system of G, choose a basis Π for Δ, and let C be the associated Weyl chamber. If ω is a dominant weight, with associated irreducible representation V^ω, we denote by ω^* the dominant weight of the dual irreducible representation $(V^\omega)^*$. We observe the following:

Lemma 3.6. *Let $\tilde{\alpha}$ be the largest root of Δ. Either $\tilde{\alpha} = \omega$ is a fundamental weight, or $\tilde{\alpha} = \omega + \omega^*$ is the sum of a fundamental weight and its dual (those two might coincide).*

Proof. Let ρ be the sum of all fundamental weights of Δ. Choose a fundamental weight ω minimizing $\langle \omega, \rho \rangle$. The adjoint representation can be viewed as a subrepresentation of $\operatorname{End} V^\omega \simeq V^\omega \otimes (V^\omega)^*$. Comparing the highest weights, we find that $\tilde{\alpha}$ can be written

$$\tilde{\alpha} = \omega + \omega^* - \sum_i n_i \alpha_i, \quad n_i \in \mathbb{N},\ \alpha_i \text{ simple roots.}$$

Taking the inner product with ρ, we find that $\langle \tilde{\alpha}, \rho \rangle \leq 2\langle \omega, \rho \rangle$ and in case of equality, we must have all n_i equal to zero i.e. $\tilde{\alpha} = \omega + \omega^*$. On the other hand, if the inequality is strict, by minimality of $\langle \omega, \rho \rangle$, the dominant weight $\tilde{\alpha}$ must be fundamental (not necessarily ω, though). This proves the lemma. ☐

Finally, we recall the following fact.

Lemma 3.7. *Assume Γ acts proximally on $V^\omega(K)$, for some local field K containing k. Then, Γ acts proximally on $V^{\omega+\omega^*}(K)$.*

Proof. This is an immediate consequence of the fact that if Γ acts proximally on a vector space V, then we may find an element γ in Γ such that both γ and γ^{-1} act proximally on V, see [1, Lemme 3.9]. ☐

According to Lemma 3.6, write $\tilde{\alpha} = \omega$ or $\tilde{\alpha} = \omega + \omega^*$. Putting together Lemma 3.5 and Lemma 3.7, we find that Lemma 3.3 holds whenever Γ acts proximally on $V^\omega(K)$ (or $V^{\omega^*}(K)$) for some local field K. Therefore, for the rest of the proof of Lemma 3.3, we assume (writing the largest root $\tilde{\alpha} = \omega + \omega^*$ or $\tilde{\alpha} = \omega$, for some fundamental weight ω):

$$\text{There is no local field } K \text{ such that } \Gamma \text{ acts proximally on } V^\omega(K). \qquad (8)$$

To prove Lemma 3.3, we start by defining a certain family of irreducible complex representations of G. For any nonzero vector X in the Weyl chamber C of Δ, we let

$$\mathcal{E}_X = \{\alpha \in \Delta \mid \langle \alpha, X \rangle \text{ is maximal}\}$$

and

$$m_X = \operatorname{card} \mathcal{E}_X.$$

Note that the largest root $\tilde{\alpha}$ of Δ always belongs to $\mathcal{E}_X$ so that $\mathcal{E}_X = \{\alpha \in \Delta \mid \langle \tilde{\alpha} - \alpha, X \rangle = 0\}$.
Finally, we define a dominant weight ω_X by

$$\omega_X = \sum_{\alpha \in \mathcal{E}_X} \alpha,$$

and denote by $\mathcal{S}_X$ the irreducible representation of G with highest weight ω_X. A simple way to check that ω_X is indeed a dominant weight is to construct $\mathcal{S}_X$ explicitly as follows. Write the decomposition of $\mathfrak{g}_{\mathbb{C}}$ into root spaces for some maximal torus T:

$$\mathfrak{g}_{\mathbb{C}} = \mathfrak{t}_{\mathbb{C}} \oplus \left(\bigoplus_{\alpha \in \Delta} \mathfrak{g}_\alpha \right).$$

Each $\mathfrak{g}_\alpha$ is one-dimensional, so write $\mathfrak{g}_\alpha = \mathbb{C} E_\alpha$. The representation $\mathcal{S}_X$ is the subrepresentation of $\bigwedge^{m_X} \mathfrak{g}_{\mathbb{C}}$ generated by the vector

$$\xi_X = \bigwedge_{\alpha \in \mathcal{E}_X} E_\alpha \in \bigwedge^{m_X} \mathfrak{g}_{\mathbb{C}}.$$

The spaces $\mathcal{S}_i$ of Lemma 3.3 will be constructed as representations $\mathcal{S}_X(K)$, where the local field K will be suitably chosen as to arrange that the action of Γ is proximal. The difficult point will be to prove the existence of a proper stable subspace under $\Gamma \cap H$, when H is a closed subgroup. For that, one crucial observation is the following fact about faces of root systems.

Lemma 3.8. *Let Δ be an irreducible root system with a given basis Π. Denote by $\tilde{\alpha}$ the largest root of Δ, and let X be a nonzero vector in the Weyl chamber C. In the case $\tilde{\alpha} = \omega + \omega^*$ and $\omega \neq \omega^*$, assume X not collinear to ω nor to ω^*. We define the* face of Δ associated to X *by*

$$\mathcal{E}_X = \{\alpha \in \Delta \mid \langle \tilde{\alpha} - \alpha, X \rangle = 0\},$$

and denote by $W_{\tilde{\alpha}}$ the stabilizer of $\tilde{\alpha}$ in the Weyl group W of Δ. Then,

$$\bigcap_{w \in W_{\tilde{\alpha}}} w \cdot \mathcal{E}_X = \{\tilde{\alpha}\}.$$

Proof. Letting $\mathcal{E}'_X = \tilde{\alpha} - \mathcal{E}_X$, we want to check that

$$\bigcap_{w \in W_{\tilde{\alpha}}} w \cdot \mathcal{E}'_X = \{0\}.$$

For sake of clarity, we deal first with the case when $\tilde{\alpha}$ is proportional to some fundamental weight $\omega = \omega_{i_0}$. Any element u in $\mathcal{E}'_X$ can be written $u = \tilde{\alpha} - \alpha$, so that

$$\langle u, \tilde{\alpha}\rangle = \|\tilde{\alpha}\|^2 - \langle \alpha, \tilde{\alpha}\rangle,$$

and, as $\tilde{\alpha}$ has maximal norm among the roots, this shows,

$$\forall u \in \mathcal{E}'_X \setminus \{0\},\ \langle u, \tilde{\alpha}\rangle > 0. \tag{9}$$

On the other hand, since the largest root $\tilde{\alpha}$ is proportional to a fundamental weight, the elements of E invariant under $W_{\tilde{\alpha}}$ are proportional to $\tilde{\alpha}$. This implies that the element $\frac{1}{|W_{\tilde{\alpha}}|}\sum_{w\in W_{\tilde{\alpha}}} w \in \operatorname{End} E$ is just the orthogonal projection to $\mathbb{R}\tilde{\alpha}$, so that

$$\frac{1}{|W_{\tilde{\alpha}}|}\sum_{w\in W_{\tilde{\alpha}}} w\cdot X = \langle X, \frac{\tilde{\alpha}}{\|\tilde{\alpha}\|^2}\rangle\tilde{\alpha},$$

is a nonzero multiple of $\tilde{\alpha}$. This implies in particular that

$$\bigcap_{w\in W_{\tilde{\alpha}}} w\cdot X^{\perp} \subset \tilde{\alpha}^{\perp}.$$

Recalling (9), we indeed find

$$\bigcap_{w\in W_{\tilde{\alpha}}} w\cdot \mathcal{E}'_X \subset \mathcal{E}'_X \cap \bigcap_{w\in W_{\tilde{\alpha}}} w\cdot X^{\perp} \subset \mathcal{E}'_X \cap \tilde{\alpha}^{\perp} = \{0\}.$$

We deal now with the case $\tilde{\alpha} = \omega + \omega^*$, with $\omega \neq \omega^*$. This means that the group G is of type A_ℓ, i.e. locally isomorphic to $SU(\ell+1)$. Note that this is exactly the case studied by Bourgain and Gamburd in [4]. We may modify the above argument in the following way. The element $\frac{1}{|W_{\tilde{\alpha}}|}\sum_{w\in W_{\tilde{\alpha}}} w$ is the orthogonal projection on the subspace $\mathbb{R}\omega \oplus \mathbb{R}\omega^*$. As X is not collinear to ω nor to ω^*, we have

$$\frac{1}{|W_{\tilde{\alpha}}|}\sum_{w\in W_{\tilde{\alpha}}} w\cdot X = a\omega + b\omega^*, \quad \text{for some } a, b > 0$$

so that

$$\bigcap_{w\in W_{\tilde{\alpha}}} w\cdot X^{\perp} \subset (a\omega + b\omega^*)^{\perp}.$$

Then we observe that any element u in $\mathcal{E}'_X$ is a sum of simple roots:

$$u = \sum_{\alpha\in\Pi} n_\alpha \alpha$$

and as $\tilde{\alpha} = \omega + \omega^*$ has maximal norm among the roots, we must have $n_\alpha \geq 1$ for α the simple root corresponding to ω or ω^*. This implies in particular

$$\forall u \in \mathcal{E}'_X \setminus \{0\},\ \langle u, a\omega + b\omega^*\rangle > 0.$$

As before, this yields

$$\bigcap_{w\in W_{\tilde\alpha}} w\cdot \mathcal{E}'_X \subset \mathcal{E}'_X \cap \bigcap_{w\in W_{\tilde\alpha}} w\cdot X^\perp \subset \mathcal{E}'_X \cap (a\omega + b\omega^*)^\perp = \{0\}.$$

□

This property of root systems implies the following result about non-irreducibility of the representations $\mathcal{S}_X$ under proper subgroups of G.

Lemma 3.9. *Let G be a connected compact simple Lie group with root system Δ, let X be a nonzero vector in the Weyl chamber C. In the case $\tilde\alpha = \omega + \omega^*$ and $\omega \neq \omega^*$, assume X is not collinear to ω nor to ω^*. If H is a proper closed positive dimensional subgroup of G such that for some γ in H, the vector ξ_X above is an eigenvector of γ whose associated eigenvalue has multiplicity one. Then, the representation $\mathcal{S}_X$ is not irreducible under the action of H.*

Proof. Denote by L the complexification of the Lie algebra of H, by $L^\perp$ its orthogonal for the Killing form, and write

$$\bigwedge^{m_X} \mathfrak{g}_{\mathbb{C}} = \bigoplus_{j=0}^{m_X} \bigwedge^j L \wedge \bigwedge^{m_X - j} L^\perp.$$

All the subspaces on the right-hand side of the formula are stable under the action of γ (in fact, of H), so that the eigenvector ξ_X, whose associated eigenvalue has multiplicity one, must belong to one of them, say

$$\xi_X \in \bigwedge^j L \wedge \bigwedge^{m_X - j} L^\perp. \tag{10}$$

The subspace $\mathcal{S}_X \cap \bigwedge^j L \wedge \bigwedge^{m_X-j} L^\perp$ is a nonzero subspace of $\mathcal{S}_X$ that is invariant under H. Suppose for a contradiction that it is equal to the whole of $\mathcal{S}_X$, i.e. that

$$\mathcal{S}_X \subset \bigwedge^j L \wedge \bigwedge^{m_X - j} L^\perp. \tag{11}$$

Let F be the subspace of $\mathfrak{g}_{\mathbb{C}}$ generated by the E_α, for α in $\mathcal{E}_X$. By (10), we have

$$F = F\cap L \oplus F \cap L^\perp.$$

As the largest root $\tilde\alpha$ is always in $\mathcal{E}_X$, the vector $E_{\tilde\alpha}$ is in F, and therefore,

$$p_L(E_{\tilde\alpha}) \in F,$$

where p_L denotes the orthogonal projections from $\mathfrak{g}_{\mathbb{C}}$ to L. Now, let w be an element of the Weyl group of Δ fixing $\tilde\alpha$. By (11) and the fact that $\mathcal{S}_X$ is stable under G, we have

$$w\cdot \xi_X \in \bigwedge^j L \wedge \bigwedge^{m_X - j} L^\perp.$$

Reasoning as before, this yields, since $\tilde\alpha$ is invariant under w,

$$p_L(E_{\tilde\alpha}) \in w\cdot F.$$

Therefore, letting w describe the stabilizer $W_{\tilde{\alpha}}$ of the largest root, we obtain

$$p_L(E_{\tilde{\alpha}}) \in \bigcap_{w \in W_{\tilde{\alpha}}} w \cdot F.$$

However, by Lemma 3.8, the intersection on the right reduces to $\mathbb{C}E_{\tilde{\alpha}}$. If $p_L(E_{\tilde{\alpha}}) \neq 0$, we find $E_{\tilde{\alpha}} \in L$. Otherwise, $E_{\tilde{\alpha}} \in L^{\perp}$. To conclude, we observe that by (11) and the fact that $\mathcal{S}_X$ is stable under G, we have, for any g in G,

$$g \cdot \xi_X \in \bigwedge^{j} L \wedge \bigwedge^{m_X - j} L^{\perp},$$

so that we can reason exactly as before, just conjugating the maximal torus T, the root-spaces and the space F by the element g. This yields

$$g \cdot E_{\tilde{\alpha}} \in L \quad \text{or} \quad g \cdot E_{\tilde{\alpha}} \in L^{\perp}.$$

Exchanging if necessary L and $L^{\perp}$, we may assume without loss of generality that for a set $A \subset G$ of positive Haar measure in G, we have

$$\forall g \in A,\ g \cdot E_{\tilde{\alpha}} \in L,$$

which is easily seen to imply $L = \mathfrak{g}_{\mathbb{C}}$ contradicting the assumption that H is a proper closed connected subgroup of G.
Thus, we have shown that $\mathcal{S}_X \cap \bigwedge^j L \wedge \bigwedge^{m_X - j} L^{\perp}$ is a proper subspace of $\mathcal{S}_X$ that is invariant under H. In particular, $\mathcal{S}_X$ is not irreducible under H. □

Remark 4. Note that the fact that $\mathcal{S}_X$ is not irreducible under H also implies that it is not irreducible under any conjugate aHa^{-1} of H.

We are now ready to conclude the proof of Proposition 3.2 by deriving Lemma 3.3.

Proof of Lemma 3.3. Clearly, it suffices to deal with maximal proper closed subgroups H. There are only finitely many such maximal subgroups, up to conjugation by elements of G. Denote by $\mathcal{T}$ a finite set of representatives modulo conjugation of all maximal closed subgroups H that admit a conjugate H_0 such that $H_0 \cap \Gamma$ is infinite. We may require that for each H_0 in $\mathcal{T}$, the intersection $\Gamma \cap H_0$ is infinite. For each such H_0, we will construct a vector space $\mathcal{S}$ over a local field K and a representation of Γ in $\mathcal{S}$ such that:

- the group Γ acts proximally and strongly irreducibly on $\mathcal{S}$,
- if H is any conjugate of H_0, then $H \cap \Gamma$ stabilizes a proper subspace of $\mathcal{S}$.

As $\Gamma \cap H_0$ is infinite, it contains a non-torsion element γ. Then, $\mathrm{Ad}\,\gamma$ has an eigenvalue λ that is not a root of unity. If k is the field generated by the coefficients of all $\mathrm{Ad}\,g$, $g \in \Gamma$, by [13, Lemma 4.1], we may choose an embedding of $\mathsf{k}(\lambda)$ into a local field K_v such that $|\lambda|_v > 1$.
Denote by Δ the root system of G and by E the Euclidean space containing it. For some $X_0 \in E$, the eigenvalues of $\mathrm{Ad}\,\gamma$ are: 1 (with multiplicity $\mathrm{rk}\,G$) and

the $e^{i\langle \alpha, X_0 \rangle}$, $\alpha \in \Delta$.
As $|\cdot|_v$ is multiplicative, there exists a unique $X \in E$ such that

$$\forall \alpha \in \Delta, \quad \log |e^{i\langle \alpha, X_0 \rangle}|_v = \langle \alpha, X \rangle.$$

We choose a basis for Δ such that X lies in the Weyl chamber C and consider the associated complex irreducible representation of G introduced earlier as $\mathcal{S}_X$. We choose a finite extension K of K_v containing all extensions of k of degree at most $\dim \mathcal{S}_X$ and such that $\mathbf{G}$ is split over K. The representation $\mathcal{S}_X$ is then defined over K, and we set $\mathcal{S} = \mathcal{S}_X(K)$. As Γ is a Zariski dense subgroup of $\mathbf{G}(K)$, $\mathcal{S}$ is a strongly irreducible and proximal representation of Γ.
On the other hand, writing the largest root $\tilde{\alpha} = \omega$ or $\tilde{\alpha} = \omega + \omega^*$, Assumption (8) implies that the element X is not collinear to ω nor to ω^*. Moreover, the vector ξ_X is the eigenvector of γ associated to the unique eigenvalue of maximal modulus in K_v, so that Lemma 3.9 shows that $\mathcal{S}_X$ is not irreducible under H_0. As we already observed, this implies that whenever H is conjugate to H_0, $\mathcal{S}_X$ is not irreducible under H.
Thus, if H is any conjugate of H_0, applying Lemma 3.10 below to the set of $\mathrm{Ad}\, g$, for $g \in \Gamma \cap H$, we obtain an extension $K' > K$ of degree at most $\dim \mathcal{S}_X$ and a proper subspace of $\mathcal{S}_X$ defined over K' that is stable under $\Gamma \cap H$. This yields a proper subspace of $\mathcal{S}$ stable under $\Gamma \cap H$ and finishes the proof. □

For convenience of the reader, we recall the following easy linear algebra lemma, which we just used in the above proof.

Lemma 3.10. *Let A be a subset of $SU(d)$ whose elements have coefficients in a field $\mathsf{k} < \mathbb{C}$, and suppose A stabilizes a proper subspace V of $\mathbb{C}^d$. Then there exists an extension $\mathsf{k}' > \mathsf{k}$ of degree at most d and a proper subspace V' defined over k' and stable under A.*

Proof. The set of solutions $x \in \mathrm{End}(\mathbb{C}^d)$ to

$$\forall a \in A,\ ax = xa, \tag{12}$$

is a vector space defined over k, it contains both the identity and the orthogonal projection on the proper stable subspace, so it has dimension at least two. Therefore, we may find a solution x that has coefficients in k and is not a homethety. Then, pick an eigenvalue λ of x, let $\mathsf{k}' = \mathsf{k}(\lambda)$ and $V' = \ker(x - \lambda I)$; this solves the problem. □

3.2 From a closed subgroup to a small neighborhood

Let S be a finite set of *algebraic* elements in G, and let $\Gamma = \langle S \rangle$ be the subgroup generated by S. We endow Γ with the word metric associated to the generating system S, and denote by $B_\Gamma(n)$ the ball of radius n centered at the identity, for that metric. If L is a proper subspace of the Lie algebra $\mathfrak{g}$ of G, we let

$$H_L = \{g \in G \,|\, (\mathrm{Ad}\, g)L = L\}.$$

The key proposition is the following.

Proposition 3.11. *Let G be a connected compact simple group and Γ a dense subgroup generated by a finite set S of algebraic elements of G. There exist a constant $C_1 = C_1(S)$ and an integer n_0 such that for any integer $n \geq n_0$, for any proper subspace $L_0 < \mathfrak{g}$, there exists a proper closed subgroup $H_1 < G$ such that*

$$B_\Gamma(n) \cap H_{L_0}^{(e^{-C_1 n})} \subset B_\Gamma(n) \cap H_1.$$

With this proposition, let us prove Theorem 3.1.

Proof of Theorem 3.1. By Theorem 2.3, it suffices to check that μ is almost Diophantine. Let C_1 be the constant given by Proposition 3.11. For H a proper closed subgroup of G we want to bound $\mu^{*n}(H^{(e^{-C_1 n})})$. If H is finite we conclude as in the proof of Lemma 3.3 using Selberg's Lemma and Kesten's Theorem, so we may as well assume that H is positive dimensional. Denote by L_0 its Lie algebra. By Proposition 3.11,

$$B_\Gamma(n) \cap H_{L_0}^{(e^{-C_1 n})} \subset B_\Gamma(n) \cap H_1,$$

and therefore, by Proposition 3.2 (taking $c_2 = \kappa > 0$),

$$\mu^{*n}(H^{(e^{-C_1 n})}) \leq \mu^{*n}(H_1) \leq e^{-c_2 n},$$

and μ is almost Diophantine. □

To prove Proposition 3.11 we want to use an effective version of Hilbert's Nullstellensatz. For that, we need to set up some notation.

Let e_i, $1 \leq i \leq d$, be a basis for $\mathfrak{g}_\mathbb{C}$, and define, for $I \subset \{1, \dots, d\}$,

$$e_I = \bigwedge_{i \in I} e_i.$$

The family $(e_I)_{|I|=l}$ is a basis for $\bigwedge^\ell \mathfrak{g}_\mathbb{C}$. Denote $\mathcal{W}_\ell \subset \bigwedge^\ell \mathfrak{g}_\mathbb{C}$ the set of pure tensors, i.e. the set of elements in $\bigwedge^\ell \mathfrak{g}_\mathbb{C}$ that can be written $v_1 \wedge v_2 \wedge \cdots \wedge v_\ell$ for some v_i's in $\mathfrak{g}_\mathbb{C}$. It is easy to check that $\mathcal{W}_\ell$ is an algebraic subvariety of $\bigwedge^\ell \mathfrak{g}_\mathbb{C}$ defined over the rationals and therefore, we may choose a finite collection of polynomials $(R_j)_{1 \leq j \leq C}$ with integer coefficients in $\binom{d}{\ell}$ variables such that for any $v = \sum v_I e_I$ in $\bigwedge^\ell \mathfrak{g}_\mathbb{C}$,

$$v \in \mathcal{W}_\ell \iff \forall j,\ R_j((v_I)_{|I|=\ell}) = 0.$$

We also define a family of polynomial maps $P_{I_0,g} : \mathbb{C}^{\binom{d}{\ell}-1} \to \bigwedge^\ell \mathfrak{g}_\mathbb{C}$ for $I_0 \subset \{1, \dots, d\}$ with $|I_0| = \ell$ and $g \in G$, in the following way. The polynomial $P_{I_0,g}$ has $\binom{d}{\ell} - 1$ variables v_I, indexed by all subsets I of $\{1, \dots, d\}$ of cardinality ℓ except I_0, and is defined by

$$P_{I_0,g}((v_I)) = g \cdot v - v,$$

where $v = e_{I_0} + \sum_{I \neq I_0} v_I e_I$.

Definition 3.12. If P is a polynomial map $\mathbb{C}^a \to \mathbb{C}^b$ with coefficients in a number field k (in the canonical bases), we define the *size* of P by

$$\|P\| = \max\{|\sigma(c)|\,;\, c \text{ coefficient of } P,\ \sigma \in \mathrm{Hom}_{\mathbb{Q}}(\mathsf{k}, \mathbb{C})\}.$$

Let k be the number field generated by the coefficients of all $\mathrm{Ad}\, g$, for $g \in \Gamma$, and denote by $\mathcal{O}_{\mathsf{k}}$ its ring of integers. We have the following obvious lemma.

Lemma 3.13. *There exists a positive integer $q = q(S)$ such that if $g \in B_\Gamma(n)$, then $q^n P_{I_0,g}$ has coefficients in $\mathcal{O}_{\mathsf{k}}$ and*

$$\|q^n P_{I_0,g}\| \leq q^{2n}.$$

We are now ready to derive Proposition 3.11. The letter C denotes any constant that depends only on G; this constant will change along the proof.

Proof of Proposition 3.11. Let L_0 be an ℓ-dimensional subspace of $\mathfrak{g}$ with orthonormal basis $(u_i)_{1\leq i\leq \ell}$. Write $u = u_1 \wedge \cdots \wedge u_\ell = \sum_I u_I e_I$. As L_0 is defined over the reals, $H_{L_0} \cdot u = \pm u$. We assume for simplicity that $H_{L_0} \cdot u = u$. [1] For some I_0, we have $|u_{I_0}| \geq \frac{1}{C}$ for some constant C depending only on $\dim G$. We let $u' = \frac{1}{|u_{I_0}|} u$, so that $\|u'\| \leq C$. We claim that if we choose C_1 large enough, then, for $n \geq n_0$ (C_1, n_0 independent of L_0), the family of polynomials $\mathcal{P} = \{R_i\} \cup \{P_{I_0,g}\}_{g \in H_{L_0}^{(e^{-C_1 n})} \cap B_\Gamma(n)}$ must have a common zero in $\mathbb{C}^{\binom{d}{\ell}-1}$. Suppose for a contradiction that this is not the case. By the above lemma, there is a positive integer q depending only on S such that for all P in $\mathcal{P}$, $q^n P$ has coefficients in $\mathcal{O}_{\mathsf{k}}$ and for all P in $\mathcal{P}$,

$$\|q^n P\| \leq q^{2n}.$$

As the $P_{I_0,g}$ have bounded degree (in fact, degree 1) we may extract from the family $q^n\mathcal{P}$ polynomials P_j, $1 \leq j \leq C$ generating the same ideal as $\mathcal{P}$. By the effective Nullstellensatz [9, Theorem IV], if the family of polynomials $\mathcal{P}$ has no common zero, then there exist an element $a \in \mathcal{O}_{\mathsf{k}}$ and polynomials Q_j with coefficients in $\mathcal{O}_{\mathsf{k}}$, such that

$$a = \sum Q_j P_j \tag{13}$$

and

$$\forall j, \quad \|Q_j\| \leq q^{Cn} \quad \deg Q_j \leq C \quad \text{and} \quad \|a\| \leq q^{Cn}. \tag{14}$$

Now, we want to evaluate (13) at u' to get a contradiction.
First, we observe that for any P in $q^n\mathcal{P}$ (in particular, for any P_j),

$$|P(u')| \leq C q^n e^{-C_1 n}.$$

Indeed, if P is one of the R_i's, we have $P(u') = 0$ because u' is a pure tensor; and if $P = P_{I_0,g}$, using that $g \in H_{L_0}^{(e^{-Cn})}$ and that H_{L_0} fixes u', we also find the

[1] Otherwise, one should use polynomials $P_{I_0,g}(v)$ defining the subvariety $\{v \,|\, g\cdot v \pm v = 0\}$.

desired estimate.
Second, by (14) and the fact that $\|u'\| \leq C$, we have, for each j,

$$|Q_j(u')| \leq Cq^{Cn}.$$

Finally, as a is a nonzero element of $\mathcal{O}_\mathsf{k}$ of size at most q^{Cn}, we have a lower bound on its complex absolute value (for a constant M depending only on $\mathcal{O}_\mathsf{k}$):

$$q^{-Mn} \leq |a|.$$

Thus,

$$q^{-Mn} \leq |a| \leq \sum |Q_j(u')||P_j(u')| \leq Cq^{Cn}e^{-C_1 n},$$

which yields a contradiction provided we have chosen C_1 large enough (in terms of C, q and M).
Now let $(v_I)_{I \neq I_0}$ be a common zero for the family $\mathcal{P}$. As, for each i, $R_i((v_I)) = 0$, the vector $v = e_{I_0} + \sum_{I \neq I_0} v_I e_I$ is a pure tensor: $v = v_1 \wedge \cdots \wedge v_\ell$. Moreover, for all g in $B_\Gamma(n) \cap H_{L_0}^{(e^{-Cn})}$, $g \cdot v = v$, so that the subspace $L_1 = \operatorname{Span} v_i$ is stable under g. In other terms, $g \in H_{L_1}$, which is what we wanted to show. □

References

[1] Y. Benoist. Sous-groupes discrets des groupes de Lie. *Notes from the 1997 European Summer School in Group Theory, Luminy July 7-18*, 1997.

[2] Y. Benoist and J.-F. Quint. *Random walks on reductive groups.* preprint, 2013. available at `www.math.u-bordeaux1.fr/~jquint/`.

[3] J. Bourgain and A. Gamburd. On the spectral gap for finitely generated subgroups of $SU(2)$. *Inventiones Mathematicae*, 171:83–121, 2008.

[4] J. Bourgain and A. Gamburd. A spectral gap theorem in $SU(d)$. *Journal of the European Mathematical Society*, 14(5):1455–1511, 2012.

[5] Jean Bourgain, Alex Furman, Elon Lindenstrauss, and Shahar Mozes. Stationary measures and equidistribution for orbits of nonabelian semigroups on the torus. *J. Amer. Math. Soc.*, 24(1):231–280, 2011.

[6] H. Kesten. Symmetric random walks on groups. *Transactions of the American Mathematical Society*, 92(2):336–354, 1959.

[7] A. Knapp. *Lie Groups Beyond an Introduction, Second Edition.* Birkhäuser, 2002.

[8] E. Lindenstrauss and N. de Saxcé. Hausdorff dimension and subgroups of $SU(2)$. *preprint*, 2013. available at `http://www.ma.huji.ac.il/~saxce`.

[9] D.W. Masser and G. Wüstholz. Fields of large transcendence degree generated by values of elliptic functions. *Invent. Math.*, 1983.

[10] N. de Saxcé. Trou dimensionnel dans les groupes de Lie semisimples compacts, via les séries de Fourier. *Journal d'Analyse Mathématique*, 120:311–331, 2013.

[11] N. de Saxcé. A product theorem in simple Lie groups. *preprint*, 2014. available at `http://www.ma.huji.ac.il/~saxce`.

[12] T.C. Tao. Product set estimates for non-commutative groups. *Combinatorica*, 28:547–594, 2008.

[13] J. Tits. Free subgroups in linear groups. *Journal of Algebra*, 20:250–270, 1972.