Séminaire Lotharingien de Combinatoire **84B** (2020)
Article #9, 12 pp.

Proceedings of the 32nd Conference on Formal Power Series and Algebraic Combinatorics (Online)

On the distribution of random words in a compact Lie group

Hariharan Narayanan*[1]

[1] *School of Technology and Computer Science*
Tata Institute of Fundamental Research, Mumbai, India

Abstract. Let G be a compact Lie group. Suppose $g_1, \dots, g_k$ are chosen independently from the Haar measure on G. Let $\mathcal{A} = \cup_{i \in [k]} \mathcal{A}_i$, where, $\mathcal{A}_i := \{g_i\} \cup \{g_i^{-1}\}$. Let $\mu_{\mathcal{A}}^{\ell}$ be the uniform measure over all words of length ℓ whose alphabets belong to $\mathcal{A}$. We give probabilistic bounds on the nearness of a heat kernel smoothening of $\mu_{\mathcal{A}}^{\ell}$ to a constant function on G in $\mathcal{L}^2(G)$. We also give probabilistic bounds on the maximum distance of a point in G to the support of $\mu_{\mathcal{A}}^{\ell}$.

Keywords: Random generation, Lie groups

1 Introduction

Let G be a compact $n-$dimensional Lie group endowed with a left-invariant Riemannian distance function d. Thus

$$\forall g, x, y \in G,\ d(x, y) = d(gx, gy).$$

We will denote by C_G a constant depending on (G, d) that is greater than 1. Suppose $g_1, \dots, g_k$ are chosen independently from the Haar measure on G. Let $\mathcal{A} = \cup_{i \in [k]} \mathcal{A}_i$, where, $\mathcal{A}_i := \{g_i\} \cup \{g_i^{-1}\}$. Let the Heat kernel at x corresponding to Brownian motion on G with respect to the distance function d started at the origin $o \in G$ for time t be $H_t(x)$. Let $\mu_{\mathcal{A}}^{\ell}$ be the uniform measure over all words of length ℓ whose alphabets belong to $\mathcal{A}$.

For the case $G = SU_n$, Bourgain and Gamburd proved [3] the existence of a spectral gap provided the entries of the generators are algebraic and the subgroup they generate is dense in G. There is a long line of work that this relates to, touching upon approximate subgroups and pseudorandomness, for which we direct the reader to the references in [3]. The question of a spectral gap when G is SU_2 for random generators of the kind we consider was reiterated by Bourgain and Gamburd in [2], being first raised by Lubotzky, Philips and Sarnak [8] in 1987 and is still open. In the setting of SU_2, our results can be viewed as addressing a quantitative version of a weak variant of this question.

*hariharan.narayanan@tifr.res.in.

Suppose $F_1, F_2, \dots$ are eigenspaces of the Laplacian L_G on G corresponding to eigenvalues $0 = \lambda_0 < \lambda_1 < \lambda_2 < \dots$. Let $f_i^1, \dots, f_i^j, \dots$ be an orthonormal basis for F_i, for each $i \in \mathbb{N}$. The Laplacian L_G is a second order differential operator, which for all twice differentiable functions f, satisfies $H_t * f = e^{tL_G} f$. G acts on functions in $\mathcal{L}^2(G)$ via T_g, the translation operator,

$$T_g f(x) = f(g^{-1}x).$$

Thus each F_i is a representation of G, though not necessarily an irreducible representation.

As stated in the introduction, let the Heat kernel at x corresponding to Brownian motion on G with respect to the distance function d started at the origin $o \in G$ for time t be $H_t(x)$. When we wish to change the starting point for the diffusion, we will denote by $H(x, y, t)$ the probability density of Brownian motion started at x at time zero ending at y at time t. Our first result, Theorem 3.2 relates to equidistribution and gives a lower bound on the probability that $\|\mu_{\mathcal{A}}^{\ell} * H_t - \frac{1}{\mathrm{vol} G}\|_{\mathcal{L}^2(G)}$ is less than a specified quantity 2η. Our second result, Theorem 3.4 provides conditions under which the set of all elements of G which can be expressed as words of length less or equal to ℓ with alphabets in $\mathcal{A}$, form a $2r-$net of G with probability at least $1 - \delta$. For constant δ, both k and ℓ can be chosen to be less than $Cn \log(1/r)$, where C is a universal constant.

Our main result on equidistribution, Theorem 3.2 immediately implies the following.

Theorem 1.1. *Let (G, d) be a tuple consisting of an n dimensional compact Lie group G and a Riemannian distance function d on it under which the Riemannian volume of G is 1. There exists a constant C_G depending only on on G and the distance function d on it such that the following is true. Let $\eta := 2^{-\ell} t^{-\frac{n}{4}}$ be sufficiently small. Let $\delta := (C_G/\eta) \exp\left(-\frac{k}{16 \ln 2}\right)$. Then, denoting by $\mathcal{A}^\ell$, the set of all ordered $\ell-$tuples with elements in $\mathcal{A}$,*

$$\mathbb{P}\left[\left\|1_G - \frac{1}{(2k)^\ell} \sum_{g \in \mathcal{A}^\ell} H_t \circ T_g\right\|_{\mathcal{L}^2(G)} \le 2\eta\right] \ge 1 - \delta. \tag{1.1}$$

Our main result on nets, Theorem 3.4 immediately implies the following.

Theorem 1.2. *Let $\delta \in (0, 1]$ be a real number. Let ϵ be a positive real number less than a sufficiently small constant depending only on G. Choose*

$$k \ge 12(n \ln \frac{1}{\epsilon} + \ln \frac{1}{\delta})$$

i.i.d random points $\{g_1, \dots, g_k\}$ from the Haar measure on G and let

$$\mathcal{A} = \{g_1, g_1^{-1}, \dots, g_k, g_k^{-1}\}.$$

Let $\ell = n \log_2(\frac{1}{\epsilon})$. Then, with probability at least $1 - \delta$, $\mathcal{A}^\ell$ is an $\epsilon-$net of G.

2 Analysis on a compact Lie group

The following is a theorem of Minakshisundaram and Pleijel [9, 10].

Theorem 2.1. *For each $x \in G$ there is an asymptotic expansion*

$$H(x,x,t) \sim t^{-n/2}(a_0(x) + a_1(x)t + a_2(x)t^2 + \dots),$$

$t \to 0$. The a_j are smooth functions on G.

Since G is equipped with a left invariant distance function, the $a_j(x)$ are constant functions. We will use the following theorem of Grigoryan from [6], where it appears as Theorem 1.1.

Theorem 2.2. *Assume that for some points $x, y \in M$ and for all $t \in (0,T)$,*

$$p_t(x,x) \leq \frac{C_1}{\gamma_1(t)},$$

and

$$p_t(y,y) \leq \frac{C_1}{\gamma_2(t)},$$

where γ_1 and γ_2 are increasing positive functions on $\mathbb{R}_+$ both satisfying

$$\frac{\gamma_i(at)}{\gamma_i(t)} \leq A\frac{\gamma_i(as)}{\gamma_i(s)} \tag{2.1}$$

for all $0 < t \leq s < T$, for some constants $a, A > 1$. Then for any $C > 4$ and all $t \in (0,T)$,

$$p_t(x,y) \leq \frac{C_2}{\sqrt{\gamma_1(\epsilon t)\gamma_2(\epsilon t)}} \exp\left(-\frac{d^2(x,y)}{Ct}\right) \tag{2.2}$$

for some $\epsilon = \epsilon(a,C) > 0$.

It follows from Theorem 2.1 that for some sufficiently small time $T > 0$, we can choose $\gamma_1(t) = \gamma_2(t) = (\frac{1}{2})t^{n/2}$ for $t \in (0,T)$ in Theorem 2.2.

This gives us the following corollary.

Corollary 2.3. *For any constant $C > 4$, there exists $T > 0$ and C_1 depending on G and C so that for all $t \in (0,T)$*

$$H(x,y,t) \leq C_1 t^{-n/2} \exp(-\frac{r^2}{Ct})$$

where n is the dimension of G and r is the distance between x and y.

Lemma 2.4. *Let $\eta > 0$. We take $\epsilon\sqrt{5\ln\frac{1}{\eta\epsilon^n}} = r$. If we choose $t = \epsilon^2$, then, for all y such that*

$$d(x,y) > r,$$

we have

$$H(x,y,t) < C_G\eta.$$

Proof. In Corollary 2.3, we may set $C = 5$ and $T = 1$ and ignore the dependence in x since the distance function is left invariant. For all $t \leq \epsilon^2$ and all y such that

$$d(x,y) > r,$$

$$\begin{aligned} H(x,y,t) &< C_1\epsilon^{-n}(\exp(-\ln\frac{1}{\eta\epsilon^n})) && (2.3)\\ &< C_1\eta. && (2.4)\end{aligned}$$

□

By Weyl's law for the eigenvalues of the Laplacian on a Riemannian manifold as proven by Duistermaat and Guillimin [5], we have the following.

Theorem 2.5.

$$\lim_{\lambda\to\infty}\frac{\lambda^{n/2}}{\sum_{\lambda_i\leq\lambda}\dim F_i} = \frac{\mathrm{vol}(B_n)\mathrm{vol}(G)}{(2\pi)^n} =: C_2,$$

where C_2 is a constant depending only on volume and dimension n of the Lie group.

This has the following corollary, which is improved upon by Theorem 2.7 below.

Corollary 2.6.

$$\sup_{i\geq 1}\frac{\dim F_i}{\lambda_i^{n/2}} = C_3,$$

where C_3 is a finite constant depending only on the Lie group and its distance function.

The following theorem is due to Donnelly (Theorem 1.2, [4]).

Theorem 2.7. *Let M be a compact $n-$dimensional Riemannian manifold and Δ its Laplacian acting on functions. Suppose that the injectivity radius of $\mathcal{M}$ is bounded below by c_4 and that the absolute value of the sectional curvature is bounded above by c_5. If $\Delta\phi = -\lambda\phi$ and $\lambda \neq 0$, then $\|\phi\|_\infty \leq c_2\lambda^{\frac{(n-1)}{4}}\|\phi\|_2$. The constant c_2 depends only upon c_4, c_5, and the dimension n of $\mathcal{M}$. Moreover the multiplicity $m_\lambda \leq c_3\lambda^{\frac{(n-1)}{2}}$ where c_3 depends only on c_2 and an upper bound for the volume of $\mathcal{M}$.*

Hörmander [7] proved this result earlier without specifying which geometric parameters the constants depended upon. Then, by the Fourier expansion of the heat kernel into eigenfunctions of the Laplacian,

$$H_t = \sum_{\lambda_i \geq 0} \sum_j a_{ij} f_{ij}.$$

where $a_{ij} = e^{-\lambda_i t} f_{ij}(0) \leq e^{-\lambda_i t}(c_2 \lambda_i^{\frac{n-1}{4}})$, where the f_{ij} for $j \in [1, \dim F_i] \cap \mathbb{N}$, form an orthonormal basis of F_i. Let

$$\tilde{H}_{t,M}(y) = \sum_{0 < \lambda_i \leq M} \sum_j a_{ij} f_{ij},$$

and

$$H_{t,M}(y) = \sum_{0 \leq \lambda_i \leq M} \sum_j a_{ij} f_{ij},$$

Lemma 2.8. *For any $M > 0$,*

$$\|\tilde{H}_{t,M}\|_{\mathcal{L}^2} < C_G t^{-n/4} \tag{2.5}$$

Proof. We note that

$$\|\tilde{H}_{t,M}\|_{\mathcal{L}^2} \leq \|H_t\|_{\mathcal{L}^2}, \tag{2.6}$$

because $\tilde{H}_{t,M}$ is the image of H_t under a projection (with respect to $\mathcal{L}^2$) onto a subspace spanned by the eigenfunctions of the Laplacian corresponding to eigenvalues in the range $(0, M]$. Thus it suffices to bound $\|H_t\|_{\mathcal{L}^2}$ from above in the appropriate manner. Choosing $\eta = 1$ in Lemma 2.4, we see that if we take $\epsilon\sqrt{5\ln(\epsilon^{-n})} = r$ and $t = \epsilon^2$, then,

for all y such that

$$d(x, y) > r,$$

we have

$$H(x, y, t) < C_G.$$

Let μ_n denote the Lebesgue measure on $\mathbb{R}^n$ and μ the volume measure on G. We next need an upper bound on $\int_{B(o,r)} H_t(y)^2 \mu(dy)$. Note that when ϵ is sufficiently small, $B(o, r)$ is almost isometric via the exponential map to a Euclidean ball of radius r in $\mathbb{R}^n$. Further, it is known that

$$\sqrt{\det g_{ij}(\exp_x(\alpha v))} = 1 - \frac{1}{6} Ric^g(v, v)\alpha^2 + o(\alpha^2), \tag{2.7}$$

where Ric denotes the Ricci tensor, and $\exp_x$, the exponential map at x. Since $Ric^g(v, v)$ is bounded above by a finite real number for v on the unit sphere,

$$\begin{aligned}
\int_{B(o,r)} H_t(y)^2 \mu(dy) &\leq C_G \left(\int_{\mathbb{R}^n} \epsilon^{-n} (\exp(-\frac{|y|^2}{5t})) \mu_n(dy) \right) \\
&\leq C_G \left(\int_{\mathbb{R}} \epsilon^{-1} (\exp(-\frac{|y|^2}{5t})) \mu_1(dy) \right)^n \\
&\leq C_G \epsilon^{-n}.
\end{aligned}$$

Therefore

$$\|H_t\|_{\mathcal{L}^2} \leq C_G \epsilon^{-n/2}. \tag{2.8}$$

□

Lemma 2.9. *For $M = 2^{\frac{2k_0}{n}}$ where*

$$k_0 \geq \max \left(\log_2 \frac{1}{\eta}, C_G + (1 + o(1)) \frac{n}{2} \log_2 \frac{1}{t} \right),$$

$$\|H_t - H_{t,M}\|_{\mathcal{L}^2} \leq \eta. \tag{2.9}$$

Proof. It follows by the $\mathcal{L}^2-$convergence of Fourier series that

$$\|H_t - H_{t,M}\|_{\mathcal{L}^2} \leq \sum_{\lambda_i \geq M} \dim(F_i) e^{-\lambda_i t} (c_2 \lambda_i^{\frac{n-1}{4}}). \tag{2.10}$$

By Weyl's law (Theorem 2.5),

$$\lim_{\lambda \to \infty} \frac{\lambda^{n/2}}{\sum_{\lambda < \lambda_i \leq 2^{\frac{2}{n}} \lambda} \dim F_i} = \frac{\mathrm{vol}(B_n) \mathrm{vol}(G)}{(2\pi)^n} =: C_2^{-1}.$$

Let, for $k \in \mathbb{N}$,

$$I_k = \left(2^{\frac{2k}{n}}, 2^{\frac{2k+2}{n}} \right]. \tag{2.11}$$

Now, for $k_0 > C_G$,

$$\begin{aligned}
\sum_{\lambda_i > 2^{\frac{2k_0}{n}}} \dim(F_i) e^{-\lambda_i t} (c_2 \lambda_i^{\frac{n-1}{4}}) &\leq \sum_{k \geq k_0} \left(\sum_{\lambda_i \in I_k} \dim(F_i) \right) \sup_{\lambda_i \in I_k} \left(\frac{c_2 \lambda_i^{\frac{n-1}{4}}}{e^{\lambda_i t}} \right) && (2.12) \\
&\leq C_2 \sum_{k \geq k_0} 2^{k+1} \sup_{\lambda_i \in I_k} \left(\frac{c_2 \lambda_i^{\frac{n-1}{4}}}{e^{\lambda_i t}} \right) && (2.13)
\end{aligned}$$

We see that

$$\sup_{\lambda_i \in I_k} \left(\frac{\lambda_i^{\frac{n-1}{4}}}{e^{\lambda_i t}} \right) < \frac{2^{\frac{(k+1)}{2}}}{\exp(2^{\frac{2k}{n}} t)} \tag{2.14}$$

$$< \exp\left(\frac{(k+1)}{2} - 2^{\frac{2k}{n}} t\right). \tag{2.15}$$

When

$$k \geq \left(\frac{n}{2}\right) \log_2 \frac{6k}{t}, \tag{2.16}$$

assuming $k > 5$, we have

$$\frac{k/t}{n/2t} \geq \log_2 \frac{\frac{5}{2}(k+1)}{t}, \tag{2.17}$$

and then, we see that

$$\exp\left(\frac{(k+1)}{2} - 2^{\frac{2k}{n}} t\right) < 2^{-2(k+1)}. \tag{2.18}$$

In order to enforce (2.16), it suffices to have

$$\frac{k}{\log_2 \frac{6k}{t}} \geq \frac{n}{2}, \tag{2.19}$$

which is implied by

$$\frac{6k}{\log_2 \frac{6k}{t}} \log_2 \left(\frac{6k}{t \log_2 \frac{6k}{t}} \right) \geq 3n \log_2 \left(\frac{3n}{t} \right). \tag{2.20}$$

This is equivalent to

$$k \left(1 - \frac{\log_2 \log_2 \frac{6k}{t}}{\log_2 \frac{6k}{t}} \right) \geq \frac{n}{2} \log_2 \left(\frac{3n}{t} \right), \tag{2.21}$$

which is in turn implied by

$$k \geq \frac{n}{2} \left(\log_2 \frac{3n}{t} \right) \left(1 - \frac{\log_2 \log_2 \frac{3n}{t}}{\log_2 \frac{3n}{t}} \right)^{-1} \tag{2.22}$$

$$= (1 + o(1)) \frac{n}{2} \log_2 \frac{3n}{t}. \tag{2.23}$$

Therefore, for any

$$k_0 > C_G + (1 + o(1))\frac{n}{2}\log_2 \frac{3n}{t},$$

$$\sum_{\lambda_i > 2^{\frac{2k_0}{n}}} \dim(F_i) e^{-\lambda_i t}(c_2 \lambda_i^{\frac{n-1}{4}}) < \frac{2^{(-k_0-1)}}{1-(1/2)} < 2^{(-k_0)}. \tag{2.24}$$

□

It follows from (2.9) that for any η, by choosing

$$k_0 = \max\left(\log_2 \frac{1}{\eta}, C_G + (1+o(1))n\log_2 \frac{1}{\epsilon}\right),$$

and

$$M \geq 2^{2k_0/n} \tag{2.25}$$

we have that

$$\|\tilde{H}_{t,M} - H_t\|_{\mathcal{L}^2} < \eta. \tag{2.26}$$

3 Equidistribution and an upper bound on the Hausdorff distance.

Let $A(V)$ denote the collection of self adjoint operators on the finite dimensional Hilbert space V. For $B \in A(V)$, we let $\|B\|$ denote the operator norm of B, equal to the largest absolute value attained by an eigenvalue of A. The cone of *non-negative definite* operators

$$\Lambda(V) = \{B \in A(V) | \forall v, \langle Av, v\rangle \geq 0\}$$

turns $A(V)$ into a poset by the relation $A \geq B$ if $A - B \in \Lambda(V)$.

We next state a matrix Chernoff bound due to Ahlswede and Winter from [1].

Theorem 3.1. *Let V be a Hilbert Space of dimension D and let $A_1, \dots, A_k$ be independent identically distributed random variables taking values in $\Lambda(V)$ with expected value $\mathbb{E}[A_i] = A \geq \mu I$ and $A_i \leq I$. Then for all $\epsilon \in [0, 1/2]$,*

$$\mathbb{P}\left[\frac{1}{k}\sum_{i=1}^{k} A_i \notin [(1-\epsilon)A, (1+\epsilon)A]\right] \leq 2D\exp\left(\frac{-\epsilon^2 \mu k}{2\ln 2}\right).$$

For any $g \in G$

$$(Id - T_g)\tilde{H}_{t,M} \tag{3.1}$$

lies in

$$\tilde{F}_M := \bigoplus_{0<\lambda_i \leq M} F_i. \tag{3.2}$$

$\tilde{F}_M$ has, by Weyl's law, a dimension that is bounded above by $O(M^{n/2})$. We will study the Markov operator $P : \tilde{F}_M \longrightarrow \tilde{F}_M$ given by

$$P(f)(x) := \frac{\sum_{g\in\mathcal{A}} (f(x) + f(gx))}{2|\mathcal{A}|}. \tag{3.3}$$

We know that $\mathcal{A} = \cup_i \mathcal{A}_i$, where, $\mathcal{A}_i = \{g_i\} \cup \{g_i^{-1}\}$. Note that P is the sum of k i.i.d operators

$$P_i := \frac{\sum_{g\in\mathcal{A}_i} (f(x) + f(gx))}{4}. \tag{3.4}$$

We see that $\forall f \in \tilde{F}_M$, and $1 \leq i \leq k$,

$$\mathbb{E}P_i(f) = (1/2)f, \tag{3.5}$$

which is equivalent to

$$\mathbb{E}P_i = (1/2)I.$$

By Theorem 3.1, for all $\epsilon \in [0, 1/2]$,

$$\mathbb{P}\left[\frac{1}{k}\sum_{i=1}^{k} P_i \notin [((1-\epsilon)/2)I, ((1+\epsilon)/2)I]\right] \leq C_G M^{n/2} \exp\left(\frac{-\epsilon^2 k}{4\ln 2}\right). \tag{3.6}$$

Setting $\epsilon = 1/2$ and substituting for M, we see that

$$\mathbb{P}\left[\frac{1}{k}\sum_{i=1}^{k} P_i \notin [(1/4)I, (3/4)I]\right] \leq \left(C_G M^{n/2}\right) \exp\left(\frac{-k}{16\ln 2}\right). \tag{3.7}$$

Let the map $x \mapsto gx$ be denoted by T_g. It follows that

$$\mathbb{P}\left[\forall f \in \tilde{F}_M, \left\|\frac{1}{2k}\sum_{g\in\mathcal{A}} f \circ T_g\right\|_{\mathcal{L}^2} \leq (1/2)\|f\|_{\mathcal{L}^2}\right] \geq 1 - \left(C_G M^{n/2}\right) \exp\left(\frac{-k}{16\ln 2}\right).$$

Iterating the above inequality ℓ times, we observe that

$$\mathbb{P}\left[\forall f \in \tilde{F}_M, \left\|\frac{1}{(2k)^\ell}\sum_{g\in\mathcal{A}^\ell} f \circ T_g\right\|_{\mathcal{L}^2} \leq (1/2)^\ell \|f\|_{\mathcal{L}^2}\right] \geq 1-\delta,$$

where

$$\delta := \left(C_G M^{n/2}\right)\exp\left(\frac{-k}{16\ln 2}\right). \tag{3.8}$$

Choosing $f = \tilde{H}_{t,M}$, we see that

$$\mathbb{P}\left[\left\|\frac{1}{(2k)^\ell}\sum_{g\in\mathcal{A}^\ell} \tilde{H}_{t,M} \circ T_g\right\|_{\mathcal{L}^2} \leq (1/2)^\ell \|\tilde{H}_{t,M}\|_{\mathcal{L}^2}\right] \geq 1-\delta,$$

By the above, and Lemmas 2.8 and 2.9, we see that

$$\mathbb{P}\left[\left\|\frac{1}{(2k)^\ell}\sum_{g\in\mathcal{A}^\ell} \tilde{H}_{t} \circ T_g\right\|_{\mathcal{L}^2} \leq \eta + 2^{-\ell}t^{-n/4}\right] \geq 1-\delta.$$

Thus, we see that

$$\mathbb{P}\left[\left\|\frac{1_G}{\mathrm{vol}G} - \frac{1}{(2k)^\ell}\sum_{g\in\mathcal{A}^\ell} H_{t} \circ T_g\right\|_{\mathcal{L}^2} \leq \eta + 2^{-\ell}t^{-n/4}\right] \geq 1-\delta. \tag{3.9}$$

We derive from this, the following theorem on the equidistribution of $\mathcal{A}^\ell$.

Theorem 3.2. *Let $2^{-\ell}t^{-\frac{n}{4}} \leq \eta \leq 2^{-C_G t^{\frac{(1+o(1))n}{2}}}$. Let $\delta = (C_G/\eta)\exp\left(-\frac{k}{16\ln 2}\right)$. Then,*

$$\mathbb{P}\left[\left\|\frac{1_G}{\mathrm{vol}G} - \frac{1}{(2k)^\ell}\sum_{g\in\mathcal{A}^\ell} H_{t} \circ T_g\right\|_{\mathcal{L}^2} \leq 2\eta\right] \geq 1-\delta. \tag{3.10}$$

Proof. This follows from (3.9) on setting $M = \eta^{-\frac{2}{n}}$ and substituting in (3.8). $\square$

Lemma 3.3. *Suppose $\epsilon\sqrt{5\ln\frac{C_G}{\epsilon^n}} = r$, and $t = \epsilon^2$ are sufficiently small. If*

$$\left\|\frac{1_G}{\mathrm{vol}G} - \frac{1}{(2k)^\ell}\sum_{g\in\mathcal{A}^\ell} H_{t} \circ T_g\right\|_{\mathcal{L}^2} \leq \sqrt{\mathrm{vol}(B_n)r^n}\left(\frac{1}{2\mathrm{vol}(G)}\right),$$

then, $\mathcal{A}^\ell$ is a $2r$-net of G.

Proof. Suppose $\mathcal{A}^\ell$ is not a $2r$-net of G. Then, there exists an element $\tilde{g}$ such that $d(\tilde{g}, \mathcal{A}^\ell) > 2r$. Let $B(r, \tilde{g})$ be the metric ball of radius r centered at $\tilde{g}$. Then, for any $g \in \mathcal{A}^\ell$, $B(r, g) \cap B(r, \tilde{g}) = \emptyset$. Applying Lemma 2.4 we see that $H_t(g^{-1}y) < \frac{1}{3\mathrm{vol}G}$ for all $g \in \mathcal{A}^\ell$ and all $y \in B(r, \tilde{g})$. Therefore,

$$\frac{1}{(2k)^\ell} \sum_{g \in \mathcal{A}^\ell} H_t \circ T_g(y) < \frac{1}{3\mathrm{vol}G}$$

for all all $y \in B(r, \tilde{g})$. This implies that

$$\left\| \frac{1_G}{\mathrm{vol}G} - \frac{1}{(2k)^\ell} \sum_{g \in \mathcal{A}^\ell} H_t \circ T_g \right\|_{\mathcal{L}^2} > \sqrt{\mathrm{vol}(B(0,r))} \left(\frac{2}{3\mathrm{vol}(G)} \right) \tag{3.11}$$

$$> \sqrt{\mathrm{vol}(B_n) r^n} \left(\frac{1}{2\mathrm{vol}(G)} \right), \tag{3.12}$$

which is a contradiction. □

Theorem 3.4. *Suppose* $\epsilon \sqrt{5 \ln \frac{C_G}{\epsilon^n}} = r$. *Choose*

$$k \geq C_G + (16 \ln 2)((1 + o(1))n \ln \frac{1}{\epsilon} + \ln \frac{1}{\delta})$$

i.i.d random points $\{g_1, \dots, g_k\}$ *from the Haar measure on* G *and let*

$$\mathcal{A} = \{g_1, g_1^{-1}, \dots, g_k, g_k^{-1}\}.$$

Let X *be the set of all elements of* G *which can be expressed as words of length less or equal to* ℓ *with alphabets in* $\mathcal{A}$, *where* $\ell \geq C_G + \frac{n}{2} \log_2(\frac{1}{\epsilon r})$. *Then, with probability at least* $1 - \delta$, *for every element* $g \in G$ *there is* $x \in X$ *such that* $d(g, x) < 2r$.

Proof. Let $\eta = 2^{-C_G} \epsilon^{(1+o(1))n}$ in Lemma 2.9. We set $\log_2 M = C_G + \log_2 \frac{1}{t^{1+o(1)}}$, by enforcing an equality in (2.25). Taking logarithms on both sides of (3.8), we see that

$$-\ln \frac{1}{\delta} = C_G + \frac{n}{2} \ln t^{-(1+o(1))} - \frac{k}{16 \ln 2}.$$

This fixes the lower bound for k in the statement of the corollary. In order to use (3.9) in conjunction with Lemma 3.3, we see that it suffices to set $2^{-\ell} t^{-\frac{n}{4}}$ to a value less than $r^{n/2}$, because for small ϵ, the value of η that we have chosen is significantly smaller than $r^{n/2}$. This shows that the theorem holds for any ℓ greater or equal to $\frac{n}{2} \log_2 \frac{1}{\epsilon r} + C_G$. □

Acknowledgements

We are grateful to Charles Fefferman, Anish Ghosh, Sergei Ivanov and Matti Lassas for helpful discussions. We thank Emmanuel Breuillard for a useful correspondence. We are grateful to Somnath Chakraborty for a careful reading. This work was supported by NSF grant #1620102 and a Ramanujan fellowship.

References

[1] R. Ahlswede and A. Winter. "Strong Converse for Identification via Quantum Channels". *IEEE Trans. Inf. Theor.* **48**.3 (Sept. 2006), pp. 569–579. Link.

[2] J. Bourgain and A. Gamburd. "On the spectral gap for finitely-generated subgroups of SU(2)". *Inventiones mathematicae* **171** (2007), pp. 83–121.

[3] J. Bourgain and A. Gamburd. "A spectral gap theorem in SU(d)". *Journal of the European Mathematical Society* **014**.5 (2012), pp. 1455–1511. Link.

[4] H. Donnelly. "Eigenfunctions of the Laplacian on Compact Riemannian Manifolds". *Asian J. Math.* **10**.1 (Mar. 2006), pp. 115–126. Link.

[5] J. Duistermaat and V. Guillemin. "The Spectrum of Positive Elliptic Operators and Periodic Bicharacteristics." *Inventiones mathematicae* **29** (1975), pp. 39–80. Link.

[6] A. Grigoryan. "Heat Kernel and Analysis on Manifolds". 2012.

[7] L. Hörmander. "The spectral function of an elliptic operator". *Acta Math.* **121** (1968), pp. 193–218. Link.

[8] A. Lubotzky, R. Phillips, and P. Sarnak. "Hecke operators and distributing points on S2. II". *Communications on Pure and Applied Mathematics* **40**.4 (1987), pp. 401–420. Link.

[9] S. Minakshisundaram. "Eigenfunctions on Riemannian Manifolds". *The Journal of the Indian Mathematical Society* **17**.4 (1953), pp. 159–165. Link.

[10] S. Minakshisundaram and A. Pleijel. "Some Properties of the Eigenfunctions of The Laplace-Operator on Riemannian Manifolds". *Canadian Journal of Mathematics* **1**.3 (1949), pp. 242–256. Link.