ON THE DISTRIBUTION OF RANDOM WORDS IN A COMPACT LIE GROUP

HARIHARAN NARAYANAN

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

The overall strategy employed here is similar to that of Landau and Russell in [11], which reproves with better constants, the result of Alon and Roichman [2] that random Cayley graphs are expanders. However, in our context of compact Lie groups, the analysis requires additional ingredients, due to the fact that $L^2(G)$ is infinite dimensional. We deal with this difficulty by restricting our attention to certain finite dimensional subspaces of $L^2(G)$. These subspaces are defined as the

1. Introduction

Let $G$ be a compact $n$-dimensional Lie group endowed with a left-invariant Riemannian metric $d$. 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 $g_1, \ldots, g_k$ are chosen independently from the Haar measure on $G$. Let $A = \cup_{i \in [k]} A_i$, where, $A_i := \{g_i\} \cup \{g_i^{-1}\}$. Let the Heat kernel at $x$ corresponding to Brownian motion on $G$ with respect to the metric $d$ started at the origin $o \in G$ for time $t$ be $H_t(x)$. Let $\mu_\ell^A$ be the uniform measure over all words of length $\ell$ whose alphabets belong to $A$. Our first result, Theorem 9 relates to equidistribution and gives a lower bound on the probability that $\|\mu_\ell^A * H_t - \frac{1}{\text{vol}(G)}\|_{L^2(G)}$ is less than a specified quantity $2\eta$. Our second result, Theorem 11 provides conditions under which the set of all elements of $G$ which can be expressed as words of length less or equal to $\ell$ with alphabets in $A$, form a $2r$-net of $G$ with probability at least $1 - \delta$. For constant $\delta$, both $k$ and $\ell$ can be chosen to be less than $C n \log(1/r)$, where $C$ is a universal constant. Lastly, by analysing the situation when $G$ is an $n$-dimensional torus, we show in Section 4 that the conditions stated in Theorem 11 are nearly optimal.

The question of a spectral gap of a natural Markov operator associated with $A$ when $G$ is $SU_2$ was reiterated by Bourgain and Gamburd in [3], being first raised by Lubotzky, Phillips and Sarnak [12] 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.

Theorem 9 relates to equidistribution and gives a lower bound on the probability that $\|\mu_\ell^A * H_t - \frac{1}{\text{vol}(G)}\|_{L^2(G)}$ is less than a specified quantity $2\eta$. Our second result, Theorem 11 provides conditions under which the set of all elements of $G$ which can be expressed as words of length less or equal to $\ell$ with alphabets in $A$, form a $2r$-net of $G$ with probability at least $1 - \delta$. For constant $\delta$, both $k$ and $\ell$ can be chosen to be less than $C n \log(1/r)$, where $C$ is a universal constant. Lastly, by analysing the situation when $G$ is an $n$-dimensional torus, we show in Section 4 that the conditions stated in Theorem 11 are nearly optimal.

The question of a spectral gap of a natural Markov operator associated with $A$ when $G$ is $SU_2$ was reiterated by Bourgain and Gamburd in [3], being first raised by Lubotzky, Phillips and Sarnak [12] 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.
spans of eigenfunctions of the Laplacian corresponding to eigenvalues that are less than certain finite values.

By a result of Dolgopyat [6], we know that if we pick two independent random elements from the Haar measure of a compact connected Lie group $G$, then the subgroup generated by these elements and their inverses is dense in $G$ almost surely. Unfortunately, the rate at which the random point set corresponding to words of a fixed length approaches $G$ in Hausdorff distance, as guaranteed by [6] is far from the rate that one would obtain if the corresponding Markov operator had a spectral gap for its action on $L^2(G)$. For this reason, the results of this paper do not follow. For the case $G = SU_n$, Bourgain and Gamburd proved [4] 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 [4]. 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 [3], being first raised by Lubotzky, Phillips and Sarnak [12] 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.

2. Analysis on a compact Lie group

We note that by known results (see for example Gray [9]),

$$\lim_{r \to 0} \frac{\text{vol}(B(r, o))}{r^n} = \text{vol}(B_n),$$

where $B(r, o)$ is the metric ball of radius $r$ around the origin.

Suppose $F_1, F_2, \ldots$ are eigenspaces of the Laplacian on $G$ corresponding to eigenvalues $0 = \lambda_0 < \lambda_1 < \lambda_2 < \ldots$. Let $f_i, f_i^1, f_i^2, \ldots$ be an orthonormal basis for $F_i$, for each $i \in \mathbb{N}$. $G$ acts on functions in $L^2(G)$ 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 metric $d$ 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 $t$.

We will use the following theorem of Cheng, Li and Yau [5].

**Theorem 1.** The fundamental solutions $H(x, y, t)$ of the heat equation decay in the following fashion. For any constant $C > 4$, there exists $C_1$ depending on $C, T$, the bound on the curvature of the Riemannian manifold $M$ and $x$ so that for all $t \in [0, T]

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

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

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

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

\[ H(x, y, t) < C \eta. \]

**Proof.** In Theorem 1, we may set \( C = 5 \) and \( T = 1 \) and ignore the dependence in \( x \) since the metric is left invariant. For all \( t \leq \epsilon^2 \) and all \( y \) such that \( d(x, y) > r \),

\[ H(x, y, t) < C_1 \epsilon^{-\eta} (\exp(-\ln \frac{1}{\eta \epsilon})) \]

(2.2)

\[ < C_1 \eta. \] (2.3)

\[ \square \]

By Weyl’s law for the eigenvalues of the Laplacian on a Riemannian manifold as proven by Duistermaat and Guillemin [8], we have the following.

**Theorem 3.**

\[ \lim_{\lambda \to \infty} \frac{\lambda^{n/2}}{\sum_{\lambda_i \leq \lambda} \dim F_i} = \frac{\text{vol}(\mathcal{B}_n) \text{vol}(G)}{(2\pi)^n} =: C_2, \]

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 5 below.

**Corollary 4.**

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

where \( C_3 \) is a finite constant depending only on the Lie group and its metric.

The following theorem is due to Donnelly (Theorem 1.2, [7]).

**Theorem 5.** Let \( M \) be a compact \( n \)-dimensional Riemannian manifold and \( \Delta \) its Laplacian acting on functions. Suppose that the injectivity radius of \( M \) 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 \( \| \phi \|_\infty \leq c_2 \lambda^{\frac{n-1}{2}} \| \phi \|_2 \). The constant \( c_2 \) depends only upon \( c_4, c_5 \), and the dimension \( n \) of \( M \). 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 \( M \).

Hörmander [10] 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 \( a_{ij} = e^{-\lambda_i t} f_{ij}(0) \leq e^{-\lambda_i t} (c_2 \lambda_i^{\frac{n-1}{2}}) \), 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 6. For any $M > 0$,
\[ \|\tilde{H}_{t,M}\|_{L^2} < C_G t^{-n/4} \]

Proof. We note that
\[ \|\tilde{H}_{t,M}\|_{L^2} \leq \|H_t\|_{L^2}, \]
because $\tilde{H}_{t,M}$ is the image of $H_t$ under a projection (with respect to $L^2$) onto a subspace spanned by the eigenfunctions of the Laplacian corresponding to eigenvalues in the range $(0, M]$. Thus it suffices to bound $\|H_t\|_{L^2}$ from above in the appropriate manner. Choosing $\eta = 1$ in Lemma 2, 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 $\mu_n$ denote the Lebesgue measure on $\mathbb{R}^n$ and $\mu$ 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 $\epsilon$ 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
\[ \sqrt{\det g_{ij}(\exp_x(\alpha v))} = 1 - \frac{1}{6} Ric^g(v, v)\alpha^2 + o(\alpha^2), \]
where $Ric$ denotes the Ricci tensor, and $\exp_x$, the exponential map at $x$.
Thus,
\[ \int_{B(o, r)} H_t(y)^2 \mu(dy) \leq C_G \left( \int_{\mathbb{R}^n} e^{-n(\exp(-|y|^2/5t))}\mu_n(dy) \right) \]
\[ \leq C_G \left( \int_{\mathbb{R}^n} e^{-1(\exp(-|y|^2/5t))}\mu_1(dy) \right)^n \]
\[ \leq C_G \epsilon^{-n}. \]
Therefore
\[ \|H_t\|_{L^2} \leq C_G \epsilon^{-n/2}. \]

Lemma 7. For $M = 2^{2k_0} \sqrt{\frac{n}{t}}$ where
\[ k_0 \geq \max \left( \log_2 \frac{1}{\eta}, C_G + (1 + o(1)) \frac{n}{2} \log_2 \frac{1}{t} \right), \]
\[ \|H_t - H_{t,M}\|_{L^2} \leq \eta. \]
Proof. It follows by the $L^2$—convergence of Fourier series that
\[ \|H_t - H_{t,M}\|_{L^2} \leq \sum_{\lambda_i \geq M} \dim(F_i) e^{-\lambda_i t} (c_2 \lambda_i^{n-1}). \]
By Weyl’s law (Theorem 3),
\[ \lim_{\lambda \to \infty} \frac{\lambda^{n/2}}{\sum_{\lambda < \lambda_i \leq 2^{2\lambda}} \dim F_i} = \frac{\text{vol}(B_n)\text{vol}(G)}{(2\pi)^n} =: C_2^{-1}. \]
Let, for \(k \in \mathbb{N}\),
\[
I_k = \left(2^{\frac{2k}{t}}, 2^\frac{2k+2}{t}\right).
\]

Now, for \(k_0 > C_G\),
\[
\sum_{\lambda_i > 2^{2k_0}} \dim(F_i)e^{-\lambda_i t}(c_2 \lambda_i^{\frac{n-1}{2}}) \leq \sum_{k \geq k_0} \left(\sum_{\lambda_i \in I_k} \dim(F_i)\right) \sup_{\lambda_i \in I_k} \left(\frac{c_2 \lambda_i^{\frac{n-1}{2}}}{e^{\lambda_i t}}\right)
\]
\[
\leq C_2 \sum_{k \geq k_0} 2^{k+1} \sup_{\lambda_i \in I_k} \left(\frac{c_2 \lambda_i^{\frac{n-1}{2}}}{e^{\lambda_i t}}\right).
\]
We see that
\[
\sup_{\lambda_i \in I_k} \left(\frac{\lambda_i^{\frac{n-1}{2}}}{e^{\lambda_i t}}\right) \leq \frac{2^{(k+1)} \exp(2^\frac{2k}{t})}{\exp(2^\frac{2k}{t})}
\]
\[
\leq \exp(\frac{(k+1)}{2} - 2^\frac{2k}{t}).
\]
When
\[
k \geq \left(\frac{n}{2}\right) \log_2 \frac{6k}{t},
\]
assuming \(k > 5\), we have
\[
\frac{k}{n/2t} \geq \log_2 \frac{\frac{k}{n/2t}(k+1)}{t},
\]
and then, we see that
\[
\exp(\frac{(k+1)}{2} - 2^\frac{2k}{t}) < 2^{-(k+1)}.
\]
In order to enforce (2.15), it suffices to have
\[
\frac{k}{\log_2 n^2} \geq \frac{n}{2},
\]
which is implied by
\[
\frac{6k}{t \log_2 \frac{n^2}{t}} \log_2 \left(\frac{6k}{t \log_2 \frac{n^2}{t}}\right) \geq 3n \log_2 \left(\frac{3n}{t}\right).
\]
This is equivalent to
\[
k \left(1 - \frac{\log_2 \log_2 \frac{6k}{t}}{\log_2 \frac{6k}{t}}\right) \geq \frac{n}{2} \log_2 \left(\frac{3n}{t}\right),
\]
which is in turn implied by
\[
k \geq \frac{n}{2} \left(\log_2 \frac{3n}{t}\right) \left(1 - \frac{\log_2 \log_2 \frac{3n}{t}}{\log_2 \frac{3n}{t}}\right)^{-1}
\]
\[
= (1 + o(1)) \frac{n}{2} \log_2 \frac{3n}{t}.
\]
Therefore, for any
\[
k_0 > C_G + (1 + o(1)) \frac{n}{2} \log_2 \frac{3n}{t}.
\]
\[
\sum_{\lambda_i > 2^{-k_0}} \dim(F_i) e^{-\lambda_i t} (c_2 \lambda_i^{n-1}) < 2^k \frac{(1 - 1/2)}{2^{(-k_0)}} < 2^{(-k_0)}.
\]

It follows from (2.8) that for any \( \eta \), by choosing
\[
k_0 = \max \left( \log_2 \frac{1}{\eta}, C_G + (1 + o(1)) n \log_2 \frac{1}{\epsilon} \right),
\]
and
\[
M \geq 2^{2k_0/n}
\]
we have that
\[
\| \tilde{H}_{t,M} - H_t \|_{L^2} < \eta.
\]

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
\[
\Lambda(V) = \{ B \in A(V) \mid \forall v, (Av, v) \geq 0 \}
\]
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 8.** Let \( V \) be a Hilbert Space of dimension \( D \) and let \( A_1, \ldots, A_k \) 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 \( \epsilon \in [0, 1/2] \),
\[
P \left[ \frac{1}{k} \sum_{i=1}^{k} A_i \notin [(1 - \epsilon)A, (1 + \epsilon)A] \right] \leq 2D \exp \left( -\frac{\epsilon^2 \mu k}{2 \ln 2} \right).
\]

For any \( g \in G \)
\[
(Id - T_g) \tilde{H}_{t,M}
\]
lies in
\[
\tilde{F}_M := \bigoplus_{0 < \lambda_i \leq M} F_i.
\]

\( \tilde{F}_M \) has, by Weyl’s law, a dimension that is bounded above by \( O(M^{n/2}) \). We will study the Markov operator \( P : \tilde{F}_M \rightarrow \tilde{F}_M \) given by
\[
P(f)(x) := \frac{\sum_{g \in A} (f(x) + f(gx))}{2|A|}.
\]

We know that \( A = \cup_i A_i \), where, \( A_i = \{g_i\} \cup \{g_i^{-1}\} \). Note that \( P \) is the sum of \( k \) i.i.d operators
\[
P_i := \frac{\sum_{g \in A_i} (f(x) + f(gx))}{4}.
\]
We see that \( \forall f \in \tilde{F}_M \), and \( 1 \leq i \leq k \),
\begin{equation}
\mathbb{E}P_i(f) = (1/2)f,
\end{equation}
which is equivalent to
\begin{equation}
\mathbb{E}P_i = (1/2)I.
\end{equation}

By Theorem 8 for all \( \varepsilon \in [0, 1/2] \),
\begin{equation}
\mathbb{P} \left[ \frac{1}{k} \sum_{i=1}^{k} P_i \notin \left(\left(1 - \varepsilon/2\right)I, \left(1 + \varepsilon/2\right)I\right) \right] \leq C_G M^{n/2} \exp \left(\frac{-\varepsilon^2 k}{4 \ln 2}\right).
\end{equation}
Setting \( \varepsilon = 1/2 \) and substituting for \( M \), we see that
\begin{equation}
\mathbb{P} \left[ \frac{1}{k} \sum_{i=1}^{k} P_i \notin \left(\left(1/4\right)I, \left(3/4\right)I\right) \right] \leq \left( C_G M^{n/2} \right) \exp \left(\frac{-k}{16 \ln 2}\right).
\end{equation}
Let the map \( x \mapsto gx \) be denoted by \( T_g \). It follows that
\begin{equation}
\mathbb{P} \left[ \forall f \in \tilde{F}_M, \left\| \frac{1}{2k} \sum_{g \in A} f \circ T_g \right\|_{L^2} \leq (1/2)\|f\|_{L^2} \right] \geq 1 - \left( C_G M^{n/2} \right) \exp \left(\frac{-k}{16 \ln 2}\right).
\end{equation}
Iterating the above inequality \( \ell \) times, we observe that
\begin{equation}
\mathbb{P} \left[ \forall f \in \tilde{F}_M, \left\| \frac{1}{2k} \sum_{g \in A} f \circ T_g \right\|_{L^2} \leq (1/2)^\ell \|f\|_{L^2} \right] \geq 1 - \delta,
\end{equation}
where
\begin{equation}
\delta := \left( C_G M^{n/2} \right) \exp \left(\frac{-k}{16 \ln 2}\right).
\end{equation}
Choosing \( f = \tilde{H}_{t,M} \), we see that
\begin{equation}
\mathbb{P} \left[ \left\| \frac{1}{2k} \sum_{g \in A^\ell} \tilde{H}_{t,M} \circ T_g \right\|_{L^2} \leq (1/2)^\ell \|\tilde{H}_{t,M}\|_{L^2} \right] \geq 1 - \delta.
\end{equation}
By the above, and Lemmas \( \S \) and \( \S \) we see that
\begin{equation}
\mathbb{P} \left[ \left\| \frac{1}{2k} \sum_{g \in A^\ell} H_t \circ T_g \right\|_{L^2} \leq \eta + 2^{-\ell} t^{-n/4} \right] \geq 1 - \delta.
\end{equation}
Thus, we see that
\begin{equation}
\mathbb{P} \left[ \left\| \frac{1}{\text{vol}G} - \frac{1}{2k} \sum_{g \in A^\ell} H_t \circ T_g \right\|_{L^2} \leq \eta + 2^{-\ell} t^{-n/4} \right] \geq 1 - \delta.
\end{equation}
We derive from this, the following theorem on the equidistribution of \( A^\ell \).
Theorem 9. Let $2^{-\ell} t^{-\frac{d}{4}} \leq \eta \leq 2^{-C_G t^{\frac{1+o(1)n}{2}}}$. Let $\delta = (C_G / \eta) \exp (-\frac{k}{16 \ln 2})$. Then,

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

Proof. This follows from (3.9) on setting $M = \eta^{-\frac{d}{4}}$ and substituting in (3.8). □

Lemma 10. Suppose $\epsilon \sqrt{5 \ln \frac{C_G}{\epsilon}} = r$, and $t = \epsilon^2$ are sufficiently small. If

$$\left(3.12\right) \quad \left\| \frac{1}{\text{vol} G} - \frac{1}{(2k)^\ell} \sum_{g \in A^\ell} H_t \circ T_g \right\|_{L^2} \leq \sqrt{\text{vol}(B_n)^{r^m}} \left( \frac{1}{2\text{vol}(G)} \right),$$

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

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

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

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

$$\left(3.11\right) \quad \left\| \frac{1}{\text{vol} G} - \frac{1}{(2k)^\ell} \sum_{g \in A^\ell} H_t \circ T_g \right\|_{L^2} > \sqrt{\text{vol}(B_0, r)^{r^m}} \left( \frac{2}{3\text{vol}(G)} \right),$$

$$\left(3.12\right) \quad > \sqrt{\text{vol}(B_n)^{r^m}} \left( \frac{1}{2\text{vol}(G)} \right),$$

which is a contradiction. □

Theorem 11. Suppose $\epsilon \sqrt{5 \ln \frac{C_G}{\epsilon}} = r$. 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 $\{g_1, \ldots, g_k\}$ from the Haar measure on $G$ and let

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

Let $X$ be the set of all elements of $G$ which can be expressed as words of length less or equal to $\ell$ with alphabets in $A$, where $\ell \geq C_G + \frac{\delta}{\epsilon} \log_2 \left( \frac{1}{\epsilon} \right)$. 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 $\eta = 2^{-C_G t^{\frac{1+o(1)n}{2}}}$. We set $\log_2 M = C_G + \log_2 \frac{1}{\epsilon}$, by enforcing an equality in (2.23). 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 10 we see that it suffices to set $2^{-\ell} t^{-\frac{d}{4}}$ to a value less than $r^{n/2}$, because for small $\epsilon$, the value of $\eta$ that we have chosen is significantly
smaller than \( r^{n/2} \). This shows that the theorem holds for any \( \ell \) greater or equal to
\[ \frac{1}{2} \log_2 \frac{1}{r} + C_G. \]

\[ \square \]

4. LOWER BOUNDS ON THE NUMBER OF GENERATORS AND WORD LENGTH REQUIRED FOR A GIVEN HAUSDORFF DISTANCE

Let us take \( \epsilon > 0, \delta > 0 \) and denote \( 2^k + \ell =: m \). We are now interested in lower bounds on the values of \( k \) and \( \ell \) as a function on \( \epsilon, \delta \) and \( m \).

In this section, we consider only the case when \( G = \mathbb{R}^n / \mathbb{Z}^n \), the unit \( n \)-dimensional torus.

The number of distinct elements that the set of all words \( A^\ell \) of length \( \ell \) in \( k \) alphabets (and their inverses) correspond to in an abelian group is less or equal to \( (2^k + \ell - 1) \). Therefore, the measure covered by a \( 2r \)-neighborhood (in an \( \ell \nolimits_2 \) sense) of \( (2^k + \ell - 1) \) elements is less or equal to \( \left( \frac{m-1}{\ell} \right)^{2^n \text{vol}(B_n)} \), for \( r < 1/2 \). Since this has to be at least 1 for \( A^\ell \) to be a \( 2r \)-net of \( G \), we obtain

\[ (4.1) \quad \left( \frac{m-1}{\ell} \right)^{2^n \text{vol}(B_n)} \geq 1. \]

We will obtain a lower bound for \( k \) using the above inequality. It is clear that a lower bound that is twice as big must hold for \( \ell + 1 \) by the identity

\[ \left( \frac{2k + \ell - 1}{\ell} \right) = \left( \frac{2k + \ell - 1}{2k - 1} \right). \]

\[ (4.2) \quad \left( \frac{m-1}{\ell} \right)^{2^n \text{vol}(B_n)} \geq \frac{1}{r^n}, \]

therefore,

\[ (4.3) \quad \ln m^{2k} - \ln (2k - 1)! + \ln (2^n \text{vol}(B_n)) \geq n \ln \frac{1}{r}. \]

Therefore

\[ (4.4) \quad k \geq \frac{n \ln \frac{1}{r}}{2 \ln m}. \]

Let us place the further constraint that \( \ell \leq k \leq 2\ell \) as was the case in our upper bound for reasonably large values of \( \delta \). We then using Stirling’s approximation see that

\[ 2k \ln 3k - (2k - 2) \ln(2k) + 2k \geq n \ln \frac{1}{r} - \ln (2^n \text{vol}(B_n)). \]

This leads to

\[ 2 \ln 2k + 2k(1 + \ln(3/2)) \geq n \ln \frac{1}{r} - \ln (2^n \text{vol}(B_n)). \]

Therefore, for sufficiently large \( n \),

\[ k \geq (2 \ln(1+\ln(3/2)))^{-1} \left( n \ln \frac{1}{r} - \ln \left( \ln \frac{1}{r} \right) - \ln (2^n \text{vol}(B_n)) - \ln (- \ln (2^n \text{vol}(B_n))) \right). \]

This can be simplified to the following weaker inequality:

\[ (4.5) \quad k \geq (2 \ln(1+\ln(3/2)))^{-1} \left( n \ln \frac{1}{r} - \ln \left( \ln \frac{1}{r} \right) \right). \]
Therefore, we also have

\[
\ell + 1 \geq (\ln(1 + \ln(3/2)))^{-1} \left( n \ln \frac{1}{r} - \ln \left( \ln \frac{1}{r} \right) \right).
\]

(4.6)

5. 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 and directing us to [6]. We are grateful to Somnath Chakraborty for a careful reading and numerous corrections. This work was supported by NSF grant #1620102 and a Ramanujan fellowship.

REFERENCES

1. Rudolf Ahlswede and Andreas Winter, “Strong converse for identification via quantum channels,” IEEE Transactions on Information Theory, 48(3):569–579, 2002.
2. Noga Alon and Yuval Roichman. Random Cayley graphs and expanders. Random Structures and Algorithms, 5:271–284, 1994.
3. Bourgain, J. and Gamburd, A. “On the spectral gap for finitely-generated subgroups of SU(2),” Invent. math. (2008) 171: 83. https://doi.org/10.1007/s00222-007-0072-z
4. Bourgain, Jean, and Gamburd, Alex. “A spectral gap theorem in SU(d).” Journal of the European Mathematical Society 014.5 (2012): 1455-1511. [http://eudml.org/doc/277218].
5. Cheng, S., Li, P., and Yau, S. (1981). On the Upper Estimate of the Heat Kernel of a Complete Riemannian Manifold. American Journal of Mathematics, 103(5), 1021-1063. doi:10.2307/2374257
6. Dolgopyat, D., “On mixing properties of compact group extensions of hyperbolic systems”, Israel J. Math. (2002) 130: 157. https://doi.org/10.1007/BF02764076
7. Donnelly, Harold. “Eigenfunctions of the Laplacian on Compact Riemannian Manifolds.” Asian J. Math. 10 (2006), no. 1, 115–126. https://projecteuclid.org/euclid.ajm/1154098927
8. Duistermaat, J.J., and Guillemin, V.W. "The Spectrum of Positive Elliptic Operators and Periodic Bicharacteristics." Inventiones mathematicae 29 (1975): 39-80. [http://eudml.org/doc/142329]
9. Gray, Alfred. “The volume of a small geodesic ball of a Riemannian manifold.” Michigan Math. J. 20 (1974), no. 4, 329–344. doi:10.1307/mmj/1029001150. https://projecteuclid.org/euclid.mmj/1029001150
10. Hörmander, Lars, The spectral function of an elliptic operator, Acta Math., 121 (1968), pp. 193–218.
11. Landau, Zeff and Russell, Alexander “Random cayley graph expanders: A simple proof of the Alon-Roichman Theorem,” Electronic Journal of Combinatorics, Volume 11, Issue 1 (2004)
12. Lubotzky, A., Phillips, R., Sarnak, P.: Hecke operators and distributing points on $S^2$. II. Commun. Pure Appl. Math. 40(4), 401–420 (1987)

School of Technology and Computer Science, Tata Institute of Fundamental Research, Mumbai
E-mail address: hariharan.narayanan@tifr.res.in