

# GENERATING AN EQUIDISTRIBUTED NET ON A UNIT $n$ -SPHERE USING RANDOM ROTATIONS

SOMNATH CHAKRABORTY AND HARIHARAN NARAYANAN

ABSTRACT. We develop a randomized algorithm (that succeeds with high probability) for generating an  $\epsilon$ -net in a sphere of dimension  $n$ . The basic scheme is to pick  $O(n \ln(1/\epsilon) + \ln(1/\delta))$  random rotations and take all possible words of length  $O(n \ln(1/\epsilon))$  in the same alphabet and act them on a fixed point. We show this set of points is equidistributed at a scale of  $\epsilon$ . Our main application is to approximate integration of Lipschitz functions over an  $n$ -sphere.

## 1. INTRODUCTION

In the present article, we develop a randomized algorithm (with high success probability) for the generation of an  $\epsilon$ -net in an unit sphere of dimension  $n$ . The basic scheme is to pick  $k := O(n \ln(1/\epsilon) + \ln(1/\delta))$  random rotations and take all possible words on length  $l := O(n \ln(1/\epsilon))$  in the same alphabet and act them on a fixed point. We show this set of points is equidistributed at a scale of  $\epsilon$ . The group  $SU(2)$  can be identified with the three dimensional sphere  $S^3$ , thus we obtain a scheme for producing an  $\epsilon$ -net of  $SU(2)$ , a task which is relevant to quantum computing in the context of the Solovay-Kitaev algorithm (although we do not address the issue of generating a sequence of elementary gates to efficiently approximate any given gate, in a non-exhaustive fashion). Our main application is to integration of Lipschitz functions over an  $n$ -sphere. The net we produce, is  $\epsilon$ -close in Hausdorff distance to the  $n$ -sphere, and is also equidistributed in the following sense (with high probability): The uniform counting measure  $\mu_{\text{net}}$  over the net is close to the uniform measure on the  $n$ -sphere  $\mu_{\text{haar}}$  in 1-Wasserstein distance. This implies that the integral of every 1-Lipschitz function on  $S^n$  with respect to  $\mu_{\text{net}}$  is  $\epsilon$ -close to its integral with respect to  $\mu_{\text{haar}}$ .

In [2], Alon and Roichman proved that, *given any  $\delta > 0$ , there exists a  $c(\delta) > 0$  such that for any finite group  $G$ , and a random subset  $S \subset G$  of order at least  $c(\delta) \log |G|$ , the induced Cayley graph  $\chi(G, S)$  has small normalized second largest eigenvalue (in absolute value):*

$$(1.1) \quad \mathbb{E} [|\lambda_2^*(\chi(G, S))|] < \delta.$$

Considering random walk on expander multigraphs, it follows that every element  $g \in G$  is an  $S$ -word of length at most  $\log |G|$ . For an irreducible representation  $\rho \in \hat{G}$ , let  $d_\rho$  be its dimension; let  $R$  be the regular representation of  $G$ , and

---

*Date:* December 12, 2018.  
*2000 Mathematics Subject Classification.* Primary 22D40.

$D = \sum_{\rho \in \hat{G}} d_\rho$ . In [13], Russel and Landau proved that (1.1) holds for all random subsets  $S \subset G$  of order at least

$$\left(\frac{2 \ln 2}{\epsilon} + o(1)\right)^2 \log |D|$$

This was obtained via an application of *tail bounds for operator-valued random variables*, as in Ahlswede and Winter [1], building upon the following observation: *the normalized adjacency matrix of  $\chi(G, S)$  is the operator*

$$(2|S|)^{-1} \sum_{s \in S} (R(s) + R(s^{-1})),$$

*presented in terms of the standard basis of  $\mathbb{C}[G]$ .*

Now let  $G$  be a compact Lie group, and  $\mu$  a left-invariant Borel probability measure on  $G$ . One considers the averaging operator  $z_\mu : L^2(G) \rightarrow L^2(G)$ , given by

$$z_\mu(f)(x) = \int_G f(xg) d\mu(g)$$

In [5], Bourgain and Gamburd established that if  $G = SU(d)$  then  $z_\mu$  has spectral radius  $< 1$  when  $\text{supp}(\mu)$  is finite algebraic subset generating a nonabelian free subgroup of  $G$ . This has since been extended to all compact connected simple Lie groups by Benoist and de Saxcé in [3], where it was shown that  $z_\mu$  has a spectral gap if and only if  $\mu$  is *almost diophantine*. A corollary to the main result in [3] is the following: if  $\mu$  is finitely-supported almost diophantine then the set of words in  $\text{supp}(\mu)$  of fixed length approaches  $G$  in Hausdorff distance.

In [15], a quantitative version of the spectral gap question was considered. It was shown that the Hausdorff distance between  $G$ , a compact connected Lie group, and the subset of fixed length words on a random essentially small finite alphabet  $S \subset G$  decays exponentially in the length of the words, with high probability. This was done via an analysis of the heat kernel with respect to a suitable finite dimensional subspace of  $L^2(G)$  and an application of *tail bounds for operator-valued random variables*. We note that the results of the present article are not implied by the results of [15], because the dimension of the Lie group  $SO_n$  is  $n(n+1)/2$ , and so the bounds from [15] for the length of the words and the number of generators, that apply for general compact Lie groups would be quadratic in  $n$  rather than linear in  $n$ . In the special case of the unitary group  $U_n$ , such a result with a quadratic dependence on dimension for the length of the words  $n$  was previously obtained by Hastings and Harrow in Theorem 5 of [10], however in their result the number of generators is specified in an indirect manner, whose dependence on  $n$  is not obvious. On the other hand, the bounds obtained in the present work are linear in  $n$ , both for the number of generators and the length of the words. In fact, for these parameters, the value of  $(2k)^l$  is close to the volumetric lower bound of  $(1/\epsilon)^{\Omega(n)}$  on the size of an  $\epsilon$ -net of  $S^n$ .

The two main results of this paper are stated below. The numberings correspond to their appearances in Sections 3 and 4 respectively. In the following statements,  $C_n$  denotes a certain positive constant depending on  $n$ . For a finite set  $S$ , the  $l$ -fold product  $S^l$  consists of all  $S$ -words of length  $l$  inside the free group generated by  $S$ .

**Theorem 3.15:**

Let  $\epsilon \in (0, \frac{1}{3n})$  and  $\delta \in (0, 1)$ ; let  $r = 2\epsilon \sqrt{\ln \frac{3C_n}{\epsilon^{2n-1}}}$ . Let  $S \subset SO_{n+1}$  consist of  $k$  iid random points, drawn from the Haar measure on  $SO_{n+1}$ , where

$$k \geq 8 \ln 2 \left( (n+4) + 2 \ln \left( \frac{1}{\delta} \right) + 6n(1+a_n) \ln \left( \frac{1}{\epsilon} \right) - \ln(n!) \right),$$

and  $a_n := \frac{2 \log_2 \log_2(5n)}{\log_2(5n)}$ . Let  $\hat{S} := S \sqcup S^{-1}$  be the (multi)set of all elements in  $S$  and their inverses. Let  $l = \frac{n}{2} \log_2 \left( \frac{1}{r\epsilon} \right) + (4 + 3a_n)n \log_2 \left( \frac{1}{\epsilon} \right)$ ; if  $r$  is sufficiently small then the probability that  $x_0 \hat{S}^l \subseteq S^n$  is an  $r$ -net in  $S^n$  is at least  $1 - \delta$ .  $\square$

**Theorem 4.14:**

For  $n > 1$ , let  $\sigma$  be the probability measure on  $S^n$  corresponding to Haar probability measure on the group of rotations  $SO_{n+1}$ . Let  $\epsilon, \delta > 0$  be sufficiently small and  $r = 2\epsilon \sqrt{\ln \frac{3C_n}{\epsilon^{2n-1}}}$ . Let  $S \subseteq SO_{n+1}$  be a random subset such that  $|S| = k$  satisfies

$$k \geq 8 \ln 2 \left( (n+4) + 2 \ln \left( \frac{1}{\delta} \right) + 6n(1+a_n) \ln \left( \frac{1}{\epsilon} \right) - \ln(n!) \right),$$

where  $a_n := \frac{2 \log_2 \log_2(5n)}{\log_2(5n)}$ . Let  $\hat{S} := S \sqcup S^{-1}$  be the (multi)set of all elements in  $S$  and their inverses. Let  $x_0 \in S^n$  and let  $\nu$  be the probability measure on  $S^n$ , uniformly supported on  $\hat{S}^l x_0$ , where

$$l = \frac{n}{2} \log_2 \left( \frac{1}{r\epsilon} \right) + (4 + 3a_n) \log_2 \left( \frac{1}{\epsilon} \right).$$

If  $r$  is sufficiently small, then the following inequality holds with probability at least  $1 - \delta$ :

$$W_1(\sigma, \nu) \leq \epsilon,$$

Here  $W_1$  is used to denote the 1-Wasserstein distance between two measures supported on  $S^n$ .  $\square$

For the remainder of this section, we assume given a real number model of computation, in which only standard algebraic operations are allowed on Gaussian random vectors, but bits are not manipulated. Thus, for  $k$  and  $l$  as described in Theorem 4.14, choose a set  $S$  consisting of  $k$  orthogonal matrices, each chosen independently from the Haar measure of  $SO_{n+1}$ . Consider all  $(2k)^l$  words of length  $l$  in these generators and their inverses. Apply the resulting matrices to the vector  $\mathbf{e}_{n+1} = (0, 0, \dots, 0, 1)^T$ . Then these  $(2k)^l$  points form an equidistributed net, that can be used for integrating a 1-Lipschitz to within an additive error of  $\epsilon$ . If we assume an oracle that outputs independent  $n$ -dimensional Gaussian random vectors when queried, then the whole process requires only  $kn$  queries to this oracle. Note that the obvious procedure of producing an equidistributed net, would require  $\epsilon^{-\Omega(n)}$  calls to the Gaussian oracle (which would then be normalized to lie on the sphere). The latter method uses exponentially more randomness than our procedure using random rotations.

**Acknowledgments.** SC would like to thank Sandeep Juneja and Jaikumar Radhakrishnan for helpful conversations. HN was partially supported by a Ramanujan fellowship.

## 2. APPLICATION OF SPHERICAL HARMONICS

This section briefly reviews the basics of harmonic analysis on the unit  $n$ -sphere  $S^n \subset \mathbb{R}^{n+1}$ . The two lemmas in this section will be used in an essential manner in deriving the computations in this section.

Let  $\sigma$  denote the standard euclidean surface probability measure on  $S^n$ . For any Borel set  $B \subset S^n$ , if  $\hat{B} := \{\alpha x : x \in B, \alpha \in [0, 1]\}$  then

$$\sigma(B) = \frac{\lambda(\hat{B})}{\lambda(D)},$$

where  $\lambda$  is the standard Lebesgue measure on  $\mathbb{R}^{n+1}$  and  $D \subseteq \mathbb{R}^{n+1}$  is the unit disk centered at origin, so that  $S^n = \partial D$ . We recall that the Lebesgue measure of the unit  $n$ -sphere in  $\mathbb{R}^n$  is

$$\Omega_n := \lambda(S^n) = \frac{2\pi^{\frac{n+1}{2}}}{\Gamma\left(\frac{n+1}{2}\right)}.$$

Now, the fact that  $\sigma$  is  $SO_{n+1}$ -invariant follows from usual rotation invariance of Lebesgue measure on  $\mathbb{R}^{n+1}$ . Hence (by unimodularity of the compact Lie group  $SO_{n+1}$  of rotations of  $S^n$ ), the measure  $\sigma$  is the unique probability measure on  $S^n$  induced by the haar measure on  $SO_{n+1}$ . For  $n > 1$ , let  $\Delta := \Delta_{S^n}$  be the negative of the Laplace-Beltrami operator on  $S^n$ . Thus, given  $g \in C^2(S^n)$ , one has

$$-\Delta(g) = \Delta_{\mathbb{R}^n}(\tilde{g})|_{S^n}$$

where  $\tilde{g} : \mathbb{R}^{n+1} - \{0\} \rightarrow \mathbb{R}$  is defined by  $\tilde{g}(x) = g(|x|^{-1}x)$ . It is well-known that the Hilbert-product space  $L^2(S^n)$  decomposes into a direct sum of the eigenspaces of  $\Delta$ , in the sense that the  $L^2$ -closure of the direct sum is  $L^2(S^n)$ :

$$(2.1) \quad L^2(S^n) = \bigoplus_{k=0}^{\infty} H_k(S^n)$$

Recall that  $H_k(S^n)$  is the space of degree- $k$  homogeneous harmonic polynomials in  $n+1$  variables, restricted to  $S^n$ ; the dimension of  $H_k(S^n)$  is

$$(2.2) \quad h_k := \binom{n+k}{n} - \binom{n+k-2}{n}$$

and the corresponding eigenvalue is  $\lambda_k := k(n+k-1)$ . Note that, for any  $n, k > 0$ , one has

$$\begin{aligned} \sum_{a=0}^k \dim H_a(S^n) &= \sum_{a=0}^k \left( \binom{n+a}{a} - \binom{n+a-2}{a-2} \right) \\ &= \binom{n+k}{k} + \binom{n+k-1}{k-1} \\ &= \dim H_k(S^{n+1}) \end{aligned}$$

One has

$$\begin{aligned}
\lim_{k \rightarrow \infty} \frac{\sum_{k \leq a \leq k \sqrt[3]{2}} \dim H_a(S^n)}{k^n} &= 2 \lim_{k \rightarrow \infty} \frac{\sum_{0 \leq a \leq \lfloor k \sqrt[3]{2} \rfloor} \dim H_a}{2k^n} - \lim_{k \rightarrow \infty} \frac{\sum_{0 \leq a \leq k} \dim H_a}{k^n} \\
&= 2 \lim_{l \rightarrow \infty} \frac{\sum_{0 \leq a \leq l} \dim H_a}{l^n} - \lim_{k \rightarrow \infty} \frac{\sum_{0 \leq a \leq k} \dim H_a}{k^n} \\
&= \lim_{k \rightarrow \infty} \frac{\sum_{0 \leq a \leq k} \dim H_a}{k^n} \\
&= \lim_{k \rightarrow \infty} \frac{\dim H_k(S^{n+1})}{k^n} \\
&= \lim_{k \rightarrow \infty} k^{-n} \binom{n+k}{k} + \lim_{k \rightarrow \infty} k^{-n} \binom{n+k-1}{k-1} \\
&= \frac{2}{n!}
\end{aligned}$$

Moreover, notice that, when  $k > 2n + 1$ , one has

$$\begin{aligned}
\binom{n+k}{k}^2 &= \frac{1}{(n!)^2} \prod_{i=1}^n (k+i)(k+n-i+1) \\
\text{AM} \geq \text{GM} \Rightarrow &< \frac{1}{(n!)^2} \prod_{i=1}^n 2k^2 \\
&< \frac{2^n k^{2n}}{(n!)^2}
\end{aligned}$$

Equivalently, writing  $H_\lambda$  for the eigenspace corresponding to eigenvalue  $\lambda$ , one gets

$$\lim_{\lambda \rightarrow \infty} \frac{\sum_{\lambda \leq a \leq \lambda \sqrt[3]{4}} \dim H_a}{\lambda^{\frac{n}{2}}} = \frac{2}{n!}$$

and for all  $\lambda > 6n^2 + 3n$ , the inequality  $\lambda_{ak} < a^2 \lambda_k$  implies

$$(2.3) \quad \frac{\sum_{\lambda \leq a \leq \lambda \sqrt[3]{4}} \dim H_a}{\lambda^{\frac{n}{2}}} < \frac{2(2^{\frac{n}{2}})}{n!}$$

where, the sum ranges over all eigenvalues in  $[\lambda, \lambda \sqrt[3]{4}]$ . Fix a point  $x_0 \in S^n$ . Let  $H_t(x)$  be the heat kernel on  $S^n$ , corresponding to Brownian motion started at  $x_0$ . That is,  $H_t(x)$  is the fundamental solution to the problem

$$\begin{aligned}
\frac{\partial u}{\partial t} &= -\Delta_{S^n} u \\
\lim_{t \rightarrow 0^+} u(t, x) &= \delta_{x_0}(x)
\end{aligned}$$

where the convergence is taken to be in the weak\* topology. A Brownian motion on  $S^n$ , started at  $x_0 \in S^n$  has infinitesimal generator  $H_{\frac{t}{2}}(x)$ . Fixing orthonormal

basis  $\phi_{k,1}, \dots, \phi_{k,h_k}$  of  $H_k := H_{\lambda_k}$  for each  $k \geq 0$ , one has

$$\begin{aligned} H_t(x) &= \sum_{k=0}^{\infty} e^{-\lambda_k t} \sum_{i=1}^{h_k} \phi_{k,i}(x_0) \phi_{k,i}(x) \\ &= \sum_{k=0}^{\infty} e^{-\lambda_k t} h_k P_{k,n}(x \cdot x_0) \end{aligned}$$

where the last equality is due to *addition theorem* of spherical harmonics (see theorem 2.26 of [14]) that correspond to the usual addition formula for trigonometric functions when  $n = 1$ ; here  $P_{k,n}(t)$  denotes the Legendre polynomial of degree  $k$  and dimension  $n + 1$ ; in explicit terms, this polynomial is

$$(2.4) \quad P_{k,n}(t) = \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} C_{2j} t^{k-2j} (1-t^2)^j$$

where the coefficients are given by

$$C_0 = 1, \quad C_{2j} = (-1)^j \frac{k(k-1) \cdots (k-2j+1)}{(2 \cdot 4 \cdots 2j)(n(n+2) \cdots (n+2j-2))}$$

One has

$$\begin{aligned} \int_{S^n} H_t(x)^2 d\sigma(x) &= \sum_{k=0}^{\infty} e^{-2\lambda_k t} (h_k)^2 \int_{S^n} (P_{k,n}(x \cdot x_0))^2 d\sigma(x) \\ &= \sum_{k=0}^{\infty} e^{-2\lambda_k t} h_k \end{aligned}$$

where the last equation is a well-known properties of Legendre polynomials (see theorem 2.29 of [14]). We note that by theorem 2.29 of [14], one has

$$(2.5) \quad H(t, x, x) = \sum_{k=0}^{\infty} e^{-\lambda_k t} h_k$$

for all  $t > 0$ . It is known that  $H_t(x) > 0$  for all  $t > 0$ .

For  $M > 0$ , let  $H_{t,M}(x)$  be defined by

$$(2.6) \quad H_{t,M}(x) := \sum_{\lambda_k \leq M} e^{-\lambda_k t} \sum_{i=1}^{h_k} \phi_{k,i}(x_0) \phi_{k,i}(x)$$

**Lemma 2.7.** *Suppose that  $t \in (0, 6^{-1})$  and for any  $\eta > 0$ , let  $M \geq 4 \frac{k_0}{n}$  where*

$$(2.8) \quad k_0 > \max \left\{ \frac{1}{2} \sqrt{\log_2 \frac{1}{\eta}}, n \log_2 \left( \frac{n}{t} \right) + 2n \log_2 \log_2 \left( \frac{n}{t} \right) \right\};$$

*then the following inequality holds:*

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

*Proof.* When  $k > n \log_2(3n)$ , one has  $4 \frac{k}{n} > 6n^2 + 3n$ . For  $k \geq 0$ , write

$$I_k = \left( 4 \frac{k}{n}, 4 \frac{k+1}{n} \right]$$

For  $k_0 > n \log_2(3n)$ , one has

$$\begin{aligned} \sum_{\lambda \geq 4 \frac{k_0}{n}} e^{-2\lambda t} \dim H_\lambda &= \sum_{k \geq k_0} \sum_{\lambda \in I_k} e^{-2\lambda t} \dim H_\lambda \\ &\leq \sum_{k \geq k_0} (\sup_{\lambda \in I_k} e^{-2\lambda t}) (\sum_{\lambda \in I_k} \dim H_\lambda) \\ &\leq \frac{2(2^{\frac{n}{2}})}{n!} \sum_{k \geq k_0} 2^{1+k} e^{-(2^{\frac{2k+n}{n}})t} \end{aligned}$$

Suppose that an integer  $k > k_0$  satisfies

$$k \geq n \log_2 \left( \frac{k}{t} \right)$$

Then

$$e^{-(2^{\frac{2k+n}{n}})t} = (e^{-2^{\frac{2k}{n}}})^{2t} < e^{-\frac{2k^2}{t}} < 2^{-17k^2}$$

Consider the inequality

$$(2.9) \quad \frac{k}{\log_2 \left( \frac{k}{t} \right)} \geq n$$

By monotone property of the logarithm function, the following inequality is equivalent to (2.9) above:

$$(2.10) \quad k \left( 1 - \frac{\log_2 \log_2 \left( \frac{k}{t} \right)}{\log_2 \left( \frac{k}{t} \right)} \right) \geq n \log_2 \left( \frac{n}{t} \right)$$

For  $x \in (2^e, +\infty)$ , the function

$$g(x) = 1 - \frac{\log_2 \log_2 x}{\log_2 x}$$

satisfies  $0 < g(x) < 1$ , has global minima  $g(2^e) = 1 - e^{-1} \log_2 e > 0.46$ , and is increasing. Since  $t \in (0, 6^{-1})$  and  $n > 1$ , the condition  $n/t > 2^e$  is satisfied; because  $k \geq n \log_2(3n)$ , the following inequality implies (2.10):

$$(2.11) \quad k \geq n \log_2 \left( \frac{n}{t} \right) \left( 1 - \frac{\log_2 \log_2 \left( \frac{n}{t} \right)}{\log_2 \left( \frac{n}{t} \right)} \right)^{-1}$$

We claim that, for  $n > 1$  and  $t \in (0, 6^{-1})$ , the following inequality holds:

$$\begin{aligned} \frac{\log_2 \left( \frac{n}{t} \right) + 2 \log_2 \log_2 \left( \frac{n}{t} \right)}{\log_2 \left( \frac{n}{t} \right)} &= 1 + \frac{2 \log_2 \log_2 \left( \frac{n}{t} \right)}{\log_2 \left( \frac{n}{t} \right)} \\ &\geq \left( 1 - \frac{\log_2 \log_2 \left( \frac{n}{t} \right)}{\log_2 \left( \frac{n}{t} \right)} \right)^{-1} \\ &= \frac{\log_2 \left( \frac{n}{t} \right)}{\log_2 \left( \frac{n}{t} \right) - \log_2 \log_2 \left( \frac{n}{t} \right)} \end{aligned}$$

This is equivalent to

$$\log_2 \left( \frac{n}{t} \right) \geq 2 \log_2 \log_2 \left( \frac{n}{t} \right)$$

Writing  $x = \frac{n}{t}$ , this is equivalent to  $\sqrt{x} \geq \log_2 x$ . The function  $h(x) = \sqrt{x} - \log_2 x$  has derivative  $h'(x) = \frac{1}{2\sqrt{x}} - \frac{1}{x \ln 2}$ , which is increasing for  $x > \frac{4}{(\ln 2)^2}$ , and  $h(12) > 0$ .

This proves the claim.

Thus,  $k_0 = n \log_2 \left(\frac{n}{t}\right) + 2n \log_2 \log_2 \left(\frac{n}{t}\right)$  implies

$$\begin{aligned}
\|H_t - H_{t,M}\|_{L^2}^2 &= \sum_{\lambda \geq 4 \frac{k_0}{n}} e^{-2\lambda t} \dim H_\lambda \\
&\leq \frac{2(2^{\frac{n}{2}})}{n!} \sum_{k \geq k_0} 2^{1+k} e^{-(2 \frac{2k+n}{n})t} \\
&\leq \frac{4(2^{\frac{n}{2}})}{n!} \sum_{k \geq k_0} 2^{1+k-17k^2} \\
&\leq \frac{2^{\frac{n}{2}}}{n!} \sum_{k \geq k_0} 2^{-16k^2} \\
&\leq \frac{2^{\frac{n}{2}-16k_0^2+1}}{n!} \\
&\leq \eta^2
\end{aligned}$$

□

*Remark 2.12.* If  $\epsilon \in (0, \frac{1}{3n})$  and  $t = \epsilon^2$ , one has

$$n \log_2 \left(\frac{n}{t}\right) + 2n \log_2 \log_2 \left(\frac{n}{t}\right) < \frac{3n}{2} \log_2 \left(\frac{1}{t}\right) \left(1 + \frac{2 \log_2 \log_2(5n)}{\log_2(5n)}\right)$$

We write

$$a_n := \frac{2 \log_2 \log_2(5n)}{\log_2(5n)}$$

Then the lemma above implies

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

for  $M = 4 \frac{k_0}{n}$  where  $k_0 > \max\{\log_2 \left(\frac{1}{\eta}\right), \frac{3n}{2} (1 + a_n) \log_2 \left(\frac{1}{t}\right)\}$ .

**Lemma 2.13.** *Let  $c = \min\{\ln \sqrt{2}, n^{-1}\}$ . For all  $t \in (0, c)$  and all  $M > 0$ , following inequality holds:*

$$(2.14) \quad \|H_{t,M}\|_{L^2}^2 < \frac{t^{-n}}{(n-1)!2^{n-2}}$$

*Proof.* For any  $M > 0$ , addition theorem implies

$$\|H_{t,M}\|_{L^2}^2 := \sum_{0 < \lambda \leq M} e^{-2\lambda t} \dim H_\lambda$$

The function  $\phi(x) = (x+a)te^{-2xt}$ , for  $x \in (0, \infty)$ , satisfies

$$\phi'(x) = te^{-2xt}(1 - 2(x+a)t), \quad \phi''(x) = -4t^2e^{-2x}(1 - (x+a)t)$$



which shows that  $\phi(x) \leq (2e)^{-1}e^{2at}$ . This yields

$$\begin{aligned}
\|H_{t,M}\|_{L^2}^2 &= \sum_{0 < \lambda_k \leq M} e^{-2k(n+k-1)t} \dim H_k \\
&\leq 2 \sum_{0 < \lambda_k \leq M} \frac{1}{(n-1)!} e^{-2k(n+k-1)t} \prod_{i=1}^{n-1} (k+i) \\
&\leq 2 \sum_{0 < \lambda_k \leq M} \frac{e^{-2k^2t}}{(n-1)!t^{n-1}} \prod_{i=1}^{n-1} (k+i) t e^{-2kt} \\
&\leq 2 \sum_{0 < \lambda_k \leq M} \frac{e^{-2k^2t}}{(n-1)!(2et)^{n-1}} \prod_{i=1}^{n-1} e^{2it} \\
&\leq \frac{t^{-(n-1)} e^{(n-1)(nt-1)}}{(n-1)!2^{n-2}} \sum_{k>0} e^{-2k^2t} \\
&< \frac{t^{-(n-1)}}{(n-1)!2^{n-2}} \sum_{k \geq 0} e^{-2kt} \\
&< \frac{t^{-(n-1)}}{(1-e^{-2t})2^{n-2}(n-1)!}
\end{aligned}$$

If  $t \in (0, \ln \sqrt{2})$  then  $1 - e^{-2t} > t$ , which implies that, for  $t \in (0, c)$  where  $c = \min\{\ln \sqrt{2}, n^{-1}\}$ , and any  $M > 0$ , one has

$$\|H_{t,M}\|_{L^2}^2 < \frac{t^{-n}}{(n-1)!2^{n-2}}$$

□

### 3. HAUSDORFF DISTANCE

We recall the following definition:

**Definition 3.1.** Given a subset  $\hat{S} \subset S^n$ , and  $\epsilon \geq 0$ , let  $\hat{S}_\epsilon$  be the union of all  $\epsilon$ -neighbourhoods of points in  $\hat{S}$ ; the Hausdorff distance  $d_H(\hat{S}, S^n)$  is defined to be

$$\begin{aligned}
d_H(\hat{S}, S^n) &:= \max\left\{ \sup_{x \in S^n} \inf_{y \in \hat{S}} d(x, y), \sup_{y \in \hat{S}} \inf_{x \in S^n} d(x, y) \right\} \\
&= \inf\{\epsilon \geq 0 : S^n \subseteq \hat{S}_\epsilon\}
\end{aligned}$$

Our analysis in this section will be based on an application of the following theorem, first appeared in [1].

**Theorem 3.2** (Ahlsvede-Winter). *Let  $V$  be a finite dimensional Hilbert space, with  $\dim V = D$ . Let  $A_1, \dots, A_k$  be independent identically distributed random variables taking values in the cone of positive semidefinite operators on  $V$ , such that  $\mathbb{E}[A_i] = A \geq \mu I$  for some  $\mu \geq 0$ , and  $A_i \leq I$ . Then, for all  $\epsilon \in [0, 0.5]$ , the following holds:*

$$(3.3) \quad \mathbb{P}\left[\frac{1}{k} \sum_{i=1}^k A_i \notin [(1-\epsilon)A, (1+\epsilon)A]\right] \leq 2D \exp\left(\frac{-\epsilon^2 \mu k}{2 \ln 2}\right)$$

Let  $S \subset SO_{n+1}$  be a non-empty subset, with  $|S| = k$ . For  $M > 9n^2$ , let

$$E_M := \bigoplus_{0 < \lambda \leq M} H_\lambda(S^n)$$

Recall (inequality 2.3) that  $\dim E_M \leq \frac{2(2M)^{\frac{n}{2}}}{n!}$ . Because  $\Delta := \Delta_{S^n}$  is  $SO_{n+1}$ -invariant, the subspace  $E_M$  is invariant under the operators

$$(3.4) \quad A_s(f)(x) := \frac{1}{2}f(x) + \frac{1}{4}(f(xs) + f(xs^{-1})), \quad s \in SO_{n+1}$$

Due to rotation invariance of the surface probability measure  $\sigma$ , the operators  $A_s : E_M \rightarrow E_M$  turns out to be self-adjoint. Positive semidefiniteness of  $A_s$  follows from the identity

$$\langle A_s f, f \rangle = \frac{1}{4} \int_{S^n} (f(x) + f(xs))^2 d\sigma(x)$$

Moreover, writing  $\mu$  for the unique right-invariant Haar (probability) measure on  $SO_{n+1}$ , one has

$$(\mathbb{E}_{s \sim \mu}[A_s]) f(x) = \frac{1}{2}f(x) + \frac{1}{4} \int_{SO(n+1)} f(xs) d\mu(s) + \frac{1}{4} \int_{SO(n+1)} f(xs^{-1}) d\mu(s)$$

Writing  $\tau : SO_{n+1} \rightarrow S^n$  for the map  $s \mapsto xs$ , one has

$$\begin{aligned} \int_{SO(n+1)} f(xs) d\mu(s) &= \int_{SO(n+1)} (f \circ \tau)(s) d\mu(s) \\ &= \int_{S^n} f(y) d(\tau_*\mu) \end{aligned}$$

where  $\tau_*\mu(E) = \mu(\tau^{-1}(E))$ . Since  $\tau_*\mu$  is rotation-invariant measure on  $S^n$ , one has  $\sigma = \tau_*\mu$ . Because  $f \in E_M \subset L_0^2(S^n)$ , one has

$$\int_{SO(n+1)} f(xs) d\mu(s) = \int_{S^n} f(y) d(\tau_*\mu) = 0$$

Therefore,  $(\mathbb{E}_{s \sim \mu}[A_s]) f(x) = \frac{1}{2}f(x)$ , which makes

$$(3.5) \quad \mathbb{E}_{s \sim \mu}[A_s] = \frac{1}{2}I, \quad s \in SO(n+1)$$

Furthermore, the operators  $I - A_s$  are positive semidefinite for all  $s \in SO(n+1)$ , because

$$\langle (I - A_s)f, f \rangle = \frac{1}{4} \int_{S^n} (f(x) - f(xs))^2 d\sigma(x).$$

**Theorem 3.6.** *Let  $S \subset SO_{n+1}$  be a set of order  $|S| = k$ , chosen independently, and uniformly at random from the Haar measure on  $SO_{n+1}$  and let  $\hat{S} := S \sqcup S^{-1}$  be the (multi)set of all elements in  $S$  and their inverses. Let  $\eta > 0$  satisfy*

$$\log_2 \frac{1}{\eta} \geq \frac{3n}{2} (1 + a_n) \log_2 \left( \frac{1}{t} \right),$$

where  $a_n := \frac{2 \log_2 \log_2(5n)}{\log_2(5n)}$ . Let  $t \in (0, c)$  where  $c = \min\{\frac{1}{6}, \frac{1}{n}\}$ . For

$$\delta = \frac{2^{\frac{n+4}{2}}}{n! \eta} \exp\left(\frac{-k}{16 \ln 2}\right)$$

and any integer  $l > 0$  satisfying  $2^l \geq \frac{t^{-\frac{n}{2}}}{\eta}$ , the following inequality holds:

$$(3.7) \quad \mathbb{P} \left[ \left\| 1_{S^n} - \frac{1}{(2k)^t} \sum_{s \in \hat{S}^l} H_t(x_0 s, x) \right\|_{L^2} \leq 2\eta \right] \geq 1 - \delta$$

*Proof.* Since  $t \in (0, c)$  and  $c = \min\{\frac{1}{6}, \frac{1}{n}\}$ , one has  $\eta^{-\frac{2}{n}} \geq 9n^2$ . Setting  $\epsilon = 0.5$  and  $M = \eta^{-\frac{2}{n}}$  in (3.3) yields

$$\mathbb{P} \left[ \frac{1}{k} \sum_{s \in S} A_s \notin \left[\frac{1}{4}I, \frac{3}{4}I\right] \right] \leq \frac{2^{\frac{n+4}{2}}}{n! \eta} \exp\left(\frac{-k}{16 \ln 2}\right)$$

Therefore, for all  $f \in E_M$ , the following inequality holds:

$$\mathbb{P} \left[ \left\| \frac{1}{k} \sum_{s \in \hat{S}} \frac{1}{4} f \cdot \tau(s) \right\|_{L^2} \leq \frac{1}{4} \|f\|_{L^2} \right] \geq 1 - \frac{2^{\frac{n+4}{2}}}{n! \eta} \exp\left(\frac{-k}{16 \ln 2}\right)$$

In particular, writing  $\tilde{H}_{t,M} := 1_{S^n} - H_{t,M}$ , one has

$$\mathbb{P} \left[ \left\| \frac{1}{2k} \sum_{s \in \hat{S}} \tilde{H}_{t,M}(xs) \right\|_{L^2} \leq \frac{1}{2} \|\tilde{H}_{t,M}\|_{L^2} \right] \geq 1 - \frac{2^{\frac{n+4}{2}}}{n! \eta} \exp\left(\frac{-k}{16 \ln 2}\right)$$

Iterating this inequality  $l > 0$  times fetches

$$(3.8) \quad \mathbb{P} \left[ \left\| \frac{1}{(2k)^l} \sum_{s \in \hat{S}^l} \tilde{H}_{t,M}(xs) \right\|_{L^2} \leq \frac{1}{2^l} \|\tilde{H}_{t,M}\|_{L^2} \right] \geq 1 - \frac{2^{\frac{n+4}{2}}}{n! \eta} \exp\left(\frac{-k}{16 \ln 2}\right)$$

Let  $\tilde{H}_t = H_t - 1_{S^n}$ ; then

$$\begin{aligned} \|\tilde{H}_{t,M}\|_{L^2}^2 &= \|\tilde{H}_{t,M} - \tilde{H}_t\|_{L^2}^2 + \|\tilde{H}_t\|_{L^2}^2 \\ &= \|H_{t,M} - H_t\|_{L^2}^2 + \|\tilde{H}_t\|_{L^2}^2 \\ &\leq \|H_{t,M} - H_t\|_{L^2}^2 + \|H_t\|_{L^2}^2 \end{aligned}$$

Hence, using lemma 2.7 and 2.13 in inequality (3.8), one derives

$$\mathbb{P} \left[ \left\| \frac{1}{(2k)^l} \sum_{s \in \hat{S}^l} \tilde{H}_t(xs) \right\|_{L^2} \leq (2^{-l} t^{-\frac{n}{2}} + \eta) \right] \geq 1 - \frac{2^{\frac{n+4}{2}}}{n! \eta} \exp\left(\frac{-k}{16 \ln 2}\right)$$

Since  $H_t(xs) = H_t(x_0 s^{-1}, x)$  and  $\hat{S}$  is inverse-symmetric, this produces (3.7).  $\square$

The following theorem has appeared in [16]:

**Theorem 3.9** (Nowak-Sjögren-Szarek). *Let  $H(t, x_0, x)$  be the heat kernel on the sphere  $S^n$ , corresponding to Brownian motion initiated at  $x_0 \in S^n$ . Let  $n \geq 1$  and fix  $T > 0$ . Let  $\phi(x) := \arccos\langle x, x_0 \rangle$  be the Riemannian distance, so that  $\phi(x) \in [0, \pi]$ . Then, for all  $0 < t \leq T$ , the inequality*

$$\frac{c}{(t + \pi - \phi)^{\frac{n-1}{2}} t^{\frac{n}{2}}} \exp\left(-\frac{\phi(x)^2}{4t}\right) \leq H(t, x_0, x) \leq \frac{C}{(t + \pi - \phi)^{\frac{n-1}{2}} t^{\frac{n}{2}}} \exp\left(-\frac{\phi(x)^2}{4t}\right)$$

holds for some constants  $c, C > 0$  depending only on  $n$  and  $T$ .

Let  $\epsilon, \eta \in (0, 1)$  and let  $x \in S^n$  be such that  $\phi(x) > 2\epsilon\sqrt{\ln \frac{1}{\eta\epsilon^{2n-1}}}$ . Then, taking  $T = 1$  in the above upperbound, one has

$$\begin{aligned} H_t(x) &\leq C_{S^n} t^{-n+\frac{1}{2}} \exp\left(-\frac{\phi(x)^2}{4\epsilon^2}\right) \\ &\leq C_{S^n} \eta \end{aligned}$$

Notice that the constant  $C_{S^n}$  is independent of the initial point  $x_0 \in S^n$ . Letting  $C_n := 1 + C_{S^n}$ , we have

$$(3.10) \quad \begin{aligned} H_{\epsilon^2}(x) &< C_n \eta \quad \forall \epsilon \in (0, 1), \\ \forall x \in S^n \text{ s.t. } r(\epsilon, \eta) &:= 2\epsilon\sqrt{\ln \frac{1}{\eta\epsilon^{2n-1}}} < \phi(x) \end{aligned}$$

**Lemma 3.11.** *Let  $\epsilon \in (0, c)$  where  $c = (n+4)^{-1}$ . If  $r = 2\epsilon\sqrt{\ln \frac{3C_n}{\epsilon^{2n-1}}}$  is sufficiently small, then the following inequality implies that  $x_0 \hat{S}^l \subseteq S^n$  is an  $r$ -net:*

$$(3.12) \quad \left\| 1_{S^n} - \frac{1}{(2k)^l} \sum_{s \in \hat{S}^l} H_t(x_0 s, x) \right\|_{L^2} \leq \frac{r^{\frac{n}{2}}}{3} \sqrt{\frac{\Gamma\left(\frac{n+1}{2}\right)}{\Gamma\left(\frac{n}{2} + 1\right)}}$$

*Proof.* Let  $0 < \eta < (3C_n)^{-1}$ ; then, for any  $\epsilon \in (0, 1)$ , and all  $x \in S^n$  satisfying the inequality

$$d(x, x_0 s) > r(\epsilon, \eta),$$

it follows from (3.10), and positivity of the heat kernel, that  $0 < H_t(x_0 s, x) < \frac{1_{S^n}}{3}$ , and (hence)

$$(3.13) \quad \frac{2_{S^n}}{3} \leq 1_{S^n} - H_t(x_0 s, x) \leq 1_{S^n}$$

Write  $B(x_0 s, r) \subseteq S^n$  for the Riemannian disk of radius  $r$ , centered at  $x_0 s \in S^n$ . Let  $B_n \subseteq \mathbb{R}^n$  denote the unit euclidean ball; one has (see [8])

$$(3.14) \quad \begin{aligned} \lim_{r \rightarrow 0} \frac{\sigma(B(x_0 s, r))}{r^n} &= \frac{\text{vol}(B_n)}{\text{vol}(S^n)} \\ &= \frac{1}{2\sqrt{\pi}} \frac{\Gamma\left(\frac{n+1}{2}\right)}{\Gamma\left(\frac{n}{2} + 1\right)} \end{aligned}$$

Here ‘‘vol’’ denotes the standard Lebesgue volume. Now suppose, if possible, that (3.12) is satisfied, and yet,  $x_0 \hat{S}^l \subseteq S^n$  is not an  $r$ -net, so that there is  $x \in S^n$  such that  $d(x, x_0 \hat{S}^l) > r$ . Writing

$$\alpha_n := \sqrt{\frac{\Gamma\left(\frac{n+1}{2}\right)}{\Gamma\left(\frac{n}{2} + 1\right)}},$$

we derive from (3.12) and (3.13)

$$\begin{aligned} \frac{r^{\frac{n}{2}} \alpha_n}{3} &\geq \left\| 1_{S^n} - \frac{1}{(2k)^l} \sum_{s \in \hat{S}^l} H_t(x_0 s, x) \right\|_{L^2} \\ &= \left\| \frac{1}{(2k)^l} \sum_{s \in \hat{S}^l} (1_{S^n} - H_t(x_0 s, x)) \right\|_{L^2} \\ &\geq \frac{2}{3} \left( \int_{B(x_0 s, r)} d\sigma(x) \right)^{\frac{1}{2}} \end{aligned}$$

which produces

$$\begin{aligned} \frac{\sigma(B(x_0s, r))}{r^n} &= \frac{1}{r^n} \int_{B(x_0s, r)} d\sigma(x) \\ &\leq \frac{\alpha_n^2}{4} \end{aligned}$$

Considering (3.14), this is impossible if  $r > 0$  is sufficiently small.  $\square$

**Theorem 3.15.** *Let  $\epsilon \in (0, \frac{1}{3n})$  be small, and  $r = 2\epsilon\sqrt{\ln \frac{3C_n}{\epsilon^{2n-1}}}$ . Let  $S \subset SO_{n+1}$  consist of  $k$  iid random points, drawn from the Haar measure on  $SO_{n+1}$ , where*

$$k \geq 8 \ln 2 \left( (n+4) + 2 \ln \left( \frac{1}{\delta} \right) + 6n(1+a_n) \ln \left( \frac{1}{\epsilon} \right) - \ln(n!) \right),$$

with  $a_n := \frac{2 \log_2 \log_2(5n)}{\log_2(5n)}$ . Let  $l = \frac{n}{2} \log_2 \left( \frac{1}{r\epsilon} \right) + (4+3a_n)n \log_2 \left( \frac{1}{\epsilon} \right)$ ; if  $r$  is sufficiently small then the probability that  $x_0\hat{S}^l \subseteq S^n$  is an  $r$ -net in  $S^n$  is at least  $1 - \delta$ .

*Proof.* One sees by the remark 2.12 (following lemma 2.7) that for any  $\eta > 0$ , if

$$k_0 > \max \left\{ \log_2 \frac{1}{\eta}, (1+a_n) \frac{3n}{2} \log_2 \left( \frac{1}{\epsilon} \right) \right\}$$

and  $M = 4 \frac{k_0}{n}$ , then the following inequality holds:

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

Let  $\eta := \epsilon^{3n(1+a_n)}$ , so that for sufficiently large  $l > 0$  (to be determined *à la* theorem 3.2) the parameter  $M = \eta^{-\frac{2}{n}}$  ensures

$$(3.16) \quad \delta = \frac{2^{\frac{n+4}{2}}}{n! \eta} \exp \left( \frac{-k}{16 \ln 2} \right)$$

Taking logarithm of (3.16), we find that it suffices to take

$$k \geq 8 \ln 2 \left( (n+4) + 2 \ln \left( \frac{1}{\delta} \right) + 2 \ln \left( \frac{1}{\eta} \right) - \ln(n!) \right)$$

Suppose that  $l > 0$  is large enough so that  $2^{-lt - \frac{n}{2}} \leq r^{\frac{n}{2}}$ ; for this to be true, we require  $l \geq \frac{n}{2} \log_2 \left( \frac{1}{r\epsilon^2} \right)$ . We enforce the inequality  $2^{-lt - \frac{n}{2}} \leq \epsilon^{3n(1+a_n)}$  by requiring

$$l \geq (4 + 3a_n)n \log_2 \left( \frac{1}{\epsilon} \right).$$

Therefore, if  $l = (4 + 3a_n)n \log_2 \left( \frac{1}{\epsilon} \right) + \frac{n}{2} \log_2 \left( \frac{1}{r\epsilon} \right)$ , then  $2^{-lt - \frac{n}{2}} \leq \min\{r^{\frac{n}{2}}, \eta\}$  holds. Since  $\epsilon > 0$  is small, one has  $\alpha_n r^{\frac{n}{2}} > 6\eta = 6\epsilon^{3n(1+a_n)}$ . Thus, by theorem 3.6, the following inequality holds:

$$(3.17) \quad \mathbb{P} \left[ \left\| 1_{S^n} - \frac{1}{(2k)^l} \sum_{s \in \hat{S}^l} H_t(x_0s, x) \right\|_{L^2} \leq \frac{r^{\frac{n}{2}} \alpha_n}{3} \right] \geq 1 - \delta.$$

The proof is complete by lemma 3.11.  $\square$

## 4. EQUIDISTRIBUTION AND WASSERSTEIN DISTANCE

Let  $(Y, d)$  be a compact connected metric space. Let  $C(Y)$  be the Banach space of continuous functions on  $Y$ , and  $\mathcal{M}(Y)$  its dual — consisting of linear functionals on  $C(Y)$  — equipped with weak\* topology; recall that, by compactness of  $Y$ , every linear functional is bounded, and hence, continuous. Let  $\mathcal{M}(Y)$  be the space of all finite Borel measures on  $Y$ . By *Reisz-Markov theorem*, there is a bijection  $\mathcal{M}(Y) \cong \mathcal{M}(Y)$ , defined by

$$\mu \mapsto (f \mapsto \int_Y f \, d\mu)$$

that is closed under addition and scalar multiplication. The space  $\mathcal{M}(Y)$  inherits the sequential topology on  $\mathcal{M}(Y)$  via this bijection. Thus, one says  $\mu_n \Rightarrow \mu$  if and only if

$$\int_Y f \, d\mu_n \rightarrow \int_Y f \, d\mu$$

for every  $f \in C(Y)$ . Since the Lipschitz functions are dense in  $C(Y)$ , it suffices to consider only the 1-Lipschitz functions in the above limit.

For probability measures  $\mu, \nu \in \mathcal{M}(Y)$ , the *Prokhorov distance*  $d_P(\mu, \nu) \geq 0$  is defined to be

$$d_P(\mu, \nu) = \inf\{\epsilon > 0 : \mu(B) \leq \nu(B_\epsilon) + \epsilon \, \forall B \in \mathcal{B}(Y)\}$$

where  $B_\epsilon := \{y \in Y : \exists b \in B, d(b, y) < \epsilon\}$ . This gives a metric on the convex subspace  $\mathcal{P}(Y) \subset \mathcal{M}(Y)$  of probability measures on  $Y$ , and — by *Prokhorov's theorem* — the induced metric topology on  $\mathcal{P}(Y)$  is the subspace of the weak topology on  $\mathcal{M}(Y)$ ; moreover, the space  $\mathcal{P}(Y)$  is compact.

We recall that, in a metric space  $(Y, d)$ , the 1-*Wasserstein distance* between two regular Borel probability measures  $\mu$  and  $\nu$  on  $X$  is defined to be

$$W_1(\mu, \nu) := \inf_{\lambda \in \Pi(\mu, \nu)} \int_{Y \times Y} d(x, y) \, d\lambda$$

where  $\Pi(\mu, \nu)$  is the space of couplings of  $\mu$  and  $\nu$ ; that is,  $\Pi(\mu, \nu)$  is the space of all regular Borel probability measures on  $Y \times Y$  such that the following holds:  $\lambda \in \Pi(\mu, \nu)$  if and only if for every Borel set  $B \in \mathcal{B}(Y)$ , one has

$$\lambda(Y \times B) = \mu(B) \quad \text{and} \quad \lambda(B \times Y) = \nu(B)$$

Let  $\text{Lip}_1(Y)$  be the space of all 1-Lipschitz functions on  $Y$ ; we recall that, for any  $c > 0$ , one says  $f \in \text{Lip}_c(Y)$  if and only if  $|f(x) - f(y)| \leq c \cdot d(x, y)$  for all  $x, y \in Y$ . The following duality theorem first appeared in [12].

**Theorem 4.1** (Kantorovič - Rubińšteín). *For any  $\mu, \nu \in \mathcal{P}(Y)$ , the following equality holds:*

$$(4.2) \quad W_1(\mu, \nu) = \sup_{\phi \in \text{Lip}_1(Y)} \left( \int_Y \phi \, d\mu - \int_Y \phi \, d\nu \right)$$

**Definition 4.3.** Let  $\epsilon > 0$ . Let  $\mu$  be a Borel probability measure on the metric space  $(Y, d)$ . A finite nonempty subset  $U \subset Y$  is said to be *strongly  $(\mu, \epsilon)$ -equidistributed* if the following inequality holds:

$$(4.4) \quad \sup_{\phi \in C(Y)} \left( \int_Y \phi \, d\mu - \frac{1}{|U|} \sum_{y \in U} \phi(y) \right) < \epsilon \|\phi\|_{C(Y)}$$

As mentioned before, for  $U \subset Y$  to be strongly  $(\mu, \epsilon)$ -equidistributed, it suffices to have a constant  $c := c(\mu)$  such that

$$(4.5) \quad \sup_{\phi \in \text{Lip}_1(Y)} \left( \int_Y \phi \, d\mu - \frac{1}{|U|} \sum_{y \in U} \phi(y) \right) < c\epsilon$$

Below we show *strong*  $(\mu, \epsilon)$ -equidistribution of a subset of  $S^n$  of appropriate size and low degree of randomness.

The following lemma will be useful in course of proving the main theorem of this subsection.

**Lemma 4.6** (Fourier convergence). *Fix  $y \in S^n$ , and let  $0 < a < b$ ; then the Fourier-Laplace expansion of  $H_t(y, x)$  converges uniformly to  $H_t(y, x)$  in  $[a, b] \times S^n$ .*

*Proof.* Fix an orthonormal basis  $\phi_{1,k}, \dots, \phi_{h_k,k}$  for the eigenspace  $H_k(S^n)$ . Then the Fourier-Laplace expansion of the heat kernel based at  $y \in S^n$  is

$$H_t(y, x) = \sum_{k=0}^{\infty} e^{-\lambda_k t} \sum_{i=1}^{h_k} \phi_{i,k}(x) \phi_{i,k}(y).$$

Write

$$\alpha_k(x) := \sum_{i=1}^{h_k} \phi_{i,k}(x) \phi_{i,k}(y)$$

so that

$$H_t(y, x) = \sum_{k=0}^{\infty} e^{-\lambda_k t} \alpha_k(x).$$

One has

$$\begin{aligned} \|\alpha_k(x)\|_{L^2}^2 &= \left( \int_{S^n} \alpha_k^2(x) \, d\sigma(x) \right) \\ &= \sum_{i=1}^{h_k} \phi_{i,k}(y)^2 \int_{S^n} \phi_{i,k}(x)^2 \, d\sigma(x) \\ &= \sum_{i=1}^{h_k} \phi_{i,k}(y)^2 \\ (4.7) \quad &= h_k \end{aligned}$$

by rotation invariance of the sum (see *Lemma 2.19 and 2.29*, [14])

$$\sum_{i=1}^{h_k} \phi_{i,k}(y)^2$$

Therefore,

$$\begin{aligned} \|\alpha_k(x)\|_{C^0(x)} &\leq \sqrt{h_k} \|\alpha_k\|_{L^2} \\ &= h_k \end{aligned}$$

and since

$$\begin{aligned} h_k &= \binom{n+k}{n} - \binom{n+k-2}{n} \\ &\leq 2 \binom{n+k-1}{n} \\ &\leq 2e^n \left(\frac{n+k-1}{n}\right)^n \\ &\leq 2e^{n+k-1}, \end{aligned}$$

this forces

$$\begin{aligned} \sup_{[a,b] \times S^n} \sum_{k=0}^{\infty} |e^{-\lambda_k t} \alpha_k(x)| &\leq \sum_{k=0}^{\infty} e^{-\lambda_k a} h_k \\ &\leq \sum_{k=0}^{\infty} 2e^{(1-ka)(n+k-1)} \\ &< \infty. \end{aligned}$$

The Weierstrass'  $M$ -test implies uniform convergence of  $H_t(x, y)$ , to a continuous function on  $[a, b] \times S^n$ ; the claim follows by uniqueness of the continuous limit.  $\square$

**Lemma 4.8.** *Let  $d(\cdot, \cdot)$  be the metric distance on  $S^n$ . Let  $\sigma$  be the uniform surface probability measure on  $S^n$ . For all  $t > 0$ , one has*

$$\int_{S^n} d(y, x)^2 H_t(y, x) d\sigma(x) \leq nt$$

*Proof.* Without loss of generality we may assume that  $S^n$  is embedded in  $\mathbb{R}^{n+1}$  as the unit sphere with center at  $-\mathbf{e}_{n+1} = (0, \dots, 0, -1)$ , and  $y = \mathbf{0}$ . We write  $H_t(x) := H_t(0, x)$ , and let  $\sigma_t^*$  be the Borel measure whose Radon-Nikodym derivative is

$$\frac{d\sigma_t^*}{d\sigma} = H_t(x)$$

Let  $\{X_u \mid u \in [0, t]\}$  be a standard Brownian motion on  $S^n$  with infinitesimal generator  $H_{\frac{t}{2}}(x)$ . For each positive integer  $m > 0$ , consider the equi-partition

$$0 = t_0 < t_1 < \dots < t_m = t$$

where  $t_{i+1} - t_i = m^{-1}t$  for  $i = 0, 1, \dots, m-1$ . Now define  $\{X_i^{(m)}\}_{i=0}^m$  as follows:

$$X_i^{(m)} = X_{\frac{it}{m}}$$

By linearity of expectation, for any integer  $m > 0$  one has

$$\begin{aligned} \mathbb{E}(\|X_m^{(m)}\|^2) &= \int_{S^n} \|x\|^2 H_t(x) d\sigma(x) \\ &= \mathbb{E}(\|X_{m-1}^{(m)}\|^2) + 2\mathbb{E}(\langle X_m^{(m)} - X_{m-1}^{(m)}, X_{m-1}^{(m)} \rangle) + \mathbb{E}(\|X_m^{(m)} - X_{m-1}^{(m)}\|^2) \\ (4.9) \quad &= 2 \sum_{i=1}^m \mathbb{E}(\langle X_i^{(m)} - X_{i-1}^{(m)}, X_{i-1}^{(m)} \rangle) + \sum_{i=1}^m \mathbb{E}(\|X_i^{(m)} - X_{i-1}^{(m)}\|^2) \end{aligned}$$

Fix a realization of the Brownian motion  $\{X_u \mid u \in [0, t]\}$ . For integer  $1 \leq i \leq m$ , we consider the tangent space  $T_{X_{i-1}^{(m)}}(S^n)$ . Write

$$Z_{i-1}^{(m)} := \operatorname{argmin}_{z \in T_{X_{i-1}^{(m)}}(S^n)} \|z\|, \quad Y_i^{(m)} := \operatorname{argmin}_{z \in T_{X_{i-1}^{(m)}}(S^n)} \|z - X_i^{(m)}\|$$



In explicit terms, one has

$$\begin{aligned} Y_i^{(m)} &= X_i^{(m)} - \langle \mathbf{e}_{n+1} + X_{i-1}^{(m)}, X_i^{(m)} - X_{i-1}^{(m)} \rangle (\mathbf{e}_{n+1} + X_{i-1}^{(m)}) \\ Z_{i-1}^{(m)} &= \langle \mathbf{e}_{n+1} + X_{i-1}^{(m)}, X_{i-1}^{(m)} \rangle (\mathbf{e}_{n+1} + X_{i-1}^{(m)}) \end{aligned}$$

Orthogonality relations such as

$$Y_i^{(m)} - X_i^{(m)} \perp Z_{i-1}^{(m)}, \quad \text{and} \quad X_i^{(m)} - Y_i^{(m)} \perp X_{i-1}^{(m)} - Z_{i-1}^{(m)}$$

are immediate; moreover, one has

$$\begin{aligned} \langle X_i^{(m)} - Y_i^{(m)}, Z_{i-1}^{(m)} \rangle &= \langle \mathbf{e}_{n+1} + X_{i+1}^{(m)}, X_{i-1}^{(m)} \rangle \langle \mathbf{e}_{n+1} + X_{i+1}^{(m)}, X_i^{(m)} - X_{i-1}^{(m)} \rangle \\ &= \langle \mathbf{n}, X_{i-1}^{(m)} \rangle \langle \mathbf{n}, X_i^{(m)} - X_{i-1}^{(m)} \rangle \end{aligned}$$

where  $\mathbf{n} = -\mathbf{e}_{n+1} - X_{i+1}^{(m)}$  is the unit normal to  $T_{X_{i-1}^{(m)}}(S^n)$  pointing inward. From the inequalities

$$\langle \mathbf{n}, X_{i-1}^{(m)} \rangle \leq 0 \leq \langle \mathbf{n}, X_i^{(m)} - X_{i-1}^{(m)} \rangle,$$

one has  $\langle X_i^{(m)} - Y_i^{(m)}, Z_{i-1}^{(m)} \rangle \leq 0$ . Hence,

$$\begin{aligned} \langle X_i^{(m)} - X_{i-1}^{(m)}, X_{i-1}^{(m)} \rangle &= \langle Y_i^{(m)} - X_{i-1}^{(m)}, Z_{i-1}^{(m)} \rangle + \langle X_i^{(m)} - Y_i^{(m)}, X_{i-1}^{(m)} - Z_{i-1}^{(m)} \rangle \\ &\quad + \langle X_i^{(m)} - Y_i^{(m)}, Z_{i-1}^{(m)} \rangle + \langle Y_i^{(m)} - X_{i-1}^{(m)}, X_{i-1}^{(m)} - Z_{i-1}^{(m)} \rangle \\ &\leq \langle Y_i^{(m)} - X_{i-1}^{(m)}, X_{i-1}^{(m)} - Z_{i-1}^{(m)} \rangle \end{aligned}$$

Suppose  $X_{i-1}^{(m)} = z$  and  $X_i = z'$  in  $S^n$ . Let  $z'' := z''(z, z') \in S^n$  be such that

$$(4.10) \quad z'' + z' - 2z = \langle \mathbf{n}, z'' + z' - 2z \rangle \mathbf{n}.$$

Since the function

$$g(z'') := \|z'' + z' - 2z - \langle \mathbf{n}, z'' + z' - 2z \rangle \mathbf{n}\|$$

takes arbitrarily small positive values, such a point  $z'' \in S^n$  — that satisfies (4.10) — exists by continuity of  $g(z'')$  and compactness of  $S^n$ . Note that

$$\begin{aligned} &\mathbb{P}\{Y_i^{(m)} - X_{i-1}^{(m)} = z'' - z - \langle \mathbf{n}, z'' - z \rangle \mathbf{n} \mid X_{i-1}^{(m)} = z\} \\ &= \mathbb{P}\{Y_i^{(m)} - X_{i-1}^{(m)} = z' - z - \langle \mathbf{n}, z' - z \rangle \mathbf{n} \mid X_{i-1}^{(m)} = z\} \end{aligned}$$

by independence of increments for Brownian motion on euclidean space. From

$$\begin{aligned} &\langle Y_i^{(m)} - X_{i-1}^{(m)}, X_{i-1}^{(m)} - Z_{i-1}^{(m)} \rangle \Big|_{X_{i-1}^{(m)}=z, X_i^{(m)}=z'} \\ &= - \langle Y_i^{(m)} - X_{i-1}^{(m)}, X_{i-1}^{(m)} - Z_{i-1}^{(m)} \rangle \Big|_{X_{i-1}^{(m)}=z, X_i^{(m)}=z''} \end{aligned}$$

we derive

$$\mathbb{E}(\langle Y_i^{(m)} - X_{i-1}^{(m)}, X_{i-1}^{(m)} - Z_{i-1}^{(m)} \rangle) = 0$$

It thus suffices to prove

**Lemma 4.11.**

$$\lim_{m \rightarrow \infty} \sum_{i=1}^m \mathbb{E}(\|X_i^{(m)} - X_{i-1}^{(m)}\|^2) = nt.$$

*Proof.* We will use the stereographic projection of  $S^n \setminus \{0\}$  onto  $\mathbb{R}^n$ . It can be shown (see for example [7]) that the image  $Y_t$  of a standard Brownian motion on  $S^n$  via the stereographic projection onto  $\mathbb{R}^n$ , where  $r = |Y_t|$ , with  $\Delta_{\mathbb{R}^n}$  being the Laplacian on  $\mathbb{R}^n$ , has an infinitesimal generator  $(1/2)\Delta_{S^n}$  that satisfies

$$\Delta_{S^n} = \left(\frac{1+r^2}{2}\right)^2 \Delta_{\mathbb{R}^n} - (n-2) \left(\frac{r(1+r^2)}{2}\right) \frac{\partial}{\partial r}.$$

Applying this to the function  $f(x) = \|x\|^2$ , we see that

$$\begin{aligned} \lim_{t \rightarrow 0} \mathbb{E}^0 Y_t^2 / t &= (1/2)\Delta_{S^n} r^2|_{r=0} \\ &= (1/2) \left(\frac{1+r^2}{2}\right)^2 \Delta_{\mathbb{R}^n} (r^2)|_{r=0} - (n-2) \left(\frac{r(1+r^2)}{4}\right) \frac{\partial}{\partial r} (r^2)|_{r=0} \\ &= n. \end{aligned}$$

It follows that for any  $i$ ,

$$m\mathbb{E}(\|X_i^{(m)} - X_{i-1}^{(m)}\|^2),$$

converges as  $m \rightarrow \infty$  to  $nt$ , proving the lemma.  $\square$

$\square$

**Corollary 4.12.** *Let  $n > 1$  and for integers  $k \geq 0$ , let  $P_{k,n}(t)$  be the Legendre polynomial of degree  $k$  and dimension  $n+1$ . Let  $h_k = \dim H_k(S^n)$  and*

$$\gamma_k = \int_{-1}^1 (1-t)^{\frac{1}{2}} (1-t^2)^{\frac{n-2}{2}} P_{k,n}(t) dt$$

*Then the following inequality holds for all  $n \geq 4$ :*

$$(4.13) \quad \sum_{k=0}^{\infty} e^{-\lambda_k t} \gamma_k h_k \leq \sqrt{nt}.$$

*Proof.* We recall the *Hecke-Funk formula*: for any function  $\chi : [-1, 1] \rightarrow \mathbb{R}$ , which satisfies the inequality

$$\int_{[-1,1]} |\chi(t)|(1-t^2)^{\frac{n-2}{2}} dt < \infty,$$

and any eigenfunction  $\phi \in \mathcal{H}_k(S^n)$  and point  $y \in S^n$  one has

$$\int_{S^n} \chi(y \cdot x) \phi(x) d\sigma(x) = \frac{\Omega_{n-1}}{\Omega_n} \phi(y) \int_{-1}^1 \chi(t) (1-t^2)^{\frac{n-2}{2}} P_k^n(t) dt$$

Consider the function  $\chi(t) = \sqrt{2}(1-t)^{\frac{1}{2}}$ , taking values in  $[0, 2]$ ; this satisfies the hypothesis in Hecke-Funk formula, and since  $d(y, x) = \sqrt{2}(1 - \langle y, x \rangle)^{\frac{1}{2}}$ , one gets

$$\int_{S^n} d(y, x) \phi(x) d\sigma(x) = \frac{\sqrt{2}\Omega_{n-1}}{\Omega_n} \phi(y) \int_{-1}^1 (1-t)^{\frac{1}{2}} (1-t^2)^{\frac{n-2}{2}} P_{k,n}(t) dt$$

Consider the Fourier- Laplace expansion of the heat kernel, as in lemma 4.6 above. By uniform convergence (lemma 4.6) of the Fourier-Laplace expansion of the heat

kernel, one has

$$\begin{aligned} \int_{S^n} d(y, x) H_t(y, x) d\sigma(x) &= \sum_{k=0}^{\infty} e^{-\lambda_k t} \left( \sum_{i=1}^{h_k} \phi_{i,k}(y) \int_{S^n} d(y, x) \phi_{i,k}(x) d\sigma(x) \right) \\ &= \frac{\sqrt{2}\Omega_{n-1}}{\Omega_n} \sum_{k=0}^{\infty} e^{-\lambda_k t} \gamma_k \left( \sum_{i=1}^{h_k} \phi_{i,k}^2(y) \right) \\ &= \frac{\sqrt{2}\Omega_{n-1}}{\Omega_n} \sum_{k=0}^{\infty} e^{-\lambda_k t} \gamma_k h_k \end{aligned}$$

Note that

$$\begin{aligned} \frac{\sqrt{2}\Omega_{n-1}}{\Omega_n} &= \sqrt{\frac{2}{\pi} \frac{\Gamma\left(\frac{n+1}{2}\right)}{\Gamma\left(\frac{n}{2}\right)}} \\ &\geq 1 \end{aligned}$$

for all  $n \geq 4$ . Hence, Lemma 4.8 together with Hölder inequality implies

$$\begin{aligned} \sqrt{nt} &\geq \int_{S^n} d(y, x) H_t(y, x) d\sigma(x) \\ &\geq \sum_{k=0}^{\infty} e^{-\lambda_k t} \gamma_k h_k \end{aligned}$$

□

**Theorem 4.14.** *For  $n > 1$ , let  $\mu$  be the probability measure on  $S^n$  corresponding to  $\sigma$ . Let  $\epsilon, \delta > 0$  be sufficiently small and  $r = 2\epsilon \sqrt{\ln \frac{3C_n}{\epsilon^{2n-1}}}$ . Let  $S \subseteq SO(n+1)$  be a random subset such that  $|S| = k$  satisfies the inequality in theorem 3.15, namely*

$$k > 8 \ln 2 \left( (n+4) + 2 \ln \left( \frac{1}{\delta} \right) + 6n(1+a_n) \ln \left( \frac{1}{\epsilon} \right) - \ln(n!) \right),$$

where  $a_n := \frac{2 \log_2 \log_2(5n)}{\log_2(5n)}$ . Let  $x_0 \in S^n$  and let  $\nu$  be the uniform probability measure on  $S^n$ , supported on  $\hat{S}^l x_0$ , where  $\hat{S} = S \cup S^{-1}$  as before and

$$l = \frac{n}{2} \log_2 \left( \frac{1}{r\epsilon} \right) + (4 + 3a_n) \log_2 \left( \frac{1}{\epsilon} \right).$$

Then, with probability at least  $1 - \delta$ , the following inequality holds:

$$W_1(\sigma, \nu) \leq \epsilon$$

*Proof.* Let  $\text{Lip}_{1,0}(S^n)$  be the set of mean-zero  $\text{Lip}_1$ -functions on  $S^n$ . By theorem 4.1, it suffices to show that

$$(4.15) \quad \sup_{\phi \in \text{Lip}_{1,0}(S^n)} \left( \int_Y \phi d\sigma - \int_Y \phi d\nu \right) < \epsilon$$

For any such function  $\phi \in \text{Lip}_{1,0}(S^n)$ , if  $\phi(x_0) = \|\phi\|_{L^\infty}$  then

$$\begin{aligned}
0 &= \int_{S^n} \phi(x) d\mu(x) \\
&= \int_{S^n} \phi(x_0) d\mu(x) + \int_{S^n} (\phi(x) - \phi(x_0)) d\mu(x) \\
&= \phi(x_0) + \int_{S^n} (\phi(x) - \phi(x_0)) d\mu(x) \\
\Rightarrow \phi(x_0) &\leq \int_{S^n} |\phi(x) - \phi(x_0)| d\mu(x) \\
&\leq \int_{S^n} d(x, x_0) d\mu(x) \\
&\leq 2
\end{aligned}$$

For sufficiently small  $t > 0$ , we let  $\nu_t^*$  be the Borel probability measure on  $S^n$  whose density is

$$\frac{d\nu_t^*(x)}{d\sigma} = \frac{1}{|\hat{S}^t|} \sum_{y \in \hat{S}^t x_0} H_t(y, x)$$

Then, for  $t = \epsilon^2$ , one has

$$\begin{aligned}
W_1(\sigma, \nu_t^*) &= \sup_{\phi \in \text{Lip}_{1,0}(S^n)} \left| \int_{S^n} \phi(x) d\sigma(x) - \int_{S^n} \phi(x) d\nu_t^*(x) \right| \\
&\leq \sup_{\phi \in \text{Lip}_{1,0}(S^n)} \int_{S^n} |\phi(x)| \cdot \left| 1_{S^n} - \frac{1}{(2k)^t} \sum_{y \in \hat{S}^t x_0} H_t(y, x) \right| d\sigma(x) \\
&\leq \sup_{\phi \in \text{Lip}_{1,0}(S^n)} \|\phi\|_{L^\infty} \cdot \int_{S^n} \left| 1_{S^n} - \frac{1}{(2k)^t} \sum_{y \in \hat{S}^t x_0} H_t(y, x) \right| d\sigma(x) \\
(4.16) \quad &\leq 2\epsilon^{3n} \quad (\text{see Theorem 3.15})
\end{aligned}$$

with probability at least  $1 - \delta$ .

For any function  $\phi \in \text{Lip}_{1,0}(S^n)$ , define  $\tilde{\phi}_t : S^n \rightarrow \mathbb{R}$  to be

$$\tilde{\phi}_t(x) = \frac{1}{|\hat{S}^t|} \sum_{y \in \hat{S}^t x_0} \phi(y) H_t(y, x)$$

From uniform convergence of the Fourier-Laplace expansion of heat-kernel, it follows that  $\int_{S^n} H_t(y, x) d\sigma(x) = 1$ ; hence, putting  $t = \epsilon^2$ , one has

$$\begin{aligned}
\int_{S^n} \tilde{\phi}_{\epsilon^2}(x) d\sigma(x) &= \frac{1}{|\hat{S}^t|} \sum_{y \in \hat{S}^t x_0} \phi(y) \int_{S^n} H_t(y, x) d\sigma(x) \\
(4.17) \quad &= \int_{S^n} \phi(x) d\nu(x).
\end{aligned}$$

Moreover,

$$\begin{aligned}
& \left| \int_{S^n} \phi(x) d\nu_t^*(x) - \int_{S^n} \tilde{\phi}_t(x) d\sigma(x) \right| \\
&= \frac{1}{(2k)^t} \left| \sum_{y \in \hat{S}^t x_0} \int_{S^n} (\phi(x) - \phi(y)) H_t(y, x) d\sigma(x) \right| \\
&\leq \frac{1}{(2k)^t} \sum_{y \in \hat{S}^t x_0} \int_{S^n} |\phi(x) - \phi(y)| H_t(y, x) d\sigma(x) \\
&\leq \frac{1}{(2k)^t} \sum_{y \in \hat{S}^t x_0} \int_{S^n} d(y, x) H_t(y, x) d\sigma(x) \\
(4.18) \quad &\leq \frac{n\sqrt{t}}{(2k)^t}
\end{aligned}$$

by lemma 4.8 and Hölder inequality applied to  $d(y, x) = d(y, x) \cdot 1_{S^n}$ . Therefore, for  $t = \epsilon^2 > 0$  sufficiently small, equations (4.16), (4.17), and (4.18) yield

$$\begin{aligned}
W_1(\mu, \nu) &\leq W_1(\mu, \nu_t^*) + W_1(\nu_t^*, \nu) \\
&\leq \epsilon
\end{aligned}$$

□

## 5. CONCLUSION

We proved two results about the finite time behavior of a random Markov Chain on the sphere  $S^n$  whose transitions correspond to rotations chosen uniformly at random. The first result states that for  $k = O(n \ln \frac{1}{\epsilon} + \frac{1}{\delta})$  random rotations and  $\ell = O(n \ln 1/\epsilon)$ , if one takes the image of the north pole on the sphere under all possible words of length  $\ell$  in the  $k$  alphabets and their inverses, one obtains an  $\epsilon$ -net with high probability. For these parameters, the value of  $(2k)^\ell$  is close to the volumetric lower bound of  $(1/\epsilon)^{\Omega(n)}$  on the size of an  $\epsilon$ -net of  $S^n$ . Secondly, we show that this  $\epsilon$ -net is equidistributed with probability at least  $1 - \delta$  in the sense that the 1-Wasserstein distance of the uniform measure on the net is within  $\epsilon$  of the uniform measure on  $S^n$ .

These results can respectively be applied to approximately minimize a 1-Lipschitz function on the sphere (by evaluation on the  $\epsilon$ -net) and in to approximately integrate a 1-Lipschitz function on the sphere. In both cases the approximation is within an additive  $\epsilon$  of the true value.

## REFERENCES

1. R. Ahlswede and A. Winter, *Strong converse for identification via quantum channels*, IEEE Trans. Inform. Theory 48 (2002), no. 3, 569579.
2. N. Alon, and Y. Roichman, *Random Cayley Graphs and Expanders*, Random Structures Algorithms 5 (1994), no. 2, 271284.
3. Y. Benoist, and N. de Saxcé, *A Spectral Gap Theorem in Simple Lie Groups*, Invent. Math. 205 (2016), no. 2, 337361.
4. J. Bourgain, *On random walks in large compact Lie groups*, Geometric aspects of functional analysis, 5563, Lecture Notes in Math. (2169), Springer, Cham, 2017
5. J. Bourgain, and A. Gamburd, *A spectral gap theorem in  $SU(d)$* , J. Eur. Math. Soc. (JEMS) 14 (2012), no. 5, 14551511.
6. ———, *On the spectral gap for finitely-generated subgroups of  $SU(2)$* , Invent. Math. 171 (2008), no. 1, 83121.
7. T. Carne, *Brownian motion and stereographic projection*, Ann. Inst. H. Poincaré Probab. Statist. 21 (1985), no. 2, 187196.
8. A. Gray, *The volume of a small geodesic ball of a Riemannian manifold*, Michigan Math. J. 20 (1973), 329344 (1974).
9. A. Grigor'yan, *Heat kernel and analysis on manifolds*, AMS/IP Studies in Advanced Mathematics (47), American Mathematical Society, Providence; International Press, Boston, ISBN: 978-0-8218-4935-4
10. M. Hastings, and A. Harrow, *Classical and quantum tensor product expanders*, Quantum Info. Comput. 9, 3 (March 2009), 336-360.
11. E. Hsu, *Stochastic analysis on manifolds*, Graduate Studies in Mathematics (38) AMS, Providence, ISBN: 0-8218-0802-8.
12. L. Kantorovič, and G. Rubinštejn, *On a space of completely additive functions* (Russian), Vestnik Leningrad Univ, 13 1958 no 7, 5259.
13. Z. Landau, and A. Russell, *Random cayley graph expanders: A simple proof of the Alon-Roichman Theorem*, Electron. J. Combin. 11 (2004), no. 1, Research Paper 62, 6 pp.
14. M. Morimoto, *Analytic functionals on the sphere*, Translations of Mathematical Monographs (178), AMS, Providence, ISBN: 0-8218-0585-1.
15. H. Narayanan, *On The Distribution Of Random Words In A Compact Lie Group*, preprint arXiv:1804.07146v1.
16. A. Nowak, P. Sjögren, and T. Szarek, *Sharp estimates of the spherical heat kernel*, to appear in J. Math. Pures Appl., available online 19 October 2018.
17. C. Villani, *Optimal transport*, Grundlehren der Mathematischen Wissenschaften (338), Springer-Verlag, Berlin, ISBN: 978-3-540-71049-3.

SCHOOL OF TECHNOLOGY AND COMPUTER SCIENCE, TATA INSTITUTE OF FUNDAMENTAL RESEARCH, MUMBAI 400005, INDIA

*E-mail address:* `chakraso@indiana.edu`

*E-mail address:* `hariharan.narayanan@tifr.res.in`