RANDOM WALKS TO SAMPLE UNIT QUATERNIONS

RENÉ RÜHR

Abstract. We study a random walk on the space of unit quaternions focusing on efficient implementation on hardware.

1. Introduction

Points on spheres, rotations and quaternions. In this note we study a randomized variant of the low-discrepancy set on the unit 2-sphere constructed in [LPS86], [LPS87]. While the applied math community is aware of the method of Lubotzky-Phillips-Sarnak, it is judged difficult to use in [Mit08] since the point sets constructed grow exponentially. The proposed random walk avoids this disadvantage.

The constructed point sets are actually obtained from the natural maps

$$\mathbb{H}^1(\mathbb{R}) \to \mathrm{SO}_3(\mathbb{R}) \to \mathbb{S}^2, \quad q \mapsto k \mapsto k.e_1$$

where the first map is the two-fold cover of the group of orientation preserving rotations $\mathrm{SO}_3(\mathbb{R})$ by the space of unit quaternions $\mathbb{H}^1(\mathbb{R})$. The unit quaternions on the other hand can be identified with the unit 3-sphere. A classical method to produce random points on the 3-sphere is due to Marsaglia [Mar72]. Random rotations are wildly used in computer graphics, and algorithms have been discussed in [Arv91], [Arv92], [Sho92]. They also become important in machine learning [Ale22], [LSDW22]. For a recent overview for random rotations, we refer to [YJLM10]. The two dimensional sphere is also important in computer graphics in the advent of ray tracing, see e.g. [PJH23] The current state-of-the-art low-discrepancy unit quaternions seems to be the Super-Fibonacci spirals [Ale22].

Before we describe the algorithms in the next session we briefly recall the concept of quaternions. Mathematical proofs are deferred to two appendices.

Unit quaternions. We introduce the space of quaternions

$$q = r + xi + yj + zk \in \mathbb{H}(\mathbb{R})$$

where $x, y, z \in \mathbb{R}$. The vectors i, j, k represent the imaginary units satisfying the multiplication laws

$$i^2 = j^2 = k^2 = -1, \quad ijk = -1.$$

By linearity, these rules define a multiplication among quaternions. Using the norm of $\mathbb{R}^4$, the unit quaternions $\mathbb{H}^1(\mathbb{R})$ are those with

$$\|q\|^2 = r^2 + x^2 + y^2 + z^2 = 1$$

and thus define elements on the 3-sphere $\mathbb{S}^3$. Since for two quaternions q_1, q_2 we have

$$\|q_1 q_2\| = \|q_1\| \|q_2\|,$$

the unit quaternions are closed under multiplication and thus provide $\mathbb{S}^3$ with a group structure. It is common to split the real scalar and the 3-dimensional imaginary part of a quaternion: Let $q_1 = r_1 + v_1$ and $q_2 = r_2 + v_2$ then the multiplication rule is

$$q_1 q_2 = (r_1 r_2 - \langle v_1, v_2 \rangle) + (r_1 v_2 + r_2 v_1 + v_1 \times v_2)$$

where the $\langle \cdot, \cdot \rangle$ denotes the inner product and $\times$ denotes the cross product.

2. Random walk on quaternions

2.1. **Quasi Monte Carlo method of LPS.** Consider the following set of six unit quaternions,

$$S_5 = \left\{ \frac{1 \pm 2i}{\sqrt{5}}, \frac{1 \pm 2j}{\sqrt{5}}, \frac{1 \pm 2k}{\sqrt{5}} \right\}.$$

Also consider all non-reducible words of length

$$S_5^n = \{s_1 ... s_n : s_i \in S_5, s_{i+1} \neq s_i^{-1}\}$$

Here we use the fact that S_5 generates a free group, meaning that there are no additional relation between the s_i that cause a word in to collapse to the identity except for the inverses. Equivalently, the graph defined on the set of words in S_5 with adjacency relations $w \sim w'$ (meaning there is $s \in S_5$ such that $w' = sw$) forms a tree of degree 6.

The low discrepancy sequence introduced by LPS is the increasing sequence of balls inside this tree, i.e. $Q_5^n = \sqcup_{k \leq m} S_5^k$.

The associated rotations to S_5 are

$$\frac{1}{5}\begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & -4 \\ 0 & 4 & -3 \end{pmatrix}, \quad \frac{1}{5}\begin{pmatrix} -3 & 0 & 4 \\ 0 & 1 & 0 \\ -4 & 0 & -3 \end{pmatrix}, \quad \frac{1}{5}\begin{pmatrix} -3 & -4 & 0 \\ 4 & -3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and their inverses. More generally, for any prime p which satisfies $p \bmod 4 = 1$ there exist exactly $p + 1$ many integer quaternions of square norm p that will generate a free group of rank $(p+1)/2$. More precisely, there are $8(p+1)$ integer quaternions on the sphere of square radius p. These come in pair of eights that are permutation in the coordinate coefficients and a global sign flip.

The next primes after $p = 5$ satisfying this congruence condition are 13 and 17. The associated quaternions of norm 13 and 17 are

$$S_{13} = \frac{1}{\sqrt{13}}\{1 \pm i \pm j \pm k, 3 \pm 2i, 3 \pm 2j, 3 \pm 2k\}$$

and

$$S_{17} = \frac{1}{\sqrt{17}}\{1 \pm 4i, 1 \pm 4j, 1 \pm 4k, 3 \pm 2i \pm 2j, 3 \pm 2j \pm 2k, 3 \pm 2k \pm 2i\}.$$

2.2. **Simple random walk.** Here is a quick description of the random walk method using S_5. Fix a starting unit quaternion q_0, say $q_0 = 1$. Choose a random element q_1 in S_5 and multiply it with q_0: $q_1 q_0$. This is the first *random* sample. Repeat for each new sample: Given the current state $q_{n-1} q_{n-2} \dots q_1 q_0$, choose a random $q_n \in S_5$ to obtain the next sample

$$q_n q_{n-1} q_{n-2} \cdots q_1 q_0.$$

The pseudo-code is given in Algorithm 1.

Algorithm 1 Random quaternions (Simple random walk)

```
Initialization: Lookup table S_5 // An array of six 4-dimensional vectors
Input: Current state q_current
Output: Sample q in H^1(R)
procedure SIMPLE RANDOM WALK
    i ← random(0, 5) // Random number in {0, 1, 2, 3, 4, 5}
    s_i ← S_5[i]
    q ← s_i q_current
    return q
end procedure
```

Algorithm 2 Random quaternions (Biased simple random walk)

```
Initialization: Lookup table S'_5 = [s_1, s_2, s_3, s_4, s_5, s_6, s_1, s_2]
Input: Current state q_current
Output: Sample q in H^1(R)
procedure BIASED SIMPLE RANDOM WALK
    i ← random(0, 7)
    s_i ← S'_5[i]
    q ← s_i q_current
    return q
end procedure
```

2.3. **Biased walk.** A slight nuisance that these numbers are not powers of two, where modulo calculation will be cheaper. Coming back to S_5, we can modify the algorithm by building a lookup table S_5^{biased} of size 8 where the last 2 elements are some duplicates of S_5. Taking a random element from this new array is equivalent of doing the random walk with biased weights. This walk will still give a sequence which asymptotically converges to the uniform measure on $\mathbb{H}^1(\mathbb{R})$. The primes (1 mod 4) below some power of two are $5, 13, 29, 61, 113, 241, 509$.

Algorithm 3 Random quaternions (Nonbacktracking random walk)

```
Initialization: Lookup table S''_5 = [s_1, s_2, s_3, s_1^{-1}, s_2^{-1}, s_3^{-1}]
Input: Current state q_current and last choice j
Output: Sample q in H^1(R)
procedure NONBACKTRACKING RANDOM WALK
    i ← (j + 4 + random(0, 4))  mod 6
    s_i ← S''_5[i]
    q ← s_i q_current
    return q
end procedure
```

2.4. **Nonbacktracking walk.** For small primes p, there is a high probability of seeing the same element that one saw two time steps ago. One can avoid this by restricting to non-backtracking paths. We again start with at a point q_0. and move with equal probability to any of the 6 neighbors $q_1 q_0$ for $q_1 \in S_5$. For the next move, we restrict to $q_2 \neq q_1^{-1}$, the non-backtracking condition. This will hold for all future times $n+1$ as well: $q_{n+1} \neq q_n^{-1}$. The set of non-backtracking paths of length n starting at q_0 is denoted by $S_5^n q_0$.

The non-backtracking walk will have to save the last step in its internal state. By using an ordering $\{s_i\}$ of the elements in S_5 in which the inverse of s_i is $s_{(i+3)\mathrm{mod}6}$, we can easily sample from the elements $i + 4 + \{0, 1, 2, 3, 4\} \mod 6$ that won't take a step back.

Algorithm 4 Random quaternions (Randomized Quasi-Monte Carlo)

Initialization: Lookup table S_5 and Q_{13}^2
Output: Sample q in $\mathbb{H}^1(\mathbb{R})$
Internal State: MC state q_{current} and QMC-index k.
procedure RQMC
  if $k = 196$ **then**
    $i \leftarrow \mathrm{random}(0, 6)$
    $k \leftarrow 0$
    $s_i \leftarrow S_5[i]$
    $q_{\text{current}} \leftarrow s_i q_{\text{current}}$
    return q_{current}
  else
    $q_i \leftarrow Q_{13}^2[k]$
    $k \leftarrow k + 1$
    return $q_i q_{\text{current}}$
  end if
end procedure

2.5. **Randomized Markov Monte Carlo.** So far we discussed the quasi-Monte Carlo method of LPS and discussed a Markov Chain Monte Carlo version by walking the tree randomly. One can combine both methods, by taking the replicated QMC sequences that are translated by some random amount. This allows to use confidence intervals from the random part but keep the error that of a QMC sequence. A survey of randomized QMC can be found in [Owe98].

For example, we can walk according to the laws of S_5 and at each step, take the QMC sequence $Q_{13}^2 = S_{13} \sqcup S_{13}^2$. Note that the cardinality of Q_{13}^2 is $14 + 14 * 13 = 196$. The advantage of using two different primes is to avoid cancellations between the MC and QMC part.

2.6. **Parallel Quasi Monte Carlo with shared memory.** Suppose we wish to produce lots of samples on a parallel compute system. There is not a straight forward implementation of the random walk method without an explicit formula for the nth word given a list of choices (other than naive multiplication). Further, random walks of short length starting at the same position will produce the same elements.

To accommodate this difficulty, we first produce S_5^m store it in shared memory. We then produce samples by randomly calculating elements from S_5^m. Here we use $m = 4$ (750 elements). We set serves as pool for random elements. Its relative large size ensures that there are not many common paths. Now each kernel will walk the walk individually. We skip the first three elements to ensure that a set of one million threads has 500 million different starting points.

Algorithm 5 Random quaternions (Parallel Quasi-Monte Carlo)

Initialization: S_5, Shared memory S_5^4
Input: i (Kernel id)
Output: Length k-array Q of quaternions per kernel
procedure INITIALIZE SHARED MEMORY
  $i_5 \leftarrow i/5$
  $i_{25} \leftarrow i_5/5$
  $i_{125} \leftarrow i_{25}/5$
  $S_5^4[i] \leftarrow 1$
  Barrier
  $j \leftarrow i_{125}$
  $S_5^4[i] = S_5[j \mod 6] * S_5^4[i]$
  Barrier
  $j \leftarrow j + 4 + i_{25} \mod 5$
  $S_5^4[i] = S_5[j \mod 6] * S_5^4[i]$
  Barrier
  $j \leftarrow j + 4 + i_5 \mod 5$
  $S_5^4[i] = S_5[j \mod 6] * S_5^4[i]$
  Barrier
  $q[i] \leftarrow S_5^4[\mathrm{random}(0, 750)] * S_5^4[\mathrm{random}(0, 195)]$
end procedure
procedure PARALLEL QMC
  for l in $1...k$ **do**
    $q[i] \leftarrow S_5^4[\mathrm{random}(0, 750)] * q[i]$
    $Q[i, k] \leftarrow q[i]$
  end for
end procedure

Naturally, the more elements each kernel produces in a loop, the better the offset of the initial cost to initialize the shared memory. To avoid modulus calculation, we could fill an array as large as the next power of two by adding elements from the next sphere in the tree. This can easily be done by initializing the shared memory with

```
shared_memory[i] =  i < 750 ? 1 : S_5[0].
```

APPENDIX A: ON THE THE THEOREM OF LUBOTZKY-PHILLIPS-SARNAK

The method of LPS is summarized well in the Bourbaki Seminar [CdV88] and discussed in book form in [Lub94b], [Sar90] from different point of views. Some further studies on the discrepancy can be found in [CF97]. Here we present the relevant theorems for this note.

Let G be a group acting via isometries on a metric space X. Let $S \subset G$ be a finite subset of G. Suppose X is endowed with a probability measure μ left invariant by G. Let $L^2(X)$ be the Hilbert space of square integrable functions on X with respect to μ. Define the averaging operator T_S on $L^2(X)$ by

$$T_S f(x) = \frac{1}{|S|} \sum_{\gamma \in S} f(\gamma . x).$$

Then the operator norm $\|T_{S_p} - \mathrm{id}\|$ where $\mathrm{id} : f \mapsto f$ will measure how fast iterates $T_{S_p}^n f$ converge to $\mu(f)$ for any square-integrable f in L^2-norm.

Now specify $G = \mathrm{SO}_3(\mathbb{R})$, $X = \mathbb{S}^2 = \mathrm{SO}_3(\mathbb{R})/\mathrm{SO}_2(\mathbb{R})$, μ the normalized Lebesgue measure on $\mathbb{S}^2$.

Let p be a prime congruent to 1 mod 4. Consider those integer quaternions $H(\mathbb{Z})$ whose square norm equals p. There are $8(p+1)$ of those. Of those, $p+1$-many have their real part odd and positive. Normalize these elements to be unit quaternions. Denote the set of such elements by S_p:

$$S_p = \left\{ \frac{q}{\sqrt{p}} \ : \ q = r + xi + yj + zk \in H(\mathbb{Z}), r^2 + x^2 + y^2 + z^2 = p, \ r = 1(2), \ r > 0 \right\}$$

Every unit quaternion defines a rotation via by Adjoint representation of SU(2). We identify S_p with its image under this representation. Then, for example, S_5 corresponds to rotations around the x, y, z axis with an angle of $\mathrm{acos}(-\frac{2}{5}) \simeq 2.21$ radians.

The associated operator T_{S_p} is known as Hecke operator. The main result of Lubotzky-Philips-Sarnak is the following spectral bound of the Hecke operator, which remarkably enough follows from Deligne's resolution of the Weil conjecture on the Riemann hypothesis over finite fields.

Theorem 2.1 ([LPS86], Theorem 1.3)**.**

$$\|T_{S_p} - \mathrm{id}\|_{L^2(X)} = \frac{2\sqrt{p}}{p+1}$$

The set S_p is symmetric, i.e. if $\gamma \in S_p$ then $\gamma^{-1} \in S_p$. Most importantly, S_p generates a free subgroup Γ_p inside $\mathrm{SO}_3(\mathbb{R})$ of rank $\frac{p+1}{2}$. Thus, the associated Cayley graph with generators S_p defined by the node set Γ_p and adjacency relations $g \sim h$ if $g = \gamma h$ for some $\gamma \in S_p$ is a tree. In particular, T_{S_p} projects from the random walk on this tree. By a theorem of Kesten [Kes59], the second largest eigenvalue of the Markov operator is at least $2\sqrt{p+1}$ which is the lower bound in Theorem 2.1.

Theorem 2.1 can be generalized twofold. First, let let S_p^n denote the set of reduced words in the alphabet S_p of length n. Equivalently, this is the sphere of radius n inside the Cayley graph. The cardinality of this set is $N = (p+1)p^{n-1}$.

Secondly, we can lift T_p and more generally the Hecke operator associated to S_p^n to $\mathrm{SO}_3(\mathbb{R})$: For $f \in L^2(\mathrm{SO}_3(\mathbb{R}))$,

$$T_{S_p^n} f(g) = \frac{1}{|S_p^n|} \sum_{\gamma \in S_p^n} f(\gamma g).$$

Here $\mathrm{SO}_3(\mathbb{R})$ is equipped with the normalized Haar measure.

Theorem 2.2 ([Sar90], Section 2.6)**.** *Let $N = |S_p^n|$.*

$$\|T_{S_p^n} - \mathrm{id}\|_{L^2(\mathrm{SO}_3(\mathbb{R}))} = \mathcal{O}\left(\frac{\log N}{N^{\frac{1}{2}}} \right)$$

This Theorem 2.1 implies the following low-discrepancy theorem.

Theorem 2.3 ([LPS86], Theorem 2.1; [CdV88], Theorem D)**.** *Let $N = |S_p^n|$. Suppose $D \subset \mathbb{S}^2$ has a C^1 boundary. Then for any $x_0 \in \mathbb{S}^2$,*

$$\left| \frac{1}{N} |\{\gamma \in S_p^n \ : \ \gamma . x_0 \in D\}| - \frac{\mathrm{area}(D)}{4\pi} \right| = \mathcal{O}\left(\frac{\log N}{N^{\frac{1}{3}}} \right)$$

Conjecturally, this bound can be improved to be $\mathcal{O}(N^{-\frac{1}{2}-\varepsilon})$ ([LPS86][Conjecture 2.4]).

Lattice method of the LPS theorems. In [LPS87] the lattice method for the analysis of Hecke operators is introduced. This allows to give a very quick proof for Theorem 2.1 and Theorem 2.2 which we now outline. The group of unit quaternions modulo its center defines an algebraic group $\mathbb{G}$ such that $\mathbb{G}(\mathbb{R}) \simeq \mathrm{SO}_3(\mathbb{R})$ and $\mathbb{G}(\mathbb{Q}_p) \simeq \mathrm{PGL}_2(\mathbb{Q}_p)$. Here $\mathbb{Q}_p$ denote the p-adic numbers. There is a cover of $\mathrm{SO}_3(\mathbb{R})$ (modulo the finite group of permutations) by the S-adic space $X = \mathbb{G}(\mathbb{Z}[\frac{1}{p}])\backslash\mathbb{G}(\mathbb{R}) \times \mathbb{G}(\mathbb{Q}_p)$, see [Lub94a]. The fiber is the compact group $K_p = \mathbb{G}(\mathbb{Z}_p)$ where $\mathbb{Z}_p$ denote the p-adic integers. Moreover, at every point x, the orbit of $\mathbb{G}(\mathbb{Q}_p).x$ is a tree. The Hecke operator T_p can be lifted from $L^2(\mathrm{SO}_3(\mathbb{R}))$ to $L^2(X)$. There, it acts by convolution with the characteristic function χ of the set $\sqcup_{\gamma\in S_p} K_p\gamma = K_p a K_p$ where $a = \mathrm{diag}\,(p, 1) \in \mathrm{PGL}_2(\mathbb{Q}_p)$. This set correspond to the first sphere of the tree. More generally, $\sqcup_{\gamma\in S_p^n} K_p\gamma = K_p a^n K_p$. The spectral gap of T_p then translates directly into decay of matrix coefficients for the action of a, which is bounded by $\sim \frac{1}{\sqrt{p}}$ [COU01].

Appendix B: Law of large numbers and a central limit theorem

The L^2 bounds on the Hecke operators imply analogous bounds for the L^∞ norm, see [GM03], [CU04]. Thus, there exists $\theta > 0$ such that for every g, every Lipschitz function f on $\mathrm{SO}_3(\mathbb{R})$,

$$\left|T_p^n(f)(g) - \mu(f)\right| = \mathcal{O}_f(\theta^n)$$

and a similar bound holds for $T_{S_p^n}$ instead of T_p^n.

We wish to show the law of large numbers for the sum of random variables $f(\gamma_k \ldots \gamma_1 g)$:

$$Y_n(\gamma_1, \ldots, \gamma_n) := \frac{1}{n}\left(f(\gamma_1 g) + f(\gamma_2\gamma_1 g) + \cdots + f(\gamma_n \ldots \gamma_1 g)\right)$$

where γ_i is chosen uniformly from $S_p \setminus \{\gamma_i\}$ (non-backtracking random walk) or uniformly among S_p (simple random walk).

For brevity, we restrict now to the simple random walk. Let ν be the uniform measure on S_p. This is the law of the walk. The space of all paths is $S_p^{\otimes\mathbb{N}}$ carrying the Bernoulli measure $\beta = \nu^{\otimes\mathbb{N}}$. The expectation $\mathbb{E}$ of Y_n with respect to β is

$$\mathbb{E}[nY_n] = \frac{1}{(p+1)^n}\sum_{\gamma_1,\ldots,\gamma_n} Y_n(\gamma_1, \ldots, \gamma_n) = Tf(g) + T^2 f(g) + \cdots + T^n f(g)$$

Applying the above operator bound,

$$\mathbb{E}[Y_n] = \mu(f) + \mathcal{O}(n^{-1})$$

since the error term sum to a geometric series bounded by a constant. Analogously one shows that the variance behaves like $\mathrm{Var}[Y_n] = (\mu(f^2) - \mu(f)^2)n^{-1} + \mathcal{O}(n^{-2})$, using that if $k > \ell$ then $T_p^k(f)T_p^\ell(f) = T_p^\ell(fT^{k-\ell}f)$.

The pointwise convergence of T_p^n implies that for any continuous function f, and any T_p-invariant probability measure on μ' on $\mathrm{SO}_3(\mathbb{R})$, we have $\mu'(f) = \mu(f)$. It follows from Breiman's Law of Large Numbers Theorem for Markov chains [Bre60], see also [BQ16][Section 3.2], which applies to both the simple random walk and the non-back tracking walk:

$$Y_n \to \mu(f).$$

We also deduce the central limit theorem, see [DS23], writing $\beta = \mathbb{P}$,

$$\mathbb{P}\left[\frac{Y_n - \mathbb{E}[Y_n]}{\sqrt{\mathrm{Var}[Y_n]}} \in (a, b)\right] \to \frac{1}{\sqrt{2\pi}}\int_a^b e^{-t^2/2}dt.$$

By the previous estimates, the fraction in the LHS is $\sqrt{n}(Y_N - \mu(f))$ which gives the usual form of the CLT. We note that related aspects of equidistribution properties of quaternions have been studied in [EMV13], [Kha17] and [Wie19].

Convergence of the biased walk. The spectral gap for the uniform averaging operator implies the spectral gap for small biases from general perturbation theory [Kat13]. Rigidity of the underlying group action implies spectral gap for arbitrary positive weights, [FS99]. Convergence can also directly deduced from the recent breakthrough of Benoist-Quint in their study of stationary measures for Lie group action on homogeneous spaces [BQ13]. They show that given a Lie group G and a lattice Γ in G (i.e. a closed discrete subgroup such that G/Γ has finite volume using the measure induced from Haar on G), a law μ supported on G such that the support of μ is dense in G. Then for any $x \in G/\Gamma$, then for almost every choice of g_1, g_2,..., where g_i is sampled according to i.i.d. sampled from μ ,

$$\frac{1}{n}\sum_{k=1}^{n} \delta_{g_k \dots g_1 . x} \to m_{G/\Gamma}.$$

Here, almost every choice means almost surely with respect to the Bernoulli measure $\mu^{\otimes \mathbb{N}}$.

This theorem holds true more generally for S-adic group, in particular for $\mathbb{G}(\mathbb{Z}[\frac{1}{p}])$ acting on X as defined above. This shows that the biased random walk converges. Recently, a Markov Chain version of the theorem of Benoist-Quint has been obtained [PS20]. While that paper only deals with real Lie group, the S-adic case is likely to hold. This would imply convergence of the biased non-backtracking walk.

Acknowledgement. The author thanks Omri Sarig, Barak Weiss and Miri Ben-Chen helpful references. This work was supported by the ISF 264/22 during his time at the Weizmann Institute of Science. The author is greatful to Omri Sarig for his hospitality.

References

[Ale22] Marc Alexa. Super-fibonacci spirals: Fast, low-discrepancy sampling of so (3). In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pages 8291–8300, 2022.

[Arv91] James Arvo. Vii.7 - random rotation matrices. In James Arvo, editor, *Graphics Gems II*, pages 355–356. Morgan Kaufmann, San Diego, 1991.

[Arv92] James Arvo. Fast random rotation matrices. In *Graphics gems III (IBM version)*, pages 117–120. Elsevier, 1992.

[BQ13] Yves Benoist and Jean-François Quint. Stationary measures and invariant subsets of homogeneous spaces (iii). *Annals of Mathematics*, pages 1017–1059, 2013.

[BQ16] Yves Benoist and Jean-François Quint. *Random walks on reductive groups*. Springer, 2016.

[Bre60] Leo Breiman. The strong law of large numbers for a class of markov chains. *The Annals of Mathematical Statistics*, 31(3):801–803, 1960.

[CdV88] Yves Colin de Verdière. Distribution de points sur une sphère. *Sem. Bourbaki*, 41(703):177–178, 1988.

[CF97] Jianjun Cui and Willi Freeden. Equidistribution on the sphere. *SIAM Journal on Scientific Computing*, 18(2):595–609, 1997.

[COU01] Laurent Clozel, Hee Oh, and Emmanuel Ullmo. Hecke operators and equidistribution of hecke points. *Inventiones mathematicae*, 144(2):327–380, 2001.

[CU04] Laurent Clozel and Emmanuel Ullmo. Équidistribution des points de hecke. *Contributions to automorphic forms, geometry, and number theory*, pages 193–254, 2004.

[DS23] Dmitry Dolgopyat and Omri M. Sarig. *Local limit theorems for inhomogeneous Markov chains*, volume 2331 of *Lect. Notes Math.* Cham: Springer, 2023.

[EMV13] J Ellenberg, P Michel, and A Venkatesh. Linnik's ergodic method and the distribution of integer points on spheres. automorphic representations and l-functions, 119–185, tata inst. *Fundam. Res. Stud. Math*, 22, 2013.

[FS99] Alex Furman and Yehuda Shalom. Sharp ergodic theorems for group actions and strong ergodicity. *Ergodic Theory and Dynamical Systems*, 19(4):1037–1061, 1999.

[GM03] Daniel Goldstein and Andrew Mayer. On the equidistribution of hecke points. *Forum Mathematicum*, 2003.

[Kat13] Tosio Kato. *Perturbation theory for linear operators*, volume 132. Springer Science & Business Media, 2013.

[Kes59] Harry Kesten. Symmetric random walks on groups. *Transactions of the American Mathematical Society*, 92(2):336–354, 1959.

[Kha17] Ilya Khayutin. Large deviations and effective equidistribution. *International Mathematics Research Notices*, 2017(10):3050–3106, 2017.

[LPS86] Alexander Lubotzky, Ralph Phillips, and Peter Sarnak. Hecke operators and distributing points on the sphere i. *Communications on Pure and Applied Mathematics*, 39(S1):S149–S186, 1986.

[LPS87] Alexander Lubotzky, Ralph Phillips, and Peter Sarnak. Hecke operators and distributing points on s2. ii. *Communications on Pure and Applied Mathematics*, 40(4):401–420, 1987.

[LSDW22] Adam Leach, Sebastian M Schmon, Matteo T. Degiacomi, and Chris G. Willcocks. Denoising diffusion probabilistic models on SO(3) for rotational alignment. In *ICLR 2022 Workshop on Geometrical and Topological Representation Learning*, 2022.

[Lub94a] Alex Lubotzky. *Discrete groups, expanding graphs and invariant measures*, volume 125. Springer Science & Business Media, 1994.

[Lub94b] Alexander Lubotzky. *Discrete groups, expanding graphs and invariant measures*, volume 125 of *Progress in Mathematics*. Birkhäuser Verlag, Basel, 1994. With an appendix by Jonathan D. Rogawski.

[Mar72] George Marsaglia. Choosing a point from the surface of a sphere. *The Annals of Mathematical Statistics*, 43(2):645–646, 1972.

[Mit08] Julie C Mitchell. Sampling rotation groups by successive orthogonal images. *SIAM Journal on Scientific Computing*, 30(1):525–547, 2008.

[Owe98] Art B Owen. Monte carlo extension of quasi-monte carlo. In *1998 Winter Simulation Conference. Proceedings (Cat. No. 98CH36274)*, volume 1, pages 571–577. IEEE, 1998.

[PJH23] Matt Pharr, Wenzel Jakob, and Greg Humphreys. *Physically based rendering: From theory to implementation*. MIT Press, forth edition, 2023.

[PS20] Roland Prohaska and Cagri Sert. Markov random walks on homogeneous spaces and diophantine approximation on fractals. *Transactions of the American Mathematical Society*, 373(11):8163–8196, 2020.

[Sar90] Peter Sarnak. *Some applications of modular forms*, volume 99. Cambridge University Press, 1990.

[Sho92] Ken Shoemake. Uniform random rotations. In *Graphics Gems III (IBM Version)*, pages 124–132. Elsevier, 1992.

[Wie19] Andreas Wieser. Linnik's problems and maximal entropy methods. *Monatshefte für Mathematik*, 190(1):153–208, 2019.

[YJLM10] Anna Yershova, Swati Jain, Steven M Lavalle, and Julie C Mitchell. Generating uniform incremental grids on so (3) using the hopf fibration. *The International journal of robotics research*, 29(7):801–812, 2010.