The Annals of Probability
1996, Vol. 24, No. 1, 74–96

THE CUT-OFF PHENOMENON FOR RANDOM REFLECTIONS[1]

BY URSULA POROD

University of California, Berkeley

For many random walks on "sufficiently large" finite groups the so-called *cut-off phenomenon* occurs: roughly stated, there exists a number k_0, depending on the size of the group, such that k_0 steps are necessary and sufficient for the random walk to closely approximate uniformity. As a first example on a continuous group, Rosenthal recently proved the occurrence of this cut-off phenomenon for a specific random walk on $\mathrm{SO}(N)$. Here we present and [for the case of $\mathrm{O}(N)$] prove results for random walks on $\mathrm{O}(N)$, $\mathrm{U}(N)$ and $\mathrm{Sp}(N)$, where the one-step distribution is a suitable probability measure concentrated on reflections. In all three cases the cut-off phenomenon occurs at $k_0 = \frac{1}{2}N \log N$.

1. Introduction and statement of results. The purpose of this paper is to give a precise estimate on the speed of convergence to stationarity (i.e., the normalized Haar measure ϑ) with respect to total variation distance $\|\cdot\|_{\mathrm{TV}}$ for a specific random walk ("random reflections") on the orthogonal group $\mathrm{O}(N)$ (Theorems 1.1 and 1.2). Our results show that, in the large N limit, these random walks exhibit the so-called *cut-off phenomenon* (see Remark 1.3).

By "random reflections" on $\mathrm{O}(N)$ we mean the random walk whose step distribution μ is the uniform probability measure concentrated on the set $\mathscr{R}$ of *reflections* [the elements of $\mathrm{O}(N)$ that leave exactly one hyperplane pointwise fixed]. Note that the set $\mathscr{R}$ is a conjugacy class; hence μ is the unique conjugate-invariant probability measure on $\mathscr{R}$.

The main problem is to estimate $\|\mu_k - \vartheta\|_{\mathrm{TV}}$ in (k, N). Here μ_k denotes the distribution of the walk at time k (i.e., the k-fold convolution power of μ). Note that in the case of random reflections, there is a parity problem. At odd times, the probability measures $\mu_1, \mu_3, \ldots$ are concentrated on $\mathrm{O}(N)^-$, the connected component of $\mathrm{O}(N)$ of orthogonal matrices of determinant -1. Similarly, at even times, $\mu_0, \mu_2, \ldots$ are concentrated on the identity component $\mathrm{SO}(N)$. Hence we separate the cases k even and k odd and define ϑ_+ and ϑ_- by

$$d\vartheta_+ := \mathbf{2}\mathbf{1}_{\mathrm{SO}(N)}\, d\vartheta$$

Received December 1993; revised April 1995.

[1]This paper is based on parts of the author's doctoral dissertation written at The Johns Hopkins University.

AMS 1991 *subject classifications*. 60J15, 60B15.

Key words and phrases. Random walk, reflection, cut-off phenomenon, Fourier analysis.

and

$$d\vartheta_- := 2\mathbf{1}_{\mathrm{O}(N)^-}\, d\vartheta.$$

Our main results follow.

THEOREM 1.1. *Let μ be the probability measure on $\mathrm{O}(N)$ defined above. For any integer $N \geq 16$ and any positive real number $c \geq c_0$ (where c_0 is some universal positive constant), we have the following: if $k = \frac{1}{2}N \log N + cN$ is an even integer, then*:

(a) $$\| \mu_k - \vartheta_+ \|_{\mathrm{TV}} \leq 10.6 e^{-c/9},$$

(b) $$\| \mu_{k+1} - \vartheta_- \|_{\mathrm{TV}} \leq 10.6 e^{-c/9}.$$

THEOREM 1.2. *Let μ be the probability measure on $\mathrm{O}(N)$ defined above. For any integer $N \geq 2$ and any positive real number c, we have the following: if $k = \frac{1}{2}N \log N - cN$ is an even integer, then*:

(a) $$\| \mu_k - \vartheta_+ \|_{\mathrm{TV}} \geq 1 + 16.4 e^{-4c} - 46.3 \frac{\log N}{N^{3/5}},$$

(b) $$\| \mu_{k-1} - \vartheta_- \|_{\mathrm{TV}} \geq 1 - 16.4 e^{-4c} - 46.3 \frac{\log N}{N^{3/5}}.$$

Note that both statement (b) in Theorem 1.1 and statement (b) in Theorem 1.2 follow immediately from the corresponding bounds [statements (a)] for $\| \mu_k - \vartheta_+ \|_{\mathrm{TV}}$. Indeed, $\| \mu_k - 2\vartheta \|_{\mathrm{TV}}$ is weakly decreasing in k and equal to $1 + \| \mu_k - \vartheta_+ \|_{\mathrm{TV}}$, for k even, and $1 + \| \mu_k - \vartheta_- \|_{\mathrm{TV}}$, for k odd; hence

$$\| \mu_{k+1} - \vartheta_- \|_{\mathrm{TV}} \leq \| \mu_k - \vartheta_+ \|_{\mathrm{TV}} \leq \| \mu_{k-1} - \vartheta_- \|_{\mathrm{TV}}.$$

Our Fourier methods for proving the upper and lower bounds for $\| \mu_k - \vartheta_+ \|_{\mathrm{TV}}$ rely on previous work by Diaconis, Rosenthal and others. To prove Theorem 1.1(a), we follow closely the outline of a proof for a similar estimate found in [9].

REMARK 1.3. Together, Theorems 1.1 and 1.2 show that random reflections exhibit the *cut-off phenomenon*: for large N, the total variation distance decreases abruptly from 1 to 0 as k increases. In particular, there is a critical number $k_0(N)$ [here $k_0(N) = \frac{1}{2}N \log N$] such that, for all $\varepsilon > 0$, $\lim_{N \to \infty} \| \mu_{k_0(N)(1+\varepsilon)} - \vartheta_+ \|_{\mathrm{TV}} = 0$ and $\lim_{N \to \infty} \| \mu_{k_0(N)(1-\varepsilon)} - \vartheta_+ \|_{\mathrm{TV}} = 1$ (similarly for ϑ_-). For background on the cut-off phenomenon see, for example, [1]. To our knowledge, the only previous results in the compact Lie group case are due to Rosenthal [9].

REMARK 1.4. Clearly, any reflection A can be written as

$$A = I_N - 2\mathbf{x}\mathbf{x}^t \quad \text{for some } \mathbf{x} \in S^{N-1},$$

where I_N denotes the identity matrix of dimension N and S^{N-1} denotes the unit sphere in $\mathbf{R}^N$. The product of two reflections $(I - 2\mathbf{x}\mathbf{x}^t)(I - 2\mathbf{y}\mathbf{y}^t)$ is a

rotation by twice the angle θ between $\mathbf{x}$ and $\mathbf{y}$, in the two-dimensional subspace of $\mathbf{R}^N$ spanned by $\mathbf{x}$ and $\mathbf{y}$. It follows that $d\mu_2 = d(\mu \star \mu) = C_*(d\vartheta \otimes c_N(\sin\theta/2)^{N-2}\, d\theta)$, where C denotes the conjugation map $C\colon \mathrm{O}(N) \times \mathrm{SO}(2) \to \mathrm{SO}(N)$, $C(A, R_\theta) = A\,\mathrm{diag}(R_\theta, 1, \ldots, 1)A^t$ [and R_θ denotes the element $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \in \mathrm{SO}(2)$.] Considering only even times k, we can view the random reflections problem also as a type of "random rotations" (with step distribution μ_2) on $\mathrm{SO}(N)$ (for which our analysis shows that a cut-off occurs at $\frac{1}{4}N \log N$). We will take this route in proving our results.

Rosenthal [9] analyzed the random rotations problem on $\mathrm{SO}(N)$ whose step distribution μ^{θ_0} is uniform measure on the set of (two-dimensional) rotations by a fixed but arbitrary angle θ_0. He shows that, in the special case of $\theta_0 = \pi$, a cut-off occurs at $\frac{1}{4}N \log N$.

REMARK 1.5. The speed of convergence in L_2 can depend rather sensitively on μ: consider, instead of μ_2, the step distribution $\overline{\mu}$ defined by $d\overline{\mu} = C_*(d\vartheta \otimes (1/(2\pi))\, d\theta)$; $\overline{\mu}_k$ is not even in L_2 for $k < \mathrm{O}(N^2)$ steps. The proof, which uses Heckman's multiplicity theory, can be found in [7] (Example 1 in Section 4). On the other hand, the proof of Theorem 1.1(a) will show that the L_2-norm of μ_k is already close to 1 for $k = \frac{1}{2}N \log N + cN$ and $c > c_0$.

REMARK 1.6. The study of our random walk on $\mathrm{O}(N)$ was motivated by an application in cryptography. To encrypt speech over telephone lines, one method calls for random 256×256 orthogonal matrices. In this connection, Sloane and Eaton have suggested random reflections as an algorithm for generating "almost" uniformly distributed random orthogonal matrices (see [11]). As the results of this paper show, this algorithm is not the fastest known: Since multiplying an $N \times N$ matrix by a reflection takes on the of order N^2 operations (multiplication and addition), the algorithm by which (loosely put) we choose an orthogonal matrix with probability $\frac{1}{2}$ from μ_k and with probability $\frac{1}{2}$ from μ_{k+1} (where $k \approx \frac{1}{2}N \log N$) requires on the of order $N^3 \log N$ operations to produce close to uniformly distributed random orthogonal matrices. On the other hand, the so-called *subgroup algorithm* (the best known algorithm) requires of order N^3 operations to produce (exactly) uniformly distributed random orthogonal matrices (for a survey of available methods, see [5]).

Random complex and quaternionic reflections. There are natural analogues of random orthogonal reflections in the unitary group $\mathrm{U}(N)$ and the symplectic group $\mathrm{Sp}(n)$. The precise statements and proofs of our results for these groups will be published in a subsequent paper [8].

Random complex reflections. As a natural analogue to random orthogonal reflections, we choose the random walk on the unitary group $\mathrm{U}(N)$ whose

step distribution ν is concentrated on the set of complex reflections (the union of conjugacy classes $\{A\,\mathrm{diag}(e^{i\theta},1,\dots,1)A^*\colon\ A\in \mathrm{U}(N),\ \theta\in[0,2\pi)\}$) and defined by $d\nu = C_*(d\vartheta_{\mathrm{U}(N)}\otimes c_N(\sin\theta/2)^{N-1}\,d\theta)$. Here C is the map C: $\mathrm{U}(N)\times[0,2\pi)\to\mathrm{U}(N)$, $C(A,\theta)=A\,\mathrm{diag}(e^{i\theta},1,\dots,1)A^*$ and $\vartheta_{\mathrm{U}(N)}$ denotes Haar measure on $\mathrm{U}(N)$. (Compare with Remark 1.4.) The result is as follows:

> Random complex reflections exhibit the cut-off phenomenon with threshold $k_0=\frac{1}{2}N\log N$.

REMARK 1.7. As pointed out in Remark 1.5, a "relatively small" change in step distribution can influence the speed of convergence significantly. Consider $\bar\nu$ defined by $d\bar\nu = C_*(d\vartheta_{\mathrm{U}(N)}\otimes(1/(2\pi))\,d\theta)$; $\bar\nu_k$ is not even in L_2 for $k<\mathrm{O}(N^2)$ steps (see [7], Example 2(a) in Section 4).

In joint (unpublished) work with Rosenthal, we have linked the cases of ν and $\bar\nu$ through the finite sequence of measures $\{\nu^a\}_{a\in\{0,1,\dots,N-1\}}$ with $d\nu^a = C_*(d\vartheta_{\mathrm{U}(N)}\otimes c_{N,a}(\sin\theta/2)^a\,d\theta)$. It turns out that ν_k^a is not in L_2 for $k<(N^2-N+1)/(2(a+1))$ steps.

Random quaternionic reflections. We further extend the notion of "random reflections" to the quaternionic case. First, we define a probability measure (call it γ) on $\mathrm{Sp}(1)$.

For any $h\in\mathrm{Sp}(1)$ the eigenvalues are $\exp(\pm i\varphi_h)$, for some $\varphi_h\in[0,2\pi)$ [we identify $\mathrm{Sp}(1)$ with $\mathrm{SU}(2)$]. We define γ to be the probability measure with density proportional to $(\sin\varphi_h/2)^{2n-2}$ with respect to Haar measure on $\mathrm{Sp}(1)$.

We consider the random walk on $\mathrm{Sp}(n)$ whose step distribution η is concentrated on the set of quaternionic reflections (the union of conjugacy classes $\{A\,\mathrm{diag}(h,1,\dots,1)A^*\colon\ A\in\mathrm{Sp}(1),\ h\in\mathrm{Sp}(n)\}$) and defined by $d\eta = C_*(d\vartheta_{\mathrm{Sp}(n)}\otimes d\gamma)$. The result is as follows:

> Random quaternionic reflections exhibit the cut-off phenomenon with threshold $k_0=\frac{1}{2}n\log n$.

See [7], Example 4 in Section 4, for the discussion of a different random walk on $\mathrm{Sp}(n)$ with rather "slow" (if any) convergence in L_2.

Organization. This paper is organized as follows. In Section 2 we present basics on random walks and Fourier analysis used throughout. The necessary background on the representation theory of compact connected Lie groups and on the computation of the required Fourier coefficients is presented in Section 3. We prove Theorem 1.1(a) in Section 4 and Theorem 1.2(a) in Section 5.

2. Random walks and Fourier analysis. A random walk on a group G is determined by its one-step probability distribution μ. The random walk starts at the identity and takes steps according to the measure μ. Thus at time $t=0$ the distribution of the walk is the measure concentrated at the identity: at time $t=1$ it is μ and at time $t=k$ the distribution is μ_k, the

k-fold convolution $\mu\star\mu\star\cdots\star\mu$ of μ:

$$\mu_k = \mu\star\mu_{k-1}.$$

Our interest is the speed of convergence to stationarity (Haar measure) with respect to *total variation distance* (and L_2-distance) for the random walks under consideration. We recall the definition of total variation distance.

DEFINITION 2.1. Let μ and ϑ be two Borel probability measures on a topological space M and let $\mathscr{B}(M)$ be the Borel sigma field of M. The *total variation distance* is defined by

$$\|\mu - \vartheta\|_{\mathrm{TV}} := \sup_{S\in\mathscr{B}(M)} |\mu(S) - \vartheta(S)| = \tfrac{1}{2}|\mu - \vartheta|(M);$$

notice that $\|\mu - \vartheta\|_{\mathrm{TV}}$ is always between 0 and 1.

If μ has density f with respect to ϑ, then

$$\|\mu - \vartheta\|_{\mathrm{TV}} = \tfrac{1}{2}\int_M |f - 1|\, d\vartheta.$$

We now present some basic facts concerning Fourier transforms and the upper bound lemma of Diaconis and Shahshahani [3, 4]. For background on representation theory see, for example, [2, 6, 12]. Let G be a compact Lie group; $\rho_0, \rho_1, \rho_2, \ldots$ are its irreducible unitary representations and $\chi_0, \chi_1, \chi_2, \ldots$ are the corresponding characters.

DEFINITION 2.2. Let ν be a finite measure of G.

(a) The Fourier transform of ν at ρ_i is defined by

$$\hat{\nu}(\rho_i) := \int_G \rho_i(g)\, d\nu(g).$$

(b) The Fourier coefficient of ν at ρ_i is defined by

$$\hat{\nu}(\chi_i) := \operatorname{trace}\hat{\nu}(\rho_i) = \int_G \chi_i(g)\, d\nu(g).$$

Fourier transforms convert convolution to multiplication:

$$\widehat{\nu^1\star\nu^2}(\rho_i) = \widehat{\nu^1}(\rho_i)\widehat{\nu^2}(\rho_i).$$

If ν is conjugate-invariant, that is, if $\nu(gSg^{-1}) = \nu(S)$, for all measurable sets $S \subseteq G$ and for all $g \in G$, a simplification occurs: $\hat{\nu}(\rho_i)$ commutes with $\rho_i(g)$, for all $g \in G$. By Schur's lemma, for each irreducible representation ρ_i, $i = 0, 1, 2, \ldots,$ there exists a scalar r_i such that $\hat{\nu}(\rho_i) = r_i I$. Clearly, $r_i = (\hat{\nu}(\chi_i))/d_i$, where d_i denotes the dimension of the irreducible representation ρ_i. Furthermore,

$$\hat{\nu}_k(\rho_i) = r_i^k I = \left(\frac{\hat{\nu}(\chi_i)}{d_i}\right)^k I$$

and

$$\hat{\nu}_k(\chi_i) = d_i r_i^k = d_i\left(\frac{\hat{\nu}(\chi_i)}{d_i}\right)^k. \tag{1}$$

THEOREM 2.3. *A finite positive measure ν on a compact Lie group G is uniquely determined by its Fourier transform* $(\hat{\nu}(\rho_i),\ i = 0, 1, 2, \dots)$.

This is a consequence of the Peter–Weyl theorem ([2], Chapter III).

COROLLARY 2.4. *If a finite positive measure ν on a compact Lie group G is conjugate-invariant, it is uniquely determined by its Fourier coefficients* $(\hat{\nu}(\chi_i),\ i = 0, 1, 2, \dots)$.

For a given irreducible representation ρ_s of G, let

$$\phi_{jk}^{(s)}, \qquad j, k = 1, 2, \dots, d_s,$$

denote the entry functions, that is, $\rho_s(g) = (\phi_{jk}^{(s)}(g))$. The Schur orthogonality relations assert that, with respect to the usual inner product in $L_2(G)$, the functions $\phi_{jk}^{(s)}$ are orthogonal to each other and of norm $d_s^{-1/2}$. That is

$$\int_G \phi_{jk}^{(s)} \cdot \overline{\phi_{lm}^{(t)}}\, d\vartheta = \delta_{st}\,\delta_{jl}\,\delta_{km}\,d_s^{-1},$$

where ϑ is normalized Haar measure on G and the bar denotes complex conjugation. It follows that the irreducible characters $\chi_0, \chi_1, \chi_2, \dots$ form an orthonormal set of functions in the Hilbert space $L_2(G)$:

$$\int_G \chi_i\, \overline{\chi}_j\, d\vartheta = \delta_{ij}.$$

The following version of the upper bound lemma can be found in [9].

LEMMA 2.5 (Upper bound lemma). *Let G be a compact Lie group, let ϑ be its normalized Haar measure and let ν be a conjugate-invariant probability measure on G. Set $l_i := \hat{\nu}(\chi_i)$. Then*

$$\|\nu - \vartheta\|_{\mathrm{TV}}^2 \le \tfrac{1}{4}\left(\sum_{i=0}^{\infty} |l_i|^2 - 1\right).$$

3. Irreducible representations and characters of SO(N). As mentioned in Remark 1.4, we will prove our upper and lower bound results (Theorems 1.1 and 1.2) by viewing our random reflections problem on O(N) as a random walk on SO(N) with step distribution μ_2. To apply Fourier methods, we must compute the Fourier coefficients $\hat{\mu}_2(\chi_i)$ for all irreducible representations ρ_i of SO(N).

In the following we cite, without proofs, basic facts from the classical (Cartan–Weyl) representation theory of compact connected Lie groups. For more details and proofs, see [2, 6, 12]. We limit the background presented here to those features of the theory necessary for the computation of the Fourier coefficients and the dimensions of the representations.

A compact connected Lie group G possesses countably many nonisomorphic irreducible representations. They are all finite dimensional. For each G,

there exists a one-to-one correspondence between the integral lattice points in a certain region C^+ of Euclidean space $\mathbf{R}^n$ (the *fundamental Weyl chamber*) and the irreducibles of the group. Given an irreducible ρ of G, the corresponding lattice point ω in C^+ is the *highest weight* of this representation. The sum of the highest weight ω and a fixed vector ψ (half the sum of the *positive roots*) serves as an index for the irreducible representation ρ. For example, for the group $\mathrm{SO}(N)$ with $N = 2n + 1$ odd, the integer lattice points in the fundamental Weyl chamber C^+, that is, the collection of highest weights, is the set of weakly increasing nonnegative integers

$$\{\omega \in \mathbf{N}_0^n : 0 \le \omega_1 \le \omega_2 \le \cdots \le \omega_n\}$$

and half the sum of the positive roots is the fixed vector

$$\psi = \left(\frac{1}{2}, \frac{3}{2}, \ldots, \frac{2n-1}{2}\right).$$

We can therefore index the irreducibles of $\mathrm{SO}(N)$ with N odd by n-tuples λ of strictly increasing half integers (odd multiples of $\frac{1}{2}$). For $N = 2n$ even, the collection of highest weights is the set

$$\{\omega \in \mathbf{Z}^n : |\omega_1| \le \omega_2 \le \cdots \le \omega_n\},$$

whereas half the sum of the positive roots is in this case the fixed vector

$$\psi = (0, 1, 2, \ldots, n-1).$$

The irreducibles of $\mathrm{SO}(N)$ with N even can therefore be indexed by n-tuples λ of integers with $|\lambda_1| < \lambda_2 < \cdots < \lambda_n$.

Let R_φ denote the two-dimensional rotation matrix

$$R_\varphi = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix},$$

let $R^{n,1}_{\varphi_1,\ldots,\varphi_n} \in \mathrm{SO}(2n+1)$ denote the block diagonal matrix

$$R^{n,1}_{\varphi_1,\ldots,\varphi_n} = \mathrm{diag}\big(R_{\varphi_1}, \ldots, R_{\varphi_n}, 1\big)$$

and let $R^{n}_{\varphi_1,\ldots,\varphi_n} \in \mathrm{SO}(2n)$ denote the block diagonal matrix

$$R^{n}_{\varphi_1,\ldots,\varphi_n} = \mathrm{diag}\big(R_{\varphi_1}, \ldots, R_{\varphi_n}\big).$$

The subgroups $\{R^{n,1}_{\varphi_1,\ldots,\varphi_n} : \varphi_i \in [0, 2\pi),\ 1 \le i \le n\}$ of $\mathrm{SO}(2n+1)$ and $\{R^{n}_{\varphi_1,\ldots,\varphi_n} : \varphi_i \in [0, 2\pi),\ 1 \le i \le n\}$ of $\mathrm{SO}(2n)$ are *maximal tori* of $\mathrm{SO}(2n+1)$ and $\mathrm{SO}(2n)$, respectively. Each element in $\mathrm{SO}(N)$ is conjugate to an element in the maximal torus. Since characters are class functions, it suffices to have a formula for the restriction of each irreducible character to the maximal torus.

The Weyl character formula for $\mathrm{SO}(N)$.

(a) $N = 2n + 1$. The irreducible representations of $\mathrm{SO}(N)$ can be indexed by n-tuples of half integers (i.e., odd multiples of $\frac{1}{2}$) $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_n)$

with $\frac{1}{2} \le \lambda_1 < \lambda_2 < \cdots < \lambda_n$. The value of the irreducible character χ_λ at an element in the maximal torus is

$$(2)\quad \chi_\lambda\big(R^{n,1}_{\varphi_1,\dots,\varphi_n}\big) = \frac{\sum_{\sigma\in S_n}\sum_{\varepsilon_m=\pm 1}\operatorname{sgn}(\sigma)\big(\prod_{i=1}^n \varepsilon_i\big)\exp\big(i\sum_{j=1}^n \varepsilon_j\lambda_{\sigma(j)}\varphi_j\big)}{\prod_{1\le r<s\le n} 2i\sin\big(\frac{1}{2}(\varphi_s \pm \varphi_r)\big)\prod_{1\le r\le n} 2i\sin\big(\frac{1}{2}\varphi_r\big)}.$$

Here S_n denotes the symmetric group, $\operatorname{sgn}(\sigma)$ denotes the sign of the permutation σ and $\sum_{\varepsilon_m=\pm 1}$ indicates summation over all choices of $\varepsilon_1 = \pm 1, \dots, \varepsilon_n = \pm 1$.

(b) $N = 2n$. The irreducible representations of $\mathrm{SO}(N)$ can be indexed by n-tuples of integers $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_n)$ with $|\lambda_1| < \lambda_2 < \cdots < \lambda_n$. The value of the irreducible character χ_λ at an element in the maximal torus is

$$(3)\qquad \chi_\lambda\big(R^{n}_{\varphi_1,\dots,\varphi_n}\big) = \frac{\sum_{\sigma\in S_n}\sum^*_{\varepsilon_m=\pm 1}\operatorname{sgn}(\sigma)\exp\big(i\sum_{j=1}^n \varepsilon_j\lambda_{\sigma(j)}\varphi_j\big)}{\prod_{1\le r<s\le n} 2i\sin\big(\frac{1}{2}(\varphi_s \pm \varphi_r)\big)}.$$

Here $\sum^*$ indicates summation over those choices of $\varepsilon_1 = \pm 1, \dots, \varepsilon_n = \pm 1$ for which $\prod_j \varepsilon_j = 1$.

The dimension d_λ of an irreducible representation ρ_λ is given by *Weyl's dimension formula*:

$$(4)\qquad d_\lambda = \lim_{\substack{\varphi_i\to 0\\ 1\le i\le n}} \chi_\lambda\big(R^{n,1}_{\varphi_1,\dots,\varphi_n}\big) = \prod_{\alpha\in R^+}\frac{\langle \alpha, \lambda\rangle}{\langle \alpha, \psi\rangle}$$

[similarly for $\mathrm{SO}(2n)$]. Here R^+ denotes the set of positive roots and $\langle \cdot, \cdot \rangle$ denotes the usual Euclidean inner product. In the case of $\mathrm{SO}(2n+1)$, $R^+ = \{e_j \pm e_i\colon 1 \le i < j \le n\} \cup \{e_i\colon 1 \le i \le n\}$, where e_i denotes the jth standard basis element of $\mathbf{R}^n$. In the case of $\mathrm{SO}(2n)$, $R^+\{e_j \pm e_i\colon 1 \le i < j \le n\}$. The following proposition is an immediate consequence of the Weyl dimension formula.

PROPOSITION 3.1. *Let d_λ denote the dimension of the irreducible representation ρ_λ of $\mathrm{SO}(N)$ corresponding to the index $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_n)$. Then for $N = 2n+1$, $n \ge 1$,*

$$(5)\qquad d_\lambda = \frac{2^n}{1!3!\cdots(2n-1)!}\left(\prod_{i=1}^n \lambda_i\right)\prod_{1\le r<s\le n}\big(\lambda_s^2 - \lambda_r^2\big)$$

and for $N = 2n$, $n \ge 2$,

$$(6)\qquad d_\lambda = \frac{2^{n-1}}{0!2!\cdots(2n-2)!}\prod_{1\le r<s\le n}\big(\lambda_s^2 - \lambda_r^2\big).$$

The main goal of this section is to compute the Fourier coefficients $\hat{\mu}_2(\chi_\lambda) = \int_{\mathrm{SO}(N)} \chi_\lambda(g)\, d\mu_2(g)$, for each index λ. Recall (see Remark 1.4) that μ_2 is the probability measure concentrated on the set of two-dimensional rotations [i.e., the union of conjugacy classes $\{AR^{n,1}_{\varphi,0,\dots,0}A^t\colon A \in \mathrm{SO}(2n+1),\ \varphi \in [0, 2\pi)\}$, similarly for $\mathrm{SO}(2n)$] induced from Haar measure on $\mathrm{SO}(N)$ and the

probability measure with density proportional to $(\sin \varphi/2)^{N-2}$ on $[0, 2\pi)$. Our first step is to compute the character value for each irreducible character at a two-dimensional rotation by the fixed angle φ. We then integrate this function of φ against the measure on $[0, 2\pi)$. For brevity, we will from now on write $\chi_\lambda(\varphi)$ instead of $\chi_\lambda(R^{n,1}_{\varphi,0,\dots,0})$ or $\chi_\lambda(R^{n}_{\varphi,0,\dots,0})$.

LEMMA 3.2. (a) *For $N = 2n + 1$ odd and any index λ,*

$$\chi_\lambda(\varphi) = \sum_{j=1}^{n} (-1)^{j-1} \frac{\sin(\lambda_j \varphi)}{2^{N-3}(\sin \varphi/2)^{N-2}} d_{\hat{\lambda}_j}^{N-2}, \tag{7}$$

(b) *For $N = 2n$ even and any index λ,*

$$\chi_\lambda(\varphi) = \sum_{j=1}^{n} (-1)^{j-1} \frac{\exp(i\lambda_j \varphi)}{2^{N-3}(\sin \varphi/2)^{N-2}} d_{\hat{\lambda}_j}^{N-2}. \tag{8}$$

Here $d_{\hat{\lambda}_j}^{N-2}$ denotes the dimension of the irreducible of $\mathrm{SO}(N-2)$ corresponding to the index $(\lambda_1, \dots, \hat{\lambda}_j, \dots, \lambda_n)$ (and the hat symbol means deletion).

PROOF. (a) $N = 2n + 1$. Use (2) and set $\varphi_1 = \varphi$. Eventually we will take the limit $\varphi_r \to 0$, for $2 \le r \le n$. We can rewrite the numerator in (2) as

$$\sum_{j=1}^{n} (-1)^{j-1} \left[\exp(i\lambda_j \varphi) - \exp(-i\lambda_j \varphi)\right] \times \sum_{\substack{\varepsilon_s = \pm 1 \\ 2 \le s \le n}} \sum_{\sigma \in S_{n-1}} \operatorname{sgn}(\sigma) \left(\prod_{s=2}^{n} \varepsilon_s \right) \exp\left(i \sum_{r=2}^{n} \varepsilon_r \lambda_{\sigma(r)} \varphi_r \right),$$

where, for brevity, we have written S_{n-1} for the set of maps from $\{2, \dots, n\}$ onto $\{1, \dots, \hat{j}, \dots n\}$. We can view such a map σ as a permutation of $\{2, \dots, n\}$ under the order preserving identification of $\{2, \dots, n\}$ with $\{1, \dots, \hat{j}, \dots, n\}$, and $\operatorname{sgn}(\sigma)$ denotes the sign of this permutation. Furthermore, we can rewrite the denominator in (2) as

$$2i \sin\frac{\varphi}{2} \prod_{2 \le s \le n} 2i \sin\left(\frac{1}{2}(\varphi_s \pm \varphi) \right) \times \prod_{2 \le k < l \le n} 2i \sin\left(\frac{1}{2}(\varphi_l \pm \varphi_k) \right) \prod_{2 \le k \le n} 2i \sin\frac{\varphi_k}{2}.$$

Taking the quotient of these two expressions and letting $\varphi_r \to 0$, for $2 \le r \le n$, yields (7).

(b) $N = 2n$. Use (3) and again set $\varphi_1 = \varphi$. Using the same notational convention as above, we can rewrite the numerator in (3) as

$$\sum_{j=1}^{n} (-1)^{j-1} \exp(i\lambda_j \varphi) \sum_{\substack{\varepsilon_r = \pm 1 \\ 2 \le r \le n}} \sum_{\sigma \in S_{n-1}} \operatorname{sgn}(\sigma) \exp\left(i \sum_{r=2}^{n} \varepsilon_r \lambda_{\sigma(r)} \varphi_r \right).$$

Similarly, the denominator in (3) can be written as

$$D \cdot \prod_{2 \le s \le n} 2i \sin\left(\tfrac{1}{2}(\varphi_s \pm \varphi)\right),$$

where

$$D = \prod_{2 \le k < l \le n} 2i \sin\left(\tfrac{1}{2}(\varphi_l \pm \varphi_k)\right).$$

Note that the second summation in the numerator can be rewritten as

$$\sum_{\substack{\varepsilon_r = \pm 1 \\ 2 \le r \le n}} \left(\sum_{\sigma \in S_{n-1}} \cdots \right) = \sum_{\substack{\varepsilon_r = \pm 1 \\ 2 \le r \le n}}^{*} \cdots + \sum_{\substack{\varepsilon_r = \pm 1 \\ 2 \le r \le n}}^{\cdot} \cdots$$

with Σ^* denoting summation over all even numbers of sign changes and $\Sigma^{\cdot}$ denoting summation over all odd numbers of sign changes. Clearly,

$$\lim_{\substack{\varphi_r \to 0 \\ 2 \le r \le n}} \frac{\Sigma^*_{\varepsilon_r = \pm 1,\, 2 \le r \le n} \cdots}{D} = d_{\hat{\lambda}_j}^{N-2}.$$

Also,

$$\lim_{\substack{\varphi_r \to 0 \\ 2 \le r \le n}} \frac{\Sigma^*_{\varepsilon_r = \pm 1,\, 2 \le r \le n} \cdots - \Sigma^{\cdot}_{\varepsilon_r = \pm 1,\, 2 \le r \le n} \cdots}{D} = 0.$$

This follows from the fact that

$$\lim_{\substack{\varphi_r \to 0 \\ 2 \le r \le n}} \frac{\Sigma^*_{\varepsilon_r = \pm 1,\, 2 \le r \le n} \cdots - \Sigma^{\cdot}_{\varepsilon_r = \pm 1,\, 2 \le r \le n} \cdots}{D \prod_{r=2}^{n} 2i \sin \varphi_r}$$

is the dimension of the irreducible representation of the *symplectic group* $\mathrm{Sp}(n-1)$ corresponding to the index $(\lambda_1, \ldots, \hat{\lambda}_j, \ldots, \lambda_n)$ (and as such is a positive integer). It follows that

$$\lim_{\substack{\varphi_r \to 0 \\ 2 \le r \le n}} \frac{\Sigma^*_{\varepsilon_r = \pm 1,\, 2 \le r \le n} \cdots + \Sigma^{\cdot}_{\varepsilon_r = \pm 1,\, 2 \le r \le n} \cdots}{D} = 2 d_{\hat{\lambda}_j}^{N-2}.$$

Altogether, this yields (8). □

NOTATION. From now on, we will write $a!!$, for $a(a-2)(a-4)\cdots 2$ or $a(a-2)(a-4)\cdots 1$, depending on whether a is even or odd, respectively.

PROPOSITION 3.3. (a) *For $N = 2n+1$ odd and any index λ,*

$$\hat{\mu}_2(\chi_\lambda) = \frac{(2n-1)!!}{0!2!\cdots(2n-2)!2^n} \frac{\prod_{1 \le r < s \le n}\left(\lambda_s^2 - \lambda_r^2\right)}{\prod_{i=1}^{n} \lambda_i}, \tag{9}$$

and for $N = 2n$ even and any index λ,

$$\hat{\mu}_2(\chi_\lambda) = \begin{cases} 0, & \text{for } \lambda \text{ with } \lambda_1 \neq 0, \\ \dfrac{(n-1)!}{1!3!\cdots(2n-3)!} \displaystyle\prod_{2 \le r < s \le n} \left(\lambda_s^2 - \lambda_r^2\right), & \text{for } \lambda \text{ with } \lambda_1 = 0. \end{cases} \tag{10}$$

PROOF. We must compute

$$\hat{\mu}_2(\chi_\lambda) = c_N \int_0^{2\pi} \chi_\lambda(\varphi) \left(\sin\frac{\varphi}{2}\right)^{N-2} d\varphi$$

with

$$c_N = \begin{cases} \dfrac{(N-2)!!}{(N-3)!!}\dfrac{1}{4}, & \text{for } N = 2n+1 \text{ odd}, \\ \dfrac{(N-2)!!}{(N-3)!!}\dfrac{1}{2\pi}, & \text{for } N = 2n \text{ even}. \end{cases}$$

(a) $N = 2n+1$. Note that $\int_0^{2\pi} \sin \lambda_j \varphi \, d\varphi = 2/\lambda_j$, for all half integers λ_j. From this and the dimension formula (5), applied to d_j^{N-2}, we get

$$\hat{\mu}_2(\chi_\lambda) = \frac{c_N}{1!3!\cdots(2n-3)!2^n} \sum_{j=1}^{n} (-1)^{j-1} \frac{1}{\lambda_j} \left(\prod_{\substack{1 \le i \le n \\ i \ne j}} \lambda_i \right) \prod_{\substack{1 \le r < s \le n \\ r,\, s \ne j}} (\lambda_s^2 - \lambda_r^2).$$

We rewrite the sum in this expression as

$$\frac{1}{\prod_{i=1}^n \lambda_i} \sum_{j=1}^{n} (-1)^{j-1} \left(\prod_{\substack{1 \le i \le n \\ i \ne j}} \lambda_i^2 \right) \prod_{\substack{1 \le r < s \le n \\ r,\, s \ne j}} (\lambda_s^2 - \lambda_r^2),$$

which, by a familiar formula for the Vandermonde determinant, is equal to

$$\frac{1}{\prod_{i=1}^n \lambda_i} \prod_{1 \le r < s \le n} (\lambda_s^2 - \lambda_r^2).$$

Simplifying constants yields (9).

(b) $N = 2n$. Clearly, $\int_0^{2\pi} \exp(i\lambda_j \varphi)\, d\varphi = 0$, for $\lambda_j \ne 0$, and 2π, for $\lambda_j = 0$ (recall that the λ_j are nonnegative integers). It follows that in this case

$$\begin{aligned} \hat{\mu}_2(\chi_\lambda) &= c_N \frac{\pi}{2^{N-4}} d_{\hat{\lambda}_1}^{N-2} \\ &= \frac{(N-2)!!}{(N-3)!!} \frac{1}{0!2!\cdots(2n-4)!2^{n-1}} \prod_{2 \le r < s \le n} (\lambda_s^2 - \lambda_r^2). \end{aligned}$$

Simplifying constants yields (10). □

4. Proof of Theorem 1.1. Here we follow the outline of the proof of Theorem 2.2 in [9].

The case $N = 2n+1$ odd. Let

$$r_\lambda := \frac{\hat{\mu}_2(\chi_\lambda)}{d_\lambda}.$$

By Lemma 2.5 and (1) it suffices to show that for any integer $n \ge 8$ and any positive real number $c \ge c_0$, where c_0 is some universal positive constant,

$$\sum_\lambda (r_\lambda)^k d_\lambda^2 - 1 \le 451 e^{-c/4.5},$$

for $k = n \log n + cn$. Recall that the sum is over all n-tuples λ of strictly increasing positive half integers. From (5) and (9) we get

$$r_\lambda = \left(\frac{(2n-1)!!}{2^n \prod_{i=1}^n \lambda_i} \right)^2.$$

The following proposition is the crux of the proof of Theorem 1.1.

PROPOSITION 4.1. *For $n \geq 8$ and all indices λ with $\lambda_n \leq 8n$,*

$$(r_\lambda)^{k/2} d_\lambda \leq (15e^{-c/9})^{b_1 + b_2 + \cdots + b_n}.$$

Here $b_i := \lambda_i - (i - \frac{1}{2})$, $1 \leq i \leq n$.

PROOF. We need the following two easy lemmas.

LEMMA 4.2 [9]. *Let $d(T) := d_\lambda$ with $\lambda = (\frac{1}{2}, \frac{3}{2}, \ldots, (2n-3)/2, T)$. Then*

$$\frac{d(T+1)}{d(T)} = \left(1 + \frac{1}{T}\right)\left(1 + \frac{2n-2}{T - n + \frac{3}{2}}\right) \leq 3\left(1 + \frac{2n}{T - n + \frac{3}{2}}\right).$$

LEMMA 4.3. *Let $r(T) := \sqrt{r_\lambda}$ with $\lambda = (\frac{1}{2}, \frac{3}{2}, \ldots, (2n-3)/2, T)$. Then*

$$\frac{r(T+1)}{r(T)} = 1 - \frac{1}{T+1} \leq \exp\left(-\frac{1}{T+1}\right).$$

We now split the proof of Proposition 4.1 into two parts. In Part A we analyze

$$\rho := \frac{d(T+1)r(T+1)^k}{d(T)r(T)^k}$$

and in Part B we prove the full statement.

Part A. From the above lemmas we have

$$\rho = \frac{d(T+1)r(T+1)^k}{d(T)r(T)^k} \leq 3\left(1 + \frac{2n}{T - n + \frac{3}{2}}\right)\exp\left(-\frac{1}{T+1}(n \log n + cn)\right).$$

We now set $b_n^* := T + 1 - (n - \frac{1}{2})$ and analyze

$$\rho \leq 3\left(1 + \frac{2n}{b_n^*}\right)\exp\left[-\frac{n \log n + cn}{n + b_n^*}\right]$$

$$\leq 3\left(\frac{1}{n} + \frac{2}{b_n^*}\right)\exp\left[\frac{b_n^* \log n - cn}{n + b_n^*}\right]$$

in three cases.

Case (a) $1 \le b_n^* \le n/\log n \le n$. Then

$$\rho \le 9\exp\left[\frac{n - cn}{2n}\right] = 9\sqrt{e}\, e^{-c/2} \le 15e^{-c/2}$$

provided $c \ge 1$.

Case (b) $n/\log n \le b_n^* \le 0.5n$. Then

$$\begin{aligned}\rho &\le 3\left(\frac{1}{n} + \frac{2\log n}{n}\right)\exp\left[\frac{0.5n\log n}{n}\right]\exp\left[\frac{-cn}{1.5n}\right]\\ &\le 9\frac{\log n}{n}n^{0.5}e^{-c/1.5} \quad (\text{since } 1 < \log n, \text{ for } n > 3)\\ &= 9\frac{\log n}{n^{0.5}}e^{-c/1.5} \le 7e^{-c/1.5},\end{aligned}$$

for $n \ge 8$ [since $f(x) = \log x/x^{0.5}$ is strictly decreasing for $x \ge 8$].

Case (c) $0.5n \le b_n^* \le 8n$. Write t for b_n^*/n. Then $0.5 \le t \le 8$ and

$$\begin{aligned}\rho &\le \frac{3}{n}\left(1 + \frac{2}{t}\right)\exp\left[\frac{tn\log n - cn}{(1+t)n}\right] = \frac{3}{n}\left(1 + \frac{2}{t}\right)n^{t/(1+t)}\exp\left(-\frac{c}{1+t}\right)\\ &= 3\left(1 + \frac{2}{t}\right)n^{-1/(1+t)}\exp\left(-\frac{c}{1+t}\right) \le 15n^{-1/9}\exp\left(-\frac{c}{9}\right) \le 15\exp\left(-\frac{c}{9}\right).\end{aligned}$$

By (a), (b) and (c), $\rho \le 15e^{-c/9}$ for $n \ge 8$, $k = n\log n + cn$.

Part B. To prove the full statement of Proposition 4.1, proceed as follows. Start with the index $\lambda^0 = (\frac{1}{2}, \frac{3}{2}, \ldots, (2n-1)/2)$, corresponding to the trivial representation, for which $d_{\lambda^0} = r_{\lambda^0} = 1$, and, step by step, increase the last number in this n-tuple by 1 until the desired λ_n from the given index $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_n)$ is reached. Clearly,

$$(r_{\tilde{\lambda}})^{k/2} d_{\tilde{\lambda}} \le (15e^{-c/9})^{b_n},$$

where $b_n := \lambda_n - (n - \frac{1}{2})$ and $\tilde{\lambda} := (\frac{1}{2}, \frac{3}{2}, \ldots, (2n-3)/2, \lambda_n)$. Then repeat this procedure for the $(n-1)$st number in $\tilde{\lambda}$ until the desired λ_{n-1} is reached and so on.

It is not hard to see that in each such unit increment we pick up a factor less than or equal to $15e^{-c/9}$. Indeed, with the notation

$$r(T_i) := \sqrt{r_b}, \qquad d(T_i) := d_b,$$
$$\text{where } b = \left(\frac{1}{2}, \frac{3}{2}, \ldots, \frac{2i-3}{2}, T_i, \lambda_{i+1}, \ldots, \lambda_n\right),$$

we have

$$\frac{r(T_i + 1)}{r(T_i)} = 1 - \frac{1}{T_i + 1} \le 1 - \frac{1}{T_i + 1 + (n - i)} \tag{11}$$

and

$$\begin{aligned}\frac{d(T_i+1)}{d(T_i)} &= \frac{T_i+1}{T_i}\prod_{s=1}^{i-1}\left(\frac{T_i+1-\lambda_s}{T_i-\lambda_s}\right)\prod_{s=1}^{i-1}\left(\frac{T_i+1+\lambda_s}{T_i+\lambda_s}\right)\\ &\quad\times\prod_{s=i+1}^{n}\left(\frac{\lambda_s^2-(T_i+1)^2}{\lambda_s^2-T_i^2}\right)\\ &\le \left(1+\frac{1}{T_i}\right)\prod_{s=1}^{i-1}\left(\frac{T_i+1-\lambda_s}{T_i-\lambda_s}\right)\prod_{s=1}^{i-1}\left(\frac{T_i+1+\lambda_s}{T_i+\lambda_s}\right) \qquad (12)\\ &= \left(1+\frac{1}{T_i}\right)\left(1+\frac{2i-2}{T_i-i+\frac{3}{2}}\right)\\ &\le \left(1+\frac{1}{T_i}\right)\left(1+\frac{2n}{T_i-i+\frac{3}{2}}\right).\end{aligned}$$

Using (11) and (12) and setting $b_i^* := T_i + 1 - (i - \frac{1}{2})$, the proof from Part A goes through with b_n^* replaced by b_i^*, for $1 \le i < n$.

This concludes the proof of Proposition 4.1. □

Writing Q for $(15e^{-c/9})^2$, we now have

$$\sum_{\lambda:\,\lambda_n\le 8n}(d_\lambda)^2(r_\lambda)^k \le \sum_{b_n=0}^{7n+\frac{1}{2}}\sum_{b_{n-1}=0}^{b_n}\cdots\sum_{b_1=0}^{b_2}Q^{b_1+b_2+\cdots+b_n}.$$

Provided we take c larger than some universal constant c_0, the right-hand side of this inequality is less than or equal to

$$\prod_{i=1}^{\infty}\left(\frac{1}{1-Q^i}\right) \le 1+2Q$$

(see [9], page 415). From this we get

$$\sum_{\lambda:\,\lambda_n\le 8n}(d_\lambda)^2(r_\lambda)^k - 1 \le 2Q = 450\,e^{-c/4.5}.$$

We still need to find an upper bound of similar form for the tail sum

$$\sum_{\lambda:\,\lambda_n> 8n}(d_\lambda)^2(r_\lambda)^k.$$

From now on we will denote the m-tuple $(\lambda_1,\ldots,\lambda_n)$ of strictly increasing positive half integers by $\lambda^{(m)}$, for $1 \le m \le n$. Accordingly, we will use

$$d_{\lambda^{(m)}} := \frac{2^m}{1!3!\cdots(2m-1)!}\prod_{i=1}^{m}\lambda_i\prod_{1\le r<s\le m}\left(\lambda_s^2-\lambda_r^2\right)$$

and

$$r_{\lambda^{(m)}} := \left(\frac{(2m-1)!!}{2^m \prod_{i=1}^m \lambda_i} \right)^2,$$

for $1 \le m \le n$. Note that $d_{\lambda^{(n)}} = d_\lambda$ and $r_{\lambda^{(n)}} = r_\lambda$. The following lemma completes the proof of Theorem 1.1.

LEMMA 4.4. *We have*

$$\sum_{\lambda^{(m)}} (d_{\lambda^{(m)}})^2 (r_{\lambda^{(m)}})^k \le 1 + 451 e^{-c/4.5}, \tag{13}$$

for $1 \le m \le n$ *and* $k = n \log n + cn$ *with* $c \ge c_0$.

PROOF. We use induction on m. For $m = 1$,

$$d_{\lambda^{(1)}} = 2\lambda_1, \qquad r_{\lambda^{(1)}} = \frac{1}{\lambda_1^2},$$

for $\lambda_1 = (2i-1)/2$, $i = 1, 2, 3, \ldots$. Therefore,

$$\begin{aligned}
\sum_{\lambda_1} (d_{\lambda^{(1)}})^2 (r_{\lambda^{(1)}})^k &= \sum_{i=1}^{\infty} \frac{1}{(2i-1)^{2k-2}} \\
&= 1 + \sum_{i=2}^{\infty} \frac{1}{(2i-1)^{2k-2}} \le 1 + \sum_{j=3}^{\infty} \frac{1}{j^{2k-2}} \\
&\le 1 + \int_2^{\infty} \frac{1}{x^{2k-2}}\, dx \\
&= 1 + \frac{1}{2k-3} \frac{1}{2^{2k-3}},
\end{aligned}$$

which can easily be seen to be less than $1 + 451 e^{-c/4.5}$, for $n \ge 3$.

Notice that in order to prove (13) for $m > 1$, we need only show that

$$\sum_{\lambda^{(m)}:\, \lambda_m > 8n} (d_{\lambda^{(m)}})^2 (r_{\lambda^{(m)}})^k \le e^{-c/4.5}.$$

Indeed,

$$\sum_{\lambda^{(m)}:\, \lambda_m \le 8n} (d_{\lambda^{(m)}})^2 (r_{\lambda^{(m)}})^k \le 1 + 450 e^{-c/4.5}$$

follows from the first part of our proof:

Proposition 4.1 still holds if we replace d_λ by $d_{\lambda^{(m)}}$ and r_λ by $r_{\lambda^{(m)}}$, because —with the obvious notation carried over from the first part—the statements of Lemmas 4.2 and 4.3 become

$$\frac{d^{(m)}(T+1)}{d^{(m)}(T)} \le 3\left(1 + \frac{2m}{T - m + \frac{3}{2}}\right) \le 3\left(1 + \frac{2n}{T - m + \frac{3}{2}}\right)$$

and

$$\frac{r^{(m)}(T+1)}{r^{(m)}(T)} \le \exp\left(-\frac{1}{T+1}\right).$$

The analysis in Part A goes through with b_n^* replaced by $b_m^* := T + 1 - (m - \frac{1}{2})$, and similarly in Part B with b_i^*, for $1 \le i < m$.

From the definitions of $d_{\lambda^{(m)}}$ and $r_{\lambda^{(m)}}$ we also see that

$$d_{\lambda^{(m)}} \le \frac{2}{(2m-1)!}\lambda_m^{2m-1} d_{\lambda^{(m-1)}} \le \lambda_m^{2m-1} d_{\lambda^{(m-1)}}$$

and

$$r_{\lambda^{(m)}} = \left(\frac{2m-1}{2\lambda_m}\right)^2 r_{\lambda^{(m-1)}} \le \frac{m^2}{\lambda_m^2} r_{\lambda^{(m-1)}},$$

for $2 \le m \le n$.

We now have

$$\sum_{\lambda^{(m)}:\ \lambda_m > 8n} (d_{\lambda^{(m)}})^2 (r_{\lambda^{(m)}})^k \le \left[\sum_{\lambda_m > 8n} \left(\frac{m}{\lambda_m}\right)^{2k} \lambda_m^{4m-2}\right] \sum_{\lambda^{(m-1)}} (d_{\lambda^{(m-1)}})^2 (r_{\lambda^{(m-1)}})^k.$$

By our induction hypothesis,

$$\sum_{\lambda^{(m-1)}} (d_{\lambda^{(m-1)}})^2 (r_{\lambda^{(m-1)}})^k \le 1 + 451 e^{-c/4.5}.$$

Since $c \ge c_0$, the value $1 + 451\ e^{-c/4.5}$ is smaller than some constant, say, 2. Then

$$\begin{aligned}\sum_{\lambda^{(m)}:\ \lambda_m > 8n} (d_{\lambda^{(m)}})^2 (r_{\lambda^{(m)}})^k &\le 2 \sum_{\lambda_m > 8n} \left(\frac{m}{\lambda_m}\right)^{2k} \lambda_m^{4m-2} \\ &\le 2n^{2k} \int_{8n-\frac{1}{2}}^{\infty} \frac{1}{x^{2k-4n+2}}\, dx.\end{aligned}$$

Since $2k - 4n + 2 \ge 2n \log n - 4n + 2 > 2$, for $n \ge 8$,

$$\begin{aligned}2n^{2k} \int_{8n-\frac{1}{2}}^{\infty} \frac{1}{x^{2k-4n+2}}\, dx &= 2n^{2k} \frac{1}{2k-4n+1} \left(8n - \frac{1}{2}\right)^{-2k+4n-1} \\ &< 2n^{2k} \left(8n - \frac{1}{2}\right)^{-2k+4n-1}\end{aligned}$$

and

$$\sum_{\lambda^{(m)}:\,\lambda_m > 8n} (d_{\lambda^{(m)}})^2 (r_{\lambda^{(m)}})^k$$
$$< 2n^{2k}\left(8n - \frac{1}{2}\right)^{-2k+4n-1}$$
$$= \exp\left[\log 2 + 2k \log n - (2k - 4n + 1)\log\left(8n - \frac{1}{2}\right)\right]$$
$$= \exp\left[(4n-1)\left[\log n + \log\left(8 - \frac{1}{2n}\right)\right]\right.$$
$$\left. -(2n \log n + 2cn)\cdot \log\left(8 - \frac{1}{2n}\right) + \log 2\right].$$

Considering that $2.07 \le \log(8 - 1/2n) \le 2.08$, for $n \ge 8$, we get

$$\sum_{\lambda^{(m)}:\,\lambda_m > 8n} (d_{\lambda^{(m)}})^2 (r_{\lambda^{(m)}})^k \le \exp[-0.14\ n \log n + 8.32n - 4cn - \log n - 1]$$
$$\le e^{-c/4.5}.$$

Since $-0.14\ n \log n + 8.32n - 4cn - \log n - 1 \le -c/4.5$ clearly holds for $n \ge 8$, $c \ge c_0$. □

Thus we have completed the proof of Theorem 1.1 for the case $N = 2n + 1$ odd.

The case $N = 2n$ even. Most steps from the proof for the case $N = 2n + 1$ carry over directly to this case. In fact, the overall outline of the proof is the same; we only need to make a few minor alterations. From (6) and (10) we get

$$r_\lambda = \left(\frac{(m-1)!}{\prod_{i=2}^n \lambda_i}\right)^2,$$

for λ with $\lambda_1 = 0$; otherwise $r_\lambda = 0$. We then must prove that for all $n \ge 8$ and $c \ge c_0$,

$$\sum_{\lambda:\,\lambda_1 = 0} (r_\lambda)^k (d_\lambda)^2 - 1 \le 451 e^{-c/4.5}.$$

Recall that $\lambda_2, \ldots, \lambda_n$ are integers with $1 \le \lambda_2 < \lambda_3 < \cdots < \lambda_n$. The index $\lambda^0 = (0, 1, 2, \ldots, n-1)$ corresponds to the trivial representation of $\mathrm{SO}(N)$ and we get, of course, $r_{\lambda^0} = d_{\lambda^0} = 1$. Lemmas 4.2 and 4.3 have the following analogues:

LEMMA 4.2′. *Let $d(T) := d_\lambda$ with $\lambda = (0, 1, 2, \ldots, n-2, T)$. Then*

$$\frac{d(T+1)}{d(T)} = \left(1 + \frac{1}{T}\right)\cdot\left(1 + \frac{2n-3}{T-n+2}\right) \le 2\cdot\left(1 + \frac{2n}{T-n+2}\right).$$

LEMMA 4.3′. *Let* $r(T) := \sqrt{r_\lambda}$ *with* $\lambda = (0, 1, 2, \ldots, n-2, T)$. *Then*

$$\frac{r(T+1)}{r(T)} = 1 - \frac{1}{T+1} \le \exp\left(-\frac{1}{T+1}\right).$$

With $b_n^* := T + 1 - (n-1)$ and $b_i^* := T_i + 1 - (i-1)$ for $1 \le i < n$, Parts A and B of the above proof clearly go through to yield the following analogue of Proposition 4.1:

PROPOSITION 4.1′. *For all indices* λ *and* $\lambda_1 = 0$ *and* $\lambda_n \le 8n$,

$$(r_\lambda)^{k/2} d_\lambda \le (15e^{-c/9})^{b_1 + b_2 + \cdots + b_n}.$$

Here $b_i := \lambda_i - (i-1)$, $1 \le i \le n$.

We therefore have, as in the case N odd,

$$\sum_{\substack{\lambda:\ \lambda_1 = 0 \\ \lambda_n \le 8n}} (d_\lambda)^2 (r_\lambda)^k - 1 \le 450\, e^{-c/4.5}.$$

As for the upper bound for the tail sum by $e^{-c/4.5}$, we again prove by induction on m that

$$\sum_{\lambda^{(m)}:\ \lambda_1 = 0} (d_{\lambda^{(m)}})^2 (r_{\lambda^{(m)}})^k \le 1 + 451\, e^{-c/4.5} \quad \text{for } 1 \le m \le n,$$

where

$$d_{\lambda^{(m)}} := \frac{2^{m-1}}{0!2!\cdots(2m-2)!} \prod_{1 \le r < s \le m} (\lambda_s^2 - \lambda_r^2)$$

and

$$r_{\lambda^{(m)}} := \left(\frac{(m-1)!}{\prod_{i=2}^m \lambda_i}\right)^2.$$

For the basis of the induction ($m = 1$) we have $d_{\lambda^{(1)}} = 1$ and $r_{\lambda^{(1)}} = 1$, so that

$$\sum_{\lambda^{(1)}:\ \lambda_1 = 0} (d_{\lambda^{(1)}})^2 (r_{\lambda^{(1)}})^k = 1.$$

Also,

$$d_{\lambda^{(m)}} \le \frac{2}{(2m-2)!} \lambda_m^{2m-2} d_{\lambda^{(m-1)}} \le \lambda_m^{2m-2} \cdot d_{\lambda^{(m-1)}},$$

$$r_{\lambda^{(m)}} = \left(\frac{m-1}{\lambda_m}\right)^2 r_{\lambda^{(m-1)}} \le \frac{m^2}{\lambda_m^2} r_{\lambda^{(m-1)}},$$

for $2 \le m \le n$.

The rest is completely analogous to the case N odd. We omit the details. □

5. Proof of Theorem 1.2. Recall that

$$\|\mu_k - \vartheta_+\|_{\mathrm{TV}} = \sup_{S \in \mathscr{B}(\mathrm{SO}(N))} |\mu_k(S) - \vartheta_+(S)|.$$

We will construct a suitable test set S to prove our lower bound result. Briefly, under Haar measure ϑ_+, χ_1, the character of the natural representation, is with high probability close to 0 (in fact, χ_1 is almost distributed as a standard normal random variable for large N). On the other hand, we show that, under μ_k with $k = \frac{1}{2}N \log N - cN$, with high probability χ_1 is still large (close to N). For a suitable positive value B, our test set S can then be chosen to be $S = \{g \in \mathrm{SO}(N)\colon -N \le \chi_1(g) \le B\}$. The idea of this proof is not new. It has been developed by Diaconis and has been applied since then by various authors [3, 9, 10].

By the orthonormality relations for the irreducible characters of a compact Lie group, we have

$$E_{\vartheta_+}(\chi_1) = 0,$$
$$E_{\vartheta_+}(\chi_1^2) = 1 \quad \text{and hence} \quad \mathrm{Var}_{\vartheta_+}(\chi_1) = 1.$$

The N-dimensional natural representation ρ_1 has highest weight $\gamma = (0, \ldots, 0, 1)$ and corresponds to the index $\lambda = (\frac{1}{2}, \ldots, n - \frac{3}{2}, n + \frac{1}{2})$, for $N = 2n + 1$, and $\lambda = (0, 1, \ldots, n - 2, n)$, for $N = 2n$. Thus Proposition 3.3 yields

$$E_{\mu_2}(\chi_1) = N\left(\frac{N-2}{N}\right)^2,$$

and by (1), we have

$$E_{\mu_k}(\chi_1) = N\left(\frac{N-2}{N}\right)^k,$$

for both N even and N odd. We also need a similar expression for $\mathrm{Var}_{\mu_k}(\chi_1) = E_{\mu_k}(\chi_1^2) - [E_{\mu_k}(\chi_1)]^2$. Note that χ_1^2 is the character of the tensor product representation $\rho_1 \otimes \rho_1$. In order to be able to use (1) for the computation of $E_{\mu_k}(\chi_1^2)$, we first need to decompose $\rho_1 \otimes \rho_1$ into its irreducible subrepresentations. We need the following two lemmas (see, e.g., [2], Chapter VI).

LEMMA 5.1. *Let χ_γ denote the character of the irreducible representation corresponding to highest weight λ. Then*

$$\chi_\gamma \chi_\omega = \chi_{\gamma+\omega} + \sum_\nu n_\nu \chi_\nu,$$

where the sum is over $\nu < \gamma + \omega$ with respect to the usual ordering of weights and the coefficients n_ν are all in $\mathbf{N}_0$.

LEMMA 5.2. *Let χ_γ denote the character of the irreducible representation corresponding to highest weight γ. Let α be a* simple root. *If $\langle \gamma, \alpha \rangle$ and*

$\langle \omega, \alpha \rangle$ are both not zero, where $\langle \gamma, \alpha \rangle := \sum_{j=1}^{n} \gamma_j \alpha_j$, then $\gamma + \omega - \alpha$ is a highest weight,

$$\chi_\gamma \chi_\omega = \chi_{\gamma+\omega} + \chi_{\gamma+\omega-\alpha} + \textit{others},$$

and $\chi_{\gamma+\omega-\alpha}$ occurs with multiplicity 1.

Lemma 5.1 tells us that $\rho_1 \otimes \rho_1$ contains exactly one copy of the irreducible representation of highest weight $\gamma + \gamma = (0, 0, \ldots, 0, 2)$. This irreducible representation of $\mathrm{SO}(N)$, call it ρ_2, corresponds to the index $\lambda = (\frac{1}{2}, \frac{3}{2}, \ldots, n - \frac{3}{2}, n + \frac{3}{2})$, for $N = 2n + 1$, and $\lambda = (0, 1, 2, \ldots, n - 2, n + 1)$, for $N = 2n$, and is of dimension $d_2 = (N(N + 1))/2 - 1$ (use Proposition 3.1). Using Proposition 3.3, we compute

$$E_{\mu_2}(\chi_2) = \left[\frac{N(N+1)}{2} - 1\right]\left(1 - \frac{4}{N+2}\right)^2.$$

Next, note that the simple root $\alpha = (0, \ldots, 0, -1, 1)$ (for N even and N odd) clearly fulfills the conditions of Lemma 5.2. It follows that $\rho_1 \otimes \rho_1$ contains exactly one copy of the irreducible representation of $\mathrm{SO}(N)$ of highest weight $\lambda = (0, \ldots, 0, 1, 1)$. We call this representation ρ_3. It corresponds to the index $\lambda = (\frac{1}{2}, \ldots, n - \frac{5}{2}, n - \frac{1}{2}, n + \frac{1}{2})$, for $N = 2n + 1$ odd, and to the index $\lambda = (0, 1, \ldots, n - 3, n - 1, n)$, for $N = 2N$ even, and is of dimension $d_3 = (N(N - 1))/2$. Using Proposition 3.3 we compute

$$E_{\mu_2}(\chi_3) = \frac{N(N-1)}{2}\left(1 - \frac{4}{N}\right)^2.$$

Finally, from the fact that $E_{\vartheta_+}(\chi_1^2) = 1$ and by the orthonormality of the irreducible characters, we see that $\rho_1 \otimes \rho_1$ contains exactly one copy of the trivial representation ρ_0.

We have established the decomposition

$$\rho_1 \otimes \rho_1 = \rho_0 \oplus \rho_2 \oplus \rho_3$$

into irreducibles, and hence

$$\chi_1^2 = 1 + \chi_2 + \chi_3.$$

Therefore,

$$E_{\mu_k}(\chi_1^2) = 1 + E_{\mu_k}(\chi_2) + E_{\mu_k}(\chi_3).$$

Altogether, we get for $\mathrm{Var}_{\mu_k}(\chi_1)$,

$$\mathrm{Var}_{\mu_k}(\chi_1) = 1 + \left[\frac{N^2 - N}{2}\right]\left(1 - \frac{4}{N}\right)^k + \left[\frac{N^2 + N}{2} - 1\right]\left(1 - \frac{4}{N+2}\right)^k - N^2\left(1 - \frac{2}{N}\right)^{2k}.$$

PROPOSITION 5.3. *For $N \geq 8$ and even integer $k = \frac{1}{2}N \log N - cN$, where $c > 0$:*

(a) $E_{\mu_k}(\chi_1) \geq 0.7e^{2c}$.
(b) $\mathrm{Var}_{\mu_k}(\chi_1) \leq 1 + (17/3)e^{4c}(\log N/N^{3/5})$.

PROOF. (a) Recall $E_{\mu_k}(\chi_1) = N(1 - 2/N)^k$. With $k = \frac{1}{2}N \log N - cN$ we have

$$\begin{aligned} N(1 - 2/N)^k &= N(1 - 2/N)^{N/2 \log N}(1 - 2/N)^{-cN} \\ &\geq N\left(1 - \frac{2}{N}\right)^{N/2 \log N} e^{2c}, \end{aligned}$$

for $N \geq 2$, since $0 \leq 1 - x \leq e^{-x}$, for $x \leq 1$. However,

$$\log\left(1 - \frac{2}{N}\right) = -\frac{2}{N} - \frac{2^2}{2N^2} - \frac{2^3}{3N^3} - \cdots \geq -\frac{2}{N} - \frac{2}{N^2}\left(\frac{1}{1 - 2/N}\right)$$

and so

$$\begin{aligned} N\left(1 - \frac{2}{N}\right)^{N/2 \log N} &= N \exp\left(\log\left(1 - \frac{2}{N}\right) \cdot \frac{1}{2}N \log N\right) \\ &\geq N^{-1/(N-2)}. \end{aligned}$$

The function $f(x) = x^{-1/(x-2)}$ is an increasing function for, say, $x \geq 8$. Therefore, $N^{-1/(N-2)} \geq 0.7$ for $N \geq 8$ and $E_{\mu_k}(\chi_1) \geq 0.7e^{2c}$.

(b) We have

$$\begin{aligned} \mathrm{Var}_{\mu_k}(\chi_1) &= 1 + \left(\frac{N^2 - N}{2}\right)\left(1 - \frac{4}{N}\right)^k \\ &\quad + \left(\frac{N^2 + N}{2} - 1\right)\left(1 - \frac{4}{N+2}\right)^k - N^2\left(1 - \frac{2}{N}\right)^{2k} \\ &\leq 1 + N^2\left[\left(1 - \frac{4}{N+2}\right)^k - \left(1 - \frac{2}{N}\right)^{2k}\right] \\ &\quad + \frac{N}{2}\left[\left(1 - \frac{4}{N+2}\right)^k - \left(1 - \frac{4}{N}\right)^k\right] \end{aligned}$$

because $(1 - 4/N)^k \leq (1 - 4/(N + 2))^k$.

Furthermore, $(1 - 2/N)^2 > 1 - 4/N$ and therefore

$$\mathrm{Var}_{\mu_k}(\chi_1) \leq 1 + \left(N^2 + \frac{N}{2}\right)\left[\left(1 - \frac{4}{N+2}\right)^k - \left(1 - \frac{4}{N}\right)^k\right].$$

The term $[(1-4/(N+2))^k-(1-4/N)^k]$ can be bounded from above by the use of the mean value theorem:

$$\begin{aligned}
&\left(1-\frac{4}{N+2}\right)^k-\left(1-\frac{4}{N}\right)^k\\
&\quad\le k\left(1-\frac{4}{N+2}\right)^{k-1}\left[\left(1-\frac{4}{N+2}\right)-\left(1-\frac{4}{N}\right)\right]\\
&\quad= k\left(1-\frac{4}{N+2}\right)^k\frac{N+2}{N-2}\frac{8}{N(N+2)}\\
&\quad\le \frac{1}{2}N\log N\exp\left(-\frac{4k}{N+2}\right)\frac{8}{(N-2)N}\\
&\quad= 4\log NN^{-2N/(N+2)}\exp\left(4c\frac{N}{N+2}\right)\frac{N}{N-2}\cdot\frac{1}{N}\\
&\quad\le \frac{16}{3}\log NN^{-2N/(N+2)}\exp(4c)\frac{1}{N}\\
&\quad\le \frac{16}{3}\exp(4c)\frac{\log N}{N^{13/5}},
\end{aligned}$$

for $N\ge 8$. [The function $f(x)=\exp(-2x/(x+2))$ is decreasing. Therefore $\exp(-2N/(N+2))\le\exp(-8/5)$, for $N\ge 8$, and $\exp(-2(N/(N+2))\log N)=N^{-2N/(N+2)}\le N^{-8/5}$, for $N\ge 8$.]

Altogether, we have

$$\mathrm{Var}_{\mu_k}(\chi_1)\le 1+\left(N^2+\frac{N}{2}\right)\frac{16}{3}e^{4c}\log N\frac{1}{N^{13/5}}\le 1+\frac{17}{3}e^{4c}\frac{\log N}{N^{3/5}},$$

and Proposition 5.3 is proved. □

We can now complete the proof of Theorem 1.2. By Chebyshev's inequality,

$$P_{\vartheta_+}(\chi_1>0.35e^{2c})\le 8.2e^{-4c}$$

and

$$P_{\mu_k}(\chi_1\le 0.35e^{2c})\le\frac{1+(17/3)e^{4c}((\log N)/N^{3/5})}{(0.35)^2e^{4c}}\le 8.2e^{-4c}+46.3\frac{\log N}{N^{3/5}},$$

so

$$\begin{aligned}
\|\mu_k-\vartheta_+\|_{\mathrm{TV}}\ge|\mu_k(S)-\vartheta_+(S)|&=\left|P_{\vartheta_+}(\chi_1\le 0.35e^{2c})-P_{\mu_k}(\chi_1\le 0.35e^{2c})\right|\\
&=\left|1-P_{\vartheta_+}(\chi_1>0.35e^{2c})-P_{\mu_k}(\chi_1\le 0.35e^{2c})\right|\\
&\ge 1-16.4e^{-4c}-46.3\frac{\log N}{N^{3/5}}.
\end{aligned}$$

□

Acknowledgment. I thank the referees for their helpful suggestions.

REFERENCES

[1] ALDOUS, D. and DIACONIS, P. (1987). Strong uniform times and finite random walks. *Adv. in Appl. Math.* **8** 69–97.
[2] BRÖCKER, TH. and TOM DIECK, T. (1985). *Representations of Compact Lie Groups*. Springer, New York.
[3] DIACONIS, P. (1977). *Group Representations in Probability and Statistics*. IMS, Hayward, CA.
[4] DIACONIS, P. and SHAHSHAHANI, M. (1986). Products of random matrices as they arise in the study of random walks on groups. *Contemp. Math.* **50** 183–195.
[5] DIACONIS, P. and SHAHSHAHANI, M. (1987). The subgroup algorithm for generating uniform random variables. *Probab. Eng. Inform. Sci.* **1** 15–32.
[6] FULTON, W. and HARRIS, J. (1991). *Representation Theory: A First Course*. Springer, New York.
[7] POROD, U. (1995). L_2-lower bounds for a speical class of random walks. *Probab. Theory Related Fields* **101** 277–289.
[8] POROD, U. (1994). The cut-off phenomenon for random reflections II: complex and quaternionic cases. Preprint.
[9] ROSENTHAL, J. S. (1994). Random rotations: characters and random walks on SO(N). *Ann. Probab.* **22** 398–423.
[10] SALOFF-COSTE, L. (1994). Precise estimates on the rate at which certain diffusions tend to equilibrium. *Math. Z.* **217** 641–677.
[11] SLOANE, N. J. A. (1983). Encrypting by random rotations. *Cryptography. Lecture Notes in Computer Science* **149** 71–128. Springer, New York.
[12] ŽELOBENKO, D. P. (1973). *Compact Lie Groups and Their Representations. AMS Trans. Math. Monographs* **40**. Amer. Math. Soc., Providence, RI.

DEPARTMENT OF STATISTICS
UNIVERSITY OF CALIFORNIA
BERKELEY , CALIFORNIA 94720
E-MAIL: up@chow.mat.jhu.edu