CONVERGENCE OF KAC'S RANDOM WALK

IGOR PAK* AND SERGIY SIDENKO*

Abstract. We study a long standing open problem on the mixing time of Kac's random walk on $SO(n,\mathbb{R})$ by random rotations. We obtain an upper bound mix $= O(n^{2.5}\log n)$ for the weak convergence which is close to the trivial lower bound $\Omega(n^2)$. This improves the upper bound $O(n^4 \log n)$ by Diaconis and Saloff-Coste [9]. The proof is a variation on the coupling technique we develop to bound the mixing time for compact Markov chains, which is of independent interest.

Introduction

The MCMC (Monte Carlo Markov Chain) method has proved extremely powerful and led to remarkable advances in both theory and practice. Despite a large body of literature, finding sharp bounds on the mixing time of finite Markov chains remains technical and exceedingly difficult (see e.g. [5, 17, 23, 28, 29]).

In this paper we study the classical Kac's random walk on $SO(n,\mathbb{R})$ by random rotations in the basis 2-dimensional planes. Our main result is the $O(n^{2.5}\log n)$ mixing time upper bound. This is sharper than previous results and within striking distance from the trivial $\Omega(n^2)$ lower bound. This random walk arose in Kac's effort to simplify Boltzmann's proof of the H-theorem [18] (see also [22]) and Hastings's simulations of random rotations [14]. Most recently, this walk has appeared in the work of Ailon and Chazelle [3] in connection with generating random projections onto subspaces.

Kac's random walk was first rigorously studied by Diaconis and Saloff-Coste [9] who viewed it as a natural example of a Glauber dynamics on $SO(n,\mathbb{R})$. They used a modified comparison technique and proved $O(n^4 \log n)$ upper bound on the mixing time, by reducing the problem to a problem of a random walk with *all* rotations, which was solved earlier by using the character estimates in [27] (see also [26]).

In the wake of the pioneer work [9], there have been a flurry of activity in the subject, aimed especially at finding sharp bounds for the eigenvalues [8, 16, 31]. In [21] Maslin was able to explicitly compute the eigenvalues, but due to the large multiplicity of the highest eigenvalue this work does not improve the mixing time of Kac's random walk, in effect showing the limitation of this approach.

It is worth mentioning that there are several notions of the mixing time in this case, and in contrast with the discrete case, the connections between them is yet to be completely understood. We use here the mixing time in terms of the weak convergence, the same as used by Diaconis and Saloff-Coste in [9].

Our approach is based on the coupling technique, a probabilistic approach which goes back to Doeblin [10] (see also [4, 19, 25]). In recent years, this technique has been further adapted to finite Markov chains, largely on combinatorial objects (see "path coupling" technique in [7, 12]). In this paper we adapt the coupling technique to compact Markov chains. While the coupling on compact groups has been studied earlier [19] (see also references therein), our approach is more general as we allow stopping when two particles are at certain distance from each other.

Let us emphasize that while natural in the context, the continuous coupling we consider does not seem to have known analogues in the context of finite Markov chains (cf. [5, 29]). In conclusion,

Date: April 11, 2007.

*Department of Mathematics, MIT, Cambridge, MA 02139; {pak,sidenko}@math.mit.edu.

let us mention that a related approach is used in [15], which develops a "distance-decreasing" (with good probability) coupling technique. While the particular coupling construction we employ can also be viewed as distance-decreasing in a certain precise sense (for the Frobenius distance on matrices), our setting is more general.

1. Kac's random walk on $SO(n, \mathbb{R})$

1.1. **Main result.**

In this section we will consider the following discrete random walk on $SO(n, \mathbb{R})$. At each step we pick a pair (i, j) of two coordinates such that $1 \le i < j \le n$, and an angle ϕ uniformly distributed on $[0, 2\pi)$. Define an *elementary rotation matrix* $R_\phi^{i,j}$:

$$R_\phi^{i,j} = \begin{pmatrix} 1 & \dots & 0 & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & \cos\phi & \dots & -\sin\phi & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & \sin\phi & \dots & \cos\phi & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \dots & 0 & \dots & 1 \end{pmatrix}$$

which differs from the identity matrix by four entries only with coordinates (i, i), (j, i), (i, j) and (j, j). *Kac's random walk* $\{A_k\}$ on $SO(n, \mathbb{R})$ is now defined as follows:

$$A_{k+1} = R_\phi^{i,j} A_k, \quad \text{for all} \quad k \ge 0,$$

where $A_0 = I$ is the identity matrix. More generally, we can assume that A_0 is chosen from any fixed initial distribution P^0 on $SO(n, \mathbb{R})$ as the upper bound below remains valid in this case.

We endow the group $SO(n, \mathbb{R})$ with the *Frobenius norm* (also called the *Hilbert-Schmidt norm*), denoted $\| \cdot \|_F$ and defined for any real $n \times n$ matrix $M = (m_{ij})$ as follows:

$$\|M\|_F = \sqrt{\sum_{1 \le i,j \le n} m_{ij}^2} = \sqrt{\operatorname{Tr}(MM^T)} = \sqrt{\sum_{1 \le i \le n} |\sigma_i|^2}, \tag{1}$$

where σ_i are the singular values of M. This defines the *Frobenius distance* $\|A - B\|_F$ between every two $n \times n$ matrices A and B.

Let $\operatorname{Lip}(K)$ be a set of all real-valued functions on $SO(n, \mathbb{R})$ such that

$$\|f\|_L = \sup_{x \ne y} \frac{|f(x) - f(y)|}{\|x - y\|_F} \le K.$$

We define the distance $\rho(P, Q)$ for two probability laws P and Q on $SO(n, \mathbb{R})$ as follows:

$$\rho(P, Q) = \sup \left\{ \left| \int f \, d(P - Q) \right| : f \in \operatorname{Lip}(1) \right\}.$$

It is well known (see e.g. [11, §11]) that ρ metrizes the weak convergence of probability laws.[1]

Theorem 1 (Main Theorem)**.** *Let P^t be the distribution of the Kac's random walk after t steps, and let U be the uniform distribution on $SO(n, \mathbb{R})$. Then, for every $\varepsilon > 0$ and*

$$t = \Omega\left(n^{2.5} \log \frac{n}{\varepsilon}\right), \quad \textit{we have} \quad \rho\left(P^t, U\right) \le \varepsilon.$$

[1] Instead of condition $\|f\|_L < 1$, it is common ([9, 11]) to bound $\|f\|_L + \|f\|_\infty$ in order to metrize the weak convergence. However, in our case all Lipschitz functions are bounded because $SO(n, \mathbb{R})$ is bounded in $\|\cdot\|_F$.

The proof of this theorem uses an explicit construction of a "weak coupling" between P^t and U, which enables us to bound $\rho\left(P^t, U\right) \leq \varepsilon$. Our "coupling lemma" is described in the next subsection. The proof of the theorem is presented in Section 2, where it is split into a sequence of lemmas. The latter are mostly technical and are proved in Section 3. We conclude with final remarks in Section 4.

1.2. **Coupling lemma.** The basic goal a of the coupling we construct it to obtain joint distribution on $SO(n,\mathbb{R}) \times SO(n,\mathbb{R})$ such that its marginals are P^t and U, and the distribution is concentrated near the main diagonal. The following lemma makes this precise in a more general setting.

Let $X \subset V$, where V is a metric space with distance $d(\cdot,\cdot)$. Let x_t and y_t, $t \geq 0$, be two Markov processes on X. A coupling is a joint process (x'_t, y'_t) on X^2 such that x'_t has the same distribution as x_t and y'_t has the same distribution as y_t. By abuse of notation we will use (x_t, y_t) to denote the coupling.

Lemma 2 (Coupling lemma)**.** *Let x_t and y_t, $t \geq 0$, be two discrete Markov processes on X as above, with distributions P^t and Q^t after t steps. Suppose there exists a coupling (x_t, y_t), such that for a stopping time*

$$T_\delta = \min\{t \mid d(x_t, y_t) < \delta\}$$

the distance $d(x_t, y_t)$ is non-increasing for $t \geq T_\delta$. Then we have:

$$\rho\left(P^t, Q^t\right) < \delta + \mathbf{P}\left(T_\delta > t\right) \cdot \sup_{x,y\in X} d(x,y).$$

1.3. **Variations on the theme.** As we mentioned in the introduction, Kac's random walk does not converge in the ℓ_2-distance. To see this, observe that after t steps with probability $1/\binom{n}{2}^t$ we rotate in the first two coordinates, so the distribution after t steps is not absolutely continuous. On the other hand, as shown by Diaconis and Saloff-Coste, there is a convergence in the ℓ_1-distance, with the mixing time $O(n^5 \log n)$. It is unclear whether our results can be used to improve this bound as well, and as far as we know, there is no general result establishing a connection in this case.

In a positive direction, our main theorem is robust enough to establish convergence for a number of other matrix distances, such as operator, spectral or trace norms. For example, we easily have:

Corollary 3. *Let $K > 1$ be a fixed constant. Then for every $\varepsilon > 0$, $f \in \mathrm{Lip}(K)$ and $t = \Omega\left(n^{2.5}\log Kn/\varepsilon\right)$ we have:*

$$\left|\int f\, d\left(P^t - U\right)\right| \leq \varepsilon.$$

Proof. Corollary follows from Theorem 1 and the observation that $f/K \in \mathrm{Lip}(1)$. □

More generally, let us give a convergence result in other norm $\|\cdot\|$ on $n\times n$ real matrices. Suppose for a constant $C > 0$ we have:

$$\|x - y\| \geq C\,\|x - y\|_F \qquad \text{for all } \ x, y \in M(n,\mathbb{R}).$$

Corollary 4. *If $\|f\|_L = K$ with respect to the norm $\|\cdot\|$, then for $\varepsilon > 0$ and*

$$t = \Omega\left(n^{2.5}\log\frac{Kn}{C\varepsilon}\right)$$

we have:

$$\left|\int f\, d\left(P^t - U\right)\right| \leq \varepsilon.$$

Proof. For all $x \neq y$ we obtain:

$$\frac{|f(x)-f(y)|}{\|x-y\|} \leq \frac{1}{C}\frac{|f(x)-f(y)|}{\|x-y\|_F}.$$

Hence, $f \in \mathrm{Lip}(K/C)$ with respect to the Frobenius norm. Now Corollary 3 implies the result. □

2. The coupling process

In this section, we construct a coupling process which decreases the Frobenius distance between two random processes with sufficiently high probability. Formally, we show that there is a probability measure on $SO(n,\mathbb{R}) \times SO(n,\mathbb{R})$ with marginals P^t and U which is concentrated near the main diagonal.

Consider now Kac's random walks $\{A_k\}$ and $\{B_k\}$, the former having the initial distribution P^0, and the latter being initially uniformly distributed. It turns out that at each step we are able to choose rotations so that the quantity $\|A_k - B_k\|_F$ is non-increasing whereas the marginal distributions of A_k and B_k remain the same as we chose the rotations randomly. Define matrices $Q_k = A_k B_k^T$, which will play a crucial role is our construction. The random walk of Q_k is induced by random walks of A_k and B_k. Indeed, if at the k-th step the matrices A_k and B_k are to be rotated by R_A and R_B respectively, then

$$Q_{k+1} = A_{k+1}B_{k+1}^T = (R_A A_k)(R_B B_k)^T = R_A\left(A_k B_k^T\right)R_B^T = R_A Q_k R_B^T.$$

In the case of orthogonal matrices, the Frobenius distance can be computed by the following simple lemma.

Lemma 5. *If A and B are orthogonal $n \times n$ matrices, then*

$$\|A-B\|_F = \sqrt{2n - 2\,\mathrm{Tr}\,(AB^T)}. \tag{2}$$

Proof. By the definition of the Frobenius norm, we have

$$\begin{aligned}\|A-B\|_F^2 &= \mathrm{Tr}\left((A-B)(A-B)^T\right) = \mathrm{Tr}\left(AA^T - BA^T - AB^T + BB^T\right)\\ &= \mathrm{Tr}\,(2I) - \mathrm{Tr}\left(BA^T + AB^T\right) = 2n - 2\,\mathrm{Tr}\left(AB^T\right),\end{aligned}$$

since $BA^T = \left(AB^T\right)^T$. □

Lemma 5 implies that minimizing the Frobenius norm $\|A_k - B_k\|_F$ is equivalent to maximizing the trace $\mathrm{Tr}\left(A_k B_k^T\right) = \mathrm{Tr}\,Q_k$. Therefore, we have to show that we can increase the trace of Q_k by choosing appropriate rotations.

Let $R_A = R_\alpha^{ij}$ be the rotation by an angle α for a coordinate pair (i,j). Choose

$$R_B = R_{\beta(\alpha)}^{ij},$$

where the angle $\beta = \beta(\alpha)$ will be determined by an explicit construction in the proof of Lemma 6. Let

$$(M)_{ij} = \begin{pmatrix} m_{ii} & m_{ij} \\ m_{ji} & m_{jj} \end{pmatrix}$$

denote the 2×2 minor of the matrix M and let

$$(Q_k)_{ij} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad (Q_{k+1})_{ij} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}.$$

Since R_A and R_B do not change other diagonal elements, the change in trace

$$\mathrm{Tr}\,Q_{k+1} - \mathrm{Tr}\,Q_k = \mathrm{Tr}\,(Q_{k+1})_{ij} - \mathrm{Tr}\,(Q_k)_{ij}$$

is determined solely by traces of the minors $(Q_k)_{ij}$ and $(Q_{k+1})_{ij}$. The following lemma allows us to derive a coupling process.

Lemma 6. *For every $\alpha \in [0, 2\pi)$ we can choose $\beta = \beta(\alpha)$ such that the following inequality holds:*

$$(a' + d') - (a + d) \geq \frac{1}{4}(b - c)^2. \tag{3}$$

Moreover, if α is a random variable with the uniform distribution on $[0, 2\pi)$, then $\beta(\alpha)$ also has the uniform distribution on $[0, 2\pi)$.

The construction of the angle $\beta = \beta(\alpha)$ is the fundamental block on which the whole coupling process construction is made. We conjecture that in fact it gives a nearly optimal coupling (see 4.1), but for technical purposes the construction in this paper is more involved.

Note that Lemma 6 shows that the efficiency of choosing the rotations depends solely on $(b-c)$, i.e. the entries of $Q_k - Q_k^T$. However, the norm of $Q_k - Q_k^T$ can be small whereas the matrix Q_k is far from the identity matrix. The following lemma shows that if at the beginning we are already sufficiently close to the identity matrix I, then the coupling decreases $\|Q_k - I\|_F$ exponentially.

Lemma 7. *Let $Q_0, Q_1, \ldots$ be a sequence obtained from coupling I and Q_0 by choosing rotations at each step as described above. If $\|Q_0 - I\|_F < 2$, then for $\delta, \epsilon > 0$ and*

$$t \geq \frac{n^2}{2} \log \frac{4}{\delta^2 \epsilon},$$

we have

$$\mathbf{P}\left(\|Q_t - I\|_F \geq \delta\right) < \epsilon.$$

The next lemma allows us to avoid the problem of small $(b - c)$ entries by adding intermediate "target matrices".

Lemma 8. *For every matrix $Q \in SO(n, \mathbb{R})$ there exists a sequence of orthogonal $n \times n$ matrices $M_0, M_1, \ldots, M_l$ which satisfies the following conditions:*

(1) $Q = M_0$ *and* $I = M_l$;
(2) $\|M_k - M_{k+1}\|_F < 1$ *for* $0 \leq k < l$;
(3) $l < \pi\sqrt{n} + 2$.

The coupling for (A_k, B_k) is defined as follows. Set $M_0 = A_0^T B_0$, $M_l = I$. By Lemma 8, we can construct a sequence of matrices $M_0, M_1, \ldots, M_l$ of length $O(\sqrt{n})$. First, couple matrices $A_0 M_1$ and B_0. Namely, at each step, choose the same coordinate pair (i, j) for R_B as for R_A, and use the construction from Lemma 6 to determine $\beta = \beta(\alpha)$. By Lemma 6, the trace of $Q_k = A_k M_1 B_k^T$ is non-decreasing as k grows. Make τ steps, where the choice of τ will be made later in such a way that the distance between $A_k M_1$ and B_k becomes smaller than $\delta < 1$ with high probability, also to be given later. For this stage Lemma 7 is applicable since the initial distance between $A_0 M_1$ and B_0 is at most 1.

Denote by A' and B' the pair of matrices obtained after coupling $A_0 M_1$ and B_0. Now couple $A' M_2$ and B', etc. Each time we change the matrix M_i to M_{i+1}, the distance between $A_k M_{i+1}$ and B_k does not exceed $1 + \delta < 2$. Therefore, we can use Lemma 7 to analyze every stage of the coupling process. Since $M_l = I$, when we have finished couplings for all matrices M_i, the distance between A_k and B_k becomes less than δ. From this point on, we always choose the same rotations for A_k and B_k, which ensures that these random walks stay at the same distance.

In total, this gives roughly $O(n^{2.5})$ rotations to make two matrices close enough, roughly $O(n^2)$ rotation per matrix M_i. In fact, it is a bit more to account for the probability of failure at each of the l sequence steps. A rigorous analysis will follow. Here we state the main lemma on the coupling process.

Lemma 9. *Let*

$$t \geq 2n^{2.5} \log \frac{13\sqrt{n}}{\delta^2 \epsilon}$$

for $0 < \delta < 1$ *and* $\epsilon > 0$*. Then*

$$\mathbf{P}\left(T_\delta > t\right) = \mathbf{P}\left(\left\|A_t - B_t\right\|_F \geq \delta\right) < \epsilon.$$

Lemma 9 easily implies the main theorem.

Proof of Theorem 1. Note that for any $x, y \in SO\left(n, \mathbb{R}\right)$ we have $\left\|x - y\right\|_F \leq 2\sqrt{n}$. Now using Lemmas 2 and 9 for $\delta = \frac{\varepsilon}{3}$, $\epsilon = \frac{\varepsilon}{3\sqrt{n}}$ and the fact that

$$\sup_{x,y \in SO(n,\mathbb{R})} \left\|x - y\right\|_F = 2\sqrt{n},$$

we get

$$\rho\left(P^t, U\right) < \frac{\varepsilon}{3} + 2\sqrt{n} \cdot \frac{\varepsilon}{3\sqrt{n}} = \varepsilon,$$

for

$$t \;=\; 2n^{2.5} \log \frac{13\sqrt{n}}{\left(\frac{\varepsilon}{3}\right)^2 \cdot \frac{\varepsilon}{3\sqrt{n}}} < 6n^{2.5} \log \frac{8n}{\varepsilon} = O\left(n^{2.5} \log \frac{n}{\varepsilon}\right).$$

□

3. Proof of results

3.1. **Proof of Lemma 2.** Let M^t be a joint distribution of P^t and Q^t, and $L = \sup_{x,y \in X} d\left(x, y\right)$. For any $f \in \mathrm{Lip}\left(1\right)$ we have:

$$\begin{aligned} \left|\int f\, d\left(P^t - Q^t\right)\right| &= \left|\iint \left(f\left(x\right) - f\left(y\right)\right) dP^t\left(x\right) dQ^t\left(y\right)\right| \\ &= \left|\iint \left(f\left(x\right) - f\left(y\right)\right) dM^t\left(x, y\right)\right| \\ &\leq \iint \left|f\left(x\right) - f\left(y\right)\right| dM^t\left(x, y\right) \\ &\leq \iint\limits_{d(x,y)<\delta} d\left(x, y\right) dM^t\left(x, y\right) + \iint\limits_{d(x,y)\geq\delta} d\left(x, y\right) dM^t\left(x, y\right) \\ &< \delta\, \mathbf{P}\left(d\left(x, y\right) < \delta\right) + L\, \mathbf{P}\left(d\left(x, y\right) \geq \delta\right) \\ &< \delta + L \cdot \mathbf{P}\left(d\left(x, y\right) \geq \delta\right), \end{aligned}$$

where the probabilities $\mathbf{P}$ are taken with respect to measure M^t. By definition of the stopping time T_δ and the assumption of non-increase of the distances after T_δ, we obtain

$$\mathbf{P}\big(d(x, y) \geq \delta\big) = \mathbf{P}\big(T_\delta > t\big),$$

and the lemma follows. □

3.2. **Proof of Lemma 6.** We have:

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \cos\beta & \sin\beta \\ -\sin\beta & \cos\beta \end{pmatrix}.$$

Therefore,

$$\begin{aligned} a' + d' &= (a\cos\alpha\cos\beta - c\sin\alpha\cos\beta - b\cos\alpha\sin\beta + d\sin\alpha\sin\beta) \\ &\quad + (a\sin\alpha\sin\beta + c\cos\alpha\sin\beta + b\sin\alpha\cos\beta + d\cos\alpha\cos\beta) \\ &= (a+d)\cos(\alpha-\beta) + (b-c)\sin(\alpha-\beta). \end{aligned}$$

Let $r = \sqrt{(a+d)^2 + (b-c)^2}$. If $r = 0$, then

$$(a' + d') = (a+d) = (b-c) = 0,$$

and the inequality (3) holds for all β. In this case we choose $\beta = \alpha$ which is uniformly distributed on $[0, 2\pi)$.

Suppose now that $r > 0$. Let us define an angle θ so that:

$$\cos\theta = \frac{a+d}{r} \quad \text{and} \quad \sin\theta = \frac{b-c}{r}. \tag{4}$$

Finally, let $\beta = \beta(\alpha) = \alpha - \theta$. Then we have:

$$a' + d' = (a+d)\cos\theta + (b-c)\sin\theta = r\cos\theta\cdot\cos\theta + r\sin\theta\cdot\sin\theta = r.$$

Observe that $\theta = \alpha - \beta$ depends only on Q_k. Therefore, if α has the uniform distribution over $[0, 2\pi)$, then so does β.

Without loss of generality we can assume that $a^2 \geq d^2$. Since $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a minor of an orthogonal matrix, we get that $|b|$ and $|c|$ are bounded from above by $\sqrt{1-a^2}$. Indeed, all rows and all columns of Q_k are of length 1, hence $a^2 + b^2 \leq 1$ and $a^2 + c^2 \leq 1$.

Now we get:

$$r^2 = (a^2 + b^2) + (c^2 + d^2) + 2(ad - bc) \leq 1 + 1 + 2\left(a^2 + \sqrt{1-a^2}\sqrt{1-a^2}\right) = 4,$$

which implies that $r \leq 2$. Finally, we have:

$$(a' + d') - (a+d) = r - r\cos\theta \geq r(1-\cos\theta)\cdot\frac{1+\cos\theta}{2} = \frac{1}{2r}\cdot(r\sin\theta)^2 \geq \frac{1}{4}(b-c)^2,$$

which completes the proof. □

3.3. **Frobenius distance via the eigenvalues.** Define $S_k = Q_k - Q_k^T$, for all $k \geq 1$. In view of Lemma 6, we need to estimate the entries of S_k depending on Q_k. The following result expresses the Frobenius norm $\|S_k\|_F$ in terms of eigenvalues of Q_k.

Let $\lambda_1, \ldots, \lambda_n$ be eigenvalues of an orthogonal $n \times n$ matrix Q. The analysis slightly differs when n is even or odd. Let $m = \lfloor \frac{n}{2} \rfloor$. Recall that if λ is an eigenvalue of Q, then $\bar{\lambda}$ is also an eigenvalue of Q. Therefore, we can order $\lambda_1, \ldots, \lambda_n$ so that for all $1 \leq i \leq m$ we have $\lambda_{2i} = \bar{\lambda}_{2i-1}$, and let $\lambda_n = 1$ if n is odd. Denote by x_i's and y_i's the real and imaginary parts of the eigenvalues, namely:

$$\lambda_{2i-1} = x_i + y_i\sqrt{-1}, \qquad \lambda_{2i} = x_i - y_i\sqrt{-1}, \qquad \text{where } 1 \leq i \leq m. \tag{5}$$

Lemma 10. *For any orthogonal $n \times n$ matrix Q the following holds:*

$$\left\|Q - Q^T\right\|_F^2 = 8\sum_{k \leq m}\left(1 - x_k^2\right). \tag{6}$$

In particular, if $\|Q - I\|_F < 2$, then

$$\left\|Q - Q^T\right\|_F^2 > 8 \sum_{k \le m} (1 - x_k) . \tag{7}$$

Proof. Let $\mathbf{v}_1$, $\mathbf{v}_2$, $\ldots$, $\mathbf{v}_n$ be the eigenvectors of Q corresponding to eigenvalues λ_1, λ_2, $\ldots$, λ_n. Since Q is orthogonal, then $Q^TQ = QQ^T = I$, and all absolute values of λ_i are 1, in particular, they are not equal to 0. Then we have for any $1 \le i \le n$

$$\mathbf{v}_i = Q^T Q \mathbf{v}_i = \lambda_i Q^T \mathbf{v}_i,$$

therefore, vectors $\mathbf{v}_1$, $\mathbf{v}_2$, $\ldots$, $\mathbf{v}_n$ are eigenvectors of Q^T with eigenvalues λ_1^*, λ_2^*, $\ldots$, λ_n^*. Now we obtain

$$\left(Q - Q^T\right) \mathbf{v}_i = (\lambda_i - \lambda_i^*)\, \mathbf{v}_i,$$

hence, the matrix $S = Q - Q^T$ has eigenvalues

$$\pm 2y_1\sqrt{-1},\ \pm 2y_2\sqrt{-1},\ \ldots,\ \pm 2y_m\sqrt{-1},$$

and its singular values are

$$2\left|y_1\right|,\ 2\left|y_1\right|,\ 2\left|y_2\right|,\ 2\left|y_2\right|,\ \ldots, 2\left|y_m\right|, 2\left|y_m\right|,$$

if $n = 2m$, and

$$2\left|y_1\right|,\ 2\left|y_1\right|,\ 2\left|y_2\right|,\ 2\left|y_2\right|,\ \ldots, 2\left|y_m\right|, 2\left|y_m\right|,\ 0,$$

if $n = 2m + 1$. In both cases the square of the Frobenius norm of S can be represented as follows:

$$\|S_k\|_F^2 = \sum_{1 \le i \le m} 2\left|2y_i\right|^2 = 8 \sum_{1 \le i \le m} y_i^2 = 8 \sum_{1 \le i \le m} \left(1 - x_i^2\right).$$

Now using (5), we conclude with (6).

From (2) it follows that if $\|Q - I\|_F < 2$ then

$$\sum_{k \le m} (1 - x_k) = \frac{n - \operatorname{Tr} Q}{2} < 1.$$

Therefore, for all $1 \le k \le m$ we get $x_k > 0$. Hence,

$$1 - x_k^2 = (1 - x_k)(1 + x_k) > 1 - x_k,$$

and (7) follows. □

3.4. **Proof of Lemma 7.** For any $n \times n$ orthogonal matrix Q, define

$$\eta(Q) = \sum_{i \le m} (1 - x_i) = \frac{n - \operatorname{Tr} Q}{2} = \frac{1}{4}\|I - Q\|_F^2 \qquad \text{and} \qquad \eta_t = \eta(Q_t). \tag{8}$$

Applying the inequality (3) for the coordinate pair (i, j) chosen at step t, we obtain:

$$\eta_t - \eta_{t+1} = \frac{1}{2}\left(\operatorname{Tr} Q_{t+1} - \operatorname{Tr} Q_t\right) \ge \frac{1}{8}\left(Q_{t,ij} - Q_{t,ji}\right)^2,$$

where $Q_{t,ij}$ is the ij-th entry of Q_t. Since

$$\|Q_t - I\|_F \le \|Q_0 - I\|_F < 2,$$

we can get the following upper bound on the expected value of η_{t+1} with respect to the choice of (i,j) :

$$\begin{aligned}\mathbf{E}\,\eta_{t+1} &\leq \eta_t - \frac{1}{8}\,\mathbf{E}\left(Q_{t,ij}-Q_{t,ji}\right)^2 \leq \eta_t - \frac{1}{8}\cdot\frac{2}{n^2}\sum_{1\leq i,j\leq n}\left(Q_{t,ij}-Q_{t,ji}\right)^2 \\ &\leq \eta_t - \frac{1}{4n^2}\left\|Q-Q^T\right\|_F^2 < \eta_t - \frac{8\eta_t}{4n^2} = \eta_t\left(1-\frac{2}{n^2}\right).\end{aligned}$$

The induction on t and the fact that $\eta_0 = \frac{1}{2}\left(n - \operatorname{Tr} Q_0\right) < 1$ give:

$$\mathbf{E}\,\eta_t < \eta_0\left(1-\frac{2}{n^2}\right)^t < \left(1-\frac{2}{n^2}\right)^t < \exp\left(-\frac{2t}{n^2}\right).$$

Now the Markov inequality implies:

$$\mathbf{P}\left(\left\|Q_t - I\right\|_F \geq \delta\right) = \mathbf{P}\left(\eta_t \geq \frac{\delta^2}{4}\right) \leq \frac{4}{\delta^2}\cdot\mathbf{E}\,\eta_t < \frac{4}{\delta^2}\exp\left(-\frac{2t}{n^2}\right).$$

Therefore, for $t \geq \frac{n^2}{2}\log\frac{4}{\delta^2\epsilon}$ we have:

$$\mathbf{P}\left(\left\|Q_t - I\right\|_F \geq \delta\right) < \epsilon.$$

□

3.5. **Proof of Lemma 8.** First, consider the case when all eigenvalues of M_0 are different. We choose all matrices $M_1,\ldots,M_l$ so that they have the same eigenvectors $\mathbf{v}_1,\ldots,\mathbf{v}_n$ as M_0 has. Let

$$\exp\left(\phi_1^i\sqrt{-1}\right),\ldots,\exp\left(\phi_n^i\sqrt{-1}\right)$$

be the eigenvalues of M_i. Without loss of generality, we can assume that all ϕ_j^i belong to $(-\pi,\pi)$ for all $i \leq l$ and $j \leq n$.

Let θ be a positive number to be chosen later and let a function $f_\theta(x)$ be defined as follows:

$$f_\theta(x) = \begin{cases} x-\theta & \text{if } x > \theta, \\ 0 & \text{if } |x| \leq \theta, \\ x+\theta & \text{if } x < -\theta. \end{cases}$$

Now let

$$\phi_j^{i+1} = f_\theta(\phi_j^i) \qquad \text{for all } j \leq n,\ i < l.$$

Note that f_θ is an odd function, therefore, we have $\phi_a^{i+1} = -\phi_b^{i+1}$ if $\phi_a^i = -\phi_b^i$ for some values of a and b. Hence, all M_i belong to $SO(n,\mathbb{R})$.

Since all matrices M_i have the same eigenvectors, we obtain that the eigenvalues of $M_{i+1}M_i^T$ are the following:

$$\exp\left(\left(\phi_1^{i+1}-\phi_1^i\right)\sqrt{-1}\right),\ldots,\exp\left(\left(\phi_n^{i+1}-\phi_n^i\right)\sqrt{-1}\right).$$

Observe that $|f_\theta(x) - x| \leq \theta$. Therefore, the real parts of the eigenvalues of $M_{i+1}M_i^T$ are at least $\cos\theta$. Thus, by Lemma 5, we have:

$$\begin{aligned}\left\|M_i - M_{i+1}\right\|_F &= \sqrt{2n - 2\operatorname{Tr} M_{i+1}M_i^T} \leq \sqrt{2n - 2n\cos\theta} \\ &< \sqrt{2n - 2n\left(1-\frac{\theta^2}{2}\right)} = \theta\sqrt{n}.\end{aligned}$$

Let us choose $\theta = 1/\sqrt{n}$. We obtain $\left\|M_i - M_{i+1}\right\|_F < 1$. On the other hand, for every $j \leq n$ we get $\phi_j^l = 0$ if

$$l = \left\lceil\frac{\pi}{\theta}\right\rceil < \pi\sqrt{n} + 1.$$

Indeed, if $\phi_j^l > 0$ for some j, then

$$\phi_j^0 \geq \phi_j^l + l\theta > \pi\sqrt{n} \cdot \frac{1}{\sqrt{n}} = \pi,$$

which contradicts the assumption $\phi_j^0 < \phi$. Analogously, ϕ_j^l cannot be negative. Therefore, all eigenvalues of M_l are equal to 1, i.e. $M_l = I$.

In case when not all eigenvalues of M_0 are different, choose any matrix M_1 within distance 1 from M_0 with distinct eigenvalues. Applying the above construction to M_1, we get the desired sequence of length at most $\pi\sqrt{n} + 2$. This completes the construction. □

3.6. **Proof of Lemma 9.** Note that for any auxiliary matrix M_k there is a probability of failing to couple two matrices. Recall that we stop the coupling procedure if we fail at a certain stage.

For each matrix M_k, $1 \leq k \leq l$, we make $\tau = \left\lceil \frac{n^2}{2} \log \frac{4}{\delta^2 \epsilon} \right\rceil$ steps. Then, by Lemma 7, we have:

$$\mathbf{P}\left(\|A_\tau M_1 - B_\tau\|_F \geq \delta\right) < \frac{\epsilon}{l}.$$

and

$$\mathbf{P}\left(\|A_{k\tau} M_k - B_{k\tau}\|_F \geq \delta \;\middle|\; \left\|A_{(k-1)\tau} M_{k-1} - B_{(k-1)\tau}\right\|_F < \delta\right) < \frac{\epsilon}{l}\,,$$

for all $2 \leq k \leq l$. Thus, after $l\tau$ steps we have:

$$\mathbf{P}\left(\|A_{l\tau} - B_{lm\tau}\|_F \geq \delta\right) < \sum_{k=1}^{l} \mathbf{P}\left(\|A_{k\tau} M_k - B_{k\tau}\|_F \geq \delta\right) < \sum_{k=1}^{l} \frac{\epsilon}{l} = \epsilon.$$

Note that $l < \pi\sqrt{n} + 2$. Hence, we can couple A_0 and B_0 with probability of success at least $1 - \epsilon$ in at most

$$t \;=\; 2\,n^{2.5} \log \frac{13\sqrt{n}}{\delta^2 \epsilon}$$

steps.

□

4. Conclusion and final remarks

4.1. In our coupling construction for technical reasons (to avoid a small eigenvalue problem) we have to choose a $O(\sqrt{n})$ sequence of "target matrices" M_i. While this sequence cannot be easily shortened, we believe that our coupling process is in fact more efficient than our results may suggest.

Recall the basic coupling process we constructed with same pair of coordinates and $\beta = \beta(\alpha)$ as in Lemma 6. We conjecture that in fact this process mixes in $O(n^2 \log n)$ time, a result supported by experimental evidence. This would further improve the upper bound of the mixing time of Kac's walk to nearly match with the trivial lower bound.

4.2. It is important to emphasize that some of the difficulty of this problem is that the modern ℓ_2-analysis of Markov chains (see e.g. [23, 28]) does not apply here. In fact, Kac's random walk does not converge in ℓ_2-distance, as we mentioned in the introduction (see also [9]).

4.3. As noted in [9], the study of Kac's random walk is strongly related to study of random walks on $SU(n, \mathbb{C})$ by random elementary 2-dimensional rotations. In fact, the technique in [9] and of this paper can be directly translated to this case. These walks are closely related and motivated by quantum computing [2, 30], more specifically by quantum random walks [1].

4.4. One can easily modify our coupling construction to obtain a $O(n^2 \log n)$ upper bound for the for the corresponding random walk on the unit sphere $S^{n-1} \subset \mathbb{R}^n$. The improvement has to do with a $O(1)$ sequence of required "target matrices" in this case.

A lower bound $\Omega(n \log n)$ was conjectured in [3, 21]. Moreover, Maslin conjectures a sharp cutoff in this case [21]. As in 4.1, it is possible that our basic coupling mixes in $O(n \log n)$, but as of now such a result seems unfeasible.

4.5. The main result in [16] (see also [31]) is the $O(n^3)$ upper bound on the convergence rate of the entropy. This is related to Kac's original question [18]. We are hopeful that our results could be used to prove stronger bounds.

4.6. The analogue of Kac's random walk on $SL(n, \mathbb{F}_q)$ was studied in [24] and is shown to mix in $O(n^3 \log n)$ steps. Unfortunately, the stopping time approach in that paper does not seem to translate to the compact case. It is unclear whether the generalized coupling approach can be used to improve Pak's bounds.

Acknowledgments. We are grateful to Dorit Aharonov, Bernard Chazelle, Persi Diaconis, Richard Dudley, Laurent Saloff-Coste and Dan Stroock for the insightful remarks and helpful conversations on the subject. Special thanks to Ravi Montenegro and Yuval Peres for finding a critical error in the early version of this paper. The first author was partially supported by the NSF.

References

[1] D. Aharonov, A. Ambainis, J. Kempe and U. Vazirani, Quantum walks on graphs, *Proc. 33rd STOC* (2001), 50–59.

[2] D. Aharonov and M. Ben-Or, Fault-tolerant quantum computation with constant error, *Proc. 29th STOC* (1997), 176–188.

[3] N. Ailon and B. Chazelle, Approximate Nearest Neighbors and the Fast Johnson-Lindenstrauss Transform, *Proc. 38th STOC* (2006), 557–563.

[4] D. Aldous, Random walks on finite groups and rapidly mixing Markov chains, in *Lecture Notes in Math.* **986** (1983), 243–297.

[5] D. Aldous and J. Fill, *Reversible Markov Chains and Random Walks on Graphs*, monograph in preparation, available at `http://www.stat.berkeley.edu/~aldous/RWG/book.html`.

[6] D. Aldous, L. Lovász and P. Winkler, Mixing times for uniformly ergodic Markov chains, *Stochastic Process. Appl.* **71** (1997), No. 2, 165–185.

[7] R. Bubley and M. E. Dyer, Path Coupling: A Technique for Proving Rapid Mixing in Markov Chains, *Proc. 38th FOCS* (1997), 223–231.

[8] E. A. Carlen, M. C. Carvalho and M. Loss, Determination of the spectral gap for Kac's master equation and related stochastic evolution, *Acta Math.* **191** (2003), No. 1, 1–54.

[9] P. Diaconis and L. Saloff-Coste, Bounds for Kac's master equation, *Comm. Math. Phys.* **209** (2000), 729–755.

[10] W. Doeblin, Exposé de la theorie des chaînes simples constantes de Markov à un nombre fini d'etats (in French), *Rev. Math. de l'Union Interbalkanique* **2** (1933), 77–105.

[11] R. M. Dudley, *Real Analysis and Probability*, Cambridge University Press, 2002.

[12] M. E. Dyer, L. A. Goldberg, C. S. Greenhill, M. Jerrum and M. Mitzenmacher, An extension of path coupling and its application to the Glauber dynamics for graph colourings, *SIAM J. Comput.* **30** (2001), 1962–1975.

[13] P. Erdös and A. Rényi, On a classical problem of probability theory, *Magyar Tud. Akad. Mat. Kutató Int. Közl.* **6** (1961), 215–220.

[14] W. Hastings, Monte Carlo sampling methods using Markov chains and their applications, *Biometrika* **57** (1970), 97–109.

[15] T. P. Hayes and E. Vigoda, Coupling with the stationary distribution and improved sampling for colorings and independent sets, *Ann. Appl. Probab.* **16** (2006), 1297–1318.

[16] E. Janvresse, Bounds on Semigroups of Random Rotations on $SO(n)$, *Theory Probab. Appl.* **47** (2003), 526–532.

[17] M. Jerrum and A. Sinclair, Approximating the Permanent, *SIAM J. Comput.* **18** (1989), 1149–1178.

[18] M. Kac, Probability and Related Topics in Physical Science, Interscience, New York, 1959.

[19] T. Lindvall, *Lectures on the Coupling Method*, New York, Wiley, 1992.

[20] L. Lovász and P. Winkler, Mixing times, in *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.* **41** (1998), 85–133.

[21] D. Maslin, The eigenvalues of Kac's master equation, *Math. Z.* **243** (2003), 291–331.

[22] H. McKean, Speed of approach to equilibrium for Kac's caricature of a Maxwellian gas, *Arch. Rational Mech. Anal.* **2** (1966), 343–367.

[23] R. Montenegro and P. Tetali, Mathematical Aspects of Mixing Times in Markov Chains, *Foundations and Trends in Theoretical Computer Science*, to appear.

[24] I. Pak, Using stopping times to bound mixing times, *Proc. 10th SODA* (1999), 953–954.

[25] J. W. Pitman, On coupling of Markov chains, *Probab. Theory Rel. Fields* **35** (1976), 315–322.

[26] U. Porod, The cut-off phenomenon for random reflections, *Ann. Probab.* **24** (1996), 74–96.

[27] J. S. Rosenthal, Random Rotations: Characters and Random Walks on $SO(N)$, *Ann. Probab.* **22** (1994), 398–423.

[28] L. Saloff-Coste, Lectures on finite Markov chains, in *Lecture Notes in Math.* **1665**, Springer, (1997), 301–413.

[29] L. Saloff-Coste, Random walks on finite groups, in *Enc. Math. Sci.* **110**, Springer (2004), 263–346.

[30] P. W. Shor, Quantum computing, *Proc. ICM Berlin*, Doc. Math. **1** (1998), 467–486.

[31] C. Villani, Cercignani's conjecture is sometimes true and always almost true, *Comm. Math. Phys.* **234** (2003), 455–490.