RANDOM WALKS ON DICYCLIC GROUP

SONGZI DU
STANFORD GSB

1. Introduction

In this paper I work out the rate of convergence of a non-symmetric random walk on the dicyclic group (Dic_n) and that of its symmetric analogue on the same group. The analysis is via group representation techniques from Diaconis (1988) and closely follows the analysis of random walk on cyclic group in Chapter 3C of Diaconis. I find that while the mixing times (the time for the random walk to get "random") for the non-symmetric and the symmetric random walks on Dic_n are both on the order of n^2, the symmetric random walk will take approximately twice as long to get "random" as the non-symmetric walk.

2. Dic_n and its Irreducible Representations

For integer $n \geq 1$ the dicyclic group (of order $4n$), Dic_n, has the presentation

$$< a, x \mid a^{2n} = 1, x^2 = a^n, xax^{-1} = a^{-1} > .$$

More concretely, Dic_n is composed of $4n$ elements: $1, a, a^2, \ldots, a^{2n-1}$, $x, ax, a^2x, \ldots, a^{2n-1}x$. The multiplications are as follows (all additions in exponents are modulo $2n$):

- $(a^k)(a^m) = a^{k+m}$
- $(a^k)(a^m x) = a^{k+m}x$
- $(a^k x)(a^m) = a^{k-m}x$
- $(a^k x)(a^m x) = a^{k-m+n}$

Date: June 18, 2008.
Contact: songzidu@stanford.edu.

Dic_2 is the celebrity among all Dic_n's and is known as the quaternion group.

It's clear that $\{1, a, a^2, \ldots, a^{2n-1}\}$ is an Abelian subgroup of Dic_n of index 2. Therefore, each irreducible representation of Dic_n has dimension less than or equal to 2 (Corollary to Theorem 9 in Serre (1977)).

When n is odd, the 1-D irreducible representations of Dic_n are:

- $\psi_0(a) = 1, \psi_0(x) = 1$
- $\psi_1(a) = 1, \psi_1(x) = -1$
- $\psi_2(a) = -1, \psi_2(x) = i$
- $\psi_3(a) = -1, \psi_3(x) = -i$

When n is even, the 1-D irreducible representations of Dic_n become:

- $\psi_0(a) = 1, \psi_0(x) = 1$
- $\psi_1(a) = 1, \psi_1(x) = -1$
- $\psi_2(a) = -1, \psi_2(x) = 1$
- $\psi_3(a) = -1, \psi_3(x) = -1$

One can work out 1-D representation ψ using the identity $\psi(axa) = \psi(x)$, and thus $\psi(a) = \pm 1$. If n is even, this means $\psi(x^2) = \psi(a^n) = 1$, thus $\psi(x) = \pm 1$ as well. When n is odd, we can have $\psi(a^n) = -1$, so $\psi(x)$ can be $\pm i$. This explains the difference in 1-D representations when n is even or odd.

The 2-D irreducible representations of Dic_n are:

$$\rho_r(a) = \begin{pmatrix} \omega^r & 0 \\ 0 & \omega^{-r} \end{pmatrix}, \rho_r(x) = \begin{pmatrix} 0 & (-1)^r \\ 1 & 0 \end{pmatrix}, \tag{1}$$

where $1 \leq r \leq n-1$ and $\omega = e^{\pi i/n}$. One can easily check that these representations are all distinct and irreducible (by checking their characters), and that indeed we have $\rho_r(xax^{-1}) = \rho_r(a^{-1})$, $\rho_r(x^2) = \rho_r(a^n)$, and $\rho_r(a^{2n}) = \rho_r(1)$.

Clearly, all $\psi_0, \ldots, \psi_3, \rho_1, \ldots, \rho_{n-1}$ are unitary representations (conjugate transposes being their inverses). They are all of the possible irreducible representations of Dic_n, because $4 + 4(n-1) = 4n$, which is the order of Dic_n.

3. AN ASYMMETRIC RANDOM WALK ON DIC_n

In this and next section, we will assume that n is odd.

Let $Q(a) = Q(x) = 1/2$ ($Q(s) = 0$ for other $s \in \mathrm{Dic}_n$), and consider the non-symmetric random walk generated on Dic_n by Q: the probability of going from s to t is $Q(ts^{-1})$, $s, t \in \mathrm{Dic}_n$. Clearly, the uniform distribution on Dic_n, $U(s) = 1/4n$, $s \in \mathrm{Dic}_n$, is a stationary distribution of random walk Q. In fact, it is the only one, as Q is irreducible and aperiodic: Q being irreducible is clear; aperiodicity of Q follows from identities $a^{2n} = 1$ and $a^{n+1}xax = 1$, and the following lemma:

Lemma 3.1. *If n is odd, the greatest common divisor of $2n$ and $n+4$ is 1.*

Proof. Suppose integer $k \geq 1$ divides both $2n$ and $n + 4$.

If k divides n, then this together with k dividing $n + 4$ implies that k divides 4 as well, i.e. $k = 1, 2$, or 4; since n is odd, this means that $k = 1$.

If k does not divide n, then k dividing $2n$ implies that 2 divides k; but this together with k dividing $n + 4$ implies that 2 divides n; thus we can't have k not dividing n. □

We are interested in how "well mixed" (or "random") the random walk Q is after k steps, i.e. the total variation distance to the uniform distribution $U(s) = 1/4n$, $s \in \mathrm{Dic}_n$:

$$\|Q^{*k} - U\|_{\mathrm{TV}} = \max_{A \subseteq \mathrm{Dic}_n} |Q^{*k}(A) - U(A)| \tag{2}$$

where Q^{*k} is the k-th convolution of Q with itself: $Q^{*1} = Q$, and $Q^{*k}(s) = \sum_{t \in \mathrm{Dic}_n} Q(st^{-1}) Q^{*k-1}(t)$ for $s \in \mathrm{Dic}_n$ and $k \geq 2$.

3.1. Upper Bound.

Our upper bound on the distance to stationarity (Equation 2) comes from Lemma 1 of Diaconis (1988), Chapter 3B:

Lemma 3.2. *For any probability measure P on a finite group G,*

$$\|P - U\|_{TV}^2 \leq \frac{1}{4} \sum_{\rho \neq 1} d_\rho \operatorname{Tr}(\hat{P}(\rho) \hat{P}(\rho)^*),$$

where $U(s) = 1/|G|$, the summation is over all non-trivial unitary (here refers to conjugate transpose) irreducible representations of G, d_ρ is the degree of the representation ρ, and $\hat{P}(\rho) = \sum_{s\in G} P(s)\rho(s)$ is the Fourier transform of P at the representation ρ.*

Specializing to $G = \mathrm{Dic}_n$ and $P = Q^{*k}$, we get that

(3)

$$\|Q^{*k} - U\|_{\mathrm{TV}}^2 \leq \frac{1}{4}\left(\sum_{i=1}^{3} \hat{Q}(\psi_i)^k(\hat{Q}(\psi_i)^k)^* + \sum_{r=1}^{n-1} 2\,\mathrm{Tr}\left(\hat{Q}(\rho_r)^k(\hat{Q}(\rho_r)^k)^*\right)\right),$$

where ψ_i and ρ_r are listed in the previous section.

For ψ_i, we find that $\hat{Q}(\psi_1)^k(\hat{Q}(\psi_1)^k)^* = 0$ and $\hat{Q}(\psi_2)^k(\hat{Q}(\psi_2)^k)^* = \hat{Q}(\psi_3)^k(\hat{Q}(\psi_3)^k)^* = 2^{-k}$.

For odd r such that $1 \leq r \leq n-1$, we have

$$\hat{Q}(\rho_r)\hat{Q}(\rho_r)^* = \frac{1}{4}\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}.$$

As a result,

$$\mathrm{Tr}\left(\hat{Q}(\rho_r)^k(\hat{Q}(\rho_r)^k)^*\right) = 2^{-k+1},$$

holds for r odd, $1 \leq r \leq n-1$.

For even r, we use the diagonalization (recall that $\omega = e^{\pi i/n}$)

(4)

$$2\hat{Q}(\rho_r) = \begin{pmatrix} \omega^r & 1 \\ 1 & \omega^{-r} \end{pmatrix} = \begin{pmatrix} \omega^{-r} & \omega^r \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & \omega^r + \omega^{-r} \end{pmatrix}\left(\frac{1}{\omega^r + \omega^{-r}}\begin{pmatrix} 1 & -\omega^r \\ 1 & \omega^{-r} \end{pmatrix}\right),$$

so that

$$\mathrm{Tr}\left(2^k\hat{Q}(\rho_r)^k(2^k\hat{Q}(\rho_r)^k)^*\right) = 4(\omega^r + \omega^r)^{2k-2},$$

and therefore, for r even, $1 \leq r \leq n-1$,

$$\mathrm{Tr}\left(\hat{Q}(\rho_r)^k(\hat{Q}(\rho_r)^k)^*\right) = \left(\cos\frac{r\pi}{n}\right)^{2k-2}.$$

Plug these into (3), we have:

$$\|Q^{*k} - U\|_{\mathrm{TV}}^2 \leq n2^{-k-1} + \frac{1}{2}\sum_{\substack{r=2 \\ r \text{ even}}}^{n-1}\left(\cos\frac{r\pi}{n}\right)^{2k-2}.$$

We need to bound the second term on the right hand side. First notice that

$$\sum_{\substack{r=2 \\ r \text{ even}}}^{n-1} \left(\cos \frac{r\pi}{n}\right)^{2k-2} = \sum_{r=1}^{(n-1)/2} \left(\cos \frac{r\pi}{n}\right)^{2k-2}.$$

We then can use $\cos(x) \leq e^{-x^2/2}$, for $x \in [0, \pi/2]$, (see Appendix for derivations of this and other cosine inequalities used in the paper) to get, for $k \geq 2$:

$$\sum_{r=1}^{(n-1)/2} \cos\left(\frac{r\pi}{n}\right)^{2k-2} \leq \sum_{r=1}^{(n-1)/2} \exp\left(-\frac{r^2\pi^2}{n^2}(k-1)\right) \leq \frac{\exp(-\pi^2(k-1)/n^2)}{1-\exp(-3\pi^2(k-1)/n^2)}.$$

Therefore, our upper bound is, for odd n and $k \geq 2$,

$$\|Q^{*k} - U\|_{\mathrm{TV}}^2 \leq n2^{-k-1} + \frac{\exp(-\pi^2(k-1)/n^2)}{2(1-\exp(-3\pi^2(k-1)/n^2))}. \tag{5}$$

3.2. **Lower Bound.** One can easily show that for any two probability measures P_1 and P_2 on a finite set X,

$$\|P_1 - P_2\|_{\mathrm{TV}} = \frac{1}{2} \max_{\substack{f:X\to\mathbb{R} \\ \|f\|\leq 1}} |P_1(f) - P_2(f)|,$$

where $P_1(f) = \sum_{x\in X} f(x)P_1(x)$, and likewise for $P_2(f)$.

For any finite group G, the uniform distribution on G, $U(s) = 1/|G|$, enjoys the property that $\hat{U}(\rho) = 0$ for any non-trivial irreducible representation ρ of G (Exercise 3 of Chapter 2B in Diaconis (1988)).

Let $f(s) = \frac{1}{2}\operatorname{Tr}\rho_r(s)$ for $s \in \mathrm{Dic}_n$, where $1 \leq r \leq n-1$ and ρ_r is as in Equation 1, we check that $f(s)$ is a real number and that $|f(s)| \leq 1$, for all $s \in \mathrm{Dic}_n$; and $U(f) = \operatorname{Tr}\hat{U}(\rho_r)/2 = 0$. Therefore, we have

$$\|Q^{*k} - U\|_{\mathrm{TV}} \geq \frac{1}{2}\left|\sum_{s\in\mathrm{Dic}_n} Q^{*k}(s)f(s)\right| = \frac{1}{4}\left|\operatorname{Tr}\left(\hat{Q}(\rho_r)^k\right)\right|. \tag{6}$$

Using the diagolization in Equation 4, we have for even r such that $1 \leq r \leq n-1$,

$$\|Q^{*k} - U\|_{\mathrm{TV}} \geq \frac{1}{4}\left|\cos\left(\frac{r\pi}{n}\right)^k\right|.$$

We can let $r = n-1$, and get for $n \geq 7$,

$$\|Q^{*k} - U\|_{\text{TV}} \geq \frac{1}{4}\cos\left(\frac{\pi}{n}\right)^k \geq \frac{1}{4}\exp\left(-\frac{\pi^2 k}{2n^2} - \frac{\pi^4 k}{12n^4} - \frac{17\pi^5 k}{120 n^5}\right),$$

by the inequality $e^{-x^2/2 - x^4/12 - 17x^5/120} \leq \cos(x)$ for $0 \leq x \leq 1/2$.

We summarize the results of this section in the following theorem:

Theorem 3.3. *Fix the probability measure Q on Dic_n such that $Q(a) = Q(x) = 1/2$.*

For any odd $n \geq 1$ and any $k \geq 2$, we have

$$\|Q^{*k} - U\|_{TV}^2 \leq n2^{-k-1} + \frac{\exp(-\pi^2(k-1)/n^2)}{2(1-\exp(-3\pi^2(k-1)/n^2))}.$$

For any odd $n \geq 7$ and any $k \geq 1$, we have

$$\frac{1}{4}\exp\left(-\frac{\pi^2 k}{2n^2} - \frac{\pi^4 k}{12n^4} - \frac{17\pi^5 k}{120n^5}\right) \leq \|Q^{*k} - U\|_{TV}.$$

4. A SYMMETRIC RANDOM WALK ON DIC_n

We now consider the symmetrization of the previous random walk: let Q be such that $Q(a) = Q(a^{2n-1}) = Q(x) = Q(a^n x) = 1/4$ ($Q(s) = 0$ for other $s \in \text{Dic}_n$); and $Q(ts^{-1})$ is still the probability of going from s to t, $s, t \in \text{Dic}_n$. As before, we assume that n is odd. Clearly, the uniform distribution $U(s) = 1/4n$, $s \in \text{Dic}_n$, is still the unique stationary distribution of this new random walk Q. And as before, we are interested in bounding Equation 2.

4.1. **Upper Bound.**

We first note that Inequality 3 still holds for our new Q.

Now, we have $\hat{Q}(\psi_1)^k(\hat{Q}(\psi_1)^k)^* = 0$, and $\hat{Q}(\psi_2)^k(\hat{Q}(\psi_2)^k)^* = \hat{Q}(\psi_3)^k(\hat{Q}(\psi_3)^k)^* = 1/4^k$.

For $1 \leq r \leq n-1$,

$$\hat{Q}(\rho_r) = \frac{1}{2}\begin{pmatrix} \cos\frac{r\pi}{n} & \frac{1}{2}(-1)^r + \frac{1}{2} \\ \frac{1}{2}(-1)^r + \frac{1}{2} & \cos\frac{r\pi}{n} \end{pmatrix}.$$

Thus, for odd r, $1 \leq r \leq n-1$,

$$\text{Tr}\left(\hat{Q}(\rho_r)^k(\hat{Q}(\rho_r)^k)^*\right) = \frac{2}{4^k}\left(\cos\frac{r\pi}{n}\right)^{2k}.$$

For even r, $1 \le r \le n-1$, we have the diagonalization

$$2\hat{Q}(\rho_r) = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \cos\frac{r\pi}{n}+1 & 0 \\ 0 & \cos\frac{r\pi}{n}-1 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}. \tag{7}$$

Thus, for even r, $1 \le r \le n-1$,

$$\operatorname{Tr}\left(\hat{Q}(\rho_r)^k(\hat{Q}(\rho_r)^k)^*\right) = \frac{1}{4^k}\left(\left(\cos\frac{r\pi}{n}+1\right)^{2k} + \left(\cos\frac{r\pi}{n}-1\right)^{2k}\right).$$

Inequality 3 therefore translates to

$$\|Q^{*k}-U\|_{\mathrm{TV}}^2 \le \frac{1}{2}\left(\frac{1}{4^k}\right) + \sum_{\substack{r=1\\ r \text{ odd}}}^{n-1}\left(\frac{1}{2}\cos\frac{r\pi}{n}\right)^{2k} + \frac{1}{2}\sum_{\substack{r=2\\ r \text{ even}}}^{n-1}\frac{1}{4^k}\left(\left(\cos\frac{r\pi}{n}+1\right)^{2k} + \left(\cos\frac{r\pi}{n}-1\right)^{2k}\right).$$

The second term in the right hand side is easily bounded:

$$\sum_{\substack{r=1\\ r \text{ odd}}}^{n-1}\left(\frac{1}{2}\cos\frac{r\pi}{n}\right)^{2k} \le \frac{n-1}{2}\frac{1}{4^k}.$$

And for the third term,

$$\begin{aligned}
&\sum_{\substack{r=2\\ r \text{ even}}}^{n-1}\frac{1}{4^k}\left(\left(\cos\frac{r\pi}{n}+1\right)^{2k} + \left(\cos\frac{r\pi}{n}-1\right)^{2k}\right)\\
&\le \sum_{r=1}^{(n-1)/2}\frac{1}{4^k}\left(1+\cos\frac{r\pi}{n}\right)^{2k} + \frac{n-1}{2}\frac{1}{4^k}\\
&\le \sum_{r=1}^{(n-1)/2}\exp(-r^2\pi^2k/2n^2) + \frac{n-1}{2}\frac{1}{4^k}\\
&\le \frac{\exp(-\pi^2k/2n^2)}{1-\exp(-3\pi^2k/2n^2)} + \frac{n-1}{2}\frac{1}{4^k},
\end{aligned}$$

where we used the inequality $(1+\cos x)/2 \le e^{-x^2/4}$ for all $x \in [0,\pi]$.

Collecting the terms together, we have,

$$\|Q^{*k}-U\|_{\mathrm{TV}}^2 \le \frac{3n-1}{4}\frac{1}{4^k} + \frac{\exp(-\pi^2k/2n^2)}{2(1-\exp(-3\pi^2k/2n^2))}.$$

4.2. **Lower Bound.** Inequality 6 is valid for our new Q as well. Using the diagonalization in (7) for ρ_{n-1} (assuming that $n > 1$), Inequality 6 implies that

$$\begin{aligned}\|Q^{*k} - U\|_{\mathrm{TV}} &\geq \frac{1}{4}\left(\frac{1}{2^k}\right)\left|\left(-\cos\frac{\pi}{n}+1\right)^k + \left(-\cos\frac{\pi}{n}-1\right)^k\right| \\ &\geq \frac{1}{4}\left(\left(\frac{1+\cos(\pi/n)}{2}\right)^k - \frac{1}{2^k}\right) \\ &\geq \frac{1}{4}\left(\exp\left(-\frac{\pi^2 k}{4n^2} - \frac{\pi^4 k}{96n^4} - \frac{\pi^5 k}{400n^5}\right) - \frac{1}{2^k}\right)\end{aligned}$$

for $n \geq 7$; in the last time we used the inequality $e^{-x^2/4-x^4/96-x^5/400} \leq (\cos x + 1)/2$ for $x \in [0, 1/2]$.

Therefore, we arrive at

Theorem 4.1. *Fix the probability measure Q on Dic_n such that $Q(a) = Q(a^{2n-1}) = Q(x) = Q(a^n x) = 1/4$.*

For any odd $n \geq 1$ and any $k \geq 1$, we have

$$\|Q^{*k} - U\|_{TV}^2 \leq \frac{3n-1}{4}\frac{1}{4^k} + \frac{\exp(-\pi^2 k/2n^2)}{2(1-\exp(-3\pi^2 k/2n^2))}$$

.

For any odd $n \geq 7$ and any $k \geq 1$, we have

$$\frac{1}{4}\exp\left(-\frac{\pi^2 k}{4n^2} - \frac{\pi^4 k}{96n^4} - \frac{\pi^5 k}{400n^5}\right) - \frac{1}{2^{k+2}} \leq \|Q^{*k} - U\|_{TV}.$$

Comparing the bounds in Theorem 3.3 to that in Theorem 4.1, we conclude that the mixing time for the non-symmetric random walk is approximately half of the mixing time of the symmetric random walk. It would be interesting to give a "purely" probabilistic proof of this phenomenon.

APPENDIX A. SOME INQUALITIES ON COSINE

Proposition A.1. *For $x \in [0, \pi/2]$, $\cos x \leq e^{-x^2/2}$.*

Proof. We will show that for $x \in [0, \pi/2]$, $\log(\cos x) \le -x^2/2$. Clearly this is true when $x = 0$. And we have

$$\frac{d \log(\cos x)}{dx} = -\tan(x) \le -x$$

because $\frac{d \tan x}{dx} = 1/\cos^2(x) \ge 1$ for $x \in [0, \pi/2]$. □

Proposition A.2. *For $x \in [0, \pi]$, $(1 + \cos x)/2 \le e^{-x^2/4}$.*

Proof. We will show that for $x \in [0, \pi]$, $\log((1 + \cos x)/2) \le -x^2/4$. Clearly it holds for $x = 0$. And we have

$$\frac{d \log \frac{1+\cos x}{2}}{dx} = -\frac{\sin(x)}{(1 + \cos(x)} \le -\frac{x}{2}$$

because

$$\frac{d \frac{\sin(x)}{1+\cos(x)}}{dx} = \frac{1}{1 + \cos(x)} \ge \frac{1}{2}$$

for $x \in [0, \pi]$. □

Proposition A.3. *For $x \in [0, 1/2]$, $e^{-x^2/2 - x^4/12 - 17x^5/120} \le \cos(x)$.*

Proof. Taylor expansion of $\log(\cos x)$ around 0 gives for any $0 < x \le 1/2$:

$$\log(\cos x) = -\frac{x^2}{2} - \frac{x^4}{12} + f(x')\frac{x^5}{120},$$

where $0 < x' < x$ and

$$f(x') = -16 \tan(x') \sec(x')^4 - 8 \tan(x')^3 \sec(x')^2$$

is the fifth derivative of $\log(\cos x)$. Clearly, $|f(x')| \le |f(1/2)| \le 17$; thus

$$\log(\cos x) \ge -\frac{x^2}{2} - \frac{x^4}{12} - \frac{17}{120}x^5$$

□

Proposition A.4. *For $x \in [0, 1/2]$, $e^{-x^2/4 - x^4/96 - x^5/400} \le (\cos x + 1)/2$.*

Proof. Taylor expansion of $\log((\cos x + 1)/2)$ around 0 gives for any $0 < x \le 1/2$:

$$\log((\cos x + 1)/2) = -\frac{x^2}{4} - \frac{x^4}{96} + f(x')\frac{x^5}{120},$$

where $0 < x' < x$ and

$$f(x') = \frac{1}{8}\sec(x'/2)^5(-11\sin(x'/2) + \sin(3x'/2))$$

is the fifth derivative of $\log((\cos x + 1)/2)$.

Since the derivative of f,

$$f'(z) = -\frac{1}{16}(33 - 26\cos(z) + \cos(2z))\sec(z/2)^6 < 0$$

for all $0 \leq z \leq 1/2$, we conclude that $f(z) < 0$ and $|f(x')| \leq |f(1/2)| \leq 0.3$.

Therefore,

$$\log((\cos x + 1)/2) \geq -\frac{x^2}{2} - \frac{x^4}{96} - \frac{0.3}{120}x^5.$$

□

REFERENCES

[1] Diaconis, Persi. Group Representations in Probability and Statistics, Institute of Mathematical Statistics Lecture Notes Vol. 11, 1988.

[2] Serre, Jean-Pierre. Linear Representations of Finite Groups. Springer-Verlag, 1977.