Mixing Times Research - Kevin

kevinxu144

February 2021

1 Non-reversible Walks

Suppose we have a lazy random walk on $\mathbb{Z}/n\mathbb{Z}$ with generators $\{a_1, \ldots, a_m\}$. We can find the eigenvalues similar to how it is done for reversible chains, but we do not get a nice cosine value:

$$\begin{aligned}
\lambda_k &= \frac{1}{2} + \frac{e^{2\pi k i a_1/n}}{2m} + \cdots + \frac{e^{2\pi k i a_m/n}}{2m} \\
&= [1 - \frac{(\pi k a_1/n)^2 + \cdots + (\pi k a_m/n)^2}{m} + O(n^{-4})] \\
&+ \left[\frac{\pi k a_1/n + \cdots + \pi k a_m/n}{m} - \frac{(\pi k a_1/n)^3 + \cdots + (\pi k a_m/n)^3}{m} + O(n^{-5})\right] i
\end{aligned}$$

A paper by Ravi Montenegro used Fill's work to derive bounds on the variation distance $d(n)$:

$$\frac{1}{2}\max_{i>0} |\lambda_i|^n \leq d(n) \leq \frac{1}{2}(1 - \lambda_{PP^*})^{n/2}\sqrt{\log \frac{1-\pi_*}{\pi_*}}$$

where λ_{PP^*} is the 2nd-largest eigenvalue of the multiplicative reversibilization PP^*.

Focusing on the lower bound gives

$$\begin{aligned}
|\lambda_k|^2 = \lambda_k \overline{\lambda_k} &= \frac{1}{4} + \frac{1}{2m}\sum_{i=1}^{m} \cos(2\pi k a_i/n) + \frac{1}{4m^2}\sum_{1\leq i,j\leq m} e^{2\pi k i(a_i - a_j)/n} \\
&= \frac{1}{4} + \frac{1}{4m} + \frac{1}{2m}\sum_{i=1}^{m} \cos(2\pi k a_i/n) + \frac{1}{2m^2}\sum_{1\leq i<j\leq m} \cos(2\pi k(a_i - a_j)/n) \\
&= 1 - \frac{1}{2m}\sum_{i=1}^{m}\left(\frac{2\pi k a_i}{n}\right)^2 - \frac{1}{2m^2}\sum_{1\leq i<j\leq m}\left(\frac{2\pi k(a_i - a_j)}{n}\right)^2 + O(n^{-4}).
\end{aligned}$$

If $cm = n$ for constant c, then the complicated term on the right becomes insignificant for large enough n, and we obtain a result very close to Katherine's for reversible walks, implying that choosing generators close to $n^{1/m}, n^{2/m}, \ldots$ yields the lowest mixing time.

Trying some small cases, the second term vanishes when $m = 1$, and we can always pick k to make $ka_1 \equiv 1 \pmod{n}$ (note that $\gcd(a_1, n) = 1$ to preserve ergodicity) in order to yield the maximum possible bound. Clearly such a walk has the same mixing time for any generator (due to every element having the same additive order) which coincides with this result.

2 Two generator case

When $m = 2$, we want to minimize $3k^2(a_1^2 + a_2^2) - 2k^2 a_1 a_2$ across all $1 \leq k < n$. For convenience we define $b_i = ka_i$, and since k, n need not be relatively prime b_i can be any nonzero element in $\mathbb{Z}_n$ (as $k \neq 0$ gives nontrivial eigenvalues). Then we need to minimize the residue

$$3b_1^2 + 3b_2^2 - 2b_1 b_2 \pmod{n}.$$

Since we are dealing with quadratic residues, we tackle the case for prime n first (and sufficiently large).

This quadratic form has discriminant $(-2)^2 - 4(3)(3) = -32$ and thus has class number 2, the two forms being the principal $x^2 - 8y^2$ and also $3x^2 + 3y^2 + 2xy$. Theorem 4.4 in Chapter 5 of the NT book states that the residue classes represented by $3x^2 + 2xy + 3y^2$ is a coset of the ones properly represented by $x^2 - 8y^2$. Since 1 is not a representation, it must be a proper coset. After some experimenting, the representations have residues $3, 11, 19, 27 \pmod{32}$ (and the shared residues $0, 4, 8, 12, 16$). By CRT (as n is odd) and Dirichlet's theorem there must be a prime number satisfying both residues, so by Theorem 5.9 in Chapter 4 of the NT book we always have some solution (b_1, b_2) that gives us 1 and therefore always hit the bound.

n	(mod 32)	CRT	sol.
3	3	67	2,2
5	3	131	2,2
7	3	99	1,6
11	3	67	2,5
13	3	131	2,7
17	3	35	$\emptyset$
17	3	579	9,14
17	11	171	3,8

Figure 1: A table of generating sets

For $n = 17$, computing the first residue modulo $17 * 32$ gave 35 which didn't work. However, redoing it with $35 + 17 * 32 = 579$ worked. So we don't need it to be a prime, but there seems to be no visible pattern for non-primes.

Fixing b_2, we solve the equation

$$3b_1^2 - 2b_2b_1 + 3b_2^2 - 1 = an$$

for some integer a. For b_1 to be integral we must have that

$$4b_2^2 - 12(3b_2^2 - 1 - an) = 12an - 32b_2^2 + 12 = a'^2$$

for some integer a', or that $-8b_2^2 + 3$ be a quadratic residue modulo n (though $n = 3$ is an extraneous case).

We can actually figure out this ideal set for n relatively prime to $2, 3$. If we let $(b_1, b_2) = (6^{-1}, -2^{-1})$, then

$$3b_1^2 + 3b_2^2 - 2b_1b_2 \equiv 1 \pmod{n}$$

as desired. This is found by considering multipliers $b_1 = cb_2$, and we can extend this to $n = 3^c$ by considering $(b_1, b_2) = (22^{-1}, 13 * 22^{-1})$. Unfortunately, it seems like integer solutions to $3x^2 - 8 = y^2$ force x to be even, so the method fails for those n.

The Pell Equation has integer solutions in the form of

$$x = (1 + \frac{\sqrt{3}}{3})(2 - \sqrt{3})^n + (1 - \frac{\sqrt{3}}{3})(2 + \sqrt{3})^n$$
$$y = (1 + \sqrt{3})(2 - \sqrt{3})^n + (1 - \sqrt{3})(2 + \sqrt{3})^n.$$

It looks like we have solutions iff $n \not\equiv 0 \pmod{4}$. Note that if we have solutions (p_1, p_2) and (q_1, q_2) for relatively prime $n = p, q$ respectively, then we are guaranteed a solution in mod pq due to CRT. Since $(0, 1)$ is a solution for $n = 2$ (kinda, because it doesn't work for $n = 2$ itself as it needs to be nonzero), we can find the ideal generating set for every n not $0 \pmod{4}$.

By investigating $n = 4$ we quickly find that the lowest residue possible is 3. Letting $(b_1, b_2) = (1, \frac{2}{3})$ gives a solution for $n = 4^c$, and it should be possible to extend this to a generator for $n \equiv 0 \pmod{4}$.

3 General case

If we have three generators, then our lower bound is

$$4b_1^2 + 4b_2^2 + 4b_3^2 - 2b_1b_2 - 2b_2b_3 - 2b_3b_1.$$

Once again setting $b_1 = b_2 = cb_3$, we have

$$(6c^2 - 4c + 4)b_3^2 \equiv 1 \pmod{n}.$$

If $6c^2 - 4c + 4$ is square then we're done, and clearly when $c = -2$ then $b_3 = 6^{-1}$ is a solution.

The general case asks to solve

$$(m+1)\sum_i b_i^2 - 2\sum_{i<j} b_ib_j \equiv 1 \pmod{n}$$

$$(m+2)\sum_i b_i^2 - \left(\sum_i b_i\right)^2 \equiv 1 \pmod{n}.$$

If we set $b_i = b_1/i$ for $1 \leq i < m$ and $b_m = b_1/c$, then we get

$$(m+1)\frac{(m-1)m(2m-1)}{6}b_m^2 - 2\sum_{i=0}^{m-2} 2^i(2^m - 2^{i+1}) \equiv 1 \pmod{n}$$

or

$$(m+1)(2^m - 1)b_m^2 - 2^{m+1}(2^{m-1} - 1) - \frac{4}{3}(4^{m-1} - 1)$$

$m(m-1)^2(5m-1)/6 - cm(m-1) + c^2$

$4d^2 - e^2 = m(m-1)^2(7m-2)/3$