1 Mathematical Backgroung

Let G be a finite group. For any subset S of G we denote by $< S >$ the subgroup of G generated by S. If $< S >= G$, S is a generator of G.

Let π, μ be two distribution on a same set Ω. The total variation distance between π and μ is denoted $\|\pi - \mu\|_{\text{TV}}$ and is defined by

$$\|\pi - \mu\|_{\text{TV}} = \max_{A \subset \Omega} |\pi(A) - \mu(A)|.$$

It is known that

$$\|\pi - \mu\|_{\text{TV}} = \frac{1}{2} \sum_{x \in \Omega} |\pi(x) - \mu(x)|.$$

Moreover, if ν is a distribution on Ω, one has

$$\|\pi - \mu\|_{\text{TV}} \leq \|\pi - \nu\|_{\text{TV}} + \|\nu - \mu\|_{\text{TV}}$$

Let P be the matrix of a markov chain on Ω. $P(x, \cdot)$ is the distribution induced by the x-th row of P. If the markov chain induced by P has a stationary distribution π, then we define

$$d(t) = \max_{x \in \Omega} \|P^t(x, \cdot) - \pi\|_{\text{TV}},$$

and

$$t_{\text{mix}}(\varepsilon) = \min\{t \mid d(t) \leq \varepsilon\}.$$

One can prove that

$$t_{\text{mix}}(\varepsilon) \leq \lceil \log_2(\varepsilon^{-1}) \rceil t_{\text{mix}}(\frac{1}{4})$$

It is known that $d(t+1) \leq d(t)$.

2 PRNG and random walk on Cayley graphs

Let S be a generator of $\mathbb{B}^N$ such that if $s \in S$, then $-s \in S$. Let ν be a distribution on S such that $\nu(s) = \nu(-s)$. The matrix P^ν, or just P^ν, or just P, is the matrix defined by: $P^\nu(x, y) = \nu(y - x)$ if $x - y \in S$ and 0 otherwise. P_S^ν is the ν-random walk on the S-Cayley graph of G.

A general results on random walks claims that the uniform distribution is stationnary for P. Moreover, if $\nu(s) > 0$ for each s, then this is the limit distribution.

Let $\mathcal{P}$ be finite subset of $\mathbb{N}$ and μ a distribution on $\mathcal{P}$. Set

$$P_{\mathcal{P},\mu} = \sum_{k \in \mathcal{P}} \mu(k) P^k.$$

With the above notation, $P_{\mathcal{P},\mu}$ is the matrix of the markov chain corresponding to the PRNG defined by Christophe, where S corresponds to the boolean functions and μ si the probability of choosing elements of $\mathcal{P}$.

Example 1 For instance let e_i be the vector of $\mathbb{B}^N$ whose i-th componenent is 1 and all other compoennts are null. Let $e_0 = 0$ and $S = \{e_i \mid 0 \leq i \leq N\}$. Choosing $\nu(e_i) = \dfrac{1}{N+1}$, we obtain the random walk defined by the *bit negation* of the paper by Christophe and JEF. The associated matrix will be denoted P_1. Choosing $\mathcal{P} = \{10, 11\}$ and $\mu(10) = \mu(11) = \dfrac{1}{2}$ provides the PRNG with steps of lengths 10 or 11 with the same probability.

Example 2 With the same notation, choosing the same S, but $\nu(e_i) = \dfrac{1}{2n}$ if $i \geq 1$ and $\nu(e_0) = 1/2$ leads to the the classical lazy random walk on $\mathbb{B}^N$ (also known as the lazy random walk on the hypercube or as the Ehrenfest Urn Model). The associated matrix will be denoted P_2.

Example 3 Choosing $S = G$ and the uniform distribution for ν corresponds to the xor approach of the paper with Raphael.

3 Results

The main result is that if the minimal element of $\mathcal{P}$ is greater or equal to the mixing time of P, then the PRNG provides a distribution whose distance to the uniform distribution is at most ε.

Let $t_P(\varepsilon)$ be the ε mixing time for P. Without loss of generality we assume that if $k \in \mathcal{P}$, then $\mu(k) > 0$.

Proposition 4 *Let $k_0 = \min\{k \mid k \in \mathcal{P}\}$. If $k_0 \geq t_P(\varepsilon)$, and if $\nu(s) > 0$ for all $s \in S$, then one has $\|P_{\mathcal{P},\mu}(x, \cdot) - \pi\|_{\mathrm{TV}} \leq \varepsilon$, where π is the uniform distribution.*

PROOF. The fact that $\nu(s) > 0$ for all $s \in S$ ensures that the uniform distribution is the limits of the markov chains induced by P (classical results on random walks).

Now,

$$
\begin{aligned}
\|P_{\mathcal{P},\mu}(x,\cdot) - \pi\|_{\mathrm{TV}} &= \|\sum_{k\in\mathcal{P}} \mu(k)P^k(x,\cdot) - \pi\|_{\mathrm{TV}} \\
&= \frac{1}{2}\sum_{y\in\mathbb{B}^N} |\sum_{k\in\mathcal{P}} \mu(k)P^k(x,y) - \frac{1}{2^N}| \\
&= \frac{1}{2}\sum_{y\in\mathbb{B}^N} |\sum_{k\in\mathcal{P}} \mu(k)P^k(x,y) - \frac{1}{2^N}\sum_{k\in\mathcal{P}} \mu(k)| \\
&= \frac{1}{2}\sum_{y\in\mathbb{B}^N} |\sum_{k\in\mathcal{P}} \mu(k)(P^k(x,y) - \frac{1}{2^N})| \\
&\leq \frac{1}{2}\sum_{y\in\mathbb{B}^N} \sum_{k\in\mathcal{P}} \mu(k)|P^k(x,y) - \frac{1}{2^N}| \\
&\leq \sum_{k\in\mathcal{P}} \mu(k) \left(\frac{1}{2}\sum_{y\in\mathbb{B}^N} |P^k(x,y) - \frac{1}{2^N}| \right) \\
&\leq \sum_{k\in\mathcal{P}} \mu(k)\|P^k(x,\cdot) - \pi\|_{\mathrm{TV}} \\
&\leq \sum_{k\in\mathcal{P}} \mu(k)\varepsilon \\
&\leq \varepsilon
\end{aligned}
$$

□

Therfore it suffices to study the mixing time of P.

4 Mixing time of P_1

See the Ehrenfest Urn Model. One can prove that for P_1,

$$t_{\mathrm{mix}}(\varepsilon) \leq N\log N + \log(\frac{1}{\varepsilon})N.$$

Better results exist see [**?**, page 83, page 267]

5 Mixing time of P_2

In practice one can compute egenvalues and use [**?**, page 155].

There are theoretical results [**?**, page 321-322] and [**?**].

6 To do

Experiments for computing mixing time for P_2.

Experiments for other P (handly built)

Which ε makes possible to pass statistical tests for our PRNGs. Other tests can be performed.

7 Future

Look at [?] for theoretical results. Explore random random walk on the hypercube.