

Approximating Permanent of a Matrix

Rishav Gupta

May 2024

Contents

1	Definitions	2
2	Classical Approximation Algorithm	3
2.1	Getting uniform sampler from a certain Markov Chain	3
2.2	Designing the desired Markov Chain	4
2.3	Approximating the number of perfect matchings	8
2.4	Complexity Analysis	10
2.5	General Weights	11
2.6	Improving the complexity	11
3	Quantum Walks	12
3.1	Syzedegy's Walk and Spectral Analysis	12
3.2	Application of Syzedegy's Walk for sampling Markov Chains . . .	15
3.3	Implementing the walk operators	20
4	Quantum Algorithm for Approximately Counting Number of Perfect Matchings	23
4.1	Multidimensional Amplitude Estimation	23
4.2	Non-destructive Amplitude Estimation	26

1 Definitions

For our case we assume the graph \mathcal{G} to be bipartite in all definitions and theorems.

- **Perfect Matching-** For a graph \mathcal{G} , a perfect matching M is a subset of edges of the graph \mathcal{G} in which each vertex has exactly one edge incident onto it.
- **Near Perfect Matching-** For a graph \mathcal{G} a near perfect matching M is a set of edges in which all vertices except exactly two vertices say u, v have exactly one edge incident onto it in M . For our case of bipartite graphs it is easy to see that the vertices u and v are in different bipartitions. Also for a near perfect matching M in which u, v are not matched we say u and v the markov are the holes of the near perfect matching M .
- **Permanent-** The permanent of a $n \times n$ matrix A is defined as follows

$$per(A) = \sum_{\sigma \in S_n} \prod_i a_{i, \sigma(i)}$$

- **Mixing time of a Markov Chain -** The mixing time $\tau_x(\delta)$ of a markov chain \mathcal{M} is defined as follows

$$\tau_x(\delta) = \min\{t | \forall s \geq t, d(P^s(x), \pi_{\mathcal{M}}) < \delta\}$$

. Where $P^s(x)$ is the distribution on the states obtained after walking on the markov chain for s steps starting from x and $\pi_{\mathcal{M}}$ is the stationary distribution of \mathcal{M} .

Let the spectral gap of the markov chain that is difference between the norm of the largest(norm) two eigenvalues (the largest being 1) of the transition probability matrix of the markov chain be denoted by γ . Then we have the following bounds on the mixing time

$$\tau_x(\delta) \leq \frac{1}{\gamma} (\log \frac{1}{\pi_{\mathcal{M}}(x)} + \log \frac{1}{\delta})$$

2 Classical Approximation Algorithm

2.1 Getting uniform sampler from a certain Markov Chain

So our objective is to generate an *FPRAS* for approximating the permanent of matrices with non negative entries. For now we will focus on the case of $0 - 1$ matrices we will show how to generalize for any non-negative matrix at last. Now notice computing the permanent of a $0 - 1$ matrix is same as counting the number of perfect matchings in the bipartite graph obtained by considering the matrix A as the bipartite adjacency matrix whose permanent we want to compute. So we will focus on generating a uniform sampler for the perfect matchings. While doing so we will get a sequence of parameters and markov chains which are parametrized by these parameters, which we will use to approximate the number of matchings and hence the permanent.

So given a bipartite graph \mathcal{G} on $2n$ vertices we need to get an almost uniform sampler on the perfect matchings of the graph \mathcal{G} .

So for making such a sampler we will make a markov chain on the space $\Omega = \mathcal{M} \cup \mathcal{N}$ that is union of perfect matchings and near perfect matchings. (We denote \mathcal{M} to be set of all perfect matchings possible on $K_{n,n}$ and \mathcal{N} to be the set of all near perfect matchings possible on $K_{n,n}$) where the probability to land on a valid matching M that is $M \in \mathcal{M}_{\mathcal{G}}$, ($\mathcal{M}_{\mathcal{G}}$ is the set of all valid perfect matchings on \mathcal{G}) in the stationary probability distribution of the markov chain is quite high like $\Omega(\frac{1}{n^2})$ and is uniform on the set $\mathcal{M}_{\mathcal{G}}$. In other words, we will get a markov chain MC with state space being Ω as defined above such that

$$\pi_{MC}(\mathcal{M}_{\mathcal{G}}) \geq \frac{1}{(4n^2 + 2)} = \Omega(1/n^2)$$

After getting such a markov chain we use the following algorithm to get an almost uniform sampler for the perfect matchings of \mathcal{G} .

Set $\hat{\delta} \leftarrow \delta / (12n^2 + 6)$.

Repeat $T = \lceil (6n^2 + 2) \ln(3/\delta) \rceil$ times:

Simulate the Markov chain for $\tau(\hat{\delta})$ steps;

output the final state if it belongs to $\mathcal{M}_{\mathcal{G}}$ and halt.

Output an arbitrary perfect matching if all trials fail.

Now consider a subset $S \subseteq \mathcal{M}_{\mathcal{G}}$ now note the following, for the final output M

$$\begin{aligned} \Pr(M \in S) &\geq \frac{\hat{\pi}(S)}{\hat{\pi}(\mathcal{M}_{\mathcal{G}})} - (1 - \hat{\pi}(\mathcal{M}_{\mathcal{G}}))^T \\ &\geq \frac{\pi(S) - \hat{\delta}}{\pi(\mathcal{M}_{\mathcal{G}}) + \hat{\delta}} - \exp(-\hat{\pi}(\mathcal{M}_{\mathcal{G}})T) \\ &\geq \frac{\pi(S)}{\pi(\mathcal{M}_{\mathcal{G}})} - \frac{2\hat{\delta}}{\pi(\mathcal{M}_{\mathcal{G}})} - \exp(-(\pi(\mathcal{M}_{\mathcal{G}}) - \hat{\delta})T) \\ &\geq \frac{\pi(S)}{\pi(\mathcal{M}_{\mathcal{G}})} - \frac{2\delta}{3} - \frac{\delta}{3} \end{aligned}$$

Hence we get an almost uniform sampler on the perfect matchings of \mathcal{G} using the promised Markov Chain.

2.2 Designing the desired Markov Chain

Now we wish to design the markov chain on the set $\Omega = \mathcal{M} \cup \mathcal{N}$ whose stationary probability distribution π has the property that when restricted to elements of \mathcal{M}_G it is uniform and $\pi(\mathcal{M}_G)$ (which is $\sum_{M \in \mathcal{M}_G} \pi(M)$) $\geq \frac{1}{(4n^2+2)}$.

For designing this Markov chain we will define a sequence of parameters each parameter will describe a markov chain which will be used to determine the parameters for the next iteration.

So we have parameters $\lambda(u, v)$ and $w(u, v)$ for each pair (u, v) where $u \in V_1(G)$ and $v \in V_2(G)$.

So initially $\lambda(u, v) = 1, w(u, v) = n, \forall (u, v) \in V_1 \times V_2$, then progressively we would make $\lambda(u, v) = 1/n!$ if $(u, v) \notin E(G)$ and $\lambda(u, v) = 1$ if $(u, v) \in E(G)$. We will have the stationary distribution of markov chains propotional to the product of λ 's of edges (at that stage) contained in the matching. So the weight of invalid perfect matchings and invalid near perfect matchings in the stationary distribution of the final markov chain would be very low. We will give details of how we iterate and how the parameters are modified in the following paragraph.

- So again we denote the value of $\lambda(u, v)$ at iteration i to be $\lambda_i(u, v)$. Also we define $\lambda_i(M) = \prod_{e \in M} \lambda_i(e)$ for $M \in \Omega$ and $\lambda_i(\mathcal{S}) = \sum_{M \in \mathcal{S}} \lambda_i(M)$ for $\mathcal{S} \subset \Omega$.
- At each iteration for some vertex v we change the λ of all non edges connected to that vertex by a factor of $e^{-1/2}$. That is for all non edges connected to v we have $\lambda(e) \rightarrow e^{-1/2} \lambda(e)$.
- Since we have n vertices and for non-edges we go from $1 \rightarrow 1/n!$ and $\log n! \leq n \log n$ so we have total of $r = n^2 \log n$ iterations.
- Now we will define the random walk which describes the Markov Chain at each iteration.
So we want the stationary probability π_i distribution of the markov chain at iteration i to be propotional to the following quantity Λ_i . (Basically $\pi_i(M) \propto \Lambda_i(M)$) Where Λ_i is defined as follows.

$$\Lambda_i(M) = \begin{cases} \lambda_i(M) w_i(u, v) & \text{if } M \in \mathcal{M}(u, v) \text{ for some } u, v; \\ \lambda_i(M), & \text{if } M \in \mathcal{M}. \end{cases}$$

- The transition from a matching M , for a random walk at iteration i (MC_i) is described as follows for the random walk-

- If $M \in \mathcal{M}$, choose an edge $e = (u, v)$ uniformly at random from M ; set $M' = M \setminus e$.
- If $M \in \mathcal{M}(u, v)$, choose z uniformly at random from $V_1 \cup V_2$.
 - * if $z \in \{u, v\}$ and $(u, v) \in E$, let $M' = M \cup (u, v)$;
 - * if $z \in V_2$, $(u, z) \in E$ and $(x, z) \in M$, let $M' = M \cup (u, z) \setminus (x, z)$;
 - * if $z \in V_1$, $(z, v) \in E$ and $(z, y) \in M$, let $M' = M \cup (z, v) \setminus (z, y)$;
 - * otherwise, let $M' = M$.
- With probability $\min\{1, \Lambda_i(M') / \Lambda_i(M)\}$ go to M' ; otherwise, stay at M .
- Now with probability $1/2$ we stay at M and with $1/2$ probability we move using above transition.

- Now for the above markov chain we can see that the stationary probability distribution is propotional to Λ_i . Now we will explain how we update w 's.

We want $w_i(u, v)$ to be close to $w_i^*(u, v)$, where $w_i^*(u, v) = \frac{\lambda_i(\mathcal{M})}{\lambda_i(\mathcal{M}(u, v))}$.

The intuition behind choosing w^* is that if $w = w^*$ then each pattern (pattern is defined as the sets $\mathcal{M} \cup \{\mathcal{M}(u, v) | (u, v) \in V_1 \times V_2\}$, there are $(n^2 + 1)$ patterns) would be equally likely in the stationary probability distribution.

- We want that $w^*(u, v)/2 \leq w(u, v) \leq 2w^*(u, v)$ because of the following theorem.

Theorem 2.1. *Assuming the weight function w_i satisfies inequality $w_i^*(u, v)/2 \leq w_i(u, v) \leq 2w_i^*(u, v)$ for all $(u, v) \in V_1 \times V_2$ with $\mathcal{M}(u, v) \neq \emptyset$, then the mixing time of the Markov chain MC_i is bounded above by $\tau_M(\delta) = O(n^6 g(\log(\pi(M)^{-1}) + \log \delta^{-1}))$.*

- This theorem is the heart of the algorithm it is proved by using a multi commodity flow and bounding the congestion(ϱ). I will use the bound on the congestion and the following theorem to give bounds for the running time of the sampler and hence the approximation algorithm.

Theorem 2.2. *For an ergodic, reversible Markov chain with self-loop probabilities $P(M, M) \geq 1/2$ for all states M , and any initial state $M_0 \in \Omega$,*

$$\tau_{M_0}(\delta) \leq \varrho \left(\ln \pi(M_0)^{-1} + \ln \delta^{-1} \right).$$

- We will analyze the complexities at last for now we will just describe how we update w 's. We will show the following relation holds

$$\frac{\Lambda_i(\mathcal{M}(u, v))}{\Lambda_i(\mathcal{M})} = \frac{\pi_i(\mathcal{M}(u, v))}{\pi_i(\mathcal{M})} = \frac{w_i(u, v)}{w_i^*(u, v)}$$

$$\begin{aligned}
\Lambda_i(\mathcal{M}(u, v)) &= \sum_{M \in \mathcal{M}(u, v)} \lambda_i(M) w_i(u, v) \\
&= w_i(u, v) \sum_{M \in \mathcal{M}(u, v)} \lambda_i(M) \\
&= w_i(u, v) \lambda_i(\mathcal{M}(u, v)) \\
&= w_i(u, v) \frac{\lambda_i(\mathcal{M})}{w_i^*(u, v)} \\
\implies \frac{\Lambda_i(\mathcal{M}(u, v))}{\Lambda_i(\mathcal{M})} &= \frac{\pi_i(\mathcal{M}(u, v))}{\pi_i(\mathcal{M})} = \frac{w_i(u, v)}{w_i^*(u, v)}
\end{aligned}$$

Now we want to use an unbiased estimator for estimating $\pi_i(\mathcal{M})$ and $\pi_i(\mathcal{M}(u, v))$ in order to get a $5/6$ factor approximation to $w^*(u, v)$. We will use this approximation to get w_{i+1} . We will use the condition on w and Theorem 2.1 to put bound on mixing time to get δ close sampler for π_i .

Although we do not know how to sample from π_i exactly, Theorem 2.1 does allow us to sample, in polynomial time, from a distribution $\hat{\pi}_i$ that is within variation distance δ of π_i . We shall see presently that setting $\delta = O(n^{-2})$ suffices in the current situation; certainly, the exact value of δ clearly does not affect the leading term in the mixing time promised by Theorem 2.1. So suppose we generate S samples from $\hat{\pi}_i$, and for each pair $(u, v) \in V_1 \times V_2$ we consider the proportion $\alpha(u, v)$ of samples with hole pair u, v , together with the proportion α of samples that are perfect matchings. (For the rest of the paragraph I will drop the i subscript as it is same for all i) Clearly,

$$\mathbb{E}\alpha(u, v) = \hat{\pi}(\mathcal{M}(u, v)) \quad \text{and} \quad \mathbb{E}\alpha = \hat{\pi}(\mathcal{M}).$$

I will also prove one fact that assuming conditions on w

$$\pi(\mathcal{M}(u, v)) \geq \frac{1}{4(n^2 + 1)}$$

Since $\Omega = \mathcal{M} \cup \mathcal{N}$ we have-

$$\begin{aligned}
&\implies \pi(\mathcal{M}) + \sum_{(u,v)} \pi(\mathcal{M}(u,v)) = 1 \\
&\implies \pi(\mathcal{M}) + \sum_{(u,v)} \frac{\lambda(\mathcal{M}(u,v))w(u,v)}{\Lambda(\Omega)} = 1 \\
&\implies \pi(\mathcal{M}) + \sum_{(u,v)} \frac{\lambda(\mathcal{M})w(u,v)}{\Lambda(\Omega)w^*(u,v)} = 1 \\
&\implies \pi(\mathcal{M}) + \sum_{(u,v)} \frac{2\lambda(\mathcal{M})}{\Lambda(\Omega)} \geq 1 \\
&\implies \pi(\mathcal{M})(1 + 2n^2) \geq 1 \\
&\implies \pi(\mathcal{M}) \geq \frac{1}{(2n^2 + 1)} \\
&\implies \pi(\mathcal{M}(u,v)) \geq \frac{1}{4(n^2 + 1)}
\end{aligned}$$

Naturally, it is always possible that some sample average $\alpha(u,v)$ will be far from its expectation, so we have to allow for the possibility of failure. We denote by $\hat{\eta}$ the (small) failure probability we are prepared to tolerate. Provided the sample size S is large enough, $\alpha(u,v)$ (respectively, α) approximates $\hat{\pi}(\mathcal{M}(u,v))$ (respectively, $\hat{\pi}(\mathcal{M})$) within ratio $c^{1/4}$, with probability at least $1 - \hat{\eta}$. Furthermore, if δ is small enough, $\hat{\pi}(\mathcal{M}(u,v))$ (respectively, $\hat{\pi}(\mathcal{M})$) approximates $\pi(\mathcal{M}(u,v))$ (respectively, $\pi(\mathcal{M})$) within ratio $c^{1/4}$. Then, we have, with probability at least $1 - (n^2 + 1)\hat{\eta}$, approximations within ratio c to all of the target weights $w^*(u,v)$.

It remains to determine bounds on the sample size S and sampling tolerance δ that make this all work. Condition on w entails

$$\mathbb{E}\alpha(u,v) = \hat{\pi}(\mathcal{M}(u,v)) \geq \pi(\mathcal{M}(u,v)) - \delta \geq \frac{1}{4(n^2 + 1)} - \delta.$$

Assuming $\delta \leq 1/8(n^2 + 1)$, it follows from any of the standard Chernoff bounds, that $O(n^2 \log(1/\hat{\eta}))$ samples from $\hat{\pi}$ suffice to estimate $\mathbb{E}\alpha(u,v) = \hat{\pi}(\mathcal{M}(u,v))$ within ratio $c^{1/4}$ with probability at least $1 - \hat{\eta}$. Again using the fact that $\pi(\mathcal{M}(u,v)) \geq 1/4(n^2 + 1)$, we see that $\hat{\pi}(\mathcal{M}(u,v))$ will approximate $\pi(\mathcal{M}(u,v))$ within ratio $c^{1/4}$ provided $\delta \leq c_1/n^2$ where $c_1 > 0$ is a sufficiently small constant. (Note that we also satisfy the earlier constraint on δ by this setting.) Hence we take $c = 5/6$ and $S = O(n^2 \log(1/\hat{\eta}))$ to get a refined estimate to w^* . For i th iteration we label this approximation to w_i^* as w'_i .

- We return w_{i+1} as w'_i . Because w'_i is within $5/6$ factor of w_i^* and w_{i+1}^* is within a factor of $e^{-1/2}$ of w_i^* . Since $5/6 \cdot e^{-1/2} = 0.505 \geq 0.5$ w_{i+1}

satisfies the condition that is within a factor of 2 of w_{i+1}^* . Hence we can repeat this step for $r = O(n^2 \log n)$ iterations to get our desired markov chain and MC_r will be our desired markov chain.

2.3 Approximating the number of perfect matchings

Now to get the number of perfect matchings we will use the following annealing scheme-

$$\Lambda_0(\Omega) \cdot \frac{\Lambda_1(\Omega)}{\Lambda_0(\Omega)} \cdot \frac{\Lambda_2(\Omega)}{\Lambda_1(\Omega)} \cdots \frac{\Lambda_r(\Omega)}{\Lambda_{r-1}(\Omega)} \cdot \frac{\Lambda_r(\mathcal{M}_G)}{\Lambda_r(\Omega)}$$

We know that $\Lambda_0(\Omega) = (n^2 + 1)n!$. We will now use MC_i to estimate $\frac{\Lambda_{i+1}(\Omega)}{\Lambda_i(\Omega)}$ and MC_r to estimate $\frac{\Lambda_r(\mathcal{M}_G)}{\Lambda_r(\Omega)}$.

Now we will explain how we estimate $\frac{\Lambda_{i+1}(\Omega)}{\Lambda_i(\Omega)}$.

First we will prove one bound that

$$\frac{1}{4e} \leq \frac{\Lambda_{i+1}(M)}{\Lambda_i(M)} \leq 4e, \forall M \in \Omega$$

For $M \in \mathcal{M}$ it is easy to the bound holds since for $\frac{\Lambda_{i+1}(M)}{\Lambda_i(M)}$, $\Lambda(M)$ as we go from $i \rightarrow i+1$ either remains same or gets reduced by a factor of $e^{-1/2}$. For $M \in \mathcal{N}$ note that since, $5/12 \leq w_i/w_{i+1} \leq 12/5$ we get that

$$\frac{5}{12e^{1/2}} \leq \frac{\Lambda_{i+1}(M)}{\Lambda_i(M)} \leq \frac{12e^{1/2}}{5}, \forall M \in \mathcal{N}$$

Hence now it is obvious that the above claim holds.

Let π_i denote the stationary distribution of the Markov chain used in phase i , so that $\pi_i(M) = \Lambda_i(M)/\Lambda_i(\Omega)$. Let Z_i denote the random variable that is the outcome of the following experiment: By running the desired Markov chain MC with parameters $\Lambda = \Lambda_i$ and $\delta = \varepsilon/80e^2r$, obtain a sample matching M from a distribution that is within variation distance $\varepsilon/80e^2r$ of π_i . Return $\Lambda_{i+1}(M)/\Lambda_i(M)$.

If we had sampled M from the exact stationary distribution π_i instead of an approximation, then the resulting modified random variable Z'_i would have satisfied

$$\mathbb{E}Z'_i = \sum_{M \in \Omega} \frac{\Lambda_i(M)}{\Lambda_i(\Omega)} \frac{\Lambda_{i+1}(M)}{\Lambda_i(M)} = \frac{\Lambda_{i+1}(\Omega)}{\Lambda_i(\Omega)}.$$

As it is, noting the particular choice for δ and bounds on the ratios, and using the fact that $\exp(-x/4) \leq 1 - \frac{1}{5}x \leq 1 + \frac{1}{5}x \leq \exp(x/4)$ for $0 \leq x \leq 1$, we must settle for

$$\exp\left(-\frac{\varepsilon}{4r}\right) \frac{\Lambda_{i+i}(\Omega)}{\Lambda_i(\Omega)} \leq \mathbb{E}Z_i \leq \exp\left(\frac{\varepsilon}{4r}\right) \frac{\Lambda_{i+i}(\Omega)}{\Lambda_i(\Omega)}.$$

Now suppose s independent trials are conducted for each i using the above experiment, and denote by \bar{Z}_i the sample mean of the results. Then $\mathbb{E}\bar{Z}_i = \mathbb{E}Z_i$ and then we have.

$$\exp\left(-\frac{\varepsilon}{4}\right) \frac{\Lambda_r(\Omega)}{\Lambda_0(\Omega)} \leq \mathbb{E}(\bar{Z}_0 \bar{Z}_1 \dots \bar{Z}_{r-1}) \leq \exp\left(\frac{\varepsilon}{4}\right) \frac{\Lambda_r(\Omega)}{\Lambda_0(\Omega)}$$

For s sufficiently large, $\prod_i \bar{Z}_i$ will be close to $\prod_i \mathbb{E}\bar{Z}_i$ with high probability. With a view to quantifying "sufficiently large," observe that in the light of bounds of the ratio,

$$\frac{\text{Var}[\bar{Z}_i]}{(\mathbb{E}\bar{Z}_i)^2} \leq \frac{64e^3}{s}$$

Thus, taking $s = \Theta(r\varepsilon^{-2})$ we get

$$\begin{aligned} \frac{\text{Var}[\bar{Z}_0 \dots \bar{Z}_{r-1}]}{(\mathbb{E}[\bar{Z}_0 \dots \bar{Z}_{r-1}])^2} &= \prod_{i=0}^{r-1} \frac{\mathbb{E}\bar{Z}_i^2}{(\mathbb{E}\bar{Z}_i)^2} - 1 \\ &= \prod_{i=0}^{r-1} \left(1 + \frac{\text{Var}\bar{Z}_i}{(\mathbb{E}\bar{Z}_i)^2}\right) - 1 \\ &\leq \left(1 + \frac{64e^3}{s}\right)^r - 1 \\ &= O(\varepsilon^2). \end{aligned}$$

So, by Chebyshev's inequality,

$$\Pr[\exp(-\varepsilon/4)\mathbb{E}(\bar{Z}_0 \dots \bar{Z}_{r-1}) \leq \bar{Z}_0 \dots \bar{Z}_{r-1} \leq \exp(\varepsilon/4)\mathbb{E}(\bar{Z}_0 \dots \bar{Z}_{r-1})] \geq \frac{11}{12},$$

assuming the constant implicit in the setting $s = \Theta(r\varepsilon^{-2})$ is chosen appropriately. Combining above with the fact that $\Lambda_0(\Omega) = (n^2 + 1)n!$, we obtain

$$\Pr[\exp(-\varepsilon/2)\Lambda_r(\Omega) \leq (n^2 + 1)n!\bar{Z}_0 \dots \bar{Z}_{r-1} \leq \exp(\varepsilon/2)\Lambda_r(\Omega)] \geq \frac{11}{12}$$

Now we wish to estimate the ratio $\frac{\Lambda_r(\mathcal{M}_G)}{\Lambda_r(\Omega)}$ which is basically the probability of hitting a valid matching in the stationary distribution of MC_r . And we know that $\frac{\Lambda_r(\mathcal{M}_G)}{\Lambda_r(\Omega)} \geq \frac{1}{(4n^2+2)}$. So now we will use a unbiased estimator to estimate this probability.

For this we will carry out the following experiment -

- By running the Markov chain MC_r and $\delta = \varepsilon/80e^2$, obtain a sample matching M from a distribution that is within variation distance $\varepsilon/80e^2$ of π_r .
- Return 1 if $M \in \mathcal{M}_G$, and 0 otherwise.

The outcome of this experiment is a random variable that we denote by Y . If M had been sampled from the exact stationary distribution π_r then its expectation would have been $\Lambda_r(\mathcal{M}_G)/\Lambda(\Omega)$; as it is, we have

$$\exp\left(-\frac{\varepsilon}{4}\right) \frac{\Lambda_r(\mathcal{M}_G)}{\Lambda_r(\Omega)} \leq \mathbb{E}Y \leq \exp\left(\frac{\varepsilon}{4}\right) \frac{\Lambda_r(\mathcal{M}_G)}{\Lambda_r(\Omega)}.$$

Let \bar{Y} denote the sample mean of $s' = \Theta(n^2\varepsilon^{-2})$ independent trials of the above experiment. Since $\mathbb{E}\bar{Y} = \mathbb{E}Y = \Omega(n^{-2})$, Chebyshev's inequality gives

$$\Pr[\exp(-\varepsilon/4)\mathbb{E}\bar{Y} \leq \bar{Y} \leq \exp(\varepsilon/4)\mathbb{E}\bar{Y}] \geq \frac{11}{12},$$

as before. Combining this with the probability for the previous ratios, we get

$$\Pr[\exp(-\varepsilon)|\mathcal{M}_G| \leq (n^2 + 1) n! \bar{Y} \bar{Z}_0 \bar{Z}_1 \cdots \bar{Z}_{r-1} \leq \exp(\varepsilon)|\mathcal{M}_G|] \geq \frac{5}{6}.$$

All this was under the assumption that the initialization procedure succeeded. But provided we arrange for the failure probability of initialization to be at most $1/12$, it will be seen that $(n^2 + 1) n! \bar{Y} \bar{Z}_0 \bar{Z}_1 \cdots \bar{Z}_{r-1}$ is an estimator for the permanent that meets the specification of an FPRAS.

2.4 Complexity Analysis

In total, the above procedure requires $rs + s' = O(\varepsilon^{-2}n^4(\log n)^2)$ samples; by Theorem 2.1, $O(n^7 \log n)$ time is sufficient to generate each sample. (Since there is no point in setting $\varepsilon = o(1/n!)$, the $\log \delta^{-1}$ term in Theorem 2.1 can never dominate.) The running time is thus $O(\varepsilon^{-2}n^{11}(\log n)^3)$. Note that this is sufficient to absorb the cost of the initialization procedure as well, which we will show is $O(n^{11}(\log n)^3)$.

Now for the initialization step that is setting up $w_i(u, v)$ for all i, u, v . Since markov chain took $O(n^7 \log n)$ steps and for each i we generated $O(n^2 \log(1/\hat{\eta}))$ and there are total $r = n^2 \log n$ iterations of i so we have total $O(n^{11}(\log n)^2 \cdot \log(1/\hat{\eta}))$ steps in the initialization process. Now we need to just set $\hat{\eta}$ hence η .

Recall that $\hat{\eta}$ is the failure probability on each occasion that we use a sample mean to estimate an expectation. If we are to achieve overall failure probability η then we must set $\hat{\eta} = O(\eta / (n^4 \log n))$, since there are

$O(n^4 \log n)$ individual estimates to make in total. And we set η to $\delta/2$ or some lesser factor of δ . Now we get total steps equals $O(n^{11}(\log n)^2 \cdot (\log(1/\eta) + \log(n)))$ since $\log(n)$ dominates over $\log(1/\delta) = \log(1/\eta)$ hence we get that the initialization process takes total $O(n^{11}(\log n)^3)$ time hence we are done.

2.5 General Weights

The algorithm is exactly the same just updating of the w_i 's and λ_i 's and their initial values is a little bit tweaked. The following is the changed pseudocode for the updates.

Initialize $\lambda(u, v) \leftarrow a_{\max}$ for all $(u, v) \in V_1 \times V_2$. Initialize $w(u, v) \leftarrow na_{\max}$ for all $(u, v) \in V_1 \times V_2$.

While there exists a pair y, z with $\lambda(y, z) > a(y, z)$ do:

Take a sample of size S from MC with parameters λ, w , using a simulation of T steps in each case.

Use the sample to obtain estimates $w'(u, v)$ satisfying condition (8), for all u, v , with high probability.

Set $\lambda(y, v) \leftarrow \max\{\lambda(y, v) \exp(-1/2), a(y, v)\}$, for all $v \in V_2$, and $w(u, v) \leftarrow w'(u, v)$ for all u, v .

Output the final weights $w(u, v)$.

Where a_{\max} and a_{\min} are the maximum and minimum non-zero entries of the matrix M whose permanent we need to compute. We actually tweak the error ratios a bit for this and get an approximation algorithm polynomial in n , $\log(a_{\max}/a_{\min})$ and obviously $1/\varepsilon$.

2.6 Improving the complexity

We would now present the enhanced complexity achieved by the paper (). The enhanced complexity is a result of better analysis of the mixing time and a different way to decrease the λ 's. In this method the λ 's for all non edges get reduced in each iteration (unlike former where we decreased all the λ 's for non edges connected to one vertex at a time in one iteration). We have the following algorithm to get the λ 's.

Algorithm for computing the cooling schedule λ , given parameters s, c, γ , and D :

Set $\hat{\lambda}_0 = 1, i = s$ and $j = 0$.

While $\hat{\lambda}_j > 1/\gamma$ do

Set $\hat{\lambda}_{j+1} = c^{-1/i} \hat{\lambda}_j$.

If $i > D + 1$ and $\hat{\lambda}_{j+1} < (s/\gamma)^{1/(i-D)}$,

Set $\hat{\lambda}_{j+1} = (s/\gamma)^{1/(i-D)}$ and decrement $i = i - 1$.

Increment $j = j + 1$.

Set $\ell = j$.

The following lemma estimates the number of intermediate temperatures in the above cooling schedule, i.e., the length ℓ of the $\hat{\lambda}$ sequence. (Previously $\ell = r = n^2 \log(n)$)

Lemma 2.3. *Let $c, \gamma > 0, D \geq 0$ and let $\hat{\lambda}_0, \dots, \hat{\lambda}_\ell$ be the sequence computed by the above algorithm. Then $\ell = O([(D+1) \log(s-D) + s/(s-D)] \log_c \gamma)$. If c and D are constants independent of s , then $\ell = O(\log s \log \gamma)$.*

The following lemma shows that for the sequence of the λ_i the value of $Z(\lambda)$ changes by a factor $\leq c$ for consecutive λ_i and λ_{i+1} .

Lemma 2.4. *Let $c, \gamma, D \geq 0$ and let Z_1, \dots, Z_q be a collection of polynomials of degree s . Suppose that for every $i \in [q]$, the polynomial Z_i satisfies the following conditions: i) Z_i has non-negative coefficients, ii) there exists $d \leq D$ such that the coefficient of x^d in Z_i is at least $Z_i(1)/\gamma$.*

Let $\hat{\lambda}_0, \hat{\lambda}_1, \dots, \hat{\lambda}_\ell$ be the sequence constructed by the above algorithm. Then

$$Z_i(\hat{\lambda}_j) \leq c Z_i(\hat{\lambda}_{j+1}) \quad \text{for every } i \in [q] \text{ and } j \in [\ell].$$

For the above algorithm we feed $s = n, c = \sqrt{2}, \gamma = n!, D = 1$. To get the λ_i 's for our implementation. This improves the number of iterations from $n^2 \log(n)$ to $O(n \log^2(n))$. Also from better analysis of mixing time we get the complexity to be $O(n^7 \log^4(n))$, which is best known classically.

3 Quantum Walks

So what we know is that the mixing time of a random walk classically is proportional to $\frac{1}{\delta}$ but we will introduce the notion of quantum walks in this section which gives us a quadratic speedup and we get the mixing time proportional to $\frac{1}{\sqrt{\delta}}$. We would want to use this speedup to get an algorithm to compute the approximate number of perfect matchings in a bipartite graph which has better complexity than the best known classical bound. For that we want to simulate the above markov chain using quantum walks.

3.1 Syzedegy's Walk and Spectral Analysis

We will first present the notion of Syzedegy's quantum walk and do a spectral analysis for it.

We start with the introduction of bipartite walks in the classical framework remarking that every walk can be made bipartite by a simple "duplicating" operation. Let X and Y be two finite sets and $P = (p_{x,y}), Q = (q_{y,x})$ be matrices describing probabilistic maps from X to Y and Y to X , respectively. Since P and Q are stochastic, we have $\sum_{y \in Y} p_{x,y} = 1$ for every $x \in X$ and $\sum_{x \in X} q_{y,x} = 1$ for every $y \in Y$, and all $p_{x,y}, q_{y,x}$ are non-negative. If we have a single probabilistic function P from X to X (i.e. a Markov chain), in order

to create a bipartite walk we can set $q_{y,x} = p_{y,x}$ for every $x, y \in X$, i.e. we set $Q = P$.

We quantize walk (P, Q) by defining two operators on the Hilbert space with basis states

$$\{|x\rangle|y\rangle \mid x \in X, y \in Y\}$$

Define states

$$\phi_x = \sum_{y \in Y} \sqrt{p_{x,y}} |x\rangle|y\rangle$$

for every $x \in X$ and

$$\psi_y = \sum_{x \in X} \sqrt{q_{y,x}} |x\rangle|y\rangle$$

for every $y \in Y$. Let $A = (\phi_x)_x$ be the matrix composed of column vectors $\phi_x (x \in X)$ and $B = (\psi_y)_y$ be the matrix composed of column vectors $\psi_y (y \in Y)$. Our walk operator, W will be the product of

$$\begin{aligned} \text{ref}_1 &= 2AA^* - I; \\ \text{ref}_2 &= 2BB^* - I. \end{aligned}$$

In expression:

$$W = \text{ref}_2 \text{ref}_1.$$

Let $\mathcal{C}(A)$ is the column space of A and $\mathcal{C}(B)$ be the column space of B . Observe that $A^*A = I_X$, therefore $(2AA^* - I)A = A$. Also, for any $\phi \in \mathcal{C}(A)^\perp$ we have $(2AA^* - I)\phi = -\phi$. Therefore ref_1 is a reflection on the subspace $\mathcal{C}(A)$. Similarly, ref_2 is a reflection on the subspace $\mathcal{C}(B)$. In the study of W a central role will be played by the matrix $D = A^*B$. We call D the discriminant of matrix of the quantized walk operator W . It follows from the definitions that

$$D_{x,y} = \sqrt{p_{x,y}q_{y,x}} \quad \text{for every } x \in X, y \in Y.$$

Definition(Quantization) Let P, Q, A, B, D, W as above. Then the quantization of bipartite walk (P, Q) is the unitary operator $W_{P,Q} = W$. We also write $A_{P,Q}$, $B_{P,Q}$ and $D_{P,Q}$ for A, B and D , respectively, if (P, Q) is not clear from the context. If $P = Q$ then we use the shorthand W_P for $W_{P,Q}$, etc. Let the columns of matrices A and B be elements of a Hilbert space H and let $A^*A = I_n, B^*B = I_m$. Then operators $\text{ref}_A = 2AA^* - I, \text{ref}_B = 2BB^* - I$ are reflections on subspaces $\mathcal{C}(A)$ and $\mathcal{C}(B)$, respectively.

In this section we compute spectra of $W = \text{ref}_A \text{ref}_B$. Our formula turns out to be very useful in the study of quantum walks. Our expressions will use the singular values and vectors of the following matrix:

(Discriminant Matrix) The discriminant matrix for $\text{ref}_B \text{ref}_A$ is

$$D(A, B) = A^*B.$$

If we allow the subspaces on which we reflect be represented by arbitrary orthonormal bases (rather than by A and B in particular) then the discriminant matrix is determined only up to unitary multipliers from left and right.

We can naturally interpret $v \rightarrow D(A, B)v$ as a map from $\mathcal{C}(B)$ to $\mathcal{C}(A)$ if we view v as a vector expressed in the $\{b_j\}_{j=1}^m$ bases and the result vector as a one expressed in the $\{a_i\}_{i=1}^n$ bases. To put this into formulas, we can define a map, where Bv is mapped into $(AA^*)Bv = AD(A, B)v$. This map is an orthogonal projection of $\mathcal{C}(B)$ to $\mathcal{C}(A)$, since AA^* is an orthogonal projector to the space $\mathcal{C}(A)$. Similarly $D(A, B)^*$ can be interpreted as an orthogonal projection from $\mathcal{C}(A)$ to the space $\mathcal{C}(B)$. Let λ be a singular value of $D(A, B)$ with associated right singular unit vector v and left singular unit vector w . Then we have

$$\begin{aligned} D(A, B)v &= \lambda w \\ D(A, B)^*w &= \lambda v. \end{aligned}$$

Since $|Bv| = |v|$, $|Aw| = |w|$, and since projections do not increase length we get:

Lemma 3.1. *All singular values of $D(A, B)$ are at most one.*

Using the above observation, for a left-right singular vector pair v, w of $D(A, B)$ we can write the associated singular value as $\cos \theta$ for some $0 \leq \theta \leq \frac{\pi}{2}$. In the linear algebra literature θ is called a canonical angle between subspaces $\mathcal{C}(A)$ and $\mathcal{C}(B)$. We have that $\theta = 0$ iff the corresponding singular vectors are in $\mathcal{C}(A) \cap \mathcal{C}(B)$. The angle θ has a geometric meaning: it is the angle between Aw and Bv (indeed, $w^*A^*Bv = \cos \theta$).

Theorem 3.2. *Theorem 1 (Spectral Lemma) Let H be a Hilbert space, $A, B \leq H$ subspaces, and let ref_A and ref_B be reflections on $\mathcal{C}(A)$ and $\mathcal{C}(B)$. Let $\cos \theta_1, \dots, \cos \theta_l$ be those singular values of $D(A, B) = A^*B$ that lie in the $(0, 1)$ open interval, and let the associated singular vector pairs be v_k, w_k for $(1 \leq k \leq l)$. Then those eigenvalues of the unitary operator $W = \text{ref}_B \text{ref}_A$ that have non-zero imaginary part are exactly*

$$e^{-2i\theta_1}, e^{2i\theta_1}, \dots, e^{-2i\theta_l}, e^{2i\theta_l}.$$

The (un-normalized) eigenvectors associated with these eigenvalues (in order) are

$$Aw_1 - e^{-i\theta_1}Bv_1, Aw_1 - e^{i\theta_1}Bv_1, \dots, Aw_l - e^{-i\theta_l}Bv_l, Aw_l - e^{i\theta_l}Bv_l.$$

In (3) the singular values are listed with multiplicity. Furthermore,

1. *On $\mathcal{C}(A) \cap \mathcal{C}(B)$ operator W acts as the identity. $\mathcal{C}(A) \cap \mathcal{C}(B)$ coincides with the set of left (right) singular vectors of $D(A, B)$ with singular value 1.*
2. *On $\mathcal{C}(A) \cap \mathcal{C}(B)^\perp$ operator W acts as reflection on the center (i.e. as $-I$). $\mathcal{C}(A) \cap \mathcal{C}(B)^\perp$ coincides with the set of left singular vectors of $D(A, B)$ with singular value 0.*

3. On $\mathcal{C}(B) \cap \mathcal{C}(A)^\perp$ operator W acts as reflection on the center. $\mathcal{C}(B) \cap \mathcal{C}(A)^\perp$ coincides with the set of right singular vectors of $D(A, B)$ with singular value 0.
4. On $\mathcal{C}(A)^\perp \cap \mathcal{C}(B)^\perp$ operator W acts as the identity.

The above is a complete description of the eigenvalues and eigenvectors of operator W acting on H .

Proof. Let $\pi_A = AA^*$ and $\pi_B = BB^*$ be the orthogonal projector operators (in H) to $\mathcal{C}(A)$ and $\mathcal{C}(B)$, respectively. Then $W = (2\pi_B - I)(2\pi_A - I)$. Since for every v, w singular vector pair with singular value $\cos \theta$ we have $\pi_A Bv = (\cos \theta)Aw$ and $\pi_B Aw = (\cos \theta)Bv$ we can conclude that the (at most) two-dimensional subspace $\langle Bv, Aw \rangle$ is invariant under the action W . Moreover, this action is a composition of two reflections, the first on axis Aw and then on axis Bv . The case when $\langle Bv, Aw \rangle$ is one dimensional gives 1-3, and we leave this easy case to the reader. The subspace $\langle Bv, Aw \rangle$ is two-dimensional if and only if $\cos \theta \in (0, 1)$. Considering that the angle between Bv and Aw is θ , the formulas for the spectrum and eigenvalues of W on $\langle Bv, Aw \rangle$ follow from the familiar expressions for the two dimensional case. In particular, it is well known that if we reflect on two axes, we obtain a rotation with an angle that is twice of the one between the axes. Since the set of left and right singular vectors form complete systems, we are done with the description of W on $\langle \mathcal{C}(A), \mathcal{C}(B) \rangle$. We need to describe W on $\langle \mathcal{C}(A), \mathcal{C}(B) \rangle^\perp = \mathcal{C}(A)^\perp \cap \mathcal{C}(B)^\perp$. On this subspace W is simply a product of two reflections on the center, therefore it is the identity. \square

3.2 Application of Syzedegy's Walk for sampling Markov Chains

Let $\mathcal{H} = \mathbb{C}^N \otimes \mathbb{C}^N$. The basis states of \mathcal{H} are denoted by $|xy\rangle$ for $x, y \in \Omega$. For $x \in \Omega$, define the normalized vectors

$$|p_x\rangle = \sum_{y \in \Omega} \sqrt{p_{xy}} |y\rangle$$

where p_{xy} denotes the transition probability from x to y . A quantum update is any unitary U that satisfies

$$U|x\rangle|0\rangle = |x\rangle|p_x\rangle$$

for some fixed state $0 \in \Omega$ and all $x \in \Omega$. We refer to the cost to realize U and its inverse U^\dagger as the quantum update cost.

To construct the quantum walk, we define the subspaces

$$\begin{aligned} \mathcal{A} &= \text{span}\{|x\rangle|0\rangle : x \in \Omega\} \\ \mathcal{B} &= U^\dagger S U \mathcal{A} \end{aligned}$$

where S denotes that the unitary operator swapping the two tensor components of \mathcal{H} . For $\mathcal{K} = \mathcal{A}, \mathcal{B}$, denote by $\Pi_{\mathcal{K}}$ the orthogonal projection onto \mathcal{K} and by

$$R_{\mathcal{K}} = 2\Pi_{\mathcal{K}} - I.$$

the reflection around \mathcal{K} .

Definition 3.1 (Quantum Walk). *The quantum walk $W(P)$ based on the classical reversible Markov chain P is defined to be the unitary operation (rotation)*

$$W(P) = R_{\mathcal{B}} \cdot R_{\mathcal{A}}$$

The quantum walk $W(P)$ can be realized by applying both U and U^\dagger twice:

$$W(P) = U^\dagger \cdot S \cdot U \cdot R_{\mathcal{A}} \cdot U^\dagger \cdot S \cdot U \cdot R_{\mathcal{A}}.$$

This is different from the definition used in the previous subsection which is.

$$\tilde{W}(P) = R_{\tilde{\mathcal{B}}} \cdot R_{\tilde{\mathcal{A}}}$$

where

$$\tilde{\mathcal{A}} = \text{span} \{ |x\rangle |p_x\rangle : x \in \Omega \} = U\mathcal{A}$$

$$\tilde{\mathcal{B}} = \text{span} \{ |p_x\rangle |x\rangle : x \in \Omega \} = U\mathcal{B}.$$

Since $W(P)$ and $\tilde{W}(P)$ are equal up to conjugation by U , we can apply the spectral analysis from previous section to determine the spectrum of $W(P)$. We refer to the subspace $\mathcal{A} + \mathcal{B}$ as the busy subspace and to its orthogonal complement, i.e., $\mathcal{A}^\perp \cap \mathcal{B}^\perp$, as the idle subspace. Clearly, the operator $W(P)$ acts as identity on the idle subspace. On the busy subspace, the spectrum of $W(P)$ is as follows.

Theorem 3.3. *Let P be a time-reversible Markov chain. Let $\theta_1, \dots, \theta_M \in (0, \frac{\pi}{2})$ be such that $|\lambda_1| = \cos(\theta_1), \dots, |\lambda_M| = \cos \theta_M$ where $M \leq N - 1$ and the remaining eigenvalues are equal to 0, i.e., $\lambda_{M+1}, \dots, \lambda_{N-1} = 0$.*

1. *On $\mathcal{A} \cap \mathcal{B}$ the operator $W(P)$ acts as the identity I . This subspace is one dimensional and is spanned by the eigenvector $|\pi\rangle|0\rangle$ where*

$$|\pi\rangle = \sum_x \sqrt{\pi_x} |x\rangle$$

is the quantum sample of the stationary distribution π of P .

2. *On $\mathcal{A} \cap \mathcal{B}^\perp$ and $\mathcal{A}^\perp \cap \mathcal{B}$ the operator $W(P)$ acts as $-I$. The dimensions of $\mathcal{A} \cap \mathcal{B}^\perp$ and $\mathcal{A}^\perp \cap \mathcal{B}$ are equal to $N - 1 - M$, i.e., the dimension of the kernel of P .*
3. *On $\mathcal{A} + \mathcal{B}$ those eigenvalues of $W(P)$ that have nonzero imaginary part are exactly $e^{\pm 2i\theta_1}, \dots, e^{\pm 2i\theta_M}$ with the same multiplicity.*

4. $W(P)$ has no other eigenvalues on $\mathcal{A} + \mathcal{B}$.

Now we have the following lemmas which lead us to the main result of how to sample using the markov chain.

Lemma 3.4. *Let $|t_0\rangle, \dots, |t_r\rangle$ be arbitrary quantum states in \mathbb{C}^d with $|\langle t_i | t_{i+1} \rangle|^2 \geq p$ for $i = 0, \dots, r-1$. Given the state $|t_0\rangle$, we can prepare a state $|\tilde{t}_r\rangle$ such that*

$$\| |\tilde{t}_r\rangle - |t_r\rangle \| \leq \epsilon_1,$$

for any $\epsilon_1 > 0$, by invoking the unitaries from $\{R_i, R_i^\dagger : i = 0, \dots, r\}$ no more than

$$L = \frac{12r \log(2r/\epsilon_1)}{\log(1/(1-p))}$$

times. Where R_i is defined as the $(2\Pi_i - 1)$, and $\Pi_i = |t_i\rangle\langle t_i|$

Lemma 3.5. *Let W be a unitary acting on \mathbb{C}^d with unique eigenvector $|\psi_0\rangle$ with eigenvalue $\lambda_0 = 1$. Denote the remaining eigenvectors and eigenvalues of W by $|\psi_j\rangle$ and $\lambda_j = e^{2\pi i \varphi_j}$ for $j = 1, \dots, d-1$, respectively. Let*

$$\Delta = \min_{j=1, \dots, d-1} |\varphi_j|$$

be the phase gap of W . Let Π be the projector onto the space spanned by $|\psi_0\rangle$ and Π^\perp the projector onto the orthogonal complement. Let R be the unitary that acts on \mathbb{C}^d as follows

$$R = \omega \Pi + \Pi^\perp.$$

Let

$$\begin{aligned} a &= \lceil \log(1/\Delta) \rceil \\ c &= \lceil \log(1/\sqrt{\epsilon_2}) \rceil \end{aligned}$$

for some $\epsilon_2 > 0$. Then, there is a quantum circuit \tilde{R} acting on $\mathbb{C}^d \otimes (\mathbb{C}^2)^{\otimes ac}$ that invokes the controlled- W gate $2^{a+1} \cdot c$ times and has the following properties: for $j = 0$,

$$\tilde{R} |\psi_0\rangle |0\rangle^{\otimes ac} = (R |\psi_0\rangle) |0\rangle^{\otimes ac}$$

and for $j \neq 0$,

$$\tilde{R} |\psi_j\rangle |0\rangle^{\otimes ac} = (R |\psi_j\rangle) |0\rangle^{\otimes ac} + |\xi\rangle,$$

where $|\xi\rangle$ is some error vector in $\mathbb{C}^d \otimes (\mathbb{C}^2)^{\otimes ac}$ with

$$\| |\xi\rangle \| \leq 2\sqrt{\epsilon_2}.$$

The above two lemmas give us the following theorem . We will quote the following paper () for the proves of the above lemmas. Lemma 3.4 is proved using Grover's Amplitude Amplification for whose proof we quote the following paper ().

Theorem 3.6. *Let P_0, P_1, \dots, P_r be classical Markov chains with stationary distributions $\pi_0, \pi_1, \dots, \pi_r$ and spectral gaps $\delta_0, \delta_1, \dots, \delta_r$, respectively. Assume the stationary distributions of adjacent Markov chains are close to each other in the sense that their stationary distributions π_i and π_{i+1} are close with respect to fidelity, i.e.,*

$$\left(\sum_{x \in \Omega} \sqrt{\pi_i(x)} \sqrt{\pi_{i+1}(x)} \right)^2 = |\langle \pi_i | \pi_{i+1} \rangle|^2 \geq p$$

for $i = 0, \dots, r-1$,

$$\min \{ \delta_i : i = 0, \dots, r \} \geq \delta,$$

and we can prepare the quantum sample $|\pi_0\rangle$. Then, for any $\epsilon > 0$, there is a quantum sampling algorithm, making it possible to sample according to a probability distribution $\tilde{\pi}_r$ that is close to π_r with respect to the total variation distance, i.e., $D(\tilde{\pi}_r, \pi_r) \leq \epsilon$.

The algorithm invokes the controlled- W_i operators at most $2^{a+1} \cdot c \cdot L$ times where

$$\begin{aligned} L &= \frac{12r \log(8r/\epsilon)}{\log(1/(1-p))} \\ a &= \lceil \log(1/\Delta) \rceil \\ c &= \left\lceil \log \left(\frac{96r \log(8r/\epsilon)}{\epsilon \log(1/(1-p))} \right) \right\rceil. \end{aligned}$$

Proof. Lemma 3.4 shows that, given the initial state $|\pi_0\rangle$, we can prepare a state $|\tilde{\pi}_r\rangle$ with $\| |\pi_r\rangle - |\tilde{\pi}_r\rangle \| \leq \epsilon_1$ by invoking the unitaries from the set $\{ R_i, R_i^\dagger : i = 0, \dots, r-1 \}$ no more than

$$L = \frac{12r \log(2r/\epsilon_1)}{\log(1/(1-p))}$$

times. In Lemma 3.4 we assumed that we can implement these exactly. However, in reality we can only implement the operators \tilde{R}_i and their inverses \tilde{R}_i^\dagger as described in Lemma 3.5. This approximation adds an error vector $|\xi\rangle$ every time an operator \tilde{R}_i or \tilde{R}_i^\dagger is applied, where $\| |\xi\rangle \| \leq 2\sqrt{\epsilon_2}$ for some $\epsilon_2 > 0$.

Let $|\tilde{\psi}\rangle$ be the state obtained by implementing Lemma 3.5 using \tilde{R}_i to approximate R_i . Then, since these operators or their inverses are invoked no more than L times we have

$$|\tilde{\psi}\rangle = |\tilde{\pi}_r\rangle_{\mathcal{H}} |0\rangle_{\mathcal{A}}^{\otimes ac'} + |\xi\rangle$$

where $c' = \lceil \log(1/\sqrt{\epsilon_2}) \rceil$ and $|\xi\rangle$ is some vector with

$$\| |\xi\rangle \| \leq 2L\sqrt{\epsilon_2}.$$

\mathcal{H} is the Hilbert space that our quantum samples live in and \mathcal{A} is the Hilbert space of the ancilla qubits that are required to implement the approximate phase gates \tilde{R}_i and their inverses.

Let

$$|\psi\rangle = |\pi_r\rangle |0\rangle^{\otimes ac}$$

be the ideal state. We choose $\epsilon_1 = \epsilon/4$ and $\epsilon_2 = \epsilon^2/(64L^2)$ so that

$$\begin{aligned} \| |\psi\rangle - |\tilde{\psi}\rangle \| &\leq \| |\psi\rangle - |\tilde{\pi}_r\rangle |0\rangle^{\otimes ac} \| + \| |\tilde{\pi}_r\rangle |0\rangle^{\otimes ac} - |\tilde{\psi}\rangle \| \\ &\leq \epsilon_1 + 2L\sqrt{\epsilon_2} \\ &= \epsilon/4 + \epsilon/4 \\ &= \epsilon/2. \end{aligned}$$

For each $x \in \Omega$, we define the projector

$$\Lambda_x = |x\rangle\langle x| \otimes |0\rangle\langle 0|^{\otimes ac}$$

acting on $\mathcal{H} \otimes \mathcal{A}$. Let

$$\Lambda_0 = I_{\mathcal{H}\mathcal{A}} - I_{\mathcal{H}} \otimes |0\rangle\langle 0|^{\otimes ac}.$$

Let $\Omega' = \Omega \cup \{0\}$. Observe that the desired distribution π is equal to the probability distribution given by

$$\pi(x) = \|\Lambda_x |\psi\rangle\|^2.$$

Our protocol yields the probability distribution

$$\tilde{\pi}(x) = \|\Lambda_x |\tilde{\psi}\rangle\|^2.$$

We now bound the total variation distance between π and $\tilde{\pi}$ from above. For a subset $S \subseteq \Omega'$, let

$$\Lambda_S = \sum_{x \in S} \Lambda_x$$

We have

$$\begin{aligned} D(\pi, \tilde{\pi}) &= \max_{S \subseteq \Omega'} |\pi(S) - \tilde{\pi}(S)| \\ &= \max_{S \subseteq \Omega'} \left| \|\Lambda_S |\psi\rangle\|^2 - \|\Lambda_S |\tilde{\psi}\rangle\|^2 \right| \\ &\leq 2 \max_{S \subseteq \Omega'} \left| \|\Lambda_S |\psi\rangle\| - \|\Lambda_S |\tilde{\psi}\rangle\| \right| \\ &\leq 2 \| |\psi\rangle - |\tilde{\psi}\rangle \| \\ &\leq \epsilon \end{aligned}$$

It follows from above lemmas that we invoke the controlled- W_i operators or their inverses at most $2^{a+1} \cdot c \cdot L$ times. \square

We would like to use the above theorem to implement our intermediate Markov Chains as they also don't change much in subsequent iterations we would like to use the above algorithm to perform our desired sampling. For that we need to implement the walk operators W_i 's. As we can see we use a metropolis filter in the classical algorithm to get a certain probability distribution. So we need to find a method which implements the walk operators W_i given a set of parameters for the metropolis rule.

3.3 Implementing the walk operators

We will try to use the ideas of the following paper () to implement a walk operator. A brief of the ideas of the paper is written below. Here we will want to prepare a distribution over eigen states of a general hamiltonian. We want a state with the following density operator

$$\rho = \sum_{i \in \Omega} \pi_i |\varphi_i\rangle \langle \varphi_i|$$

, Where φ_i are the eigenstates of a general hamiltonian and π is the stationary probability distribution of a Markov chain over Ω whose transition rule is guided by a metropolis filter. We have

$$\pi_i m_{ij} = \pi_j m_{ji}$$

$$m_{ij} = s_{ij} \cdot z_{ij}$$

$$s_{ij} = s_{ji}$$

$$z_{ij} = \min\{1, \frac{\pi_j}{\pi_i}\}$$

We will denote π_i by $e^{-\beta E_i}$, just to follow the notation of the paper. We will design an unitary for which we get the above state by tracing out from an unique eigenvector with eigenvalue 1 on a certain subspace.

Now the implementation of the paper is as follows.

Now, let us include into our Hilbert space an extra qubit initialized in $|0\rangle$ and define a more compact notation,

$$|i\rangle \equiv |\varphi_i\rangle |\tilde{\varphi}_i\rangle |0\rangle$$

The information of a Markov chain can be encoded in a pair of unitary operators U_X and U_Y (We will define the construction of U_X in the following part),

$$U_X|i\rangle = \sum_k (\sigma_{ik} |\varphi_i\rangle |\varphi_k\rangle |0\rangle + \gamma_{ik} |\varphi_i\rangle |\varphi_k\rangle |1\rangle)$$

$$U_Y|j\rangle = \sum_m (\sigma_{jm} |\varphi_m\rangle |\varphi_j\rangle |0\rangle + \gamma_{jm} |\varphi_j\rangle |\varphi_m\rangle |1\rangle)$$

where $\sigma_{ik} \equiv \alpha_{k\bar{i}} \sqrt{z_{ik}}$, $\gamma_{ik} \equiv \alpha_{k\bar{i}} \sqrt{1 - z_{ik}}$, and $\alpha_{k\bar{i}} \equiv \langle \varphi_k | K | \tilde{\varphi}_i \rangle$. Here K is an unitary operator which encodes the transition without the metropolis filter (we will go in detail in the construction part). Note that U_Y can be obtained from U_X by controlled-SWAP operation.

From the definitions of U_X and U_Y we get that -

$$\langle j | U_X^\dagger U_Y | i \rangle = |\alpha_{j\bar{i}}|^2 (z_{ij} z_{ji})^{1/2},$$

where we used $\langle \varphi_i | \tilde{\varphi}_j \rangle = \langle \varphi_j | \tilde{\varphi}_i \rangle$. On the other hand,

$$\langle i | U_X^\dagger U_Y | i \rangle = |\alpha_{i\bar{i}}|^2 + \sum_k |\alpha_{k\bar{i}}|^2 (1 - z_{ik}),$$

which, as we shall see, can be interpreted as the probability of not undergoing a transition.

Construction of the operator W - Now, using above equation, we obtain the following decomposition:

$$\langle j | U_X^\dagger U_Y | i \rangle = \langle j | D_\pi^{1/2} | j \rangle \langle j | M | i \rangle \langle i | D_\pi^{-1/2} | i \rangle$$

where $D_\pi \equiv \sum_{j=0}^{N-1} \pi_j |j\rangle \langle j|$ is a diagonal matrix, and $M \equiv \sum_{i,j} m_{ij} |j\rangle \langle i|$, with $m_{ii} \equiv \langle i | U_X^\dagger U_Y | i \rangle$ and $m_{ij} \equiv |\alpha_{j\bar{i}}|^2 z_{ij}$ for $j \neq i$ is the transition matrix of the Markov chain. Within the subspace $\{|i\rangle\}$, the above equation implies that $U_X^\dagger U_Y$ and M are similar matrices, which means that they have the same set of eigenvalues λ_k . This property allows us to construct an operator

$$W \equiv (2\Lambda_2 - I) (2\Lambda_1 - I) \quad ,$$

where

$$\Lambda_1 \equiv \sum_{i=0}^{N-1} |i\rangle \langle i| \quad \text{and} \quad \Lambda_2 \equiv U_X^\dagger U_Y \Lambda_1 U_Y^\dagger U_X.$$

The spectral properties of W can be seen in the following way: define $|\alpha_k\rangle \equiv \sum_{i=0}^{N-1} a_{ki} |i\rangle$ to be the eigenvectors of $\Lambda_1 U_X^\dagger U_Y \Lambda_1$, the eigenvalue equation can be written as

$$\Lambda_1 U_X^\dagger U_Y |\alpha_k\rangle = \lambda_k |\alpha_k\rangle.$$

On the other hand, using the fact that $\Lambda_1 U_X^\dagger U_Y \Lambda_1 = \Lambda_1 U_Y^\dagger U_X \Lambda_1$, we have,

$$\Lambda_2 |\alpha_k\rangle = \lambda_k U_X^\dagger U_Y |\alpha_k\rangle.$$

Now if we start with vectors within Λ_1 , W can be block-diagonalized into subspace of 2×2 matrices w_k spanned by the basis $\{|\alpha_k\rangle, U_X^\dagger U_Y |\alpha_k\rangle\}$. Explicitly,

$$w_k = \begin{bmatrix} \cos(2\theta_k) & -\sin(2\theta_k) \\ \sin(2\theta_k) & \cos(2\theta_k) \end{bmatrix},$$

where $\cos \theta_k \equiv \lambda_k$. Note that the eigenvalues of w_k is $e^{\pm i\theta_k}$. In the case of $k = 0$ where $\lambda_0 = 1$ (or $\theta_0 = 0$), $w_0 = I$ is simply an identity. Now we get that ,

$$|\alpha_0\rangle = \sum_{i=0}^{N-1} \sqrt{\pi_i} |i\rangle.$$

Recall that $|i\rangle \equiv |\varphi_i\rangle |\tilde{\varphi}_i\rangle |0\rangle$, the state $|\alpha_0\rangle$ becomes the Gibbs thermal state $\rho_{th} = e^{-\beta H} / \text{Tr} [e^{-\beta H}]$ when the other qubits are traced out.

One of the most important features about W is that the minimum eigenvalue gap $\Delta_{\min} \equiv |2\theta_1|$ of W is less than two times the square root of the gap $\delta \equiv 1 - \lambda_1$ of the transition matrix M (using $2\theta \geq |1 - e^{2i\theta}| = 2\sqrt{1 - \cos^2 \theta}$)

$$\Delta_{\min} \geq 2\sqrt{\delta}$$

Construction of U_X - Here we show how one may construct the unitary operator U_X defined as

$$U_X |i\rangle = \sum_k (\sigma_{ik} |\varphi_i\rangle |\varphi_k\rangle |0\rangle + \gamma_{ik} |\varphi_i\rangle |\varphi_k\rangle |1\rangle),$$

where

$$\sigma_{ik} \equiv \alpha_{k\tilde{i}} \sqrt{z_{ik}} \quad , \quad \gamma_{ik} \equiv \alpha_{k\tilde{i}} \sqrt{1 - z_{ik}}$$

and

$$\alpha_{k\tilde{i}} \equiv \langle \varphi_k | K | \tilde{\varphi}_i \rangle.$$

Here K is an unitary operator which plays the same role as the spin-flip in the classical Metropolis method(K in the basis $\{|\varphi_i\rangle\}_i$ is kind of equivalent to transition without the metropolis filter), and z_{ik} is the Metropolis filter . Note that U_Y can be obtained from U_X by a controlled-SWAP. We assume that K is symmetrical in the computational basis:

$$\langle x' | K | x \rangle = \langle x | K | x' \rangle.$$

We are now ready to consider the explicit procedure for constructing U_X . Starting with the paired state

$$|\varphi_i\rangle |\tilde{\varphi}_i\rangle$$

we apply the "kick" operator K to $|\tilde{\varphi}_i\rangle$, and write

$$K |\tilde{\varphi}_i\rangle = \sum_k \alpha_{k\tilde{i}} |\varphi_k\rangle.$$

Next, we implement the Metropolis filter by performing a controlled-rotation (based on the difference of the eigenvalues):

$$|\varphi_i\rangle |\varphi_k\rangle |0\rangle \rightarrow |\varphi_i\rangle |\varphi_k\rangle (\sqrt{z_{ik}} |0\rangle + \sqrt{1 - z_{ik}} |1\rangle),$$

where

$$z_{ij} \equiv \left\{ 1, e^{-\beta(E_j - E_i)} \right\}$$

This creates a state as described by definition of U_X .

For our use we will have $|q\rangle \equiv |M_q\rangle|M_q\rangle|0\rangle$ where $|M_q\rangle$ will have $n\lceil\log(n)\rceil$ qubits where we will have n registers of $\lceil\log(n)\rceil$ qubits representing if register i has $|j\rangle$ on it then in the matching M_q the i th vertex in left bipartition is connected to the j th vertex in the right bipartition. For us $|\varphi_i\rangle = |\tilde{\varphi}_i\rangle = |M_i\rangle$ as described above. And for implementing the kick operator we could have an extra register. Now when we want to apply kick operator on $|M_i\rangle|M_i\rangle|0\rangle$ to get $|M_i\rangle\sum_j \alpha_{ij}|M_j\rangle|0\rangle$ we could just use an ancilla and apply H gate on that ancilla to get a superposition over all outcomes of a random coin toss as described in the classical algorithm and according to it we will modify the second register to get M_j from M_i according to the toss outcome then we will uncompute the ancilla register using $|M_i\rangle$ and $|M_j\rangle$.

4 Quantum Algorithm for Approximately Counting Number of Perfect Matchings

In this section we will try to give an algorithm using the above sections to give a $\tilde{O}(n^5)$ quantum algorithm for approximately counting number of perfect matchings in a bipartite graph.

We know from the analysis of the (envaz) paper that the Markov Chains we get in the (envaz) paper in every iteration has spectral gap of order $O(1/n^4)$ and so if we use the method described in Theorem 3.6 to construct we will use $\tilde{O}(n^2)$ many applications of W_{i+1} to get from π_i to π_{i+1} . To construct W_i we will use the method from section 3.3. Also for knowing the parameters in order to construct W_{i+1} we need to sample from π_i without destructing π_i . For doing this we will describe an algorithm to do amplitude estimation for multiple states without destroying the original superposition. So our complexity is like $\tilde{O}(n^2)$ for the mixing of markov chain $\tilde{O}(n^2)$ samples at each iteration and $\tilde{O}(n)$ iterations. So in total we have $\tilde{O}(n^5)$ complexity.

4.1 Multidimensional Amplitude Estimation

In order to sample from the states at each iteration we will use the following technique to get the amplitude of each state (here for each hole pattern) using the walk operators. We have the following lemmas from the paper (multidimamp).

First of all we will give some definitions-

Definition 4.1 (Quantum Probability Oracle). *Let $p \in \Delta^n$ be a probability distribution. We say that O_p is a quantum probability oracle for p if*

$$O_p|0\rangle = \sum_{i=1}^n \sqrt{p_i}|i\rangle |\psi_i\rangle$$

for some quantum states $|\psi_1\rangle, \dots, |\psi_n\rangle$. That is, applying O_p to the $|0\rangle$ state and measuring the first register is the same as sampling from p .

We can't implement quantum probability oracle multiple times we have one copy of the state which we get after applying the probability oracle and the walk operator for which the output of the probability oracle is a unique eigenvector with eigenvalue 1 on the busy subspace. So we will modify the main theorem a little bit since we want the theorem to give us answers in terms of quantum walk operator rather than quantum probability oracle.

Definition 4.2 (Oracles for functions). *Let $f : D \rightarrow [0, 1]$ be a $[0, 1]$ valued function from a discrete domain D . A probability oracle for the function f is a unitary U_f that acts as*

$$U_f |x\rangle |0\rangle |0\rangle = |x\rangle \left(\sqrt{f(x)} |1\rangle |\psi_1^x\rangle + \sqrt{1-f(x)} |0\rangle |\psi_0^x\rangle \right).$$

Definition 4.3 (Phase oracle). *A phase oracle for the function f is a unitary U_f that acts as*

$$U_f |x\rangle = e^{if(x)} |x\rangle.$$

We want to implement phase oracle for the function $\langle x, p \rangle$. Upon implementation of phase oracle we could use the following algorithm to do all state amplitude estimation in one go -

Let $k = \lceil \log(4/\varepsilon) \rceil$. Consider the following algorithm:

1. Start in a n -register all zero state, where each register as k qubits:

$$|0^k\rangle \dots |0^k\rangle$$

2. Apply Hadamard gates to all qubits to obtain

$$\bigotimes_{i=1}^n \left(\frac{1}{\sqrt{2^k}} \sum_{x_i=0}^{2^k-1} |x_i\rangle \right) = \frac{1}{2^{kn/2}} \sum_{x \in \{0, 2^k-1\}^n} |x\rangle$$

- 3.

$$\begin{aligned} \frac{1}{2^{kn/2}} \sum_{x \in \{0, 2^k-1\}^n} e^{i\langle x, p \rangle} |x\rangle &= \frac{1}{2^{kn/2}} \sum_{x \in \{0, 2^k-1\}^n} e^{i \sum_i x_i p_i} |x\rangle \\ &= \frac{1}{2^{kn/2}} \sum_{x \in \{0, 2^k-1\}^n} \left(\prod_{i=1}^n e^{i x_i p_i} \right) |x\rangle \\ &= \bigotimes_{i=1}^n \left(\frac{1}{\sqrt{2^k}} \sum_{x_i=0}^{2^k-1} e^{i x_i p_i} |x_i\rangle \right) \end{aligned}$$

4. Apply the k -qubit inverse QFT to each of the n registers and measure each register.

Now we would want to approximately implement the phase oracle given one copy of the distribution state and the walk operator for the distribution.

We have the following algorithm to approximately implement U_f for $f = \langle x, p \rangle$ using O_p as follows

Lemma 4.1. *Let U_p be a quantum probability oracle for a distribution $p \in \Delta^n$. Let $k \geq 1$ be an integer and let $D = \left\{0, \frac{1}{2^k}, \dots, \frac{2^k-1}{2^k}\right\}$ be a discretization of $[0, 1]$. Then a probability oracle $U_{\tilde{f}}$ for a function \tilde{f} can be constructed such that \tilde{f} is an additive μ -approximation of $f(x) : D^n \rightarrow [0, 1] : x \mapsto \langle x, p \rangle$ using 2 queries to U_p and $\tilde{O}(n \text{ polylog}(1/\mu))$ two-qubit gates.*

Proof. We start in a state $|x\rangle|0\rangle|0\rangle|0\rangle|0\rangle$. First we apply $U_f \otimes I$ to obtain

$$|x\rangle \left(\sum_{i=1}^n \sqrt{p_i} |i\rangle |\psi_i\rangle \right) |0\rangle |0\rangle$$

Now, for each $i \in [n]$ we do the following conditioned on i being in the second register:

1. In the last register, compute an approximation of $2 \arcsin(\sqrt{x_i})/\pi$ such that the approximation is in $[0, 1]$.
2. Conditioned on the first bit of the approximation rotate the second to last register from $|0\rangle$ to $|1\rangle$ over an angle $\pi/4$.
3. Continue for the other bits: rotate over an angle $\pi/8$ conditioned on the second bit, then $\pi/16$, and so on.
4. Uncompute the last register.

Note that we can approximate the arcsin very efficiently, only introducing a logarithmic overhead in terms of the precision. In the end the second to last register will be rotated over an angle very close to $2 \arcsin(x_i)/\pi \times \pi/2 = \arcsin(x_i)$. We finish the analysis as if the angle was exact. We end up with (after dropping the last register which is now $|0\rangle$ again)

$$|x\rangle \sum_{i=1}^n \sqrt{p_i} |i\rangle |\psi_i\rangle (\sqrt{x_i} |1\rangle + \sqrt{1-x_i} |0\rangle) = |x\rangle \sum_{i=1}^n \sqrt{p_i x_i} |i\rangle |\psi_i\rangle |1\rangle + \dots |0\rangle.$$

5. The ℓ_2 -norm of the $|1\rangle$ part of the state is $\sqrt{\sum_{i=1}^n \sqrt{p_i x_i}} = \sqrt{\langle x, p \rangle}$. We conclude that the state can be written as

$$\sqrt{\langle x, p \rangle} |x\rangle |\psi_{x,1}\rangle |1\rangle + \sqrt{1 - \langle x, p \rangle} |x\rangle |\psi_{x,0}\rangle |0\rangle,$$

and hence we have implemented a probability oracle for f . Now let the steps of the above algorithm after construction of $|x\rangle \left(\sum_{i=1}^n \sqrt{p_i} |i\rangle |\psi_i\rangle \right) |0\rangle |0\rangle$ be denoted by Q .

□

Now we will use the following theorem from (tophase) -

Theorem 4.2. *Let $p : X \rightarrow [0, 1]$, and suppose $U_p : \mathcal{H} \otimes \mathcal{H}_{aux.} \rightarrow \mathcal{H} \otimes \mathcal{H}_{aux.}$ is a probability oracle with an n -qubit auxiliary Hilbert space $\mathcal{H}_{aux.} = \mathbb{C}^{2^n}$. Let $\varepsilon \in (0, 1/3)$, then we can implement an ε -approximate phase oracle O such that for any phase oracle O_p and for all $|\psi\rangle \in \mathcal{H}$*

$$\|O|\psi\rangle|0\rangle^{\otimes(n+a)} - O_p|\psi\rangle|0\rangle^{\otimes(n+a)}\| \leq \varepsilon,$$

using $\mathcal{O}(\log(1/\varepsilon))$ applications of U_p and U_p^\dagger , with $a = \mathcal{O}(\log \log(1/\varepsilon))$.

Note that in the above paper we use U_p and U_p^\dagger in the form of

$$G_U = (2\Pi_1 - 1)U_p^\dagger(2\Pi_2 - 1)U_p$$

where $\Pi_1 = (I \otimes (|0\rangle\langle 0|)^{\otimes n})$ and $\Pi_2 = I \otimes (I_{n-1} \otimes |1\rangle\langle 1|)$

From the paper we need to implement powers of G_U on the register $|x\rangle|\vec{0}\rangle$.

Now consider H to be the quantum operator $H = U_p(2\Pi_1 - I)U_p^\dagger(2\Pi_2 - I)$. Now note that $G^m|x\rangle|\vec{0}\rangle = U_p^\dagger H^m(U_p|x\rangle|\vec{0}\rangle)$. Since we initially have $U_p|x\rangle|\vec{0}\rangle$ prepared for us upon application of powers of H and implementing their powers of sum we get $e^{i\langle x, p \rangle} U_p|x\rangle|\vec{0}\rangle$ in approximation. So now we could uncompute the bits used in Lemma 4.1 and apply quantum phase estimation on the register of $|x\rangle$ as mentioned earlier then measure to get approximation for p_i 's then after measurement we will be left with the probability distribution state in the remaining register which we can reuse for sampling and computing mean of λ_{i+1}/λ_i (using non destructive method mentioned below) and also for the construction of stationary distribution for next iteration. Now in order to implement H we need to implement $U_p(2\Pi_1 - I)U_p^\dagger$ which we can easily do using the walk operator W by doing phase estimation using W and reflecting controlled on the phase to be equal to 0 then doing inverse of phase estimation. To do this we need to apply $W \tilde{O}(1/\sqrt{\delta})$ which in our case is $\tilde{O}(n^2)$ many times. So we get the following version of the theorem from (multidimamp) paper.

Theorem 4.3. *Let $p \in \Delta^n$ and let U_p be a quantum probability oracle acting on q qubits for p . Let $\varepsilon > 0$. An approximation \tilde{p} such that $\|p - \tilde{p}\|_\infty \leq \varepsilon$ can be found with error probability at most δ using $\mathcal{O}(\ln(n/\delta)/\varepsilon \cdot \frac{1}{\sqrt{\Delta}})$ applications of W and $\tilde{O}(\ln(\delta)qn/\varepsilon)$ two-qubit gates. Where Δ is the spectral gap of the markov chain classically, whose walk operator is W .*

4.2 Non-destructive Amplitude Estimation

Lemma 4.4. *Consider a quantum algorithm that consists of applying a unitary U on a state $|\psi\rangle|0\rangle^{\otimes k}$ and measuring the last k qubits in the standard basis. Let $\pi(1), \dots, \pi(2^k)$ denotes the probabilities of measuring the outcomes $1, \dots, 2^k$*

respectively. Then, given a lower bound $\lambda \leq \sum_{i=1}^{2^k} \pi(i)^2$ and a success parameter $\eta \in (0, 1)$, one can sample $i \in \{1, \dots, 2^k\}$ from the distribution

$$i \sim \frac{\pi(i)^2}{\sum_{j=1}^{2^k} \pi(j)^2}$$

and restore the state $|\psi\rangle$ with probability at least $1 - \eta$ by using $O(\log(1/\eta)/\sqrt{\lambda})$ applications of U, U^\dagger and $\mathbb{I} - 2|\psi\rangle\langle\psi|$.

Proof. Proof. Let $U(|\psi\rangle|0\rangle^{\otimes k}) = \sum_i \alpha_i |\psi_i\rangle |i\rangle$ denote the state computed by the unitary U . Define the "uncomputation" unitary $U_{\text{uncomp}} = (U^\dagger \otimes \mathbb{I}_{\mathbb{C}^{2^k}})(\mathbb{I}_{\mathcal{H}} \otimes \text{CNOT})(U \otimes \mathbb{I}_{\mathbb{C}^{2^k}})$ that consists of running U , copying the output register into a new register and running the inverse U^\dagger . Then, the amplitude of $|\psi\rangle|0\rangle|i\rangle$ in the state obtained by applying U_{uncomp} on $|\psi\rangle|0\rangle^{\otimes k}|0\rangle^{\otimes k}$ is

$$(\langle\psi|\langle 0|\langle i|)U_{\text{uncomp}}(|\psi\rangle|0\rangle|0\rangle) = \left(\sum_j \alpha_j^* \langle\psi_j|\langle j|\langle i|\right) \left(\sum_j \alpha_j |\psi_j\rangle|j\rangle|j\rangle\right) = |\alpha_i|^2 = \pi(i)$$

We run fixed-point amplitude amplification [YLC14] on the projector $\Pi = |\psi\rangle\langle\psi| \otimes |0\rangle\langle 0| \otimes \mathbb{I}$ and the state $U_{\text{uncomp}}(|\psi\rangle|0\rangle|0\rangle)$, using the amplitude lower bound $\|\Pi U_{\text{uncomp}}(|\psi\rangle|0\rangle|0\rangle)\|^2 \geq \lambda$ and the amplification parameter η . The probability of measuring $|\psi\rangle|0\rangle$ in the first two registers of the resulting state is at least $1 - \eta$, in which case the last register collapses to $\frac{1}{\sqrt{\sum_i \pi(i)^2}} \sum_i \pi(i)|i\rangle$.

Thus, we can restore $|\psi\rangle$ and sample $i \sim \frac{\pi(i)^2}{\sum_j \pi(j)^2}$ (by measuring the last register) with success probability at least $1 - \eta$. The algorithm requires $O(\log(1/\eta)/\sqrt{\lambda})$ applications of (controlled) $U_{\text{uncomp}}, U_{\text{uncomp}}^\dagger, \mathbb{I} - 2\Pi$ and $\mathbb{I} - 2|\psi\rangle\langle\psi|$. Proof. Let $U(|\psi\rangle|0\rangle^{\otimes k}) = \sum_i \alpha_i |\psi_i\rangle |i\rangle$ denote the state computed by the unitary U . Define the "uncomputation" unitary $U_{\text{uncomp}} = (U^\dagger \otimes \mathbb{I}_{\mathbb{C}^{2^k}})(\mathbb{I}_{\mathcal{H}} \otimes \text{CNOT})(U \otimes \mathbb{I}_{\mathbb{C}^{2^k}})$ that consists of running U , copying the output register into a new register and running the inverse U^\dagger . Then, the amplitude of $|\psi\rangle|0\rangle|i\rangle$ in the state obtained by applying U_{uncomp} on $|\psi\rangle|0\rangle^{\otimes k}|0\rangle^{\otimes k}$ is

$$(\langle\psi|\langle 0|\langle i|)U_{\text{uncomp}}(|\psi\rangle|0\rangle|0\rangle) = \left(\sum_j \alpha_j^* \langle\psi_j|\langle j|\langle i|\right) \left(\sum_j \alpha_j |\psi_j\rangle|j\rangle|j\rangle\right) = |\alpha_i|^2 = \pi(i)$$

We run fixed-point amplitude amplification [YLC14] on the projector $\Pi = |\psi\rangle\langle\psi| \otimes |0\rangle\langle 0| \otimes \mathbb{I}$ and the state $U_{\text{uncomp}}(|\psi\rangle|0\rangle|0\rangle)$, using the amplitude lower bound $\|\Pi U_{\text{uncomp}}(|\psi\rangle|0\rangle|0\rangle)\|^2 \geq \lambda$ and the amplification parameter η . The probability of measuring $|\psi\rangle|0\rangle$ in the first two registers of the resulting state is at least $1 - \eta$, in which case the last register collapses to $\frac{1}{\sqrt{\sum_i \pi(i)^2}} \sum_i \pi(i)|i\rangle$.

Thus, we can restore $|\psi\rangle$ and sample $i \sim \frac{\pi(i)^2}{\sum_j \pi(j)^2}$ (by measuring the last register) with success probability at least $1 - \eta$. The algorithm requires $O(\log(1/\eta)/\sqrt{\lambda})$ applications of (controlled) $U_{\text{uncomp}}, U_{\text{uncomp}}^\dagger, \mathbb{I} - 2\Pi$ and $\mathbb{I} - 2|\psi\rangle\langle\psi|$. \square

Lemma 4.5. *Let $|\psi\rangle$ be a quantum state and Π be a projection operator with $p = \|\Pi|\psi\rangle\|^2$. Given $t \geq 1$ and $\eta \in (0, 1/2)$, the nondestructive amplitude estimation algorithm *Nd-Amplitude* $(|\psi\rangle, \Pi, t, \eta)$ outputs an estimate $\tilde{p} \in (0, 1)$ such that*

$$|\tilde{p} - p| < \frac{\sqrt{p(1-p)}}{t} + \frac{1}{t^2}$$

with probability at least $1 - \eta$. Moreover, if $p \leq 1/(4t^2)$ then it outputs $\tilde{p} = 0$ with probability at least $1 - \eta$. The algorithm needs one copy of $|\psi\rangle$, which is restored at the end of the computation with probability at least $1 - \eta$, and $O(t \log(1/\eta))$ applications of the reflection operators $\mathbb{I} - 2|\psi\rangle\langle\psi|$ and $\mathbb{I} - 2\Pi$.

Proof. Proof. The standard analysis of the amplitude estimation algorithm (Theorems 11 and 12 in [BHMT02]) shows that, after t steps, it outputs with probability at least $8/\pi^2$ one of two values $\tilde{p} \in \{\tilde{p}_1, \tilde{p}_2\}$ that both satisfy $|\tilde{p}_i - p| < 2\pi \frac{\sqrt{p(1-p)}}{t} + \frac{\pi^2}{t^2}$. Moreover, if $p \leq 1/(4t^2)$ then the probability to output $\tilde{p} = 0$ is at least $8/\pi^2$. Thus, by taking the median of $O(\log(1/\eta))$ independent runs of amplitude estimation, we obtain $\tilde{p} \in \{\tilde{p}_1, \tilde{p}_2\}$, or $\tilde{p} = 0$ when $p \leq 1/(4t^2)$, with probability at least $1 - \eta/2$. We apply the amplified uncomputation result (Lemma 4.4) on this algorithm with amplitude lower bound $\lambda = 1/8$ and success parameter $\eta/2$. If the algorithm succeeds, the probability to sample $\tilde{p} \in \{\tilde{p}_1, \tilde{p}_2\}$ is at least $\frac{2(1/2 - \eta/4)^2}{2(1/2 - \eta/4)^2 + (\eta/2)^2} \geq 1 - \eta/2$, and when $p \leq 1/(4t^2)$ the probability of $\tilde{p} = 0$ is at least $\frac{(1 - \eta/2)^2}{(1 - \eta/2)^2 + (\eta/2)^2} \geq 1 - \eta/2$. \square

We will use this version of non-destructive amplitude estimation in order to get the mean of the Λ_{i+1}/Λ_i before preparing the stationary distribution for the next iteration. So finally, we will have all the estimates that we use in the classical algorithm so we will now just multiply the ratios to get the final answer.