Lecture 6
Quantum Markov Chains

February 13, 2020

Plan

1. Classical Markov chains
2. Quantum Markov chains
3. Applications

1. Classical Markov chains

Example: Complex network

- Web network
  - $\geq 10^{10}$ pages
  - average number of 38 hyper-links per page
  - total number of hyperlinks $\geq 3.8\ 10^{11}$
- Twitter
  - $\approx 5\ 10^8$ users ($\approx 3.5\ 10^8$ active users)
  - a user follows about 100 other users
  - number of following-type social relations $\approx 5.\ 10^{10}$

Complex network analysis

- Unknown and changing topology
- Crawling the entire network is slow (ex: limit on the number of requests, Twitter $\leq 1/$min)
- Needs methods of sublinear/linear complexity

Exercise : counting the number of nodes

- Assumption: possible to sample uniformly among a set
- Question: give a method of sublinear complexity to estimate the size of the set

Counting the number of nodes

$$\begin{aligned}
T &\stackrel{\text{def}}{=} \text{number of samples to get the first collision} \\
\mathbb{E}(T) &= 2 + \frac{n-1}{n} + \frac{(n-1)(n-2)}{n^2} + \cdots + \frac{(n-1)(n-2)\cdots 1}{n^{n-1}} \\
&= \sqrt{\frac{\pi n}{2}} + 2/3 + O\left(\frac{1}{\sqrt{n}}\right) \\
\sigma(T) &= O(\sqrt{n}) \\
\text{estimator } \hat{n} &= \frac{2\left(T - \frac{2}{3}\right)^2}{\pi}
\end{aligned}$$

Random walk/Markov chain

- Complex network : uniform sampling ?
- Idea : random walks, Markov chains

Example : graph coloring

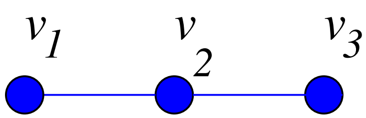
Definition 1. [graph coloring] *an assignment* $f : V \to \{1, \cdots, q\}$ *is a* q*-coloring of the graph* $G(V, E)$ *iff for all edges* $\{x, y\}$ *of* G *we have*

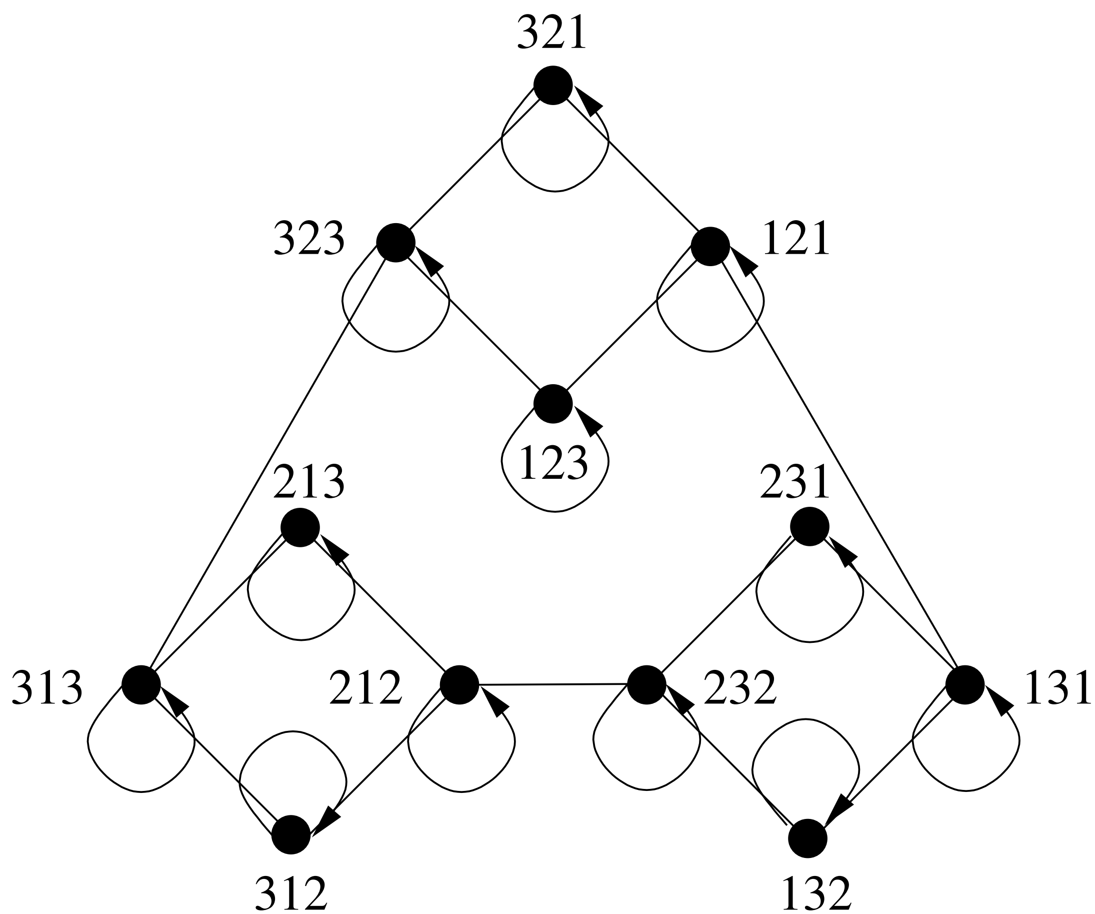
$$f(x) \neq f(y)$$

Problem 1.
Input: a graph G*, an integer* q
Output: The number of q*-colorings of* G

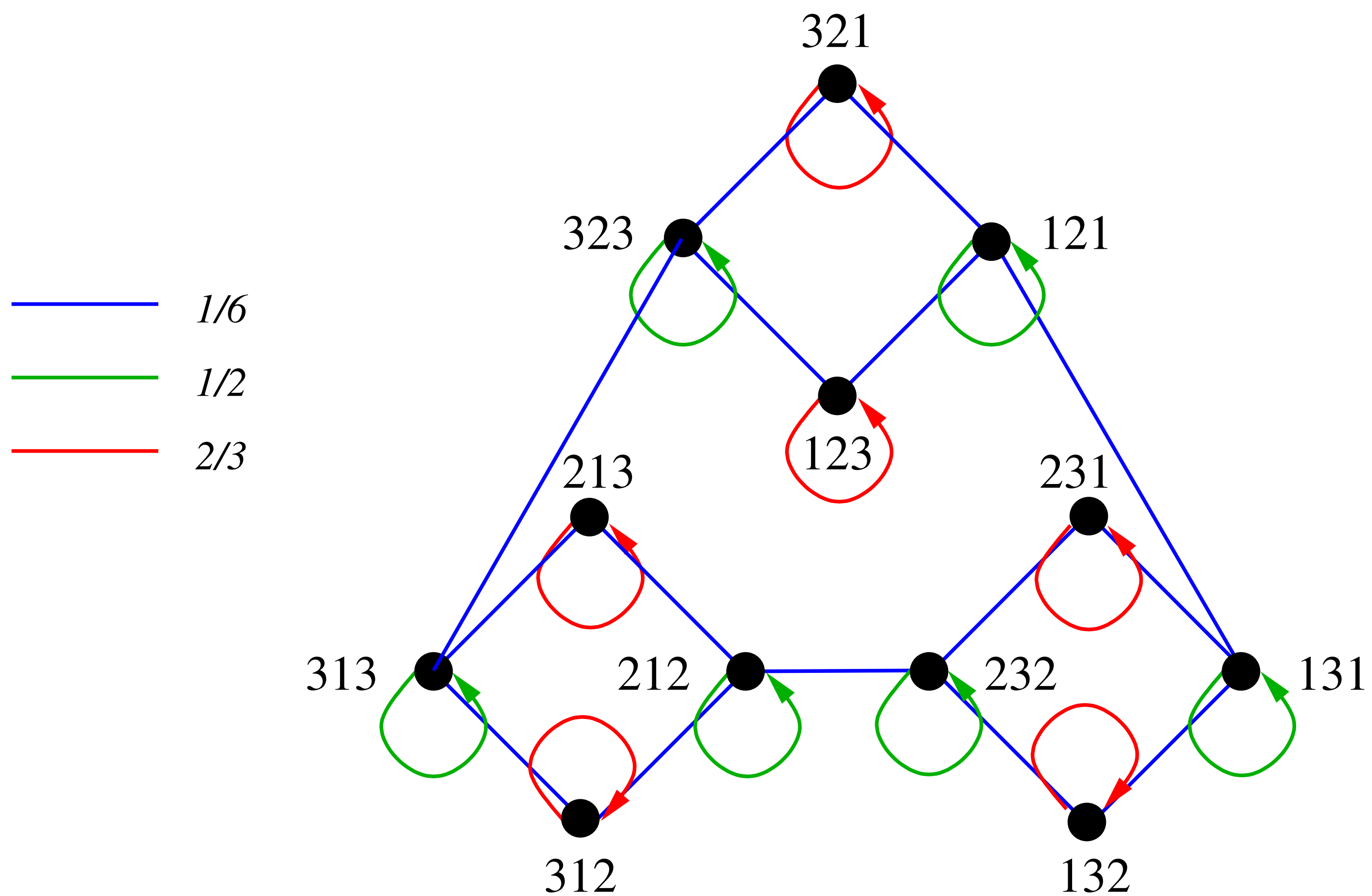
- Fundamental idea: define a random walk on a auxiliary graph
  - vertices: all possible colorings
  - edges: two colorings are adjacent iff they differ only in one vertex at most
  coloring $(c_1, \cdots c_i \cdots c_n) \in \{1, \cdots, q\}^n \to$ coloring $(c_1, \cdots c_i' \cdots c_n) \in \{1, \cdots, q\}^n$

Example: $|V| = 3$, $q = 3$





The transition probabilities



The approach/fundamental idea

- Define local transformation configuration $\rightarrow$ another configuration
- We can specify the transition probabilities to realize a certain asymptotic probability distribution

Random walk

1. Start in an arbitrary configuration
2. perform enough few random transitions

$\Rightarrow$ distribution of the endpoint very close to the probability distribution we want to emulate

Markov chain

Definition 2. [time-invariant Markov chain] *A time invariant Markov chain is a sequence of random variables $X_0, X_1, \cdots$ taking their values in a finite set Ω which is such that for all t and all $(a_0, \cdots, a_t) \in \mathcal{X}^{t+1}$ we have*

$$\begin{aligned} \mathbf{Prob}(X_t = a_t | X_{t-1} = a_{t-1} \cdots X_0 = a_0) &= \mathbf{Prob}(X_t = a_t | X_{t-1} = a_{t-1}) \text{ (dep. only on } X_{t-1}\text{)} \\ &= \mathbf{P}(a_{t-1}, a_t,) \text{ (time-invariance)} \end{aligned}$$

Definition 3. [transition probabilities matrix] *The matrix $(P(x,y))_{\substack{x\in\Omega \\ y\in\Omega}}$ is the transition probabilities matrix of the time-invariant Markov chain*

Definition 4. [graph associated to the Markov chain]

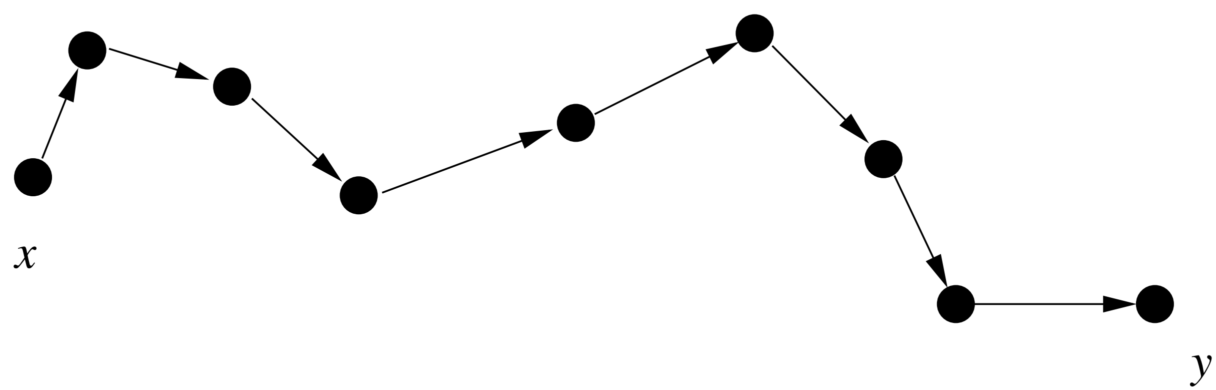
- *vertex set* Ω
- *edge* $x \to y \Leftrightarrow P(x,y) > 0$

Fundamental properties

Fact 1. *For all x, y in Ω and any t*

$$\mathbf{Prob}(X_t = y | X_0 = x) = \mathbf{P}^t(x, y)$$

Definition 5. [irreducible chain] *A Markov chain is irreducible iff for any pair $(x, y) \in \mathcal{X}^2$, there exists $t > 0$ such that $P^t(x, y) > 0$*



path of length t from x to $y \Rightarrow$ the graph associated to the Markov chain is strongly connected

Fundamental properties (II)

Definition 6. [aperiodic chain] *A Markov chain is aperiodic iff for any pair* $(x, y) \in \Omega^2$,

$$\mathit{gcd}\{t : \ P^t(x, y) > 0\} = 1$$

Definition 7. [stationary distribution] *a probability distribution* π *on* Ω *is a stationary distribution for the Markov chain iff for all* $y \in \Omega$

$$\pi(y) = \sum_{x \in \Omega} \pi(x) P(x, y)$$

Theorem 1. *If the Markov chain is aperiodic and irreducible then*

- *all the eigenvalues* $\lambda \neq 1$ *of* $\mathbf{P}$ *are such that* $|\lambda| < 1$
- 1 *is an eigenvalue of* $\mathbf{P}$ *of multiplicity* 1
- *there is a unique stationary distribution* π
- *for any* x, $y \in \Omega$, *we have*
$$\lim_{t \to \infty} P^t(x, y) = \pi(y)$$

  (the chain is ergodic)

Fundamental properties

Definition 8. [reversible Markov chain] *A Markov chain is reversible iff there exists* $\pi : \Omega \to [0, 1]$ *such that for all* x, $y \in \Omega$ *we have*

$$\pi(x)P(x, y) = \pi(y)P(y, x) \tag{1}$$

Fact 2. *For an irreducible Markov chain such a* π *satisfying* (1) *is proportional to the stationary distribution*

$$\sum_{x\in\Omega} \pi(x)P(x, y) = \sum_{x\in\Omega} \pi(y)P(y, x) = \pi(y)$$

$\Rightarrow$ can be used to define “locally” the chain to give a prescribed stationary distribution

Counting with Markov chains

- Choose $\mathbf{P}$ to be symmetric: stationary distribution is the uniform distribution
- Roughly speaking, an ergodic Markov chain is rapidly mixing if $P^t(x, y) \approx \pi(y)$ already for rather small t
- Use the Markov chain and X_0 X_t, $X_{2t}, \cdots$ are $\approx$ distributed according to the stationary distribution=uniform distribution

Spectral analysis

Assumption 1. $\mathbf{P}$ *is symmetric*

- the chain is irreducible iff G is connected
- the chain is aperiodic iff G is not bipartite

In such a case the eigenvalues of $\mathbf{P}$ satisfy

$$\lambda_1 = 1 > \lambda_2 \geq \lambda_3 \geq \cdots \geq \lambda_m > -1$$

Definition 9. [spectral gap] *The spectral gap δ of the Markov chain is defined as*

$$\delta \stackrel{\text{def}}{=} 1 - \max\{|\lambda_i|,\ 2 \leq i \leq m\}$$

Spectral analysis (II)

$$
\begin{aligned}
\mathbf{v} &\stackrel{\text{def}}{=} \text{starting probability distribution} \\
\mathbf{v}_i &\stackrel{\text{def}}{=} \text{eigenvector of } \mathbf{P} \text{ corresp. to } \lambda_i \\
\mathbf{v}_1 &= \frac{1}{n}(1, \cdots, 1)^T = u \\
\mathbf{v} &= \sum_i \alpha_i \mathbf{v}_i \\
\alpha_1 &= 1 \\
\mathbf{v}\mathbf{P}^t &= \left(\sum_i \alpha_i \mathbf{v}_i\right) \mathbf{P}^t \\
&= \mathbf{v}_1 + \sum_{i \geq 2} \alpha_i \lambda_i^t \mathbf{v}_i \\
\left\|\mathbf{v}\mathbf{P}^t - u\right\|^2 &= \left\|\sum_{i \geq 2} \alpha_i \lambda_i^t \mathbf{v}_i\right\|^2 = \sum_{i \geq 2} |\alpha_i|^2 |\lambda_i|^{2t} \leq (1-\delta)^{2t} \|v\|^2 \leq (1-\delta)^{2t}
\end{aligned}
$$

Spectral analysis (III)

$$t = \frac{\ln(1/\eta)}{\delta} \Rightarrow \left\| \mathbf{v}\mathbf{P}^t - u \right\| \leq \eta$$

Problem 2.
Input: graph $G(V, E)$, $f : V \to \{0, 1\}$ with $f(v) = 1$ iff v is marked
Output: a marked vertex

- technique : iterate
  (i) random walk on G with transition probabilities matrix $\mathbf{P}$
  (ii) perform $\theta(1/\delta)$ steps of the random walk
  (iii) output the corresponding vertex and check if it is marked

- S setup cost: the cost to set up the initial probability distribution $\mathbf{v}$
- U update cost: the cost to perform one step of the random walk
- C check cost: the cost to check if a vertex is marked
- ε: the proportion of marked vertices

Complexity for finding a marked vertex = $\boxed{S + \frac{1}{\varepsilon}\left(C + \frac{1}{\delta}U\right)}$

Application to the coloring problem

Theorem 2. *Assume that for a graph $G(V,E)$ we have an almost uniform sampler with time complexity $T(n,\delta)$ where $n = |V|$, δ deviation from uniformity, then we can construct a randomized approximation scheme for the number N of q-colorings which has time complexity*

$$O\left(\frac{m^2}{\varepsilon^2} T\left(n, \frac{\varepsilon}{6m}\right)\right)$$

where $m \stackrel{\text{def}}{=} |E|$ and ε the specified error bound

$$\mathbf{Prob}((1-\varepsilon)N \leq Y \leq (1+\varepsilon)N) \geq 3/4$$

where Y is the estimator

- polynomial in m!

The key algorithmic technique

$$
\begin{aligned}
G &= G_m > G_{m-1} > \cdots > G_1 > G_0 \\
G_{i-1} & \quad \text{obtained from } G_i \text{ by removing one edge } e_i \\
|\Omega(G)| &\overset{\text{def}}{=} \#\text{ of } q\text{-colorings of } G \\
|\Omega(G)| &= \frac{|\Omega(G_m)|}{|\Omega(G_{m-1})|} \times \cdots \times \frac{|\Omega(G_1)|}{|\Omega(G_0)|} \times |\Omega(G_0)| \\
|\Omega(G_0)| &= q^n \\
\rho_i &\overset{\text{def}}{=} \frac{|\Omega(G_i)|}{|\Omega(G_{i-1})|}
\end{aligned}
$$

- Estimating ρ_i:
  - uniform sampling on the q-colorings from $\Omega(G_{i-1})$ by random walk on $\Omega(G_{i-1})$
  - estimate the proportion of samples that lie in $\Omega(G_i)$: endpoints of e_i have $\neq$ colors

2. Quantum walks

A first try

$$P_{ij} \quad = \quad \left\{ \begin{array}{ll} 1/\deg(j) & (i,j) \in E \\ 0 & \text{otherwise} \end{array} \right\}$$

$$|j\rangle \quad \xrightarrow{U?} \quad |\partial_j\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{\deg(j)}} \sum_{k:(j,k)\in E} |k\rangle$$

Problem: $|\partial_j\rangle$ and $|\partial_k\rangle$ may not be orthogonal...

- Can be fixed by going to a larger Hilbert space

Simplifying assumption

- Quantum random walk on a d-regular graph with N vertices with transition probabilities

$$\begin{aligned} P_{xy} &= \frac{1}{d} \quad \text{if edge between } x \text{ and } y \\ &= 0 \quad \text{otherwise} \\ &\Downarrow \\ \text{stat. dist. } \pi_x &= \frac{1}{N} \end{aligned}$$

Basic definitions

- State space: generated by $\{|x\rangle\,|y\rangle\,, xy \in E\}$
- Good and bad states:

$$\mathcal{M} \stackrel{\text{def}}{=} \text{set of marked states}$$

$$N \stackrel{\text{def}}{=} \text{number of vertices}$$

$$M \stackrel{\text{def}}{=} \text{number of marked states} = |\mathcal{M}|$$

$$|G\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{M}} \sum_{x \in \mathcal{M}} |x\rangle\,|\psi_x\rangle \quad \text{where}$$

$$|\psi_x\rangle \stackrel{\text{def}}{=} \sum_{y : xy \in E} \frac{1}{\sqrt{d}}\,|y\rangle$$

$$|B\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{N-M}} \sum_{x \notin \mathcal{M}} |x\rangle\,|\psi_x\rangle$$

$$\sin\theta \stackrel{\text{def}}{=} \sqrt{\frac{M}{N}} = \sqrt{\varepsilon}$$

$$|U\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{N}} \sum_{x \in V} |x\rangle\,|\psi_x\rangle = \sin\theta\,|G\rangle + \cos\theta\,|B\rangle$$

The cost model

- Setup cost S: cost of constructing $\frac{1}{\sqrt{N}} \sum_{x \in V} |x\rangle\,|\bar{0}\rangle$ from $|\bar{0}\rangle\,|\bar{0}\rangle$
- Update cost S: cost of realizing any of the unitary

$$|x\rangle\,|\bar{0}\rangle \quad \overset{\overrightarrow{U}}{\mapsto} \quad |x\rangle \sum_{y : xy \in E} \frac{1}{\sqrt{d}}\,|y\rangle$$

$$|\bar{0}\rangle\,|y\rangle \quad \overset{\overleftarrow{U}}{\mapsto} \quad \sum_{x : xy \in E} \frac{1}{\sqrt{d}}\,|x\rangle\,|y\rangle$$

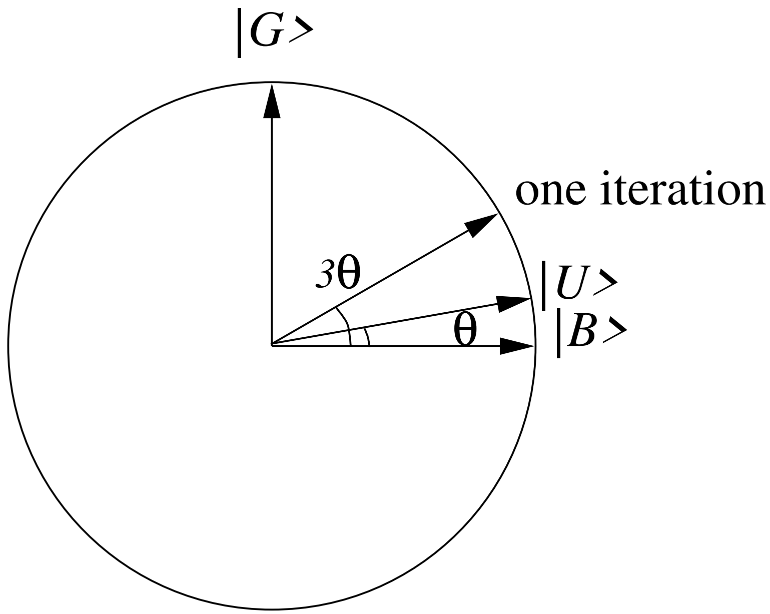
  and their inverses
- Checking cost C: cost of realizing

$$|x\rangle\,|y\rangle \mapsto \begin{cases} -\,|x\rangle\,|y\rangle & \text{if } x \in \mathcal{M} \\ \,|x\rangle\,|y\rangle & \text{otherwise} \end{cases}$$

The quantum walk search algorithm

1. Setup the starting state $|U\rangle$
2. Repeat $O(1/\sqrt{\epsilon})$ times
   (i) reflect through $|B\rangle$
   (ii) reflect through $|U\rangle$
3. measure the first register and check whether x is marked

The Grover/quantum walk picture



$$|\psi_t\rangle = \sin((2t+1)\theta)\,|G\rangle + \cos((2t+1)\theta)\,|B\rangle$$

$$\text{choose } t \approx \frac{\pi}{4\theta} = O\left(\frac{1}{\sqrt{\varepsilon}}\right)$$

$$\sin((2t+1)\theta) \approx 1$$

Reflection through $|U\rangle$ by applying $W(P)$

$$
\begin{aligned}
\mathcal{A} &\stackrel{\text{def}}{=} \text{span}\{|x\rangle\,|\psi_x\rangle : \; x \in V\} \\
\text{ref}(\mathcal{A})\,|v\rangle &= |v\rangle \quad \text{if } |v\rangle \in \mathcal{A} \\
&= -\,|v\rangle \quad \text{if } |v\rangle \in \mathcal{A}^{\perp} \\
\mathcal{B} &\stackrel{\text{def}}{=} \text{span}\{|\psi_y\rangle\,|y\rangle : \; y \in V\} \\
\text{ref}(\mathcal{B})\,|v\rangle &= |v\rangle \quad \text{if } |v\rangle \in \mathcal{B} \\
&= -\,|v\rangle \quad \text{if } |v\rangle \in \mathcal{B}^{\perp} \\
W(P) &\stackrel{\text{def}}{=} \text{ref}(\mathcal{B})\text{ref}(\mathcal{A})
\end{aligned}
$$

- $W(P)$ is the unitary analogue of P

Implementing $W(P)$

$$\mathsf{Ref}(\mathcal{A}) : |x\rangle\,|\psi_x\rangle \xrightarrow{\overrightarrow{U}^{-1}} |x\rangle\,|\bar{0}\rangle \xrightarrow{\mathbf{Id}\otimes\mathsf{Ref}(\bar{0})} |x\rangle\,|\bar{0}\rangle \xrightarrow{\overrightarrow{U}} |x\rangle\,|\psi_x\rangle$$

$$\mathsf{Ref}(\mathcal{B}) : |\psi_y\rangle\,|y\rangle \xrightarrow{\overleftarrow{U}^{-1}} |\bar{0}\,|y\rangle\rangle \xrightarrow{\mathsf{Ref}(\bar{0})\otimes\mathbf{Id}} |\bar{0}\rangle\,|y\rangle \xrightarrow{\overleftarrow{U}} |\psi_y\rangle\,|y\rangle$$

- Cost $4U$ to implement $W(P)$

Exercise

1. Give a basis of the orthogonal of the space W generated by the $|x\rangle\,|\psi_x\rangle$'s
2. Use this to prove that the previous transformations implement $W(P)$

Solution

1. $\overrightarrow{U}\,|x\rangle\,|y\rangle$ for $y \neq \bar{0}$ are in this space and form necessarily a basis of the space $W^{\perp}$ (dimension consideration)
2. $$\overrightarrow{U}\,|x\rangle\,|y\rangle \xrightarrow{\overrightarrow{U}^{-1}} |x\rangle\,|y\rangle \xrightarrow{\mathbf{Id}\otimes \mathsf{Ref}(\bar{0})} -|x\rangle\,|y\rangle \xrightarrow{\overrightarrow{U}} -\overrightarrow{U}\,|x\rangle\,|y\rangle$$

Exercise: Grover reflection vs. $W(P)$ in the complete graph with loops

1. Consider the Grover reflection $\mathbf{H}^{\otimes n}\mathbf{R}\mathbf{H}^{\otimes}$. What is its effect on the basis $\{|\bar{i}\rangle : i \in \{0,1\}^n\}$ where $|\bar{i}\rangle \stackrel{\text{def}}{=} \mathbf{H}^{\otimes n}|i\rangle$?
2. Consider the complete graph with loops, i.e. any x is connected to any other y (including x). Express the operator $W(P)$ in a basis of $\mathcal{A}+\mathcal{B}$ that seems the most appropriate to you
3. Compare both results

Solution: Grover reflection vs. $W(P)$ in the complete graph with loops

1.

$$\begin{aligned}\mathbf{H}^{\otimes n}\mathbf{R}\mathbf{H}^{\otimes}\left|\bar{0}\right\rangle &= \left|\bar{0}\right\rangle \\ \mathbf{H}^{\otimes n}\mathbf{R}\mathbf{H}^{\otimes}\left|\bar{i}\right\rangle &= -\left|\bar{i}\right\rangle \text{ if } i \neq 0\end{aligned}$$

2. Consider a unitary transform on the Hilbert space $\mathcal{V} = \text{Span}\{|x\rangle\,,\ x \in V\}$, a unitary transform $\mathbf{U}$ on $\mathcal{V}$ such that $\mathbf{U}\,|0\rangle = \frac{1}{\sqrt{|V|}}\sum_{x\in V}|x\rangle$ and let $|\bar{x}\rangle \stackrel{\text{def}}{=} \mathbf{U}\,|x\rangle$

$$\begin{aligned}\mathcal{A} &= \text{Span}\{|x\rangle\,|\bar{0}\rangle\,,\ x \in V\} \\ &= \text{Span}\{|\bar{x}\rangle\,|\bar{0}\rangle\,,\ x \in V\} \\ \mathcal{B} &= \text{Span}\{|\bar{0}\rangle\,|\bar{y}\rangle\,,\ y \in V\} \\ \mathcal{A}\cap\mathcal{B} &= \text{Span}\{|\bar{0}\rangle\,|\bar{0}\rangle\} \\ W(P)\,|\bar{0}\rangle\,|\bar{0}\rangle &= |\bar{0}\rangle\,|\bar{0}\rangle \\ W(P)\,|\bar{0}\rangle\,|\bar{x}\rangle &= -\,|\bar{0}\rangle\,|\bar{x}\rangle \quad \text{for } x \neq 0 \\ W(P)\,|\bar{x}\rangle\,|\bar{0}\rangle &= -\,|\bar{x}\rangle\,|\bar{0}\rangle \quad \text{for } x \neq 0\end{aligned}$$

The spectrum of $W(P)$

Theorem 3. *Let P be an ergodic and reversible Markov chain. The spectrum of $W(P)$ on $\mathcal{A} + \mathcal{B}$ can be characterized by*

- $|U\rangle = \frac{1}{\sqrt{N}} \sum_{x \in X} |x\rangle |\psi_x\rangle$ *is the unique* 1*-eigenvector*
- *for every eigenvalue λ of P $e^{\pm 2i\theta}$ is an eigenvalue of $W(P)$ where $\cos\theta = |\lambda|$*
- *the remaining eigenvalues are -1*

The phase gap

Definition 10. [phase gap] *The phase gap $\Delta(P)$ of $W(P)$ is defined as 2θ where θ is the smallest angle in $(0, \pi/2]$ s.t. $\cos\theta$ is a singular value of P (i.e. $\cos\theta = |\lambda|$ where λ is an eigenvalue of P)*

Fact 3.

$$\Delta(P) \geq 2\sqrt{\delta(P)}$$

$$\begin{aligned}
\delta &= 1 - \cos\theta \\
\Delta &= 2\theta \\
&\geq |1 - e^{2i\theta}| \\
&= 2|\sin\theta| \\
&= 2\sqrt{1 - \cos^2\theta} \\
&\geq 2\sqrt{\delta}
\end{aligned}$$

Exercise : implementing Ref($|U\rangle$)

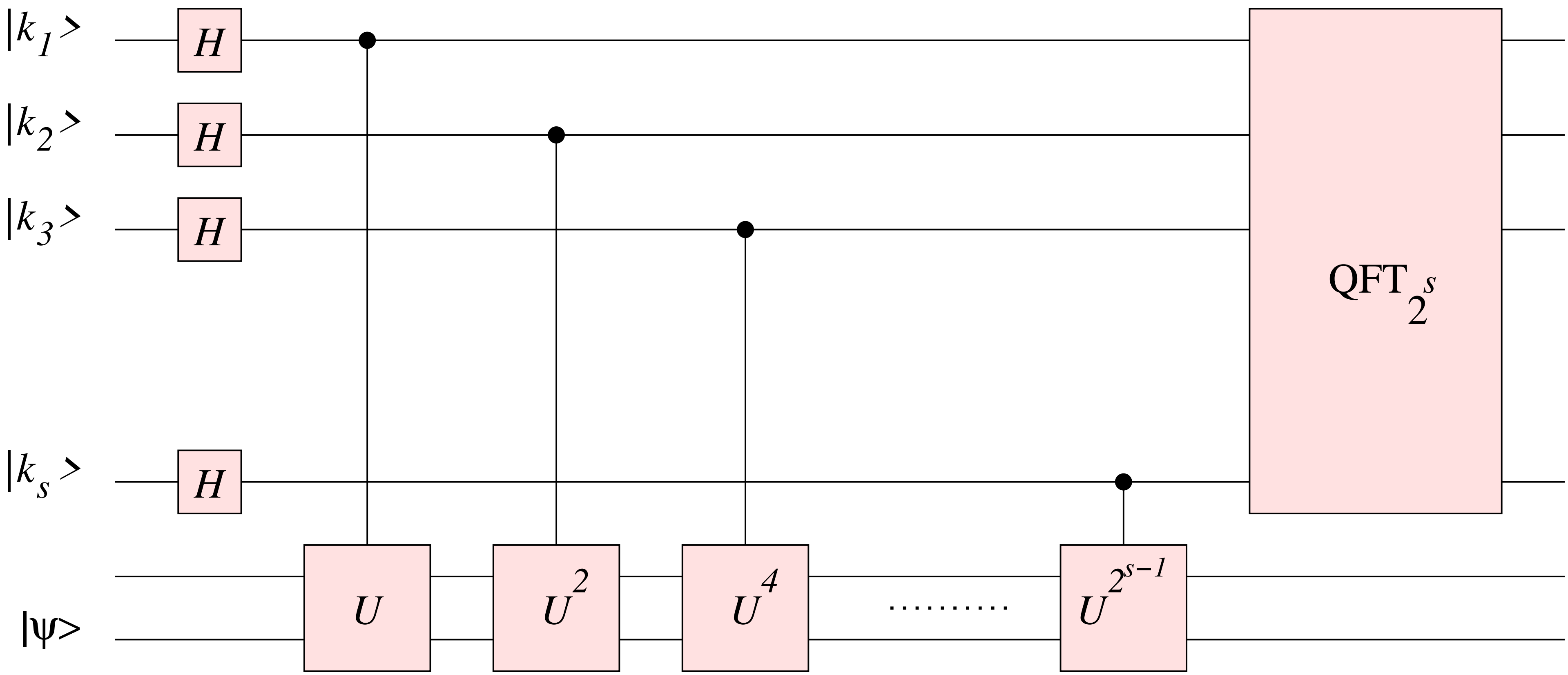
Use these results to show that Ref($|U\rangle$) can be implemented with complexity $O\left(\frac{1}{\sqrt{\delta}}\right)$ calls to c-$W(P)$.

Phase estimation

Theorem 4. *For every unitary operator U acting on m qubits, there exists a quantum circuit $\mathbf{PE}(U)$ acting on $m + s$ qubits satisfying the following properties*

1. *the circuit $\mathbf{PE}(U)$ uses $2s$ Hadamard gates, $O(s^2)$ controlled phase rotations and makes 2^{s+1} calls to c-U*
2. *for any eigenvector $|\psi\rangle$ with eigenvalue 1, $\mathbf{PE}(U)\,|\psi\rangle\,|0^s\rangle = |\psi\rangle\,|0^s\rangle$*
3. *if $U\,|\psi\rangle = e^{2i\theta}\,|\psi\rangle$ then $\mathbf{PE}(U)\,|\psi\rangle\,|0^s\rangle = |\psi\rangle\,|\omega\rangle$ where $|\,\langle 0^s|\omega\rangle\,| = \frac{\sin(2^s\theta)}{2^s \sin\theta}$*

The circuit


$|k_1\rangle$
$|k_2\rangle$
$|k_3\rangle$
$|k_s\rangle$
$|\psi\rangle$
H
H
H
H
U
U^2
U^4
$U^{2^{s-1}}$
QFT_{2^s}

Realizing Ref$(|U\rangle)$

For an eigenvector $|\psi\rangle$ of $W(P)$ with eigenvalue $e^{2i\theta}$

$$|\psi\rangle\,|\bar{0}\rangle \xrightarrow{\mathbf{PE}} |\psi\rangle\left|\tilde{\theta}\right\rangle \mapsto (-1)^{\tilde{\theta}\neq 0}\,|\psi\rangle\left|\tilde{\theta}\right\rangle \xrightarrow{\mathbf{PE}^{-1}} (-1)^{\tilde{\theta}\neq 0}\,|\psi\rangle\,|\bar{0}\rangle$$

The complexity of searching with quantum walks

- Setup cost S: the cost of constructing $|U\rangle$
- Checking cost C: the cost of the unitary map $|x\rangle|y\rangle \mapsto (-1)^{m(x)}|x\rangle|y\rangle$ where $m(x) = 1$ is x is marked and 0 otherwise
- Update cost U: $1/4$ of the cost of one step of the quantum walk, i.e. of $W(P)$

$$\text{Complexity for finding a marked vertex} = \boxed{S + \frac{1}{\sqrt{\varepsilon}}\left(C + \frac{1}{\sqrt{\delta}}U\right)}$$

Comparison of all the strategies

- S setup cost
- U update cost
- C checking cost

standard search	random walk search	amplitude amplification	quantum random walk
repeat $\frac{1}{\epsilon}$ times – apply $\mathcal{A}$ – check	apply $\mathcal{A}$ repeat $\frac{1}{\epsilon}$ times – repeat $\frac{1}{\delta}$ times update – check	repeat $\frac{1}{\sqrt{\epsilon}}$ times – apply $\mathcal{A}\mathbf{R}\mathcal{A}^{-1}$ – check	apply $\mathcal{A}$ repeat $\frac{1}{\sqrt{\epsilon}}$ times – repeat $\frac{1}{\sqrt{\delta}}$ times update – check
$\frac{1}{\varepsilon}(S+C)$	$S+\frac{1}{\varepsilon}(\frac{1}{\delta}U+C)$	$\frac{1}{\sqrt{\varepsilon}}(C+S)$	$S+\frac{1}{\sqrt{\varepsilon}}(\frac{1}{\sqrt{\delta}}U+C)$

Exercise : the complete graph

Let G be the complete graph on N vertices. Let P be the transition probabilities associated to the standard random walk associated to G, i.e.

$$\begin{aligned} P_{xx} &= 0 \\ P_{xy} &= \frac{1}{N-1} \end{aligned}$$

1. What are the eigenvalues of P ?
2. What is the spectral gap of P ?
3. What is the cost of finding a marked vertex in G (the cost is measured in terms of the number of queries) ?
4. Compare this with Grover's algorithm.

Solution: the complete graph

1. P has eigenvalue 1 and since $P + \frac{1}{N-1}\mathbf{Id}$ has rank $1 \Rightarrow$ eigenvalue 0 with multiplicity $N-1 \Rightarrow P$ has eigenvalue $-\frac{1}{N-1}$ with multiplicity $N-1$.
2. $\delta = \frac{N-2}{N-1}$
3. - $\varepsilon = \frac{1}{N}$
   - $S = U = 0$
   - $C = 1$

   Cost $= O(\frac{1}{\sqrt{N}})$
4. Same cost as Grover's algorithm. The Hilbert space is different though.

The Johnson graph

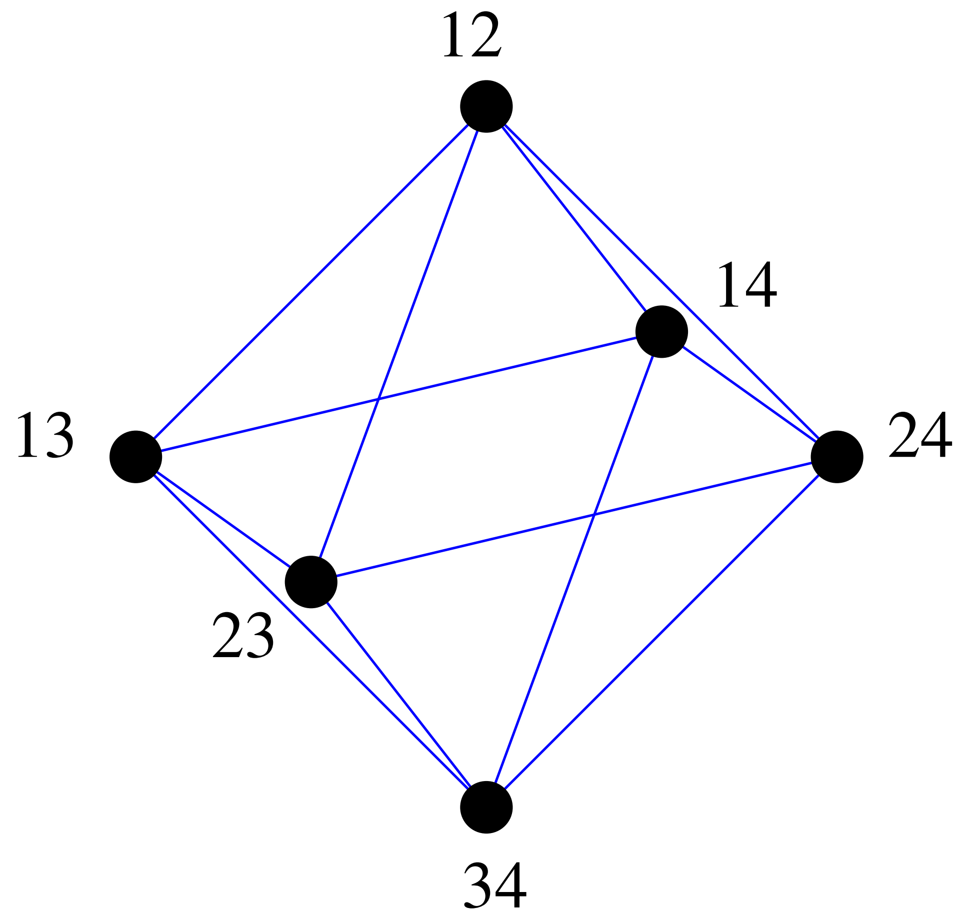
Definition 11. [Johnson graph] *The Johnson graph $J(n, r)$ has*

- *vertex set the subsets of r elements of $\{1, \cdots, n\}$*
- *two subsets R and R' are linked by an edge iff $|R \cap R'| = r - 1$*

Fact 4.

- $J(n, r)$ *is* $r(n-r)$*-regular*
- *spectral gap* $\delta = \frac{n}{r(n-r)}$

$J(4,2)$



Exercise: the collision problem again

Consider the following collision problem,

- Input: a function $f : \{0,1\}^n \mapsto \{0,1\}^n$
- Assumes: f is either one-to-one or there is exactly one pair $\{x,y\}$ such that $f(x) = f(y)$ and $x \neq y$
- Output: the pair $\{x,y\}$ that collides for f or $\emptyset$ if this pair does not exist.

1. Give the best quantum algorithm based on Grover's problem to solve this problem
2. Give a quantum algorithm based on the Johnson graph to improve on the query complexity of the previous algorithm
3. By using the lower bound $\Omega(2^{n/3})$ on the query complexity of the collision problem for a 2 to 1 function, show that the aforementioned collision problem has a query complexity of $\Omega(2^{n/3})$

Solution for collision finding

$N \stackrel{\text{def}}{=} 2^n$

1. Algorithm 1:
   - query f in L random places
   - check whether the $N-L$ remaining candidates have a collision with one of the L elements

   The whole algorithm applies now amplitude amplification on Algorithm 1

   Analysis:
   - Cost of Algorithm 1: $L + O(\sqrt{N-L}) = L + O(\sqrt{N})$
   - probability of success L/N
   - Total cost : $\sqrt{L/N}\left(L + O(\sqrt{N-L}\right)$, optimize $\Rightarrow L = \sqrt{N}$ gives a total cost of $O(2^{3n/4})$

2. Algorithm:
   - Choose R random places for f and keep track of their values by f
   - perform a random walk on the Johnson graph $J(N, R)$ and check each time if the set of R elements contains the collision we look for (a vertex is marked iff it contains the collision)

   Analysis:
   - Setup cost $S = R + 1$ create a uniform superposition over all edges xy of the Johnson graph and add the values of the set $x \cup y$ ($= r + 1$ queries)
   - Checking cost $C = 0$ since checking whether x is marked (contains the collision) does not require additional query of f
   - Update cost $U = O(1)$ we have to query at least one new additional element
   - proportion of marked vertices

   $$\varepsilon = \frac{R}{N}\frac{R-1}{N-1}$$

   - spectral gap $\delta = O(1/R)$

   Total cost:

   $$S + \frac{1}{\sqrt{\varepsilon}}\left(C + \frac{1}{\sqrt{\delta}}U\right) = O(R + N/\sqrt{R})$$

   minimal for $R = N^{2/3}$ and gives a total query complexity of $O(2^{2n/3})$

3. Idea: randomly choose $\sqrt{n}$ preimages for the 2 to 1 function. With probability $\Omega(1)$ there is a single collision among them. Use now the optimal collision finding algorithm on them. Assume that it has query complexity $f(N')$ when there are N' elements. We know that

$$f(2^{n/2}) = \Omega(2^{n/3})$$

This implies

$$f(2^n) = \Omega(2^{2n/3})$$

proving that the previous collision finding algorithm has optimal query complexity

Finding a triangle in a graph

Consider the following triangle-finding problem

- Input: the adjacency matrix of a graph on n vertices
- Output: vertices a, b and c forming a triangle

1. Show the lower bound $\Omega(n^2)$ on the query complexity of a classical algorithm
2. Give a more efficient quantum algorithm based on Johnson's graph

Solution: triangle finding

1. Take a bipartite graph with $\Omega(n^2)$ edges. All of them have to checked to verify that there is no triangle.
2. Consider the Johnson graph $J(n, r)$.
   Each vertex = set of r vertices + result of querying all the edges of the induced subgraph.
   marked vertex=vertex whose associated subgraph contains one edge of the triangle.
   Analysis
   - $$\varepsilon = \Omega(r^2/n^2)$$
   - Setup cost $S = \binom{r}{2}$
   - Update cost $U = 2r - 2$ =remove information from $r - 1$ edges + query $r - 1$ additional edges

Checking cost C:

Algorithm for deciding whether for a given subset R of size r and another additional vertex u whether u forms a triangle with two vertices of R:

- Random walk on the Johnson graph $J(r, r^{2/3})$ of subsets R' of size $r' = r^{2/3}$ of R
- spectral gap $\approx 1/r^{2/3}$
- fraction of marked vertices $O(r'^2/r^2) = O(r^{2/3})$
- we mark R' iff it forms the sought triangle with u
- setup cost $= O(r^{2/3})$ (for each vertex v of R' query whether uv is an edge)
- update cost $=O(1)$

Total checking cost $= O(r^{2/3})$

Combine this with a Grover search for $u \Rightarrow C = O(\sqrt{n}r^{2/3})$

Total cost:

$$S + \frac{1}{\sqrt{\varepsilon}}\left(C + \frac{1}{\sqrt{\delta}}U\right) = O\left(r^2 + \frac{n}{r}\left(\sqrt{n}r^{2/3} + r^{3/2}\right)\right)$$

minimal for $r = n^{3/5}$ and query complexity of $O(n^{13/10})$