Lecturer: Tongyang, scribed by Rui Yang
Date: November 10, 2023

Lecture 12

Quantum walks (Continued)

- Hitting time
- Element distinctness

1 Hitting time

Determining marked vertices in the complete graph

Let $G = (V, E)$ be a complete graph of $N = 2^n$ vertices. We want to distinguish the following two scenarios:

(1) All vertices are the same, and the random walk is given by the transition matrix:

$$P = \frac{1}{N} e_N e_N^\top \quad e_N = (1, 1, \cdots, 1)^\top.$$

(2) There are M marked item (vertices). WLOG, we may assume that they are the 1st, 2nd, ... M-th vertices for better notations (of course we do not have access to this information). In this case, the transition matrix is

$$\widetilde{P} = \begin{cases} \delta_{ij} & i \in [M] \\ P_{ij} & i \in \{M+1, \cdots, N\} \end{cases}$$

In other words, the random walk will stop at marked vertices. Its transition matrix can also be written in the block partitioned form:

$$\tilde{P} = \begin{pmatrix} I_M & 0 \\ \frac{1}{N} e_{N-M} e_M^\top & \frac{1}{N} e_{N-M} e_{N-M}^\top \end{pmatrix}.$$

Here e_{N-M} and e_M are all -1 vectors of length $N - M$ and M, respectively.

For the random walk defied by P, the stationary state is $\pi = \frac{1}{N} e_N$, and the spectral gap is 1 .

$$\begin{pmatrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{pmatrix} \quad \text{eigenvalue: N, 0, } \ldots, 0 \qquad D_{ij} = \sqrt{P_{ij} P_{ji}}$$

P is symmetric $\Rightarrow$ Its discriminant matrix $D = P$.

For the random walk defined by $\tilde{P}$. the stationary state $\tilde{\pi} = \left(\frac{1}{M} e_M, 0, \cdots, 0\right)$. Its discriminant matrix $\tilde{D} = \begin{pmatrix} I_m & 0 \\ 0 & \frac{1}{N} e_{N-M} e_{N-m}^\top \end{pmatrix}$ with eigenvalues $\underbrace{1, \ldots, 1}_{M}, \frac{N-M}{N}, \underbrace{0, \cdots, 0}_{N-M-1}$

$\Rightarrow$ spectral gap $= 1 - \frac{N-M}{N} = \frac{M}{N} := \varepsilon$

Remark 1.1.

$$\text{Ergodic} = \text{irreducible} + \text{aperiodic}$$

$$\text{reversible: } \pi_i P_{ij} = \pi_j P_{ji}$$

Note that the theory of quantum walks works for reversible random walks. For reducible Markov chains, spectral gap = 1 - the second largest eigenvalue smaller than 1.

Classically, the cost is $O\left(\frac{N}{M}\right) = O\left(\frac{1}{\varepsilon}\right)$.

Quantumly, we start with $|\psi_0\rangle = |0^n\rangle \otimes (H^{\otimes n}|0^n\rangle)$.

Note that $|\tilde{\pi}\rangle = \sum_{i=1}^{M} \frac{1}{\sqrt{M}}|i\rangle$ is the stationary state (with eigenvalue 1) and $|\tilde{v}\rangle = \sum_{i=M+1}^{N} \frac{1}{\sqrt{N-M}}|i\rangle$ is an eigenstate of $\widetilde{D}$ with eigenvalue $\frac{N-M}{N} = 1-\varepsilon$.

$$|\phi_0\rangle = \sqrt{\frac{M}{N}}\,|0^n\rangle\,|\tilde{\pi}\rangle + \sqrt{\frac{N-M}{N}}\,|0^n\rangle\,|\tilde{v}\rangle = \sqrt{\varepsilon}\,|0^n\rangle\,|\tilde{\pi}\rangle + \sqrt{1-\varepsilon}\,|0^n\rangle\,|\tilde{v}\rangle.$$

Due to qubitization, we have $O_{\widetilde{D}}^k\,|\psi_0\rangle = \sqrt{\varepsilon}\,|0^n\rangle\,T_k(1)|\tilde{\pi}\rangle + \sqrt{1-\varepsilon}\,|0^n\rangle\,T_k(1-\varepsilon)|\tilde{v}\rangle + \left|\tilde{\perp}_k\right\rangle$, where $\left|\tilde{\perp}_k\right\rangle$ is an unnormalized state satisfying $(|0^n\rangle\langle 0^n| \otimes I_N)|\tilde{\perp}_k\rangle = 0$.

If we measure the first system, $P_\gamma\,[0^n] = \varepsilon + (1-\varepsilon)T_k^2(1-\varepsilon)$. $\quad (T_k(1) = 1)$

On the other hand, $O_D^k\,|\psi_0\rangle = |0^n\rangle\,T_k(1)|\pi\rangle = |0^n\rangle\,|\pi\rangle$ $\qquad\qquad$ $\epsilon = \frac{M}{N} \leqslant \frac{1}{2}$.

If we measure the first system. $\Pr\,[0^n] = 1$.

To distinguish between these two cases, $T_k^2(1-\varepsilon)$ should be small. In order to having $T_k(1-\varepsilon) \approx 0$, we take $k \approx \frac{\pi}{2\arccos(1-\epsilon)} \approx \frac{\pi}{2\sqrt{2\varepsilon}}$, and $\Pr\,[0^n] \approx \varepsilon$.

Therefore, we can distinguish the two cases w.h.p. by $O(1/\sqrt{\varepsilon})$ steps of quantum walks.

Remark 1. Compared to Grover search, the two algorithms have similarity in "amplification", but the oracles are different. Grover can also find marked vertex, but the example above is a decision problem.

Remark 2. With a little bit more effort, the above example can be extended to quantum walls on regular graphs, i. e., all vertices have the same degree. In that case, if the graph has spectral gap δ (for the complete graph, $\delta = 1$), and we want to decide between no marked item and M marked items, $\varepsilon = \frac{M}{N}$, the classical random wack has cost $O(1/\delta\varepsilon)$, whereas quantum walk has cost $O(1/\sqrt{\delta\varepsilon})$.

Remark 3. There are different forms of quantum walks. In history, an important class is the Szegedy quantum walk (taught in 2022) defined by

$$|\psi_j\rangle := |j\rangle \otimes \sum_{k=1}^{N} \sqrt{P_{jk}}|k\rangle = \sum_{k=1}^{N} \sqrt{P_{jk}}|j,k\rangle. \quad \Pi = \sum_{j=1}^{N} |\psi_j\rangle\langle\psi_j|\,.$$

$$U = \text{SWAP}(2\Pi - I). \quad U^2 = \text{SWAP}(2\Pi - I)\,\text{SWAP}(2\Pi - I) = \left(2(\text{SWAP}\cdot\Pi)(\text{SWAP}\cdot\Pi)^\dagger - I\right)(2\Pi - I),$$

same as a block encoding of $T_2(D)$ using qubitization up to a similarity transformation.

2 Element distinctness

Problem: We are given a black-box function $f : \{1, 2, \cdots, N\} \to S$, where S is a finite set. Goal: Determine whether there exist two $x, y \in \{1, 2, \cdots, N\}$ such that $f(x) = f(y)$.

Putting this in another way: this is to decide f is injective or not.

Note that element distinctness is also an "unstructured" problem: no requirement beyond x and y.

In fact, it's at least as hard as unstructured search: suppose $\exists x \neq y \ s.t. \ f(x) = f(y)$. Assume $x = 1$, we need to find the $y \in \{2, 3, \cdots, N\}$ such that $f(y) = f(x)$.

Therefore, clearly it takes $\begin{cases} \Omega(N) \text{ classical queries} \\ \Omega(\sqrt{N}) \text{ quantum queries} \end{cases}$ to solve the element distinctness problem.

Can we achieve a nontrivial quantum algorithm here?

Quantum oracle: $O_f|i\rangle|z\rangle = |i\rangle\,|f(i) + z\rangle \quad \forall i \in [N], \forall z \in \mathbb{R}$. WLOG. the numbers in the second register can be saved perfectly.

Consider this: We query f in l randomly chosen places, and apply Grover on the N $- l$ inputs to check whether one of them has same function value to the l chosen ones.

(If two of the l chosen ones have same function value, we have finished. WLOG, they are all different.)

Total cost: $l + O(\sqrt{N - l})$.

Success probability: Need to cover at least one of x and y.

$$\Pr = 1 - \Pr[x \text{ and } y \text{ not selected }] = 1 - \frac{\begin{pmatrix} N-2 \\ l \end{pmatrix}}{\begin{pmatrix} N \\ l \end{pmatrix}} = 1 - \frac{\frac{(N-2)!}{l!(N-2-l)!}}{\frac{N!}{l!(N-l)!}} = 1 - \frac{(N-l)(N-l-1)}{N(N-1)}$$

$$l \leq N, 2N - l - 1 \geqslant N - 1 \qquad = \frac{l(2N-l-1)}{N(N-1)} \geqslant \frac{l}{N}.$$

Amplitude amplification: the overall complexity:

$$O\left(\sqrt{\frac{N}{l}}(l + O(\sqrt{N-l})\right) = O\left(\sqrt{Nl} + \frac{N}{\sqrt{l}}\right)$$

AM-GM inequality: $\sqrt{Nl} + \frac{N}{\sqrt{l}} \geqslant 2\sqrt{\sqrt{Nl} \cdot \frac{N}{\sqrt{l}}} = 2N^{3/4}$.

Taking $l = \Theta\left(N^{1/4}\right)$, overall complexity: $O\left(N^{3/4}\right)$.

So far, we have a quantum upper bound $O\left(N^{3/4}\right)$. and a quantum lower bound of $\Omega(\sqrt{N})$. In fact, both of them can be improved.

Lower bound: In Assignment 3, we study the collision problem:

Black-box $f : \{1, 2, \ldots N\} \to S$ for some $|S| \geqslant \frac{N}{2}$, with the promise that f is either one-to-one or two-to-one (for any $x \in \{1, 2, \cdots, N\}$, $\exists$! (exist unique) $x' \in \{1, 2, \cdots, N\}$ such that $x \neq x', \ f(x) = f(x')$).

Research paper: Aaronson and Shi. Quantum lower bounds for the collision and the element distinctness problem. JACM 2004.

Collision: $\Omega\left(N^{1/3}\right)$.

This implies that $\Omega\left(N^{2/3}\right)$ quantum query lower bound for element distinctness.

Proof. Assume we have an instance of the collision problem.

Randomly choose $\sqrt{N}$ inputs of the collision function, and run the element distinctness algorithms on them.

- If the function is two-to-one, by the birthday paradox, there is some pair of elements in this set mapping to the same value with high probability.
- This will be detected by the element distinctness algorithm.

Therefore, if element distinctness can be solved in $o\left(N^{2/3}\right)$ quantum queries, the collision problem will be solved in $o(\sqrt{N})^{2/3}) = o(N^{1/3})$ quantum queries, contradicting the Aaronson-Shi lower bound. ■

Remained question: Can we close the gap between $O\left(N^{3/4}\right)$ and $\Omega\left(N^{2/3}\right)$?

Quantum walk algorithm (Ambainis)

Consider the Hamming graph $H(N, M)$.
Vertices: M-tuple of values from $\{1, 2, \cdots, N\}$ (so there are N^M vertices)
Edges: Two vertices are connected if and only if they differ in exactly one coordinate.
At each vertex, we store the values of the function at the corresponding inputs. In other words, the vertex $(x_1, x_2, \ldots, x_M) \in \{1, 2, \ldots, N\}^M$ is represented by the state

$$|x_1, x_2, \cdots, x_M, f(x_1), \cdots, f(x_M)\rangle .$$

Consider the search problem on this Hamming graph.
Marked vertex: Those containing some $x \neq y$ with $f(x) = f(y)$
Note that given the stored function values, we can check whether we are at a marked vertex with no additional queries.
In the case where the elements are not all distinct (say $f(a) = f(b)$), the total number of marked vertices is at least:
# of vertices: both a and b appear exactly one among all X_i.

$$\begin{pmatrix} M \\ 2 \end{pmatrix} \cdot 2 \cdot (N-2)^{M-2} = M(M-1) \cdot (N-2)^{M-2}$$

$\uparrow \quad (a \quad b)$
places $(b \quad a)$

$\Rightarrow$ The fraction of marked vertices is at least $\varepsilon \geqslant \frac{M(M-1)(N-2)^{M-2}}{N^M}$.
To analyze the quantum walk, we also need the eigenvalues of the stochastic matrix. The adjacency matrix of the Hamming graph $H(N.M)$ is $A = \sum_{i=1}^{M} (J-i)^{(i)}$, where J denotes the $n \times n$ all-1 matrix, and the superscript (i) indicates that this matrix acts on the i^{th} coordinate.
Formally: $A = (J-I) \otimes I \otimes \ldots \otimes I + I \otimes (J-I) \otimes I \otimes \cdots \otimes I + \cdots + I \otimes I \otimes \cdots \otimes I \otimes (J-I)$.