Introduction to Quantum Computing — Lecturer: Tongyang Li, scribed by Rui Yang
Fall 2023, Peking University — *Date: November 3, 2023*

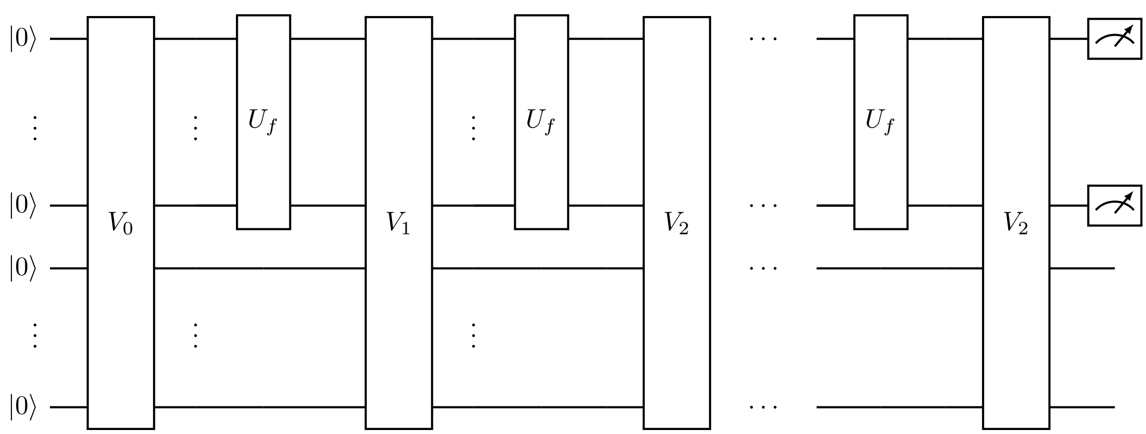
Lecture 10

Unstructured Search and Discrete-time Quantum Walk

- Lower bound of Grover search
- Random walks
- Block encoding

1 Lower Bound of Grover Search

After all, a quantum algorithm for searching looks below: $N = 2^n$



$|\psi_t\rangle :=$ state after V_t, the t-th non-query operation, assuming no marked item.
$|\psi_t^x\rangle_{:} =$ state after V_t, assuming a unique marked item x.

To solve the unstructured search problem, we must have $\| \, |\psi_T\rangle - |\psi_T^x\rangle \, \| \geqslant c$ for a constant c. Since the algorithm must work for any x, we must have

$$\sum_{x=1}^{N} \| \, |\psi_T\rangle - |\psi_T^x\rangle \, \| \geqslant cN$$

Since $|\psi_0^x\rangle = |\psi_0\rangle$ for all x, $\sum_{x=1}^{N} || \psi_0\rangle - |\psi_0^x\rangle \, \| = 0$.

$$
\begin{aligned}
\| \left|\psi_t\right\rangle - \left|\psi_t^x\right\rangle \| &= \| V_t \left(\psi_{t-1}\right\rangle - V_t U_x \left|\psi_{t-1}^x\right\rangle \| && U_x = I - 2|x\rangle\langle x|, \text{ the black box} \\
&= \| \left|\psi_{t-1}\right\rangle - U_x |\psi_{t-1}^x\rangle \| && \text{when the marked item is } x. \quad U_x^2 = I \\
&= \| U_x \left|\psi_{t-1}\right\rangle - \left|\psi_{t-1}^x\right\rangle \| \\
&= \| \left(U_x \left|\psi_{t-1}\right\rangle - \left|\psi_{t-1}\right\rangle\right) + \left(\left|\ \psi_{t-1}\right\rangle - \left|\psi_{t-1}^x\right\rangle\right) \| && \text{triangle inequality} \\
&\leq \| U_x \left|\psi_{t-1}\right\rangle - \left|\psi_{t-1}\right\rangle \| + \| \left|\psi_{t-1}\right\rangle - \left|\psi_{t-1}^x\right\rangle \|.
\end{aligned}
$$

$\left|\psi_t\right\rangle = \sum_{y=1}^N \alpha_{y_t} |y\rangle \left|\phi_y\right\rangle$ collect all the vectors where the first subsystem is y
$\left|\phi_y\right\rangle$ is normalized. $\sum_{y=1}^N \left|\alpha_{y,t}\right|^2 = 1$.

$$
U_x \left|\psi_t\right\rangle = \sum_{y \neq x} \alpha_{y,t} |y\rangle \left|\phi_y\right\rangle - \alpha_{x,t} |x\rangle \left|\phi_x\right\rangle = \left|\psi_t\right\rangle - 2\alpha_{x,t} |x\rangle \left|\phi_x\right\rangle.
$$

$$
\Rightarrow \| U_x \left(p_t\right\rangle - \left|\psi_t\right\rangle \| = 2 \left|\alpha_{x,t}\right|.
$$

This further implies

$$
\| \left|\psi_T^x\right\rangle - \left|\psi_T\right\rangle \| \leqslant 2 \sum_{j=1}^{T-1} \left|\alpha_{x,j}\right|. \qquad (\sum_i a_i^2)(\sum_i b_i^2) \geqslant (\sum_i a_i b_i)^2
$$

$$
\begin{aligned}
\Rightarrow CN \leqslant \sum_{x=1}^N \| \left|\psi_T\right\rangle - \left|\psi_T^x\right\rangle \| &\leqslant 2 \sum_{x=1}^N \sum_{j=1}^{T-1} \left|\alpha_{x,j}\right| = 2 \sum_{j=1}^{T-1} \sum_{x=1}^N \left|\alpha_{x,j}\right|. \\
&\leqslant 2 \sum_{j=1}^{T-1} \sqrt{N} \cdot \sqrt{\sum_{x=1}^N \left|\alpha_{x,j}\right|^2} = 2\sqrt{N}(T-1)
\end{aligned}
$$

$2\sqrt{N}(T-1) \geqslant CN \Rightarrow T = \Omega(\sqrt{N})$.

Corollary 1.1. *Grover search is optimal for unstructured search.*

Remark 1.2. From a high-level picture, OR gives a quadratic quantum speedup. Is this the best we can achieve for total functions?

For a total function $f : \{0.1\}^N \to \{0,1\}$, denote $D(f), R(f), Q(f)$ to be its classical deterministic, classical randomized, and quantum query complexities.

It was widely conjectured that $R(f) = O\left(Q(f)^2\right)$ for a long time.

Aaronson, Ben-David, and Kothari, STOC 2016: $\exists f$ st. $R(f) = \tilde{\Omega}\left(Q(f)^{2.5}\right)$.

State-of-the-art:

1. $\forall$ total f, $D(f) = O\left(Q(f)^4\right)$. [Ambainis-Balodis-Belovs-Lee-Santha-Smotrovs, JACM 2017]
2. total f, $D(f) = \Omega(Q(f)^4)$. [Aaronson-Ben-David-Kothari-Rao-Tal, STOC 2021]
3. total f, $R(f) = \Omega\left(Q(f)^3\right)$. [Bansal-Sinha STOC 2021]

   (since $D(f) \geqslant R(f), R(f) = O\left(Q(f)^4\right)$. [Sherstov-Storozhenko-Wu STOC 2021]

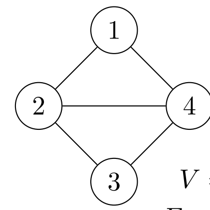
2 Discrete-time Quantum Walk

Generalize unstructured search? Break the symmetry in a general sense.

A common tool to characterize discrete objects: graphs $G = (V, E)$

Grover: basically a problem on complete graph

$$
\begin{tikzcd}
\text{totally unstructured} \arrow[d] & \text{more structured} \arrow[d] \\
\text{complete graph} \arrow[r, "\text{generalize}"] \arrow[d] & \text{a graph} \arrow[d] \\
\text{Grover search} & \text{quantum walk}
\end{tikzcd}
$$



$V = \{1, 2, 3, 4\}$
$E = \{(1, 2), (1, 4),$
$(2, 3), (2, 4), (3, 4)\}$

2.1 Random walks

Classical random walk on graphs. Given a graph $G = (V, E)$, a random walk is given by a transition matrix P. with its entry P_{ij} denoting the probability of the transition from vertex i to vertex j.

Such a P is called a stochastic matrix, satisfying: $P_{ij} \geqslant 0 \quad \forall i, j; \sum_j P_{ij} = 1 \quad \forall i$.

Properties of random walks (Markov Chains):

- Irreducible: Any vertex can be reached from any other vertex in a finite number of steps.
- Aperiodic: There exists no integer greater than 1 that divides the length of every cycle of the graph.
- Ergodic: Both irreducible and aperiodic.

Theorem 2.1 (Perron-Frobenius Theorem)**.** *Any ergodic random walk P has a unique stationary state π such that $\pi_i > 0\ \forall i, \quad \sum_i \pi_i = 1$, and $\sum_i \pi_i P_{ij} = \pi_j\ \forall j$.*

In other words, π is the left eigenvector of P with eigenvalue 1.

- Reversible: The detailed balance condition $\pi_i p_{ij} = \pi_j p_{ji} \quad \forall i, j$ is satisfied.
- Discriminant matrix: A matrix D where $D_{ij} = \sqrt{P_{ij} P_{ji}} \quad \forall i, j$.
  D is real symmetric, and hence Hermitian.

Proposition 2.2. *If a random walk is ergodic and reversible, then the stationary state $|\pi\rangle = \sum_i \sqrt{\pi_i} |i\rangle$ is an eigenvector of D with eigenvalue 1, i.e. $D\,|\pi\rangle = |\pi\rangle$. Furthermore, $D = \mathrm{diag}(\sqrt{\lambda}) \cdot P \cdot (\mathrm{diag}(\sqrt{\lambda}))^{-1}$, where $\mathrm{diag}(\sqrt{\lambda}) = \begin{pmatrix} \sqrt{\lambda_1} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \sqrt{\lambda_N} \end{pmatrix}$. Hence, the set of (left) eigenvalues of P and the set of the eigenvalues of D are the same.*

Proof. For any i,

$$
\begin{aligned}
(D|\pi\rangle)_i &= \langle i|D|\pi\rangle && \Big(D = \textstyle\sum_{i,j} D_{ij} |i\rangle\langle j|\Big) \\
&= \textstyle\sum_j D_{ij} \langle j|\pi\rangle \\
&= \textstyle\sum_j \sqrt{P_{ij} P_{ji}} \sqrt{\pi_j} && (\text{reversibility:} \ \ \pi_i P_{ij} = \pi_j P_{ji}) \\
&= \textstyle\sum_j P_{ij} \sqrt{\pi_i} = \sqrt{\pi_i}.
\end{aligned}
$$

Furthermore. for any i, j, $\quad (D)_{ij} = \sqrt{P_{ij}P_{ji}} = \sqrt{\pi_i}P_{ij}\left(\sqrt{\pi_j}\right)^{-1} = \left(\operatorname{diag}(\sqrt{\lambda}) \cdot P \cdot \operatorname{diag}(\sqrt{\lambda})^{-1}\right)_{ij}$. Therefore, $D = \operatorname{diag}(\sqrt{\lambda}) \cdot P \cdot \operatorname{diag}(\sqrt{\lambda})^{-1}$. ■

2.2 Block encoding

Now, how shall we define quantum walks?

A simplest idea (say for unweighted graph): $\quad |j\rangle \to |\,\partial_j\rangle := \frac{1}{\sqrt{\deg(j)}}\sum_{k:(j,k)\in E}|k\rangle$

What's the issue with this? Not a unitary map in general.

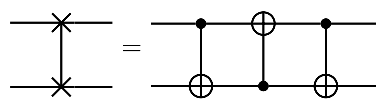
$$\langle 2|4\rangle = 0$$
$$\langle \partial_2|\partial_4\rangle = \left(\frac{1}{\sqrt{3}}\langle 1| + \frac{1}{\sqrt{3}}\langle 3| + \frac{1}{\sqrt{3}}\langle 4|\right)\left(\frac{1}{\sqrt{3}}|1\rangle + \frac{1}{\sqrt{3}}|2\rangle + \frac{1}{\sqrt{3}}|3\rangle\right) = \frac{2}{3}$$

Instead, we consider: $\mathrm{Op}\,|0^n\rangle\,|j\rangle = \sum_k \sqrt{P_{jk}}|k\rangle|j\rangle$.

The discriminant matrix looks good-it's symmetric. Can we make that?

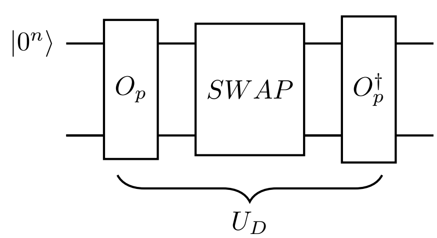
We also introduce the n-qubit swap operator: $\mathrm{SWAP}\,|i\rangle\,|j\rangle = |j\rangle|i\rangle \quad \forall i, j \in \{0,1\}^n$.

(SWAP can be implemented by $\begin{pmatrix} n \\ 2 \end{pmatrix} = O\left(n^2\right)$ 2-qubit swap gates. In total, SWAP can be implemented by $O\left(n^2\right)$ CNOTs.)



$$\mathrm{SWAP}\,|i\rangle|j\rangle = |j\rangle|i\rangle$$
$$\forall i, j \in \{0,1\}$$

We consider



UD: 1 step quantum walk.

Proposition 2.3. $\forall i, j \in [N]$, $\langle 0^n|\langle i\,|U_D|\,0^n\rangle|\,j\rangle = D_{ij}$. *Intuitively,* $U_D = \begin{pmatrix} D & \cdot \\ \cdot & \cdot \end{pmatrix} = |0^n\rangle\langle 0^n| \otimes D + \cdots$. *Such a form is called a block encoding of* D. .

Proof.

For any j, $|0^n\rangle\,|j\rangle \xrightarrow{Op} \sum_k \sqrt{P_{jk}}|k\rangle|j\rangle \xrightarrow{\mathrm{SWAP}} \sum_k \sqrt{P_{jk}}\,|j\rangle\,|k\rangle$.

Meanwhile $|0^n\rangle\,|i\rangle \xrightarrow{Op} \sum_{k'} \sqrt{P_{ik'}}\,|k'\rangle\,|i\rangle$. $\qquad \delta_{x,y} = \begin{cases} 1 & x = y \\ 0 & x \neq y \end{cases}$

So the inner product gives

$$\langle 0^n | \langle i | U_D | O^n \rangle | j \rangle = \sum_{k \cdot k'} \sqrt{P_{ik'}} \sqrt{P_{jk}} \delta_{k',j} \delta_{i,k} = \sqrt{P_{ij}} \sqrt{P_{ji}} = D_{ij}.$$

■

Next: What can be obtain by using the block encoding?

Denote the eigendecomposition of D as $D = \sum_i \lambda_i |v_i\rangle \langle v_i|$.

Far each eigenstate $|v_i\rangle$,

$$U_D |0^n\rangle |v_i\rangle = |0^n\rangle D |v_i\rangle + \left|\tilde{\perp}_i\right\rangle = \lambda_i |0^n\rangle |v_i\rangle + \left|\tilde{\perp}_i\right\rangle \tag{*}$$

Here $\left|\tilde{\perp}_i\right\rangle$ is an unnormalized state satisfying $\Pi \left|\tilde{\perp}_i\right\rangle = 0$, where

$$\Pi = |0^n\rangle \langle 0^n| \otimes I$$

(*) should give a normalized state, so we may write $\left|\tilde{\perp}_i\right\rangle = \sqrt{1-\lambda_i^2} |\perp_i\rangle$, where $| \perp_i\rangle$ is a normalized state.

Suppose $\lambda_i \neq \pm 1$. First, notice that $U_D^\dagger = U_D$ $\quad$ $(ABC)^\dagger = C^\dagger (AB)^\dagger = C^\dagger B^\dagger A^\dagger$

$$U_D^\dagger = \left(\mathrm{Op}\,\mathrm{SWAP}\,\mathrm{Op}^\dagger\right)^\dagger = \left(\mathrm{Op}^\dagger\right)^\dagger \mathrm{SWAP}^\dagger\,\mathrm{Op}^\dagger = \mathrm{Op}\,\mathrm{SWAP}\,\mathrm{Op}^\dagger = U_D$$

Apply U_D to both sides of $(*)$, we have $\left(U_D^2 = U_D^\dagger U_D = I\right)$

$$\begin{aligned}
|0^n\rangle |v_i\rangle &= \lambda_i U_D |0^n\rangle |v_i\rangle + \sqrt{1-\lambda_i^2} U_D |\perp_i\rangle \\
&= \lambda_i \left(\lambda_i |0^n\rangle |v_i\rangle + \sqrt{1-\lambda_i^2} |\perp_i\rangle\right) + \sqrt{1-\lambda_i^2} U_D |\perp_i\rangle .
\end{aligned}$$

$$\Rightarrow \left(1-\lambda_i^2\right) |0^n\rangle |v_i\rangle = \sqrt{1-\lambda_i^2}\lambda_i |\perp_i\rangle + \sqrt{1-\lambda_i^2} U_D |\perp_i\rangle$$

$$\Rightarrow \quad U_D |\perp_i\rangle = \sqrt{1-\lambda_i^2} |0^n\rangle |v_i\rangle - \lambda_i |\perp_i\rangle .$$