Grover's Search

Yu-Hsuan Huang Cheng-Wei Lin

National Chiao Tung University

January 10, 2020

Overview

Intended Outcome. Leverage matrix analysis and used it on Grover's search and BBBV bound. Understand how would quantum evolution corresponds to our matrix method.

- Preliminary
- Quantum "rules"
- Preimage finding problem
- Housholder transform
- Grover's search
- BBBV's bound
- Consequences

Preliminary

Definition (Lebesgue Space)

Given a measure space X, μ its p-Labesgue space collects all finite energy mapping to $\mathbb{C}$,

$$\mathcal{L}^p(X) := \left\{ f : X \to \mathbb{C}, \int_X |f|^p \mathrm{d}\mu < \infty \right\}.$$

Specifically, we denote $\mathbb{C}^X := \mathcal{L}^2(X)$ with inner product,

$$\langle x, y \rangle := \int_X \bar{f} \cdot g \mathrm{d}\mu,$$

and norm $\|x\| := \langle x, x \rangle$.

Preliminary

Theorem (Riesz, Fisher)

The $\mathbb{C}^X$ *is topologically complete, i.e. any Cauchy sequence,* $\{x_i\}_{i\in\mathbb{N}} \subseteq \mathbb{C}^X$ *with* $\forall \epsilon > 0 \exists N, \|x_n - x_m\| < \epsilon, \forall n, m > N$*, has limit,*

$$\lim_{i\to N} x_i \in \mathbb{C}^X.$$

If X is finite, then we could choose μ as discrete measure, then

$$\mathbb{C}^X = \left\{ f : X \to \mathbb{C}, \sum_{x\in X} |f(x)|^2 < \infty \right\}.$$

For any $x \in X$, denote ket $|x\rangle : \begin{cases} x \mapsto 1 \\ x' \mapsto 0, \text{ for } x \neq x' \end{cases}$ and bra $\langle x| := |x\rangle^* := \langle x, \cdot\rangle \in \mathrm{Hom}(\mathbb{C}^X, \mathbb{C})$.

Preliminary

Definition

Given a linear map between Hilbert spaces $L : V \to W$, it's adjoint $L^* : W \to V$ is the only operator [Riesz, Frechet] satisfying,

$$\langle Lv, w \rangle_W = \langle v, L^* w \rangle_V.$$

When $W = V$ and $L \circ L^* = L^* \circ L = \mathrm{Id}$, L is said to be unitary.

If V, W are finite dimensional $\mathcal{L}^2$ spaces, then operator could be represented as a matrix and its adjoint is just the conjugate transpose matrix. The unitary operators are just those unitary matrices.

Preliminary

Definition (local operators)

Consider $\mathbb{C}^{\{0,1\}^J}$, $J \subseteq \mathbb{N}$ composed of countably many 2 dimensional Lebesgue spaces, i.e. it could be written as the tensor space,

$$\mathbb{C}^{\{0,1\}^K} = \bigotimes_{j \in J} \mathbb{C}^{\{0,1\}}.$$

A operator L is said to be r-local iff, $\exists R \subseteq J$ of size r and $L_R \in \mathrm{GL}(\mathbb{C}^{\{0,1\}^R})$ that

$$L = \left(\bigotimes_{j \in J - R} \mathrm{Id} \right) \otimes L_R.$$

Quantum "Rules"

Definition (quantum circuit)

A quantum circuit with n-qubits and t gates is composed of a sequence of $O(1)$-local unitary operators $\{U_i\}_{1\leq i\leq t} \subseteq \mathbb{C}^{\{0,1\}^n}$. With initial input state $|\psi_0\rangle$, the circuit induces a unitary evolution $\{|\psi_i\rangle\}_{0\leq i\leq n}$ as following,

$$|\psi_i\rangle = U_i|\psi_{i-1}\rangle.$$

Definition (measurement)

Given a quantum state $|\psi\rangle \in \mathbb{C}^X$ measurement is specified by a set of orthogonal projection operators $\{P_j\}_{j\in J}$, i.e.

- $\bigoplus_{j\in J} \mathrm{Im}(P_j) = \mathbb{C}^X$,
- $\mathrm{Im}(P_i) \perp \mathrm{Im}(P_j)$, for $i \neq j$,
- $P_j^2 = P_j, \forall j \in J$.

The measurement result would yield j with probability $\|P_j|\psi\rangle\|^2$.

Quantum "Rules"

For example, take Hadamard tansform $H^{\otimes n}$ as example,

$$H^{\otimes n} = \frac{1}{\sqrt{2^n}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{\otimes n}.$$

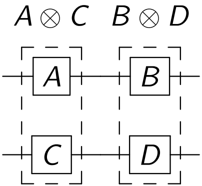
This maps as follows,

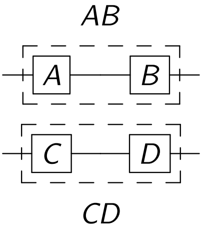
$$|x\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{x' \in X} (-1)^{x \cdot x'} |x'\rangle.$$

Specifically define $|+\rangle = H|0\rangle$ and $|-\rangle = H|1\rangle$, Also we have,

$$H|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x' \in X} |x'\rangle.$$

Quantum "Rules"

$(A \otimes C)(B \otimes D) \sim$ 

$=$ 

$\sim AB \otimes CD$

First Look

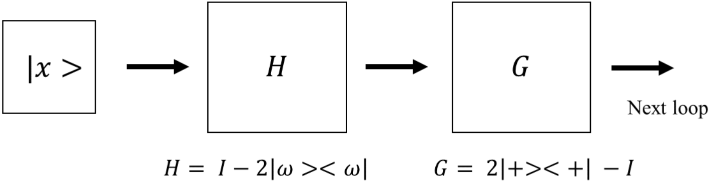
Definition (preimage finding problem)

In a preimage finding finding problem, one is given access to the quantum oracle of $f : \{0,1\}^n \to \{0,1\}$ in the following form,

$$O_{\pm} : |x\rangle \to (-1)^{f(x)}|x\rangle,$$

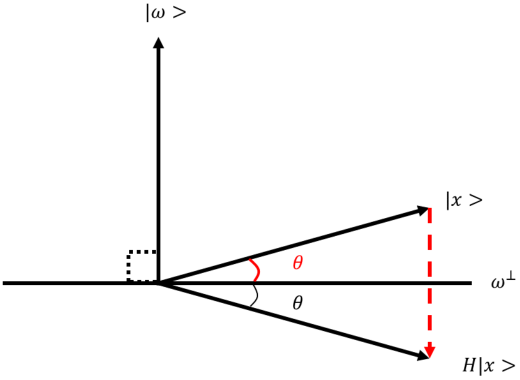
and asked to find any x_0 such that $f(x_0) = 1$.

First Look



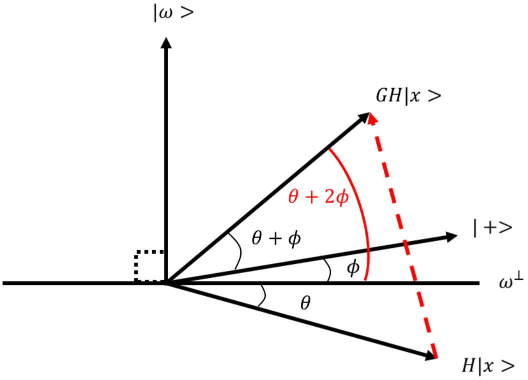
(Here H represent Householder transform instead of Hadamard.)

First Look



(Here H represent Householder transform instead of Hadamard.)

First Look



(Here *H* represent Householder transform instead of Hadamard.)

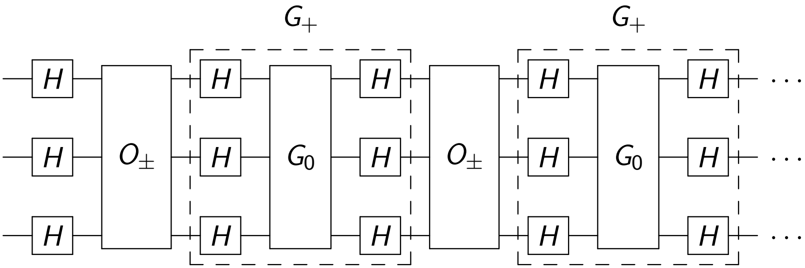
Unstructural Search

Theorem (Grover's search)

The preimage finding problem could be solved in $O(\sqrt{\frac{N}{k}})$ quantum queries and $O(n\sqrt{\frac{N}{k}})$ gates where $N := 2^n$ and $k = \#\{x : f(x) = 1\}$ with the following algorithm,

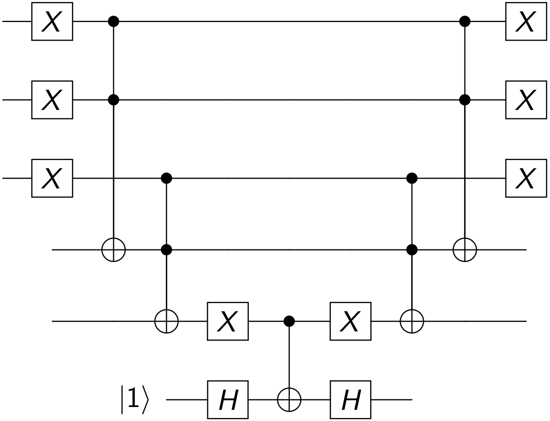
- *Initialize the state $|\psi_0\rangle = |0\rangle$.*
- *Apply Hadamard transform $|\psi_1\rangle = H|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{i\in\{0,1\}^n} |i\rangle$.*
- *Apply $G_+ \circ O_\pm$ for $O(\sqrt{\frac{N}{k}})$ iterations, $|\psi_{i+1}\rangle = G_+ \circ O_\pm|\psi_i\rangle$, where*
$$G_+ = 2|+\rangle\langle+| - I.$$
- *Measure the final state in computational basis with the projection matrices*
$$\{P_x := |x\rangle\langle x|\}_{x\in\{0,1\}^n} \subseteq \mathbb{C}^{\{0,1\}^n}.$$

Unstructural Search



Unstructural Search

$G_0 =$



Unstructural Search

Proof.

Well-definedness. First of all, since $\sigma(G_n) = \{\pm 1\}$ and Hermitian, G_+ is unitary. Also we have,

$$G_+ = 2|+\rangle\langle +| - I = H \circ G_0 \circ H,$$

where

$$G_0 := 2|0\rangle\langle 0| - I : \begin{cases} |x\rangle \mapsto -|x\rangle, & \text{for } x \neq 0 \\ |0\rangle \mapsto |0\rangle. \end{cases}$$

Check that G_0 could be constructed in $O(n)$ gates!

Convergence. Suppose

$$|\psi_i\rangle = \sum_{x:f(x)=1} a_i|x\rangle + \sum_{x:f(x)=0} b_i|x\rangle.$$

Define mean value $\mu_i := \frac{-k}{N} a_i + \frac{(N-k)}{N} b_i$.

Unstructural Search

Proof.

We have,

$$a_{i+1} = 2\mu_i + a_i = \frac{N-2k}{N} a_i + \frac{2N-2k}{N} b_i, \text{ and } b_i = \sqrt{\frac{1-ka_i^2}{N-k}}.$$

Suppose $ka_i^2 = \sin^2(\theta_i)$, then $a_i = \frac{\sin(\theta_i)}{\sqrt{k}}$ and $b_i = \frac{\cos(\theta_i)}{\sqrt{N-k}}$.

$$\begin{aligned}\sin(\theta_{i+1}) &= \frac{N-2k}{N\sqrt{k}} a_i + \frac{2N-2k}{N\sqrt{k}} b_i \\ &= \frac{N-2k}{N} \sin(\theta_i) + \frac{2\sqrt{(N-k)k}}{N} \cos(\theta_i) \\ &= \sin(\theta_i + \phi),\end{aligned}$$

where $\sin(\phi) = \frac{2\sqrt{(N-k)k}}{N}$.

Unstructural Search

Proof.

Note that $\phi \in \Theta\left(\sqrt{\frac{k}{N}}\right)$ is independent of i and thus, in order that

$$\begin{aligned}\Omega(1) &\leq \Pr[\text{measure result } x : f(x) = 1] \\ &= ka_i^2 = k\sin^2(\theta_i) = k\sin^2(\theta_1 + (i-1)\phi),\end{aligned}$$

the iteration count $i \in \Theta(\sqrt{\frac{N}{k}})$ would be enough. Also, since each iteration would cost $\Theta(n)$ gates, in total $\Theta(n\sqrt{\frac{N}{k}})$ gates are enough. $\square$

Query Lower Bound

We now introduce a restricted version of BBBV bound for pre-image finding problem.

Theorem (Bennett, Bernstein, Brassard, Vazirani)

In order to solve for pre-image finding problem with $k = 1$, $\Omega(\sqrt{N})$ quantum queries are required.

Lemma

Suppose $|\phi\rangle, |\psi\rangle \in \mathbb{C}^X$ with $\||\phi\rangle\| = \||\psi\rangle\| = 1$ and $\||\phi\rangle - |\psi\rangle\| \leq \epsilon$. Given measurement matrices $\{P_j\}_{j\in J}$ the probability difference is bounded as following,

$$\sum_{j\in J} \left| \|P_j|\phi\rangle\|^2 - \|P_j|\psi\rangle\|^2 \right| = \sum_{j\in J} |\langle\phi|P_j|\phi\rangle - \langle\psi|P_j|\psi\rangle| \leq 4\epsilon.$$

Query Lower Bound

Proof.

Suppose $|\delta\rangle = |\phi\rangle - |\psi\rangle$ and,

$$P_j|\phi\rangle = \alpha_j, \quad P_j|\psi\rangle = \beta_j, \quad \gamma_j = P_j|\delta\rangle = \alpha_j - \beta_j.$$

Then

$$\begin{aligned} \alpha_j\alpha_j^* - \beta_j\beta_j^* &= (\beta_j + \gamma_j)(\beta_j^* + \gamma_j^*) - \beta_j\beta_j^* \\ &= \beta_j\beta_j^* + \gamma_j\gamma_j^* + \beta_j\gamma_j^* + \gamma_j\beta_j^* - \beta_j\beta_j^* \\ &= \gamma_j\gamma_j^* + \beta_j\gamma_j^* + \gamma_j\beta_j^*. \end{aligned}$$

Therefore,

$$\sum_{j\in J} |\langle\phi|P_j|\phi\rangle - \langle\psi|P_j|\psi\rangle| \leq \sum_{j\in J} \left|\gamma_j\gamma_j^* + \beta_j\gamma_j^* + \gamma_j\beta_j^*\right|$$
$$\leq \langle\delta|\delta\rangle + \langle\psi|\delta\rangle + \langle\delta|\psi\rangle \leq \epsilon^2 + 2\epsilon \leq 4\epsilon.$$

Query Lower Bound

Proof of main theorem.

Any q-query algorithm is of form

$$U_q O_\pm U_{q-1} \dots U_1 O_\pm U_0.$$

For some $\tilde{x} \in X$ pick $f(x) = \begin{cases} 1, & \text{for } x = \tilde{x}, \\ 0, & \text{otherwise.} \end{cases}$ Let

$$|\psi_{\tilde{x}}^i\rangle = O_\pm U_{i-1} |\psi_{\tilde{x}}^{i-1}\rangle,$$
$$|\psi_0^i\rangle = U_{i-1} |\psi_{\tilde{x}}^{i-1}\rangle.$$

We are bounding $\| U_q |\psi_{\tilde{x}}^q\rangle - U_q |\psi_0^q\rangle \| = \| |\psi_{\tilde{x}}^q\rangle - |\psi_0^q\rangle \|$.

Query Lower Bound

Proof of main theorem.

Note that,

$$
\begin{aligned}
& \| |\psi_{\tilde{x}}^{i}\rangle - |\psi_{0}^{i}\rangle \| \\
& \leq \| O_{\pm} U_{i-1} |\psi_{\tilde{x}}^{i-1}\rangle - U_{i-1} |\psi_{0}^{i-1}\rangle \| \\
& \leq \| O_{\pm} U_{i-1} |\psi_{\tilde{x}}^{i-1}\rangle - U_{i-1} |\psi_{\tilde{x}}^{i-1}\rangle \| + \| U_{i-1} |\psi_{\tilde{x}}^{i-1}\rangle - U_{i-1} |\psi_{0}^{i-1}\rangle \| \\
& \leq \| O_{\pm} U_{i-1} |\psi_{\tilde{x}}^{i-1}\rangle - U_{i-1} |\psi_{\tilde{x}}^{i-1}\rangle \| + \| |\psi_{\tilde{x}}^{i-1}\rangle - |\psi_{0}^{i-1}\rangle \|.
\end{aligned}
$$

Let $U_{i-1}|\psi_{\tilde{x}}^{i-1}\rangle = \sum_x \alpha_x |x\rangle$, then

$$\| O_{\pm} U_{i-1} |\psi_{\tilde{x}}^{i-1}\rangle - U_{i-1} |\psi_{\tilde{x}}^{i-1}\rangle \| \leq 2|\alpha_{\tilde{x}}|.$$

By Cauchy-Schwartz Inequality when running all possilbe $\tilde{x}$,

$$\sum_{\tilde{x} \in X} |\alpha_{\tilde{x}}| \leq \sqrt{\sum_{\tilde{x} \in X} |\alpha_{\tilde{x}}^2| \cdot N} \leq \sqrt{N}.$$

Query Lower Bound

Proof of main theorem.

Therefore,

$$\begin{aligned}
&\sum_{\tilde{x}\in X} \| |\psi^i_{\tilde{x}}\rangle - |\psi^i_0\rangle \| \\
&\leq \sum_{\tilde{x}\in X} \left(\| O_{\pm} U_{i-1} |\psi^{i-1}_{\tilde{x}}\rangle - U_{i-1} |\psi^{i-1}_{\tilde{x}}\rangle \| + \| |\psi^{i-1}_{\tilde{x}}\rangle - |\psi^{i-1}_0\rangle \| \right) \\
&\leq \sum_{\tilde{x}\in X} \left(\sqrt{N} + \| |\psi^{i-1}_{\tilde{x}}\rangle - |\psi^{i-1}_0\rangle \| \right) \leq q\sqrt{N},
\end{aligned}$$

We have that $\mathbb{E}_{\tilde{x} \xleftarrow{\$} X} [\| |\psi^i_{\tilde{x}}\rangle - |\psi^i_0\rangle \|] \leq \frac{q}{\sqrt{N}}$. Together with previous lemma, in order to find preimage with $\Omega(1)$ probability, we require $q \geq \Omega(\sqrt{N})$. $\square$

Consequences

Corollary

The post quantum security for any symmetrical cryptosystem is cut in half.

Corollary (Brassard, Hoyer, Tapp)

Hash collision could be found in $O(N^{\frac{1}{3}})$ *queries.*

Corollary (complexity theoretic result)

There is an quantum oracle A *that*

$$\mathrm{NP}^A \not\subseteq \mathrm{BQP}^A.$$

Summary and Take-aways

- Quantum computation is just unitary evolution driven by local unitaries.
- The Grover diffusion operator G_+ is in fact negative Householder transform.
- For upper bound proof, need to prove for well-definedness and convergence speed.
- For lower bound proof, need to consider general case. (any potential algorithm)
- Grover search produces quadratic and only quadratic speedup, quantum computation is not the cure-all!