Introduction to Quantum Information Processing

Lecture 12

Michele Mosca

Overview

- Hidden subgroup problem
- Quantum Searching

Abelian Hidden Subgroup Problem

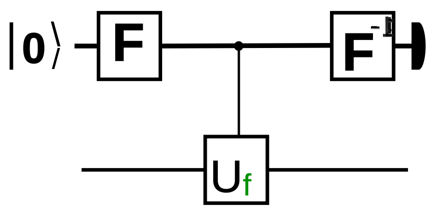
$$G = Z_{M_0} \times Z_{M_1} \times \cdots \times Z_{M_n}$$

$f : G \longrightarrow X \qquad K \leq G$

$f(y) = f(x)$ iff $x - y \in K$

Find generators for K

Network for AHS



AHS Algorithm in standard basis

$$\sum_{x} |x\rangle |f(x)\rangle$$

$$= \sum_{M} |W+K\rangle |f(M)\rangle$$

$$\xrightarrow{F^{-1}} \sum_{M} \left(\; s_0 \quad s_1 \quad s_n \; \right) |f(M)\rangle$$

$\in K^{\perp}$

AHS for Z_2^n in eigenbasis

(Simon's Problem)

$$|\Psi_s\rangle = \sum (-1)^{x \cdot s} |f(x)\rangle \qquad s \in K^{\perp}$$

is an eigenvector of $f(x) \rightarrow f(x \oplus y)$

$$\sum_{x} |x\rangle |f(x)\rangle \xrightarrow{F^{-1}} \sum_{s \in K^{\perp}} \left(\; s \; \right) |\Psi_s\rangle$$

Other applications of Abelian HSP

- Any finite Abelian group G is the direct sum of finite cyclic groups $\langle g_1 \rangle \oplus \langle g_2 \rangle \oplus \cdots \oplus \langle g_n \rangle$
- But finding generators $g_1, g_2, \cdots, g_n$ satisfying $G = \langle g_1 \rangle \oplus \langle g_2 \rangle \oplus \cdots \oplus \langle g_n \rangle$ is not always easy, e.g. for $G = Z_N^*$ it's as hard as factoring N
- Given any polynomial sized set of generators, we can use the Abelian HSP algorithm to find new generators that decompose G into a direct sum of finite cyclic groups.

Examples:

Deutsch's Problem: $G = \{0,1\}$ $X = \{0,1\}$

$K = \{0\}$ or $\{0,1\}$

Order finding: $G = Z$ X any group

$f(x) = a^x$ $K = rZ$

Example:

Discrete Log of $b = a^k$ to base a:

$G = Z_r \times Z_r$ X any group

$f(x, y) = a^x b^y$

$K = \langle k, -1 \rangle$

Examples:

Self-shift equivalences: $G = GF(q)^n$

$$X = GF(q)[X_1, X_2, \ldots, X_n]$$

$$f(a_1, a_2, \ldots, a_n) = P(X_1 - a_1, \ldots, X_n - a_n)$$

$$K = \{(a_1, \ldots, a_n) : P(X_1 - a_1, \ldots, X_n - a_n) = P(X_1, \ldots, X_n)\}$$

What about non-Abelian HSP

- Consider the symmetric group $G = S_n$
- S_n is the set of permutations of n elements
- Let G be an n-vertex graph
- Let $X_G = \{\pi(G) \mid \pi \in S_n\}$
- Define $f_G : S_n \to X_G \quad f_G(\pi) = \pi(G)$
- Then $f_G(\pi_1) = f_G(\pi_2) \Leftrightarrow \pi_1 K = \pi_2 K$
  where $K = AUT(G) = \{\pi \mid \pi(G) = G\}$

Graph automorphism problem

- So the hidden subgroup of f_G is the automorphism group of G
- This is a difficult problem in NP that is believed not to be in BPP and yet not NP-complete.

Other

Progress on the Hidden Subgroup Problem in non-Abelian groups (not an exhaustive list)

•Ettinger, Hoyer arxiv.gov/abs/quant-ph/9807029

•Roetteler,Beth quant-ph/9812070

• Ivanyos,Magniez,Santha arxiv.org/abs/quant-ph/0102014

•Friedl, Ivanyos,Magniez,Santha,Sen quant-ph/0211091 (Hidden Translation and Orbit Coset in Quantum Computing); they show e.g. that the HSP can be solved for solvable groups with bounded exponent and of bounded derived series

•Moore,Rockmore,Russell,Schulman, quant-ph/0211124

Searching Problem

- A function $f:\{0,1\}^n \rightarrow \{0,1\}$
- A black box $O_f : |x\rangle|b\rangle \rightarrow |x\rangle|b \oplus f(x)\rangle$
- Let $X_1 = f^{-1}(1) \qquad X_0 = f^{-1}(0) \qquad t = |X_1|$
- Find an $x \in X_1$
- Let $|\Psi_1\rangle = \sum_{x \in X_1} \alpha_x |x\rangle \qquad |\Psi_0\rangle = \sum_{y \in X_0} \alpha_y |y\rangle$

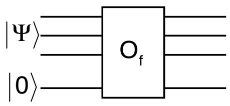
$$\sum_{x \in X_1} |\alpha_x|^2 = 1 \qquad \sum_{y \in X_0} |\alpha_y|^2 = 1$$

Searching Problem

- E.g. $|\Psi_1\rangle = \sum_{x \in X_1} \frac{1}{\sqrt{t}} |x\rangle \qquad |\Psi_0\rangle = \sum_{y \in X_0} \frac{1}{\sqrt{N-t}} |y\rangle$

Searching Problem

- Given one copy of $|\Psi\rangle = \alpha|\Psi_1\rangle + \beta|\Psi_0\rangle$
- We can measure an $x \in X_1$ with probability $|\alpha|^2$
- Idea:



$\alpha|\Psi_1\rangle|1\rangle + \beta|\Psi_0\rangle|0\rangle$

- Can we force the system to measure $|1\rangle$ in the 2nd qubit? Can we amplify that amplitude?

Searching Problem

NO!

- Given N copies of $\alpha|\Psi_1\rangle|1\rangle + \beta|\Psi_0\rangle|0\rangle$ we will measure at least one $|1\rangle$ with probability

$$1-(1-|\alpha|^2)^N \approx \frac{N}{|\alpha|^2}$$

- Can we do better than that by just measuring these N states?

Searching Problem

NO!

- Given a network that implements $A|0\rangle \to |\Psi\rangle$, and the black box O_f , can we do any better?

Searching Problem

YES!

- Note that $|\Psi\rangle = \sin\left(\frac{\theta}{2}\right)|\Psi_1\rangle + \cos\left(\frac{\theta}{2}\right)|\Psi_0\rangle$ for some θ and states $|\Psi_1\rangle, |\Psi_0\rangle$
- Consider the operator $Q = AU_0A^{-1}O_f$

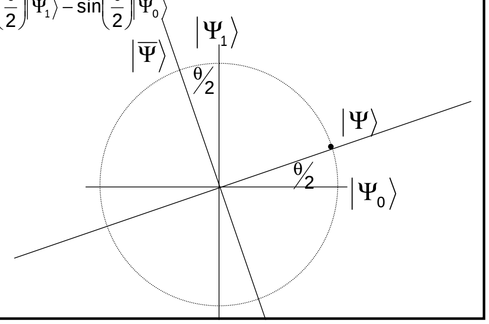
(redefine $O_f : |x\rangle \to (-1)^{f(x)}|x\rangle$)

- We define $U_0 : |x\rangle \to -|x\rangle, x \neq 0$

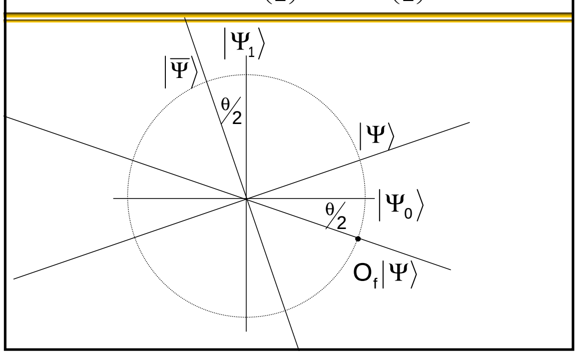
  $|0\rangle \to |0\rangle$

$$|\Psi\rangle = \sin\left(\frac{\theta}{2}\right)|\Psi_1\rangle + \cos\left(\frac{\theta}{2}\right)|\Psi_0\rangle$$

$$|\overline{\Psi}\rangle = \cos\left(\frac{\theta}{2}\right)|\Psi_1\rangle - \sin\left(\frac{\theta}{2}\right)|\Psi_0\rangle$$



$$O_f|\Psi\rangle = -\sin\left(\frac{\theta}{2}\right)|\Psi_1\rangle + \cos\left(\frac{\theta}{2}\right)|\Psi_0\rangle$$



Searching Problem

- Notice that

$$AU_{\bar{0}}A^{-1}A|0\rangle = A|0\rangle$$

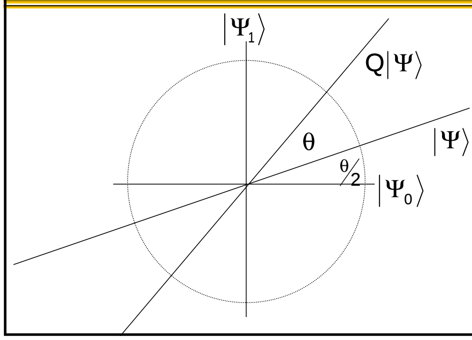
$$AU_{\bar{0}}A^{-1}A|x\rangle = -A|x\rangle, x \neq 0$$

- Thus $AU_{\bar{0}}A^{-1}|\Psi\rangle = |\Psi\rangle$

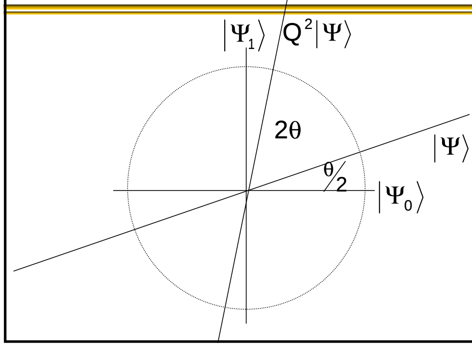
$$AU_{\bar{0}}A^{-1}|\overline{\Psi}\rangle = -|\overline{\Psi}\rangle$$

$$|\overline{\Psi}\rangle = \cos\left(\frac{\theta}{2}\right)|\Psi_1\rangle - \sin\left(\frac{\theta}{2}\right)|\Psi_0\rangle$$

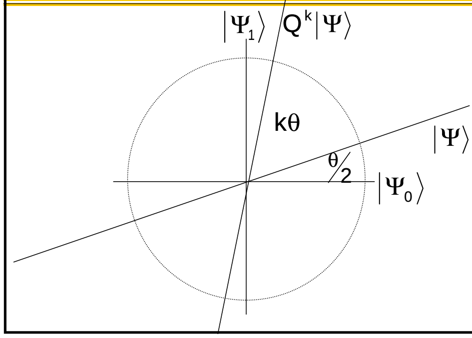
$AU_{\bar{0}}A^{-1}O_f|\Psi\rangle = \sin\left(\frac{3\theta}{2}\right)|\Psi_1\rangle + \cos\left(\frac{3\theta}{2}\right)|\Psi_0\rangle$



$Q^2|\Psi\rangle = \sin\left(\frac{5\theta}{2}\right)|\Psi_1\rangle + \cos\left(\frac{5\theta}{2}\right)|\Psi_0\rangle$



$$Q^k|\Psi\rangle = \sin\left(\frac{(2k+1)\theta}{2}\right)|\Psi_1\rangle + \cos\left(\frac{(2k+1)\theta}{2}\right)|\Psi_0\rangle$$



Searching Algorithm

- Choose k so that $\sin\left(\frac{(2k+1)\theta}{2}\right)^2 \approx 1$
- Note that $|\alpha| = \left|\sin\left(\frac{\theta}{2}\right)\right| \approx \frac{\theta}{2}$
- So we want $\frac{(2k+1)\theta}{2} \approx \frac{\pi}{2}$

$$k \approx \frac{\pi}{2\theta} - \frac{1}{2} \approx \frac{\pi}{4|\alpha|} \in O\left(\frac{1}{|\alpha|}\right)$$

Searching Algorithm

- Note that a classical algorithm would have to evaluate f a number of times in $\Theta\left(\frac{1}{|\alpha|^2}\right)$
- We therefore get a "square-root" speed-up.
- E.g. if A simply prepares a uniform superposition of all strings, then $\left|\sin\left(\frac{\theta}{2}\right)\right| = \sqrt{\frac{t}{N}}$
- We can find a solution with $\Theta\left(\sqrt{\frac{N}{t}}\right)$ quantum applications vs $\Theta\left(\frac{N}{t}\right)$ classical applications

Recap

- Given operator

$$A|0\rangle = |\Psi\rangle = \sin\left(\frac{\theta}{2}\right)|\Psi_1\rangle + \cos\left(\frac{\theta}{2}\right)|\Psi_0\rangle$$

$$|\Psi_1\rangle = \sum_{x \in X_1} \alpha_x |x\rangle \quad |\Psi_0\rangle = \sum_{y \in X_0} \alpha_y |y\rangle \quad \sum_{x \in X_1} |\alpha_x|^2 = 1 \quad \sum_{y \in X_0} |\alpha_y|^2 = 1$$

- Define

$$Q = AU_{\bar{0}}A^{-1}O_f$$

$$O_f : |x\rangle \rightarrow (-1)^{f(x)}|x\rangle$$

$$U_{\bar{0}} : |x\rangle \rightarrow -|x\rangle, x \neq 0$$

$$|0\rangle \rightarrow |0\rangle$$

Using Q

$$Q^k|\Psi\rangle = \sin\left(\frac{(2k+1)\theta}{2}\right)|\Psi_1\rangle + \cos\left(\frac{(2k+1)\theta}{2}\right)|\Psi_0\rangle$$

- Choose k so that $\sin\left(\frac{(2k+1)\theta}{2}\right)^2 \approx 1$
- I.e. $k \in O\left(\frac{1}{|\alpha|}\right)$
- What if we don't know θ ?

Amplitude Estimation Problem

- Given operator

$$A|0\rangle = |\Psi\rangle = \sin\left(\frac{\theta}{2}\right)|\Psi_1\rangle + \cos\left(\frac{\theta}{2}\right)|\Psi_0\rangle$$

- Estimate $\sin^2\left(\frac{\theta}{2}\right)$

Application: Counting

- E.g. $$A|0\rangle = \sum_{x\in\{0,1\}^n} \frac{1}{\sqrt{2^n}}|x\rangle$$

$$|\Psi_1\rangle = \sum_{x\in X_1} \frac{1}{\sqrt{t}}|x\rangle \qquad |\Psi_0\rangle = \sum_{y\in X_0} \frac{1}{\sqrt{N-t}}|y\rangle$$

- So $$A|0\rangle = \sqrt{\frac{t}{N}}|\Psi_1\rangle + \sqrt{\frac{N-t}{N}}|\Psi_0\rangle$$
- So $$\sin\left(\frac{\theta}{2}\right) = \sqrt{\frac{t}{N}}$$

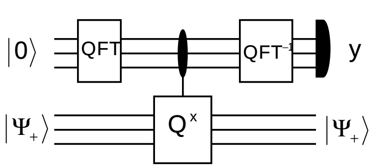
Eigenvectors of Q

$$|\Psi_+\rangle = \frac{1}{\sqrt{2}}|\Psi_1\rangle + \frac{i}{\sqrt{2}}|\Psi_0\rangle$$

$$|\Psi_-\rangle = \frac{1}{\sqrt{2}}|\Psi_1\rangle - \frac{i}{\sqrt{2}}|\Psi_0\rangle$$

$$Q|\Psi_+\rangle = e^{i\theta}|\Psi_+\rangle \qquad Q|\Psi_-\rangle = e^{-i\theta}|\Psi_-\rangle$$

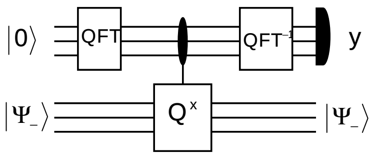
Amplitude Estimation ≈ Eigenvalue Estimation



$$\frac{y}{N} \approx \theta$$

$$\sin^2\left(\frac{y}{2N}\right) \approx \sin^2\left(\frac{\theta}{2}\right)$$

Amplitude Estimation ≈ Eigenvalue Estimation

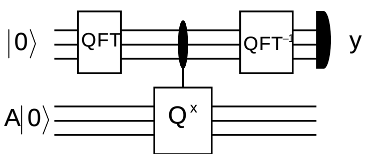


$$\frac{y}{N} \approx 2\pi - \theta$$

$$\sin^2\left(\frac{y}{2N}\right) \approx \sin^2\left(\frac{\theta}{2}\right)$$

Amplitude Estimation ≈ Eigenvalue Estimation

$$A|0\rangle = \frac{-i}{\sqrt{2}} e^{i\theta} |\Psi_+\rangle + \frac{i}{\sqrt{2}} e^{-i\theta} |\Psi_-\rangle$$



$$\sin^2\left(\frac{y}{2N}\right) \approx \sin^2\left(\frac{\theta}{2}\right)$$

- To search, we need to pick k so that

$$\sin\left(\frac{(2k+1)\theta}{2}\right)^2 \approx 1$$

- Amplitude estimation can help us estimate θ and pick a good k (analysis is not so easy)

How can this help us search?

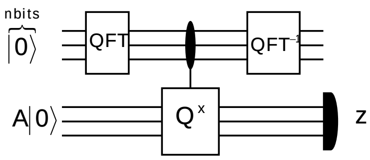
- Alternatively, note that the amplitude estimation network produces states

$$\frac{-i}{\sqrt{2}} e^{i\theta}|\widetilde{\theta}\rangle|\Psi_+\rangle + \frac{i}{\sqrt{2}} e^{-i\theta}|\widetilde{2\pi-\theta}\rangle|\Psi_-\rangle$$

- As the eigenvalue estimates become more orthogonal, the second register becomes closer and closer to an equal mixture of

$$\frac{1}{2}|\Psi_+\rangle\langle\Psi_+| + \frac{1}{2}|\Psi_-\rangle\langle\Psi_-| = \frac{1}{2}|\Psi_1\rangle\langle\Psi_1| + \frac{1}{2}|\Psi_0\rangle\langle\Psi_0|$$

≈



$$\text{Prob}(f(z)=1) \in \frac{1}{2} - O\left(\frac{1}{2^n\theta}\right)$$

$$\text{Prob}(f(z)=1) \underset{n\to\infty}{\to} \frac{1}{2}$$

- So for each n=1,2,3,4,..., we try twice to find a satisfying x
- This means that once $2^n > \frac{1}{\theta}$ we will find a satisfying x with probability in

$$\frac{3}{4} - O\left(\frac{1}{2^n\theta}\right)$$

- This means the expected running time is in

$$O\left(\frac{1}{\theta}\right)$$