Lecture 15 CPSC 447/547 - Intro to QC

Grover's Search Algorithm

Outline

- Unstructured search problem
- Reflection Operators.

So far in lectures, we've been using quantum algorithms that follow the same recipe:

1. Uniform superposition
2. Query an oracle in superposition
3. Directly measure or transform-then-measure.

- Can we use a quantum oracle differently?
- What more tasks can we do if we use oracle repeatly?

To answer those questions, we need to understand the role of an oracle better.

Phase Oracle (revisited)

$$O_f^{\pm}|x\rangle = (-1)^{f(x)}|x\rangle$$

$$O_f^{\pm}\left(\sum_x \alpha_x |x\rangle\right) = \sum_x \alpha_x (-1)^{f(x)}|x\rangle$$

Observation: "Negate α_x to $-\alpha_x$ if $f(x)=1$".

What if: $f(x)=1$ very rare.

E.g. $f(x) = \begin{cases} 1 & \text{if } x = z, \text{ for some } z \in \{0,1\}^n. \\ 0, & \text{otherwise.} \end{cases}$

"There exists a single input, s.t. f evaluates to 1".

What is $O_f^{\pm}$ in this case?

$$O_f^{\pm}|x\rangle = \begin{cases} -|x\rangle & \text{if } |x\rangle = |z\rangle \\ |x\rangle & \text{otherwise} \end{cases}$$

We have seen this type of transformation: "Reflection!"

$$R_z^{\pm} = I - 2\Pi_z \quad , \text{where } \Pi_z = |z\rangle\langle z|$$

reflection

projector on to $|z\rangle$ hyperplane.

$$\Rightarrow (I - 2\Pi_z)|z\rangle = |z\rangle - 2|z\rangle\cancel{\langle z|z\rangle}^{1} = -|z\rangle$$

and $(I - 2\Pi_z)|x\rangle = |x\rangle - 2|z\rangle\cancel{\langle z|x\rangle}^{0}$ for $|x\rangle \perp |z\rangle$

$$= |x\rangle$$

$$\Rightarrow \quad O_f^{\pm} = R_z^{\pm} = \text{"Reflection through (hyperplane of) } |z\rangle\text{"}.$$

<u>Example</u> "Reflection through $|0^n\rangle$".

$$R_0^{\pm}|x\rangle = \begin{cases} -|x\rangle & \text{if } |x\rangle = |0^n\rangle \\ |x\rangle & \text{otherwise.} \end{cases}$$

$$|\psi\rangle = \sum_x \alpha_x |x\rangle \xrightarrow{R_0^{\pm}} |\phi\rangle = -\alpha_0|0^n\rangle + \sum_{x\neq 0^n} \alpha_x |x\rangle.$$

Unitary matrix for $R_0^{\pm}$:

$$R_0^{\pm} = I - 2\Pi_0 = I - 2|0^n\rangle\langle 0^n|.$$

Can we implement $R_0^{\pm}$ with quantum circuit?

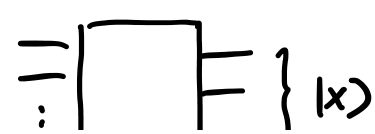
Circuit Implementation of Reflections.

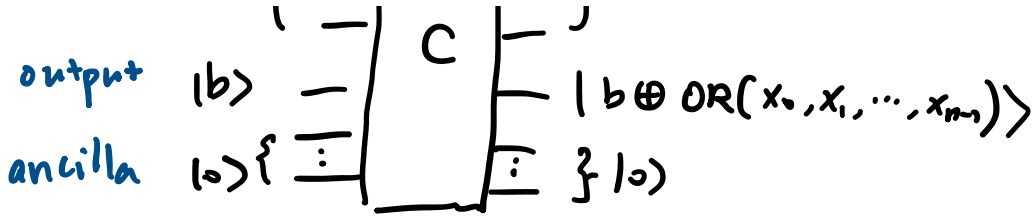
① <u>Example</u> $R_0^{\pm}$: Negate $|x\rangle$ if and only if $x = 0^n$

i.e., $\text{NOT}(\text{OR}(x_0, x_1, \cdots, x_{n-1}))$

Using the Boolean circuit for OR function?

- OR function can be implemented by $O(n)$ Toffoli gates.
- Make it reversible.

Input $|x\rangle$  $|x\rangle$



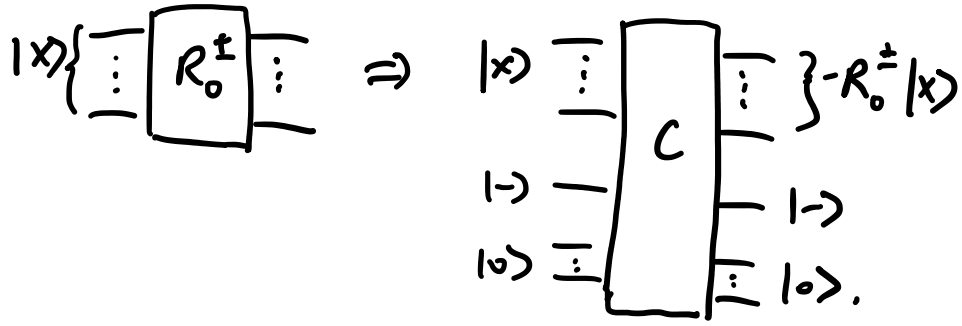
- Build $R_0^{\pm}$: $|x\rangle \longrightarrow (-1)^{OR(x_0, \cdots x_{n-1})}|x\rangle$.

Let $|b\rangle = |-\rangle$, then

$$|x\rangle|b\rangle|0\rangle = |x\rangle|-\rangle|0\rangle \xrightarrow{C} (-1)^{OR(x_0 \cdots x_{n-1})}|x\rangle|-\rangle|0\rangle \quad ☺$$

$$= -R_0^{\pm}|x\rangle|-\rangle|0\rangle$$

So

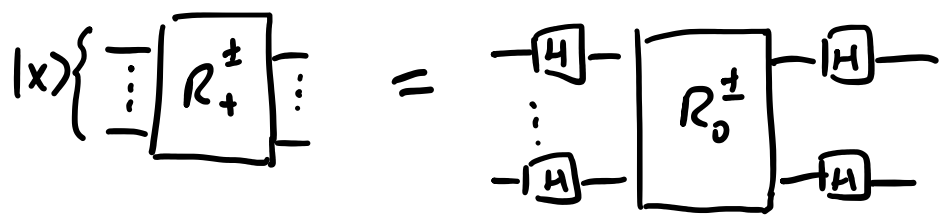


② <u>One more example</u>: Reflection through $|+^n\rangle$.

$$R_+^{\pm}|x\rangle = \begin{cases} -|x\rangle & \text{if } |x\rangle = |+^n\rangle \\ |x\rangle & \text{otherwise.} \end{cases}$$

Unitary Matrix : $R_+^{\pm} = I - 2|+^n\rangle\langle+^n|$

Circuit Implementation (using $R_0^{\pm}$)



1. Change $|+^n\rangle$ to $|0^n\rangle$

1. Change $|+\rangle$ to $|0\rangle$,
2. Reflect through $|0^n\rangle$.
3. Change back.

Use Reflections for (unstructured) search (Grover)

Prob. Given an oracle access to function

$$f: \{0,1\}^n \to \{0,1\},$$

$$f(x) = \begin{cases} 1 & \text{if } x = z \text{ for some } z \in \{0,1\}^n \\ 0 & \text{otherwise} \end{cases}$$

Want to find z.

"Search for x s.t. $f(x) = 1$".

Quantum Strategy:

Design a quantum state $|\psi\rangle$ s.t.

when we measure, we obtain $|z\rangle$ with high prob.

Initial: $|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle$ "uniform superposition"
(like a uniform random guess)

$\downarrow$ Some quantum circuit

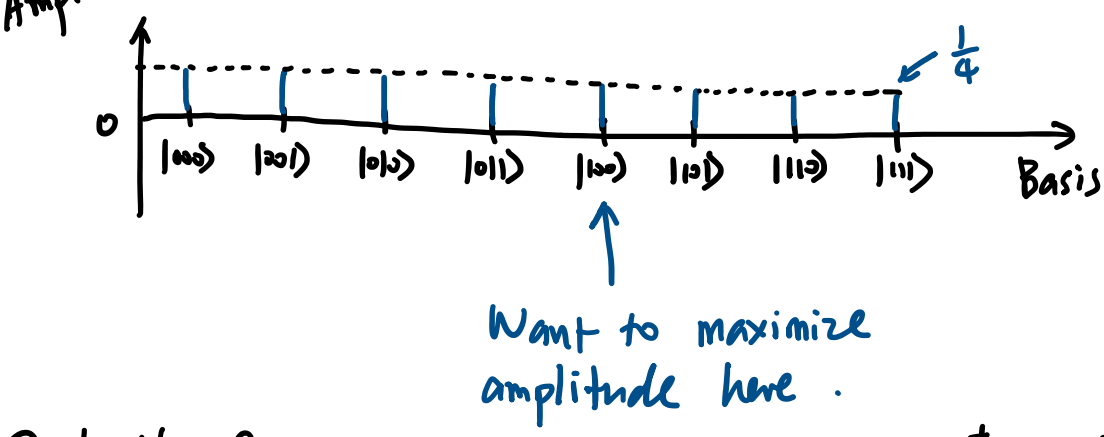
Final: $|\psi\rangle \approx |z\rangle$ "as close to correct answer z as possible".

Let's see how we can <u>amplify the amplitude</u> on $|z\rangle$.

<u>Example</u>: $n=3$. $f(x)=1$ if $x=100$, and $f(x)=0$ otherwise.

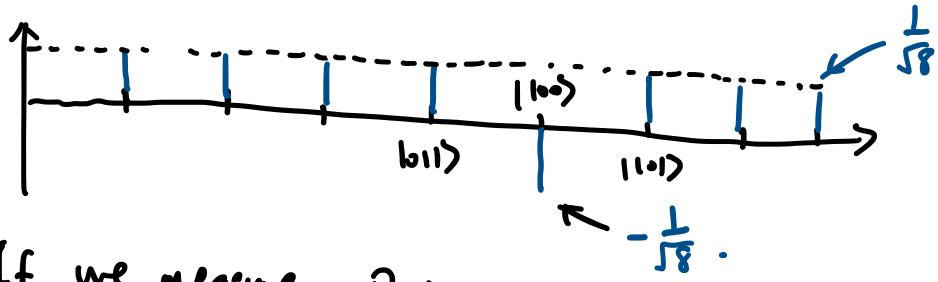
We start with $|\psi\rangle = \frac{1}{\sqrt{8}}\sum_x |x\rangle = \frac{1}{\sqrt{8}}\big(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle\big)$.

Amplitude of $|\psi\rangle$



① Let's first try the phase oracle. $O_f^{\pm} = R_{100}^{\pm}$

Amplitude of $O_f^{\pm}|\psi\rangle$



If we measure, $\text{Prob}(|100\rangle) = \left(-\frac{1}{\sqrt{8}}\right)^2 = \frac{1}{8}$. ☹.

But at least we've "singled out" $|100\rangle$ after $O_f^{\pm}$.

② Keep going: Next try $R_+^{\pm} = I - 2|+^n\rangle\langle +^n|$

what's $(-R_+^{\pm})O_f^{\pm}|\psi\rangle$? (Actually, need $-R_+^{\pm}$)

$$R_+^{\pm} O_f^{\pm}|\psi\rangle = \left(2\underbrace{|+^3\rangle\langle +^3|}_{} - I\right)\Big(\underbrace{\tfrac{1}{4}\sum_{x\neq 100}|x\rangle - \tfrac{1}{4}|100\rangle}_{}\Big)$$

$$\langle +^n | \left(\underbrace{\sum_x \alpha_x |x\rangle} \right) = \left(\frac{1}{\sqrt{2^n}} \sum_y \langle y| \right) \left(\sum_x \alpha_x |x\rangle \right)$$

$$= \frac{1}{\sqrt{2^n}} \sum_y \sum_x \alpha_x \underbrace{\langle y|x\rangle}_{\delta_{xy}}$$

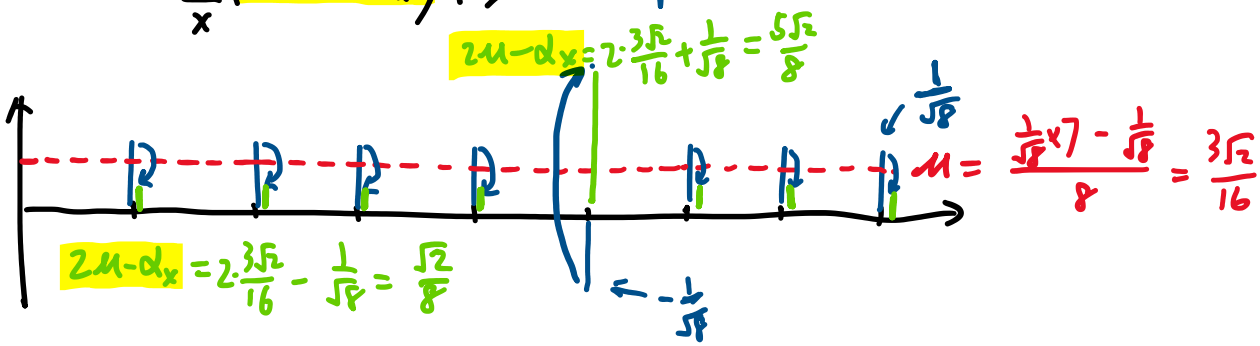
$$= \frac{\sum_x \alpha_x}{\sqrt{2^n}} = \sqrt{2^n} \cdot \mu \,, \quad \mu = \frac{\sum_x \alpha_x}{2^n} .$$

Mean of amplitudes

So, $(-R_+^{\pm}) \left(\sum_x \alpha_x |x\rangle \right)$

$$= 2 \cdot \sqrt{2^n} \mu |+^n\rangle - \sum_x \alpha_x |x\rangle$$

$$= \sum_x (2\mu - \alpha_x) |x\rangle$$ "Flip around mean"!



Before: $\frac{1}{\sqrt{8}}|000\rangle + \frac{1}{\sqrt{8}}|001\rangle + \frac{1}{\sqrt{8}}|010\rangle + \frac{1}{\sqrt{8}}|011\rangle - \frac{1}{\sqrt{8}}|100\rangle + \frac{1}{\sqrt{8}}|101\rangle + \cdots + \frac{1}{\sqrt{8}}|111\rangle$.

After: $\frac{\sqrt{2}}{8}|000\rangle + \frac{\sqrt{2}}{8}|001\rangle + \frac{\sqrt{2}}{8}|010\rangle + \frac{\sqrt{2}}{8}|011\rangle + \frac{5\sqrt{2}}{8}|100\rangle + \frac{\sqrt{2}}{8}|101\rangle + \cdots + \frac{\sqrt{2}}{8}|111\rangle$.

This is better! Amp on $|100\rangle$ is amplified. ☺

Next lecture: Can we amplify more?

What if we keep going: $(-R_+^{\pm}) O_f^{\pm}$?

How many iterations until the prob of obtaining $|100\rangle$ is high enough?

If overhead fuel is high enough: