Lecture 11 CPSC 447/547 - Intro to QC

Quantum Algorithms

Outline

- Deutsch-Jozsa, Bernstein-Vazirani
- Fourier Sampling.

Recall from last lecture,

Oracle: $-\boxed{O_f^{\pm}}-$: $|x\rangle \xrightarrow{O_f^{\pm}} (-1)^{f(x)}|x\rangle$.

We mentioned last time that the power of quantum oracles stems from superposition access to f

Let's create a superposition input:

(E.g. 1 qubit)

$$|0\rangle - \boxed{H} - \boxed{O_f^{\pm}} -$$

Before $O_f^{\pm}$:

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

After $O_f^{\pm}$:

$$\frac{1}{\sqrt{2}}(-1)^{f(0)}|0\rangle + \frac{1}{\sqrt{2}}(-1)^{f(1)}|1\rangle.$$

$$= \frac{1}{\sqrt{2}}(-1)^{f(0)}\left[|0\rangle + (-1)^{f(1)-f(0)}|1\rangle\right]$$

Now consider the following scenarios: $\boxed{f: \{0,1\} \to \{0,1\}}$

(1) If $f(0) = f(1)$

① If $f(0) = f(1)$:

$$\frac{1}{\sqrt{2}}(-1)^{f(0)}\left[|0\rangle + (-1)^{0}|1\rangle\right] = \cancel{(-1)^{f(0)}}|+\rangle$$

② If $f(0) \neq f(1)$:

$$\frac{1}{\sqrt{2}}(-1)^{f(0)}\left[|0\rangle + (-1)^{\pm 1}|1\rangle\right] = \cancel{(-1)^{f(0)}}|-\rangle$$

Recall from HW, we can distinguish $|+\rangle$ and $|-\rangle$:

$$\left(-\boxed{H}-\boxed{\mathcal{M}} \right)$$

$$|0\rangle - \boxed{H} - \boxed{O_f^{\pm}} - \boxed{H} - \boxed{\mathcal{M}},$$

<u>Remark</u>: • We can use $O_f^{\pm}$ (once) to tell if $f(0) = f(1)$ or $f(0) \neq f(1)$.

• Classically (if we did not have superposition access to f), we need at least 2 queries to f.

Even better if we use more qubits!

Deutsch-Jozsa

<u>Prob</u> Given an oracle $O_f^{\pm}$ to a function

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

and we're promised that:

$$\begin{cases} \text{Either } f(x) = 0 \text{ for all } x. & \text{"constant"} \\ \text{Or half of inputs } x \text{ give } f(x) = 0 \end{cases}$$

the other half give $f(x)=1$. } balanced.

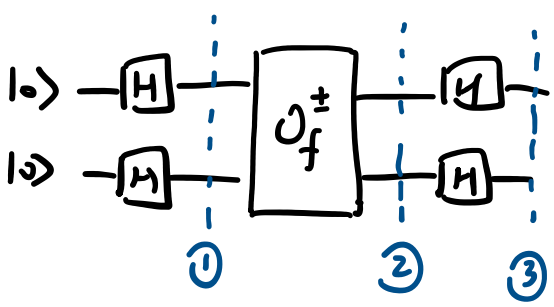
Try to decide which case.

Example. $n=2$. Truth table for f:

input		constant $f(x)=0$	balanced $f = \text{XOR}$
0	0	0	0
0	1	0	1
1	0	0	1
1	1	0	0

Create uniform superposition: $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$

How to prepare?



① : $(H \otimes H)|00\rangle = |+\rangle \otimes |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

$= \frac{1}{2}|00\rangle + |01\rangle + |10\rangle + |11\rangle$.

"Hadamard each qubit" gives uniform superposition

↳ we'll come back to this later.

② Suppose f is XOR, what's the state?

$$\frac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle)$$

Suppose $f(x)=0$, then

$$\frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right)$$

③ Suppose f is XOR. state after $H \otimes H$?

$$\frac{1}{2}\left(|++\rangle - |+-\rangle - |-+\rangle + |--\rangle\right) \leftarrow \text{What's this?}$$

$$= |11\rangle$$

"Interference" — cancellation of amplitudes.

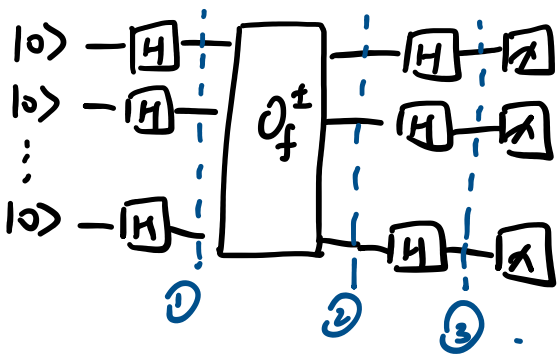
Suppose $f(x) = 0$, then state is

$$\frac{1}{2}\left(|++\rangle + |+-\rangle + |-+\rangle + |--\rangle\right)$$

$$= |00\rangle$$

We can distinguish which case by measurements $-\boxed{\measuredangle}$.

More generally.



① $|+\rangle \otimes |+\rangle \otimes \cdots \otimes |+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \cdots \otimes \frac{|0\rangle+|1\rangle}{\sqrt{2}}$

$$= \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \quad \text{"uniform superposition".}$$

② After $O_f^{\pm}$:

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle = \begin{cases} \text{if } f(x)=0 \text{ "constant"} \\ \quad \frac{1}{\sqrt{2^n}} \sum_x |x\rangle \\ \text{if } f \text{ "balanced"} \end{cases}$$

③ After $H^{\otimes n}$: $\left(\frac{1}{\sqrt{2^n}} \left(\sum_{x: f(x)=0} |x\rangle - \sum_{y: f(y)=1} |y\rangle \right) \right)$

$$\begin{cases} \text{If } f(x)=0 \text{ "constant"}: & |0\rangle^{\otimes n} \\ \text{if } f \text{ "balanced"}: & \text{What is this? (Seem like a mess)} \end{cases}$$

Amplitude on $|0\rangle^{\otimes n}$?

$|x\rangle = |0|10\rangle$

$H^{\otimes n}|x\rangle = |+--+\rangle$

Amp on $|0000\rangle = \left(\frac{1}{\sqrt{2}}\right)^4$

$$\frac{1}{\sqrt{2^n}} \left(\sum_x \left(\frac{1}{\sqrt{2}}\right)^n - \sum_y \left(\frac{1}{\sqrt{2}}\right)^n \right) = 0$$

equal b/c balanced!

$\Downarrow$

For any $|x\rangle$, amp on $|0\rangle^{\otimes n} = \left(\frac{1}{\sqrt{2}}\right)^n$.

Measure: prob of getting $|0\rangle^{\otimes n} = \begin{cases} 1 & \text{if constant.} \\ 0 & \text{if balanced.} \end{cases}$

So, we can decide "constant"/"balanced" with 1 query!

Can we do more? Let's understand $H^{\otimes n}$ better.

Boolean Fourier Transform $(H^{\otimes n})$

We saw: $H^{\otimes n}\left(\sum_x \alpha_x |x\rangle\right) = \sum_x \alpha_x \underbrace{H^{\otimes n}|x\rangle}$

Example: $n=3$, $|x\rangle = |010\rangle$

$$H^{\otimes 3}|010\rangle = |+-+\rangle = \frac{1}{\sqrt{2^3}} (|0\rangle+|1\rangle) \otimes (|0\rangle-|1\rangle) \otimes (|0\rangle+|1\rangle)$$

$$= \frac{1}{\sqrt{2^3}} \left(|000\rangle + |001\rangle - |010\rangle - |011\rangle + |100\rangle + |101\rangle - |110\rangle - |111\rangle \right)$$

$$= \frac{1}{\sqrt{2^n}} \sum_y \text{sign-of-}y \, |y\rangle .$$ What's sign of y here?

What's the pattern?

Sign of y = Product of signs for $i = 1, 2, \cdots, n$.

$$\begin{cases} y_i = 0 : & +1 \text{ always.} \\ y_i = 1 : & (-1)^{x_i} \end{cases}$$

$$\Rightarrow \text{sign for } |y\rangle = \prod_{i : y_i = 1} (-1)^{x_i} = (-1)^{\sum_i x_i \cdot y_i \pmod 2}$$

$$\Rightarrow \quad H^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_y (-1)^{\sum_i x_i y_i \bmod 2} |y\rangle .$$

$$\Rightarrow \quad H^{\otimes n} \left(\frac{1}{\sqrt{2^n}} \sum_y (-1)^{\sum_i x_i y_i \bmod 2} |y\rangle \right) = |x\rangle .$$

<u>Remark</u>: $H^{\otimes n}$ can extract x from $\sum_i x_i y_i \bmod 2$.

In other words, we can hide x in function

$$\frac{1}{\sqrt{2^n}} \sum_y (-1)^{f(y)} |y\rangle = \frac{1}{\sqrt{2^n}} \sum_y (-1)^{\sum_i x_i y_i \bmod 2} |y\rangle .$$

Then use $H^{\otimes n}$ to reveal x by $O_f^{\pm}$ and $H^{\otimes n}$.

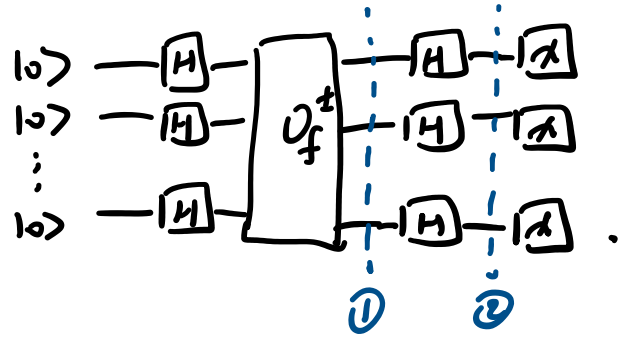
<u>Bernstein-Vazirani</u>

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

where $f(v) = x \cdot v \equiv \sum x_i y_i \bmod 2$

for some secret string $x \in \{0,1\}^n$.

Want to find x.



① : $\frac{1}{\sqrt{2^n}} \sum_y (-1)^{f(y)} |y\rangle = \frac{1}{\sqrt{2^n}} \sum_y (-1)^{\sum x_i y_i \bmod 2} |y\rangle$

② : $|x\rangle \leftarrow$ Cool!

$\Rightarrow$ Measurement outcome is exactly x!