Lecture 17

Tuesday, October 22, 2024 8:56 AM

Recall

- $f: \{0,1\}^n \longrightarrow \{0,1\}$ where f is assumed to be either constant or balanced

Ex $n=2$

x	$f(x)$	or
00	0	1
01	0	1
10	0	1
11	0	1

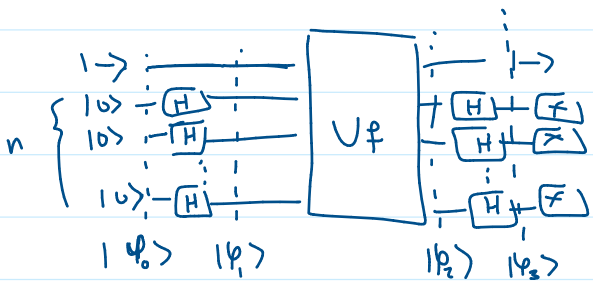
constant

x	$f(x)$					
00	0	1	1	0	0	1
01	0	1	0	1	1	0
10	1	0	1	0	1	0
11	1	0	0	1	0	1

balanced

- We need $2^{n-1}+1$ classically
- In quantum, we need 1 evaluation

Deutsch-Jozsa Algorithm



$$|\varphi_3\rangle = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} \sum_{z\in\{0,1\}^n} (-1)^{f(x)+x.z} |z\rangle$$

Recall in D

$$|\varphi_3\rangle = \begin{cases} (-1)^{b_0} |0\rangle & b_0 = b_1 \\ (-1)^{b_0} |1\rangle & b_0 \neq b_1 \end{cases}$$

Let assume that we measure $|x\rangle = |0..0\rangle$

The amplitude would be

$f(x)$ is constant

$f(x)\ x.z = x_{n-1}.z_{n-1} + x_{n} \dots + x_0 z_0$

$$\frac{1}{2^n} \sum_{z\in\{0,1\}^n} (-1)^{f(x)+0} = \frac{1}{2^n} \sum_{z\in\{0,1\}^n} (-1)^{f(x)} = \frac{1}{\cancel{2^n}} \cancel{2^n} (-1)^{f(x)} = (-1)^{f(x)} \text{ if const}$$

$f(x)=0$: 1 $\quad$ $f(x)=1$: -1

- If $f(x)$ is constant, we will measure $|00\dots0\rangle$ with 1 prob
-

$$|\varphi_3\rangle = \frac{1}{2^n} \sum_{z\in\{0,1\}^n} (-1)^{f(x)} = \frac{1}{2^n} \cdot 0 = 0$$

- When f is balanced, prob. of measuring $|00\dots0\rangle$ is 0

Secret dot product string

- Let $f: \{0,1\}^n \longrightarrow \{0,1\}$

$f(x) = x \dots$

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

$f(x) = x \cdot s$ where s is a secret string

$= x_{n-1}s_{n-1} + \dots + x_1 s_1 + x_0 s_0$

<u>Ex</u> What is S?

$S = 101$

x	$f(x)$
000	0
001	1
010	0
011	1
100	1
101	0
110	1
111	0

$S = ?$ fudel = 110

x	$f(x)$
000	0
001	0
010	1
011	1
100	1
101	1
110	0
111	0

$\to$ 3rd 0

$\to$ 2nd 1

$\to$ first bit 1

Let s be n-bit, how many f evaluations?

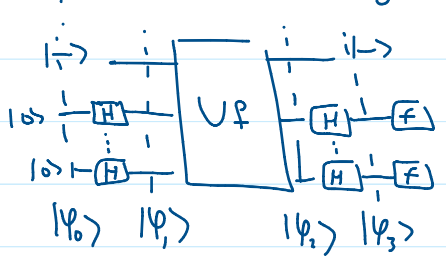
<u>Ex</u> $n=3$, I test

001
010
100

I need n evaluation classically

- In Quantum, we need 1 evaluation

BV
Bernstein-Vazirani Algorithm



$$|\varphi_3\rangle = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} \sum_{z\in\{0,1\}^n} (-1)^{f(x)+x.z} |z\rangle = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} \sum_{z\in\{0,1\}^n} (-1)^{x.s+x.z} |z\rangle$$

$$= \frac{1}{2^n} \sum_{x\in\{0,1\}^n} \sum_{z\in\{0,1\}^n} (-1)^{x(s+z)} |z\rangle$$

Let's assume the output is $|z\rangle = |s\rangle$

$$\frac{1}{2^n} \sum_x (-1)^{x(z+s)} |s\rangle \qquad \text{but } z+s = s+s$$

$$= \frac{1}{2^n} \sum_x (-1)^{x.0} |s\rangle = \frac{1}{2^n} \sum (-1)^0 |s\rangle$$

$$= \frac{1}{2^n} (2^n) |s\rangle = 1 |s\rangle$$

001
001
000

011
011
000

$$= \frac{1}{2^n} \sum_x (-1) |s\rangle = \frac{1}{2^n} \sum_x (-1) \quad |s\rangle$$

$$= \frac{1}{2^n} (2^n) |s\rangle = 1 |s\rangle$$

- We will measure $|s\rangle$ with 1 prob.

Secret XOR

Let $f: \{0,1\}^n \to \{0,1\}^n$, and we are promised that

$f(x) = f(y)$ $\qquad$ $f(\overset{x}{001}) = f(\overset{y}{010})$

iff $x = s \oplus y$ $(y = s \oplus x) \longrightarrow s = x \oplus y$

Ex $\quad n = 3$

$\quad s = 110$

x x	y $x \oplus s$
000	110
001	111
010	100
011	010
100	010
101	011
110	000
111	001

x	$f(x)$
000	110
001	000
010	111
011	001
100	111
101	001
110	110
111	000

$x = \overset{000}{\cancel{011}}, \; y = \overset{110}{\cancel{100}}$

$s = \cancel{011 \oplus 100} = 111$

$000 \oplus 110 = 110$

What is s?