Lecture 18

Thursday, October 24, 2024 9:00 AM

Secret XOR

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

$f(x) = f(y)$ $\quad f(\overset{x}{0}01) = f(\overset{y}{010})$

iff $x = s \oplus y$ $(y = s \oplus x) \longrightarrow s = x \oplus y$ & $s \neq 0$

Ex $n = 3$

$s = 110$

x	y = x⊕s
000	110
001	111
010	100
011	101
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

$x = 000$, $y = 110$

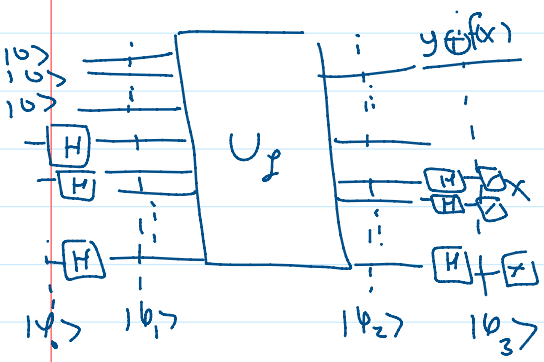
$s = 000 \oplus 110 = 110$

$s = 011 \oplus 100 = 111$

What is s?

- Classically, we need $2^{n-1}+1$ (worst case) ~~$n+2$~~
- In Quantum? (n)

Simon's Algorithm



$|\psi_0\rangle = |00\ldots0\rangle|00\ldots0\rangle$

$|\psi_1\rangle = |++\ldots+\rangle|00\ldots0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle\,|00\ldots0\rangle$

$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle\,|f(x)\rangle$

$|\psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} H^{\otimes n}|x\rangle\,|f(x)\rangle$

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

$H|x\rangle = \begin{cases} H|0\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ H|1\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{cases}$

$\frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^x |1\rangle\right)$

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

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

Let the output be $|\hat{f}\rangle = |100\ldots01\rangle$

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

We know that $\hat{f} = f(\hat{x}) = f(\tilde{x})$ and $\hat{x} = \hat{x} \oplus s$

$$|\varphi_3\rangle = \frac{1}{\sqrt{2^n}} \frac{1}{\sqrt{2}} \left(\sum_{z \in \{0,1\}^n} \left[(-1)^{\hat{x} \cdot z} + (-1)^{\tilde{x} \cdot z} \right] |z\rangle \right) |\hat{f}\rangle$$

$$(-1)^{\hat{x} \cdot z} + (-1)^{\tilde{x} \cdot z} = \begin{cases} \pm 2 & \hat{x} \cdot z = \tilde{x} \cdot z \\ 0 & \hat{x} \cdot z \neq \tilde{x} \cdot z \end{cases}$$

To know $|z\rangle$

$$\hat{x} \cdot z = \tilde{x} \cdot z \bmod 2$$

$$\hat{x} \cdot z + \tilde{x} \cdot z = \tilde{x} \cdot z + \tilde{x} \cdot z \bmod 2$$

$$(\hat{x} + \tilde{x}) \cdot z = 0 \bmod 2$$

$$s \cdot z = 0 \bmod 2$$

If we run the algorithm, we will get $|z\rangle$ that we know $z \cdot s = 0 = z_{n-1} \cdot s_{n-1} + z_{n-2} s_{n-2} + \ldots + z_1 s_1 + z_0 s_0 = 0$

Ex Quantum — solver

$s = 110$

$z_1 = |001\rangle$ $\quad z_1 \cdot s = 0 \Rightarrow s_0 = 0$

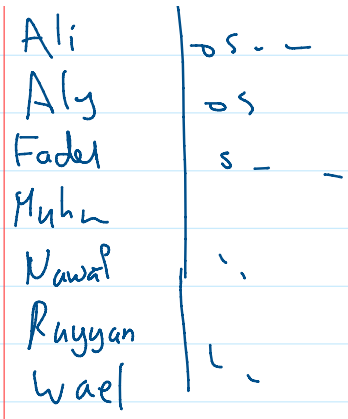
$z_2 = |110\rangle$ $\quad z_2 \cdot s = 0 \Rightarrow s_2 + s_1 = 0$ $\quad s_2 + s_1 = 0$ $\quad s_2 = s_1$

$z_3 = |111\rangle$ $\quad z_3 \cdot s =$ $\quad s_2 + s_1 + s_0 = 0$ $\quad s_2 + s_1 = 0$

Grover's algorithm

names	mobile
Abd	osb
Ali	os
Alm	

$2^n = |N|$ entries $O(2^n)$



$2^n = |V|$ entries $O(2^n)$

$O(\sqrt{2^n})$