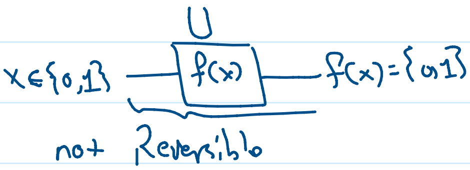
Lecture 14

Tuesday, October 15, 2024 9:17 AM

Quantum Oracles



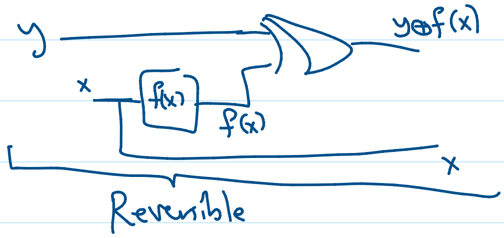
0	1
1	1

0	0
1	0

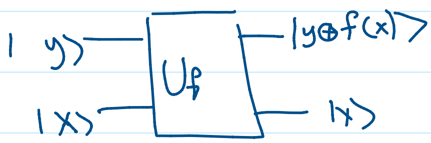
0	0
1	1

0	1
1	0

- But $f(x)$ is not necessarily reversible



$I \otimes U_f$



$|x\rangle|y\rangle \xrightarrow{U_f} |x\rangle|y \oplus f(x)\rangle$

Since we have two outputs $f(0)$ & $f(1)$

1. $|x\rangle|0\rangle \xrightarrow{U_f} |x\rangle|0 \oplus f(0)\rangle = |x\rangle|f(0)\rangle$
2. $|x\rangle|0\rangle \xrightarrow{U_f} |x\rangle|0 + f(1)\rangle = |x\rangle|f(1)\rangle$

Ex

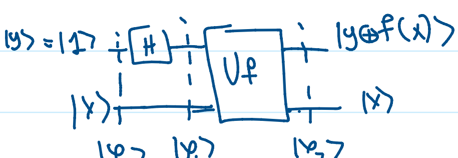
$f(0) = 1 = f(1)$

Then the oracle produce

$|0\rangle|0\rangle \xrightarrow{U_f} |0\rangle|1\rangle$ $\qquad U_f \begin{pmatrix}1\\0\\0\\0\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$ $\Rightarrow \begin{pmatrix}U_{11} & U_{12} & U_{13} & U_{14}\\ U_{21} & U_{22} & U_{23} & U_{24}\\ U_{31} & U_{32} & U_{33} & U_{34}\\ U_{41} & U_{42} & U_{43} & U_{44}\end{pmatrix}\begin{pmatrix}1\\0\\0\\0\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$ $\qquad U_{11}=0$, $U_{20}=1$, $U_{31}=0$, $U_{41}=0$

$|1\rangle|0\rangle \xrightarrow{U_f} |1\rangle|1\rangle$ $\qquad U_f \begin{pmatrix}0\\0\\1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$

Let's try the oracle but we set $|y\rangle \to |-\rangle$



$|\varphi_1\rangle$

$|\varphi_0\rangle$

$|x\rangle|y\rangle \xrightarrow{I \otimes X} |x\rangle|1\rangle \xrightarrow{I \otimes H} |x\rangle|-\rangle \to |x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$\to \frac{1}{\sqrt{2}}(|x\rangle|0\rangle - |x\rangle|1\rangle)$ $\qquad |\varphi_2\rangle$

$$\longrightarrow \frac{1}{\sqrt{2}}\left(|x\rangle|0\rangle - |x\rangle|1\rangle\right) \qquad |\psi_2\rangle$$

$$\xrightarrow{U_f} \frac{1}{\sqrt{2}}\left(|x\rangle|0\oplus f(x)\rangle - |x\rangle|1\oplus f(x)\rangle\right)$$

$$\longrightarrow \frac{1}{\sqrt{2}}\left(|x\rangle|f(x)\rangle - |x\rangle|\overline{f(x)}\rangle\right)$$

$$= \begin{cases} \frac{1}{\sqrt{2}}\left(|x\rangle|0\rangle - |x\rangle|1\rangle\right) & f(x)=0 \\ \frac{1}{\sqrt{2}}\left(|x\rangle|1\rangle - |x\rangle|0\rangle\right) & f(x)=1 \end{cases}$$

$$= \begin{cases} (+1)|x\rangle|-\rangle & f(x)=0 \\ (-1)|x\rangle|-\rangle & f(x)=1 \end{cases}$$

$$= \underbrace{(-1)^{f(x)}|x\rangle}|-\rangle \longrightarrow (-1)^{f(x)}|x\rangle|0\rangle$$

A trick called <u>Phase kickback</u>