Week 3 : Theory Solutions

Question 1

We know that the an oracle O_f acts as

$$O_f \left|x\right\rangle \left|b\right\rangle \longrightarrow \left|x\right\rangle \left|b\right\rangle$$

If $\left|b\right\rangle = \left|-\right\rangle$, then

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

Now, if $f(x) = 0$, then we have

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

Again if $f(x) = 1$, then we have

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

Now from 1 and 2, we get

$$\left|\psi\right\rangle = O_f \left|x\right\rangle \left|-\right\rangle = (-1)^{f(x)} \left|x\right\rangle \left|-\right\rangle.$$

Question 2

The quantum oracle circuit for the Boolean function $f(x) = (x_1 \cdot x_2) \oplus (x_3 \cdot x_4)$ can be given as in Figure 1

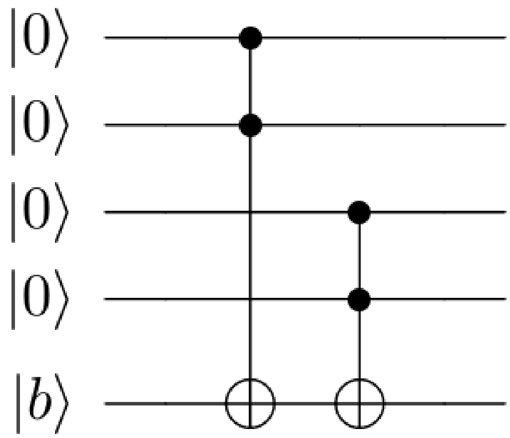

Figure 1

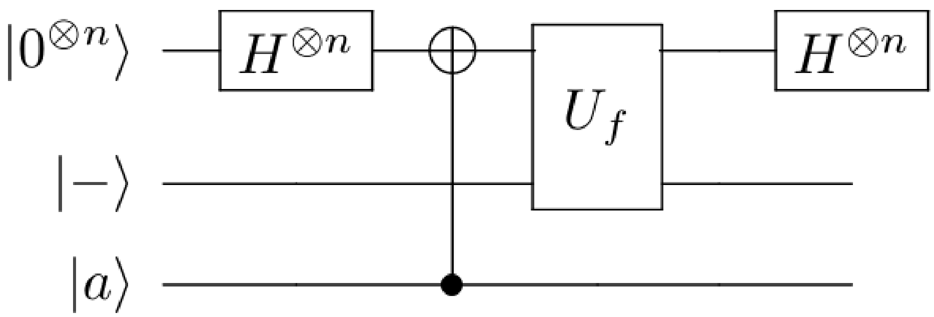

Figure 2

Question 3

The circuit that outputs $|y\rangle$ with probability $Pr(|y\rangle) = \left[\sum_x (-1)^{f(x \oplus a)} (-1)^{(x \oplus a) \cdot y}\right]^2$ on providing $|0^n\rangle$ and $|a\rangle$ as input and an oracle O_f can be given as in Figure 2

Quesiton 4

We are given that the initial state is $|\psi\rangle = sin(\theta)\,|0\rangle + cos(\theta)\,|1\rangle$. Now, we need to get to the final state $|\psi'\rangle = sin(\theta')\,|0\rangle + cos(\theta')\,|1\rangle$ where $sin^2(\theta)$ is very close to 1. That imples we need $\theta' \approx \frac{\pi}{2}$. Now, we know that in k iterations of amplitude amplification, θ becomes $(2k+1)\theta$. So, we need k such that

$$\begin{aligned}(2k+1)\theta &= \theta' \\ &\approx \frac{\pi}{2}\end{aligned}$$

$$\implies k = \left\lfloor \tfrac{\pi}{4\theta} - \tfrac{1}{2} \right\rfloor.$$

We take the floor because k has to be an integer.

Question 5

We have $|\psi\rangle = A|0\rangle = cos(\theta)|0\rangle + sin(\theta)|1\rangle$. In matrix form, we have

$$|\psi\rangle = \begin{bmatrix} cos(\theta) \\ sin(\theta) \end{bmatrix}$$

and so $S_0|\psi\rangle$ is

$$S_0|\psi\rangle = \begin{bmatrix} -cos(\theta) \\ sin(\theta) \end{bmatrix}.$$

Now, the operator $|\psi\rangle\langle\psi|$ can be written as a matrix as

$$|\psi\rangle\langle\psi| = \begin{bmatrix} cos(\theta) \\ sin(\theta) \end{bmatrix} \begin{bmatrix} cos(\theta) & sin(\theta) \end{bmatrix} = \begin{bmatrix} cos^2(\theta) & cos(\theta)sin(\theta) \\ sin(\theta)cos(\theta) & sin^2(\theta) \end{bmatrix}$$

So the operator $2(|\psi\rangle\langle\psi|) - I$ can be given as

$$2(|\psi\rangle\langle\psi|) - I = \begin{bmatrix} 2cos^2(\theta) - 1 & 2cos(\theta)sin(\theta) \\ 2sin(\theta)cos(\theta) & 2sin^2(\theta) - 1 \end{bmatrix} = \begin{bmatrix} cos(2\theta) & sin(2\theta) \\ sin(2\theta) & -cos(2\theta) \end{bmatrix}$$

Hence on applying the operator $-(2(|\psi\rangle\langle\psi|) - I)$ on $S_0|\psi\rangle$, we get,

$$\begin{aligned} |\psi'\rangle &= -(2(|\psi\rangle\langle\psi|) - I)S_0|\psi\rangle \\ &= \begin{bmatrix} cos(2\theta) & sin(2\theta) \\ sin(2\theta) & -cos(2\theta) \end{bmatrix} \begin{bmatrix} cos(\theta) \\ sin(\theta) \end{bmatrix} \\ &= \begin{bmatrix} cos(3\theta) \\ sin(3\theta) \end{bmatrix} \end{aligned}$$

Question 6

Given a function $f : \{0,1\}^n \longrightarrow \{0,1\}^k$, the necessary condition for Simon's algorithm to work is that $f(x) = f(y)$ if and only if $x = y \oplus s$ for some fixed shift s. Now, we can see that if there is a fixed shift s, two elements from the domain map to a single element in the range. Hence the range has to be at least half the size of the domain. Hence we need $k \geq n - 1$.