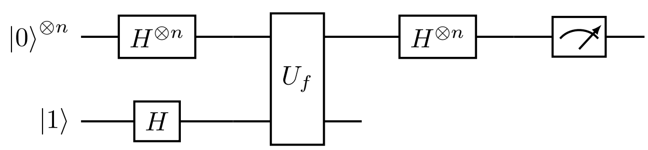
Quantum Computing - Assignment 2

Kishlaya Jaiswal

September 30, 2020

Exercise 1

Proof. .



where $f : \mathbb{Z}_2^n \to \mathbb{Z}_2,\ f(x) = \sum a_i x_i$

First we prepare the state:

$$|0\rangle^{\otimes n} \otimes |1\rangle$$

Applying $n+1$ Hadamard gates, we get:

$$\left(\frac{1}{2^{n/2}}\sum_x |x\rangle\right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \frac{1}{2^{n/2}}\frac{1}{\sqrt{2}}\sum_x |x\rangle|0\rangle - |x\rangle|1\rangle$$

Applying U_f, we get:

$$\frac{1}{2^{n/2}}\frac{1}{\sqrt{2}}\sum_x |x\rangle|f(x)\rangle - |x\rangle|\overline{f(x)}\rangle = \left(\frac{1}{2^{n/2}}\sum_x (-1)^{f(x)}|x\rangle\right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

Let us carefully examine the first n qubits at this point.
First, say $x = x_1 \dots x_n$, then

$$(-1)^{f(x)}|x\rangle = (-1)^{a_1x_1 + \cdots a_nx_n}|x_1 \dots x_n\rangle = \Big((-1)^{a_1x_1}|x_1\rangle\Big) \otimes \cdots \otimes \Big((-1)^{a_nx_n}|x_n\rangle\Big)$$

Thus, the first n qubits are:

$$\begin{aligned}\frac{1}{2^{n/2}}\sum_x (-1)^{f(x)}|x\rangle &= \left(\sum_{x_1}\frac{(-1)^{a_1x_1}|x_1\rangle}{\sqrt{2}}\right) \otimes \cdots \otimes \left(\sum_{x_n}\frac{(-1)^{a_nx_n}|x_n\rangle}{\sqrt{2}}\right) \\ &= \left(\frac{|0\rangle + (-1)^{a_1}|1\rangle}{\sqrt{2}}\right) \otimes \cdots \otimes \left(\frac{|0\rangle + (-1)^{a_n}|1\rangle}{\sqrt{2}}\right)\end{aligned}$$

Now we recall that

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

Thus applying n Hadamard gates to the first n qubits, we get:

$$|a_1 \dots a_n\rangle$$

$\square$

Exercise 2

Proof. First we prove by induction on n that for $x \in \{0,1\}^n$,

$$H^{\otimes n}|x\rangle = \frac{1}{2^{n/2}} \sum_{z\in\{0,1\}^n} (-1)^{x.z}|z\rangle$$

For $n = 1$, it follows immediately as

$$H|x\rangle = \frac{1}{\sqrt{2}}\sum_z (-1)^{x.z}|z\rangle = \frac{|0\rangle + (-1)^x|1\rangle}{\sqrt{2}}$$

Suppose it is true for some $n \geq 1$, then for any $x' \in \{0,1\}^{n+1}$, write $x' = xx_{n+1}$ where $x \in \{0,1\}^n$, then

$$\begin{aligned}
H^{\otimes n+1}|x'\rangle &= H^{\otimes n+1}(|x\rangle \otimes |x_{n+1}\rangle) \\
&= H^{\otimes n}|x\rangle \otimes H|x_{n+1}\rangle \\
&= \frac{1}{2^{n/2}} \sum_{z\in\{0,1\}^n} (-1)^{x.z}|z\rangle \otimes \left(\frac{|0\rangle + (-1)^{x_{n+1}}|1\rangle}{\sqrt{2}}\right) \\
&= \frac{1}{2^{n+1/2}} \sum_{z\in\{0,1\}^n} (-1)^{x.z++x_{n+1}.0}|z\rangle \otimes |0\rangle + (-1)^{x.z+x_{n+1}.1}|z\rangle \otimes |1\rangle \\
&= \frac{1}{2^{n+1/2}} \sum_{z'\in\{0,1\}^{n+1}} (-1)^{x'.z'}|z'\rangle
\end{aligned}$$

Now, we consider

$$\begin{aligned}
H\left(\frac{|x\rangle + |y\rangle}{\sqrt{2}}\right) &= H\left(\frac{|x\rangle + |s\oplus x\rangle}{\sqrt{2}}\right) \\
&= \frac{1}{\sqrt{2}}H|x\rangle + \frac{1}{\sqrt{2}}H|s\oplus x\rangle \\
&= \frac{1}{\sqrt{2}}\frac{1}{2^{n/2}}\sum_z (-1)^{x.z}|z\rangle + \frac{1}{\sqrt{2}}\frac{1}{2^{n/2}}\sum_z (-1)^{x.z+s.z}|z\rangle \\
&= \frac{1}{2^{n+1/2}}\sum_z (-1)^{x.z}\left(1 + (-1)^{s.z}\right)|z\rangle \\
&= \frac{1}{2^{n-1/2}}\sum_{s.z=0} (-1)^{x.z}|z\rangle \\
&= \frac{1}{2^{n-1/2}}\sum_{z\perp s} (-1)^{x.z}|z\rangle
\end{aligned}$$

□

Exercise 3

Proof. $|S\rangle = \sum_{s\in S}\frac{1}{2^{m/2}}|s\rangle$

$$\begin{aligned}
H|S\rangle &= \sum_{s\in S}\frac{1}{2^{m/2}}H|s\rangle \\
&= \sum_{s\in S}\frac{1}{2^{m/2}}\frac{1}{2^{n/2}}\sum_w (-1)^{s.w}|w\rangle \\
&= \sum_w \frac{1}{2^{(n+m)/2}}\left(\sum_{s\in S}(-1)^{s.w}\right)|w\rangle
\end{aligned}$$

Claim: $w \in S^{\perp} \implies \sum_{s\in S}(-1)^{s.w} = 2^m$
Because if $w \in S^{\perp} \implies s.w = 0, \forall s \in S \implies \sum_{s\in S}(-1)^{s.w} = |S| = 2^m$

Claim: $w \notin S^{\perp} \implies \sum_{s\in S}(-1)^{s.w} = 0$
Fix a basis $\{s_1, s_2, \ldots, s_m\}$ for S. Since $w \notin S^{\perp}$, there exists i such that $s_i.w = 1$. Now for any $s \in S$, $s = c_1 s_1 + \cdots + c_m s_m$, where $c = (c_1, c_2, \ldots) \in \mathbb{Z}_2^m$. Thus,

$$\begin{aligned}
\sum_{s\in S}(-1)^{s.w} &= \sum_{c\in\mathbb{Z}_2^m}(-1)^{c_1 s_1.w}(-1)^{c_2 s_2.w}\ldots(-1)^{c_m s_m.w} \\
&= (1+(-1)^{s_1.w})(1+(-1)^{s_2.w})\ldots(1+(-1)^{s_i.w})\ldots(1+(-1)^{s_m.w}) \\
&= (1+(-1)^{s_1.w})(1+(-1)^{s_2.w})\ldots(1+(-1))\ldots(1+(-1)^{s_m.w}) \\
&= 0
\end{aligned}$$

Therefore,

$$H\,|S\rangle = \frac{1}{2^{(n-m)/2}}\sum_{w\in S^{\perp}}|w\rangle$$

Furthermore, for any $y \in \mathbb{Z}_2^n$

$$\begin{aligned}
H\,|y+S\rangle &= \sum_{s\in S}\frac{1}{2^{m/2}}H\,|y+s\rangle \\
&= \sum_{s\in S}\frac{1}{2^{(n+m)/2}}\sum_{w}(-1)^{(y+s).w}\,|w\rangle \\
&= \frac{1}{2^{(n+m)/2}}\sum_{w}(-1)^{y.w}\left(\sum_{s\in S}(-1)^{s.w}\right)|w\rangle \\
&= \frac{1}{2^{(n-m)/2}}\sum_{w\in S^{\perp}}(-1)^{y.w}\,|w\rangle
\end{aligned}$$

□

Exercise 4

Proof. Suppose $X_j = i$ is known. So $V_i = \langle w_1, \ldots w_i\rangle$ has dimension j.

$$P[X_{j+1} = i+1] = P[w_{i+1} \notin V_i] = 1 - P[w_{i+1} \in V_i] = 1 - \frac{2^j}{2^m}$$

$$\begin{aligned}
P[X_{j+1} = i+2] &= P[w_{i+2} \notin V_i, w_{i+1} \in V_i] \\
&= P[w_{i+2} \notin V_i]P[w_{i+1} \in V_i] \\
&= \frac{2^j}{2^m}\left(1 - \frac{2^j}{2^m}\right)
\end{aligned}$$

Similarly,

$$\begin{aligned}
P[X_{j+1} = i+k] &= P[w_{i+k} \notin V_i, w_{i+k-1} \in V_i, \ldots w_{i+1} \in V_i] \\
&= P[w_{i+k} \notin V_i]P[w_{i+k-1} \in V_i]\ldots P[w_{i+1} \in V_i] \\
&= \left(1 - \frac{2^j}{2^m}\right)\left(\frac{2^j}{2^m}\right)^{k-1}
\end{aligned}$$

Let $p_j = 2^j/2^m$, then

$$\begin{aligned}
E[X_{j+1} \mid X_j = i] &= \sum_{k \geq 1} (i+k) P[X_{j+1} = i+k] \\
&= \sum_{k \geq 1} (i+k)\,(1-p_j)\,p_j^{k-1} \\
&= i\,(1-p_j) \sum_{k \geq 1} p_j^{k-1} + (1-p_j) \sum_{k \geq 1} k p_j^{k-1} \\
&= i + \frac{1}{1-p_j}
\end{aligned}$$

As $E[X_{j+1} \mid X_j] = X_j + \frac{1}{1-p_j}$ and $E[X_{j+1}] = E[E[X_{j+1} \mid X_j]]$, we get $E[X_{j+1}] = E[X_j] + \frac{1}{1-p_j}$ Similarly, we can calculate $E[X_1] = \frac{1}{1-p_0}$. Thus,

$$\begin{aligned}
E[X_m] &= E[X_{m-1}] + \frac{1}{1-p_{m-1}} \\
&= \sum_{j=0}^{m-1} \frac{1}{1-p_j} \\
&= \sum_{j=0}^{m-1} \frac{2^m}{2^m - 2^j} \\
&= \sum_{j=0}^{m-1} 1 + \frac{2^j}{2^m - 2^j} \\
&= m + \left(\sum_{j=1}^{m} \frac{1}{2^j - 1} \right) \\
&< m + \left(\sum_{j=1}^{m} \frac{1}{2^{j-1}} \right) && (\text{as } 1 \leq 2^{j-1} \forall j \geq 1) \\
&< m + \left(\sum_{j=0}^{\infty} \frac{1}{2^j} \right) \\
&= m + 2
\end{aligned}$$

Thus, $E[X_m] < m + 2$ $\square$