Homework 1

Quantum Mechanics

January 22, 2023 C Seitz

Problem 1. *No-cloning theorem*

Solution. Assume we have a unitary copying operator U and two quantum states $|\phi\rangle$ and $|\psi\rangle$. Suppose this unknown copying operator U could transform $|s\rangle$ to either $|\phi\rangle$ or $|\psi\rangle$.

$$|\psi\rangle \otimes |s\rangle \xrightarrow{U} |\psi\rangle \otimes |\psi\rangle$$
$$|\phi\rangle \otimes |s\rangle \xrightarrow{U} |\phi\rangle \otimes |\phi\rangle$$

If U is unitary, then it preserves inner products, so

$$(\langle\psi| \otimes \langle s|)(|\phi\rangle \otimes |s\rangle) = \langle\psi|\phi\rangle \otimes \langle s|s\rangle = \langle\psi|\phi\rangle$$

After the copying transformation, we have

$$\begin{aligned}(\langle\psi| \otimes \langle\psi|)(|\phi\rangle \otimes |\phi\rangle) &= \langle\psi|\phi\rangle \otimes \langle\psi|\phi\rangle \\ &= (\langle\psi|\phi\rangle)^2\end{aligned}$$

We demanded that the inner product be preserved, so these two results must be equivalent. However, there is only a solution when $|\psi\rangle = |\phi\rangle$ or $\langle\psi|\phi\rangle = 0$. Therefore, the copying circuit only works for orthogonal states, and not a general ket.

■

Problem 2. *Quantum Teleportation*

Solution.

The objective is for Alice to teleport to Bob a qubit in a state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, which can be done by using an entangled EPR pair. There three qubits in total: $|\psi\rangle$ and an entangled EPR pair $|\beta_{00}\rangle$. The first qubit in the EPR pair is kept by alice and the second is given to Bob. Since the EPR pair is entangled, the three qubits are in a state

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle)$$

Alice then sends this state through a CNOT gate, where the qubit $|\psi\rangle$ is the control bit and the first qubit of the EPR pair is the target bit. This of course flips the second bit for the second two terms:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle)$$

Then the first qubit is sent through a Hadamard gate. As a minor detour, the Hadamard gate, does

$$\begin{aligned} |0\rangle &\to (|0\rangle + |1\rangle)/\sqrt{2} = |+\rangle \\ |1\rangle &\to (|0\rangle - |1\rangle)/\sqrt{2} = |-\rangle \end{aligned}$$

Therefore, the effect on $|\psi_1\rangle$ is:

$$\begin{aligned} |\psi_1\rangle &= \frac{1}{2}(\alpha|000\rangle + \alpha|100\rangle + \alpha|011\rangle + \alpha|111\rangle \\ &+ \beta|010\rangle + \beta|001\rangle - \beta|110\rangle - \beta|101\rangle) \\ &= \frac{1}{2}(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) \\ &+ |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)) \end{aligned}$$

Therefore, if Alice measures her two qubits, say in state $|00\rangle$, she can communicate this to bob over a classical communication channel, and Bob then knows the superposition of his qubit. Bob can then apply the necessary quantum gate to transform his qubit to $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

■

Problem 3. *Deutsch Algorithm, Deutch-Josza Algorithm*

Solution.

Suppose we have some boolean function $f : \{0,1\} \to \{0,1\}$. Deutch's algorithm can determine whether the function f is constant or balanced exponentially faster than a classical computer. If f is constant then $f(0) = f(1)$; however, if f is balanced then $f(0) \neq f(1)$.

We start with the two qubits prepared in state $|\psi_0\rangle = |0\rangle |1\rangle$. Each qubit is Hadamard transformed to give

$$\begin{aligned}
|\psi_1\rangle &= \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \\
&= \frac{1}{2}(|0\rangle |0\rangle - |0\rangle |1\rangle + |1\rangle |0\rangle - |1\rangle |1\rangle)
\end{aligned}$$

The state then goes through an oracle U_f, which implements the transformation $|\alpha\rangle |\beta\rangle \to |\alpha\rangle |\beta \oplus f(\alpha)\rangle$. Note that $\oplus$ is addition modulo two, which is essentially an XOR operation. Thus, after transformation, the state is

$$\begin{aligned}
|\psi_2\rangle &= \frac{1}{2}(|0\rangle |0 \oplus f(0)\rangle - |0\rangle |1 \oplus f(0)\rangle + |1\rangle |0 \oplus f(1)\rangle - |1\rangle |1 \oplus f(1)\rangle) \\
&= \frac{1}{2}(|0\rangle (|0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle) + |1\rangle (|0 \oplus f(1)\rangle - |1 \oplus f(1)\rangle)) \\
&= \frac{1}{2}\Big((-1)^{f(0)} |0\rangle (|0\rangle - |1\rangle) + (-1)^{f(1)} |1\rangle (|0\rangle - |1\rangle)\Big)
\end{aligned}$$

Then we Hadamard transform the first qubit:

$$\begin{aligned}
|\psi_3\rangle &= \frac{1}{2}\Big((-1)^{f(0)}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) + (-1)^{f(1)}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)\Big) \\
&= \frac{1}{2}((-1)^{f(0)} + (-1)^{f(1)})(|00\rangle - |01\rangle) + ((-1)^{f(0)} - (-1)^{f(1)})(|10\rangle - |11\rangle))
\end{aligned}$$

Writing it in this way makes it clear how we determine if the function is constant or balanced. If it is constant($f(0) = f(1)$) then the the second term vanishes. So, if we measure the first qubit, it will be in state $|0\rangle$. However, if it is balanced ($f(0) \neq f(1)$), then the first term vanishes and the first qubit will be measured in state $|1\rangle$.

This algorithm generalizes to the case where the function $f : \{0,1\}^n \to \{0,1\}$. This is where the power of quantum computing really shines. Classically, (if f can be constant or balanced and nothing else), we would need

$2^{n-1}+1$ function calls. But a quantum computer can do this in a single function call. Similar to before, we have $|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle$. We Hadamard transform like before, but note that when we Hadamard transform a bit string of length n, we transform each bit individually. Our n-bit string is all zeros so we get

$$H^{\otimes n}|0,0...,0\rangle = |+\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}}\sum_{\alpha\in 0,1^n}|\alpha\rangle$$

Thus

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}}\sum_{\alpha\in 0,1^n}|\alpha\rangle\otimes|-\rangle$$

Looking at the last line from $|\psi_2\rangle$ in Deutsch's algorithm above, we can see that the effect of the oracle U_f is efficiently summarized as:

$$U_f|\psi_1\rangle = \frac{1}{\sqrt{2^n}}\sum_{\alpha\in\{0,1\}}(-1)^{f(\alpha)}|\alpha\rangle\otimes|-\rangle$$

Therefore, for the n-bit case, we get

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

We Hadamard transform the first qubit again, but α can be mixtures of 0's and 1's so its a bit more complicated

$$\begin{aligned}
|\psi_3\rangle &= \frac{1}{\sqrt{2^n}}\sum_{\alpha\in\{0,1\}^n}(-1)^{f(\alpha)}H^{\otimes n}|\alpha\rangle\otimes|-\rangle \\
&= \frac{1}{\sqrt{2^n}}\sum_{\alpha\in\{0,1\}^n}(-1)^{f(\alpha)}\left(\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{\alpha\cdot x}|x\rangle\right)\otimes|-\rangle \\
&= \frac{1}{2^n}\sum_{\alpha\in\{0,1\}^n}\sum_{x\in\{0,1\}^n}(-1)^{f(\alpha)}(-1)^{\alpha\cdot x}|x\rangle\otimes|-\rangle
\end{aligned}$$

where $\alpha \cdot x = \alpha_0 x_0 \oplus \alpha_1 x_1 \oplus ....$ A bit of rearranging (and dropping the second qubit because it doesn't matter) gives

$$|\psi_3\rangle = \sum_{x \in \{0,1\}^n} \left(\frac{1}{2^n} \sum_{\alpha \in \{0,1\}^n} (-1)^{f(\alpha)} (-1)^{\alpha \cdot x} \right) |x\rangle$$

The term in parentheses is the expansion coefficient for state $|x\rangle$. It turns out that if f is constant, then this expansion coefficient is ± 1 for $x = |0\rangle^{\otimes n}$ and zero for all other x. However, if f is balanced, the sum over α is more complex (but presumably it is not zero). It's difficult to say exactly how it would look, but we can say that it depends on what $f(\alpha)$ actually is. Ultimately, we would measure some state other than $x = |0\rangle^{\otimes n}$ when f is balanced, because the sum over α would be zero for that state.

■