Quantum Information Processing Assignment 4

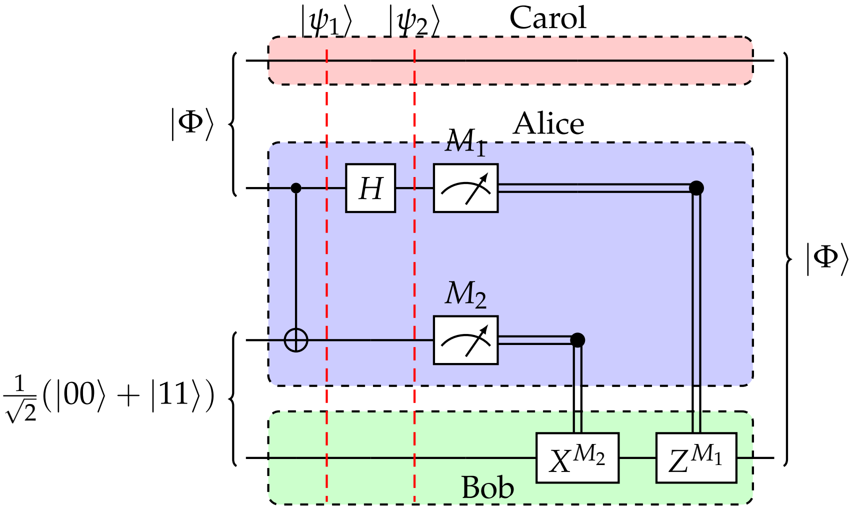
Name: Nate Stemen (20906566) **Due:** Thur, Oct 8, 2020 11:59 PM
Email: `nate.stemen@uwaterloo.ca` **Course:** QIC 710

I worked with Chelsea Komlo and Wilson Wu on this assignment.

Problem 1

Teleporting entanglement?

Solution. We start with writing down the circuit for our teleportation of an entangled state.



Where we've assumed the end state is $|\Phi\rangle$ which we will prove. We've labeled $|\psi_1\rangle$ and $|\psi_2\rangle$ as intermediary states that we will expand below. To start lets first write down the total state of the sysem (4 qubits) that are at play.

$$\begin{aligned} |\Phi\rangle \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}\,[\\ &\alpha_{00}\,|0\rangle_C\,|00\rangle_A\,|0\rangle_B + \alpha_{00}\,|0\rangle_C\,|01\rangle_A\,|1\rangle_B \\ &+ \alpha_{01}\,|0\rangle_C\,|10\rangle_A\,|0\rangle_B + \alpha_{01}\,|0\rangle_C\,|11\rangle_A\,|1\rangle_B \\ &+ \alpha_{10}\,|1\rangle_C\,|00\rangle_A\,|0\rangle_B + \alpha_{10}\,|1\rangle_C\,|01\rangle_A\,|1\rangle_B \\ &+ \alpha_{11}\,|1\rangle_C\,|10\rangle_A\,|0\rangle_B + \alpha_{11}\,|1\rangle_C\,|11\rangle_A\,|1\rangle_B\,] \end{aligned}$$

Where we're using the convention that the first qubit in Alice's state is the one from Carol, and the second one is the one shared with Bob. Now the first step of the teleportation protocol is to CNOT Alice's qubits. If we do this we then get the following state (omiting the factor of $\frac{1}{\sqrt{2}}$ in front).

$$\begin{aligned} |\psi_1\rangle = \quad &\alpha_{00}\,|0\rangle_C\,|00\rangle_A\,|0\rangle_B + \alpha_{00}\,|0\rangle_C\,|01\rangle_A\,|1\rangle_B \\ &+ \alpha_{01}\,|0\rangle_C\,|11\rangle_A\,|0\rangle_B + \alpha_{01}\,|0\rangle_C\,|10\rangle_A\,|1\rangle_B \\ &+ \alpha_{10}\,|1\rangle_C\,|00\rangle_A\,|0\rangle_B + \alpha_{10}\,|1\rangle_C\,|01\rangle_A\,|1\rangle_B \\ &+ \alpha_{11}\,|1\rangle_C\,|11\rangle_A\,|0\rangle_B + \alpha_{11}\,|1\rangle_C\,|10\rangle_A\,|1\rangle_B \end{aligned}$$

Now we need to apply a Hadamard to the first of Alice's qubits.

$$\begin{aligned}|\psi_2\rangle = \quad & \alpha_{00}\,|0\rangle_C\,|{+0}\rangle_A\,|0\rangle_B + \alpha_{00}\,|0\rangle_C\,|{+1}\rangle_A\,|1\rangle_B \\ & + \alpha_{01}\,|0\rangle_C\,|{-1}\rangle_A\,|0\rangle_B + \alpha_{01}\,|0\rangle_C\,|{-0}\rangle_A\,|1\rangle_B \\ & + \alpha_{10}\,|1\rangle_C\,|{+0}\rangle_A\,|0\rangle_B + \alpha_{10}\,|1\rangle_C\,|{+1}\rangle_A\,|1\rangle_B \\ & + \alpha_{11}\,|1\rangle_C\,|{-1}\rangle_A\,|0\rangle_B + \alpha_{11}\,|1\rangle_C\,|{-0}\rangle_A\,|1\rangle_B\end{aligned}$$

Now, adding the normalization constants and expanding the plus/minus states out we have

$$\begin{aligned}|\psi_2\rangle = \frac{1}{2}\Big[&\alpha_{00}(|0\rangle_C\,|00\rangle_A\,|0\rangle_B + |0\rangle_C\,|10\rangle_A\,|0\rangle_B + |0\rangle_C\,|01\rangle_A\,|1\rangle_B + |0\rangle_C\,|11\rangle_A\,|1\rangle_B) \\ &+ \alpha_{01}(|0\rangle_C\,|01\rangle_A\,|0\rangle_B - |0\rangle_C\,|11\rangle_A\,|0\rangle_B + |0\rangle_C\,|00\rangle_A\,|1\rangle_B - |0\rangle_C\,|10\rangle_A\,|1\rangle_B) \\ &+ \alpha_{10}(|1\rangle_C\,|00\rangle_A\,|0\rangle_B + |1\rangle_C\,|10\rangle_A\,|0\rangle_B + |1\rangle_C\,|01\rangle_A\,|1\rangle_B + |1\rangle_C\,|11\rangle_A\,|1\rangle_B) \\ &+ \alpha_{11}(|1\rangle_C\,|01\rangle_A\,|0\rangle_B - |1\rangle_C\,|11\rangle_A\,|0\rangle_B + |1\rangle_C\,|00\rangle_A\,|1\rangle_B - |1\rangle_C\,|10\rangle_A\,|1\rangle_B)\Big]\end{aligned}$$

Now we need to group these elements by Alice's qubits since we are momentarily going to measure them.

$$\begin{aligned}2\,|\psi_2\rangle = \quad & |00\rangle_A\,(\alpha_{00}\,|0\rangle_C\,|0\rangle_B + \alpha_{01}\,|0\rangle_C\,|1\rangle_B + \alpha_{10}\,|1\rangle_C\,|0\rangle_B + \alpha_{11}\,|1\rangle_C\,|1\rangle_B) \\ & + |01\rangle_A\,(\alpha_{00}\,|0\rangle_C\,|1\rangle_B + \alpha_{01}\,|0\rangle_C\,|0\rangle_B + \alpha_{10}\,|1\rangle_C\,|1\rangle_B + \alpha_{11}\,|1\rangle_C\,|0\rangle_B) \\ & + |10\rangle_A\,(\alpha_{00}\,|0\rangle_C\,|0\rangle_B - \alpha_{01}\,|0\rangle_C\,|1\rangle_B + \alpha_{10}\,|1\rangle_C\,|0\rangle_B - \alpha_{11}\,|1\rangle_C\,|1\rangle_B) \\ & + |11\rangle_A\,(\alpha_{00}\,|0\rangle_C\,|1\rangle_B - \alpha_{01}\,|0\rangle_C\,|0\rangle_B + \alpha_{10}\,|1\rangle_C\,|1\rangle_B - \alpha_{11}\,|1\rangle_C\,|0\rangle_B)\end{aligned}$$

Written in this form we can more easily see what happens when we measure Alice's qubits. If we measure them and get 00, we can see the state collapses to Carol and Bob sharing the general state $|\Phi\rangle$, with Bob having the second qubit (as desired). No other operations need to be performed (just like during the regular teleportation protocol and the sender measures 00).

Just as in the teleportation protocol, the result of Alice's measurement is sent to Bob where he conditionally applies a Pauli X if Alice's second qubit measures 1, and then again conditionally applies a Pauli Z if Alice's first qubit measures 1. Applying these transformations to Bob's state does exactly the necessary phase and bit flips to get the state back into $|\Phi\rangle$. This proves that an entangled state can be teleported and remain entangled during the process. This also shows that Bob and Carol now share the entangled state $|\Phi\rangle$. What a fun question...

Problem 2

A simple collision-finding problem.

(a) How many queries to f does a *classical* algorithm require to find a collision? The algorithm must always succeed (the error probability for any run should be 0).

(b) Show how to solve this problem by a *quantum* algorithm that makes one single query to f. The algorithm must always succeed (the error probability for any run should be 0)

Solution. (a) A classical algorithm would require 3 queries to f in order to guarantee 100% success. This is because the first two queries could result in different values, but the third will always give something you've already seen (provided the first two queries were different).

(b) It's important to note here that there are six such functions on domain $\{0,1\}^2$ that are two-to-one functions.

a	$f_0(a)$
00	0
01	0
10	1
11	1

a	$f_1(a)$
00	0
01	1
10	0
11	1

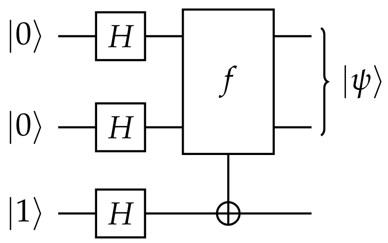
a	$f_2(a)$
00	0
01	1
10	1
11	0

a	$f_3(a)$
00	1
01	1
10	0
11	0

a	$f_4(a)$
00	1
01	0
10	1
11	0

a	$f_5(a)$
00	1
01	0
10	0
11	1

We've arranged the tables so that the tables aligned vertically are similiar in the sense that they are the negation of each other. That is $f_0(a) = \neg f_3(a)$, $f_1(a) = \neg f_4(a)$, and $f_2(a) = \neg f_5(a)$. Back to the circuit. Lets take the system through the following circuit.

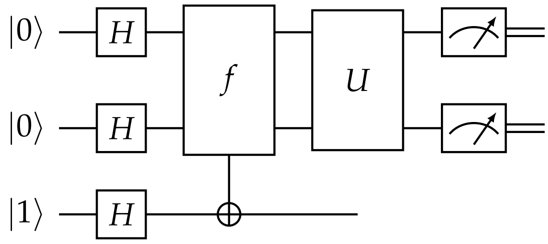


We can now calculate what $|\psi\rangle$ looks like for each f_i using the fact that the state after f

is applied is $\left|-\right\rangle \sum_{a\in\{0,1\}^2}(-1)^{f(a)}\left|a\right\rangle$.

$$\begin{aligned}
f_0 \mapsto \left|\psi_0\right\rangle &= \left|00\right\rangle + \left|01\right\rangle - \left|10\right\rangle - \left|11\right\rangle \\
f_1 \mapsto \left|\psi_1\right\rangle &= \left|00\right\rangle - \left|01\right\rangle + \left|10\right\rangle - \left|11\right\rangle \\
f_2 \mapsto \left|\psi_2\right\rangle &= \left|00\right\rangle - \left|01\right\rangle - \left|10\right\rangle + \left|11\right\rangle \\
f_3 \mapsto \left|\psi_3\right\rangle &= -\left|00\right\rangle - \left|01\right\rangle + \left|10\right\rangle + \left|11\right\rangle \\
f_4 \mapsto \left|\psi_4\right\rangle &= -\left|00\right\rangle + \left|01\right\rangle - \left|10\right\rangle + \left|11\right\rangle \\
f_5 \mapsto \left|\psi_5\right\rangle &= -\left|00\right\rangle + \left|01\right\rangle + \left|10\right\rangle - \left|11\right\rangle
\end{aligned}$$

Now here we can note that similar to how $f_0(a) = \neg f_3(a)$, we have $\left|\psi_0\right\rangle = -\left|\psi_3\right\rangle$ which holds for the other pairs we made above as well. Also important to note that $\left|\psi_0\right\rangle$ is orthogonal to every other $\left|\psi_i\right\rangle$ except $\left|\psi_3\right\rangle$. In particular though $\left|\psi_0\right\rangle$, $\left|\psi_1\right\rangle$, and $\left|\psi_2\right\rangle$ are all orthogonal. This means we can find a U such that $U\left|\psi_0\right\rangle = \left|00\right\rangle$, $U\left|\psi_1\right\rangle = \left|01\right\rangle$, $U\left|\psi_2\right\rangle = \left|10\right\rangle$. When we then measure our state we will get one of 00, 01, or 10. If we measure 00, then we know our state was either $\left|\psi_0\right\rangle$ or $\left|\psi_3\right\rangle$ and hence 00, and 01 collide when fed into f. If we measured 01, we know our state was either $\left|\psi_1\right\rangle$ or $\left|\psi_4\right\rangle$ and hence 00, and 10 collide. Lastly, if we measure 10, we know our state was either $\left|\psi_2\right\rangle$ or $\left|\psi_5\right\rangle$ and hence 00 and 11 collide. The circuit bellow is a representation of the quantum compuutation portion of our algorithm.



Thus we've shown an algorithm that solves this problem with only one query to f.

Problem 3

A variant of Simon's problem.

(a) Show that if you find any three colliding points a, b, x then r, s and $r \oplus s$ ca be deduced from that.

(b) Give a quantum circuit that makes one query to f and products the state

$$\frac{1}{\sqrt{2^n}} \sum_{a \in \{0,1\}^n} |a\rangle \, |f(a)\rangle \tag{1}$$

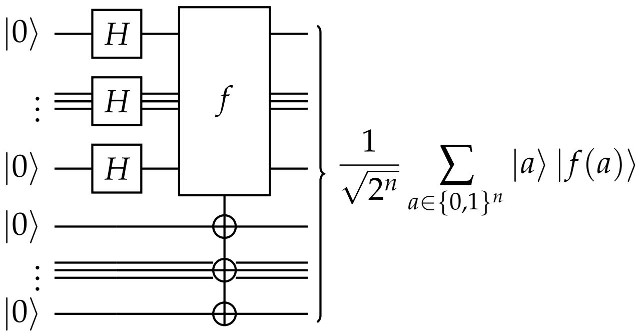
(c) For the state in eq. (1), suppose that the last n qubits are measured (in the computational basis), and then a Hadamard transform is applied to each of the first n qubits, and then those qubits are measured (in the computational basis). Explain what the outcome is, where your answer should be supported by full calculations.

Solution. (a) Start by taking the XOR of a with b.

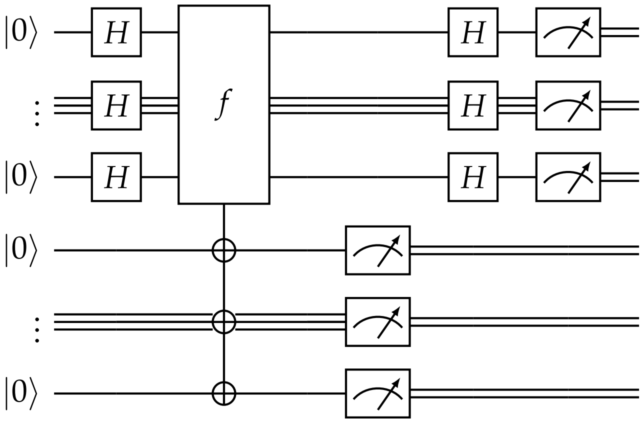
$$\begin{aligned} a \oplus b &= a \oplus (a \oplus r) \\ &= (a \oplus a) \oplus r \\ &= 0^n \oplus r \\ &= r \end{aligned}$$

This same procedure can be done with $a \oplus c$ to get s. With these values we can XOR them together to get $r \oplus s$.

(b) The following circuit gives the desired state.


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

(c) I think it's easiest to see what's happening if we draw out the circuit.



In order to get a grasp on what happens when we measure things here it'll help if we rewrite eq. (1) using the fact that f is a four-to-one function. First let $T \subset \{0,1\}^n$ contain exactly one element from each colliding quartet. Then notice that $\{0,1\}^n = T \cup (T \oplus r) \cup (T \oplus s) \cup (T \oplus r \oplus s)$. With this we can rewrite our state eq. (1) as follows.

$$\sum_{a \in T} |a\rangle |f(a)\rangle + |a \oplus r\rangle |f(a \oplus r)\rangle + |a \oplus s\rangle |f(a \oplus s)\rangle + |a \oplus r \oplus s\rangle |f(a \oplus r \oplus s)\rangle$$

Using the fact that f is a four-to-one function we can again rewrite this pulling out the $|f\rangle$ terms.

$$\sum_{a \in T} (|a\rangle + |a \oplus r\rangle + |a \oplus s\rangle + |a \oplus r \oplus s\rangle) |f(a)\rangle$$

Written in this form we see when we measure the last n qubits we will obtain $f(a)$ for some random a and it collapses the sum to just a particular a. This leaves us with $|a\rangle + |a \oplus r\rangle + |a \oplus s\rangle + |a \oplus r \oplus s\rangle$. Now we need to apply Hadamards to each of qubits left. To do this we will use the general formula below.

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

Applying this to our state we have the following expansion.

$$\begin{aligned}
\frac{1}{\sqrt{2^n}} \sum_{z \in \{0,1\}^n} & (-1)^{a \cdot z} |z\rangle + (-1)^{(a \oplus r) \cdot z} |z\rangle + (-1)^{(a \oplus s) \cdot z} |z\rangle + (-1)^{(a \oplus r \oplus s) \cdot z} |z\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{z \in \{0,1\}^n} \Big((-1)^{a \cdot z} + (-1)^{(a \oplus r) \cdot z} + (-1)^{(a \oplus s) \cdot z} + (-1)^{(a \oplus r \oplus s) \cdot z} \Big) |z\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{z \in \{0,1\}^n} (-1)^{a \cdot z} \Big(1 + (-1)^{r \cdot z} + (-1)^{s \cdot z} + (-1)^{(r \oplus s) \cdot z} \Big) |z\rangle
\end{aligned}$$

This is the outcome state. Presumably there is some reasoning we can follow just as we did with Simon's problem to measure this, get a string perpendicular to something, and then run that a bunch of times. The difference here is that in order to have terms go to zero, one has to be $+1$, and the other two have to be -1. So I'm not exactly sure how to make this happen though, and what the associated probabilities are for each measurement.