Quantum Computing Assignment 9

Brennan W. Fieck

April 14$^{\text{th}}$, 2017

Problem 6.3.1. In the Deutsch algorithm, when we consider U_f as a single-qubit operator $\hat{U}_{f(x)}$, $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$ is an eigenstate of $\hat{U}_{f(x)}$, whose associated eigenvalues gives us the answer to the Deutsch problem. Suppose we were not able to prepare this eigenstate directly. Show that if we instead input $|0\rangle$ to the target qubit, and otherwise run the same algorithm, we get an algorithm that gives the correct answer with probability $\frac{3}{4}$ (note this also works if we input $|1\rangle$ to the second qubit). Furthermore, show that with probability $\frac{1}{2}$ we know for certainty that the algorithm has produced the correct answer
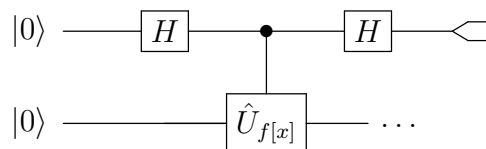
Hint: write $|0\rangle$ in the basis of eigenvectors of U_f.

Solution.
I couldn't find this stated anywhere in the text, but it's true that $|+\rangle$ is an eigenstate of U_f. Here's a brief proof:

$$U_f|x\rangle|+\rangle = \frac{|x\rangle|0 \oplus f[x]\rangle + |x\rangle|1 \oplus f[x]\rangle}{\sqrt{2}} = |x\rangle|+\rangle \forall x \in \{0,1\}$$

Note that the eigenvalue is simply 1. We can "de"compose $|0\rangle$ as $|0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}}$. The actual circuit we're investigating here is:

Before the first Hadamard gate, the system is in the state $|00\rangle$, and afterward it is transformed into the state $(H \otimes I_2)|00\rangle = |+0\rangle$. Application of the c-$\hat{U}_f$ is worked out below.

$$\texttt{let } |\psi_2\rangle \equiv \text{c-}\hat{U}_f(H \otimes I_2)|00\rangle = \frac{U_f|00\rangle + U_f|10\rangle}{\sqrt{2}}$$

Note that I thought it'd make everything easier to take advantage of the fact that c-$\hat{U}_f$ was defined such that c-$\hat{U}_f|x\rangle|y\rangle \equiv U_f|x\rangle|y\rangle$.

$$= \frac{|0\rangle|0 \oplus f[0]\rangle + |1\rangle|0 \oplus f[1]\rangle}{\sqrt{2}} = \frac{|0\rangle|f[0]\rangle + |1\rangle|f[1]\rangle}{\sqrt{2}}$$

Now there are a couple of cases to consider. Either f is constant, or it's balanced - which can be expressed equivalently as either $f[0] == f[1]$ or $f[0] \neq f[1]$. Also, whether f is balanced or not, we have to consider that $f[0] = 0$ or 1 (together with the information about f being balanced, the value of $f[0]$ will determine the value of $f[1]$ and vice-versa).

$$= \begin{cases} f[0] == f[1] : & \begin{cases} f[0] == 0 : & \frac{|0\rangle|0\rangle + |1\rangle|0\rangle}{\sqrt{2}} = |+\rangle|0\rangle \\ f[0] == 1 : & \frac{|0\rangle|1\rangle + |1\rangle|1\rangle}{\sqrt{2}} = |+\rangle|1\rangle \end{cases} = |+\rangle|f\,[z \in \{0,1\}\rangle] \\[2em] f[0] \neq f[1] : & \begin{cases} f[0] == 0 : & \frac{|0\rangle|0\rangle + |1\rangle|1\rangle}{\sqrt{2}} \\ f[0] == 1 : & \frac{|0\rangle|1\rangle + |1\rangle|0\rangle}{\sqrt{2}} \end{cases} = \text{No closed form I'm aware of.} \end{cases} = |\psi_2\rangle$$

Now, if we once again apply the $H \otimes I_2$ gate to this guy, if f is constant we'll get a nice, clean $|0\rangle|f[z \in \{0,1\}]\rangle$ state, and it'll be

$$(H \otimes I_2)\,|\psi_2\rangle = \begin{cases} f[0] == 0 : & \frac{|+\rangle|0\rangle + |-\rangle|1\rangle}{\sqrt{2}} = \frac{|00\rangle + |10\rangle + |01\rangle - |11\rangle}{2} \\[1em] f[0] == 1 : & \frac{|+\rangle|1\rangle + |-\rangle|0\rangle}{\sqrt{2}} = \frac{|01\rangle + |11\rangle + |00\rangle - |10\rangle}{2} \end{cases} = \frac{|00\rangle + |01\rangle + (-1)^{f[0]}(|10\rangle - |11\rangle)}{2}$$

when f is balanced. So if the function f happens to be constant, we'll always measure that first qubit to be 0. However, if f is balanced, one is equally likely to measure a 1 or a 0. Therefore, for half of the possible outputs - specifically 1 - we know with absolute certainty that the function is balanced. Furthermore, a measurement of 0 will occur always if f is constant and occur 50% of the time if f is balanced, so the probability of being correct is $1/2 + 1/2(1/2) = 3/4$.

□

Problem 7.1.4.

(a) Give a concise description of the operation performed by the square of the QFT.

(b) What are the eigenvalues of the QFT?

Solution.

(a) Since QFT_N is the Nth root of I_N, the square of the QFT is

$$\left(\sqrt[N]{I_N}\right)^2 = \sqrt[N/2]{I_N}$$

What this gives you is a transformation back to the original input, but with the entries reversed except for the first one: a massive swap-type operation. Mathematically, if

$$|x\rangle = \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_{N-2} \\ x_{N-1} \end{bmatrix}$$

then

$$\text{QFT}_N\text{QFT}_N|x\rangle = \begin{bmatrix} x_0 \\ x_{N-1} \\ x_{N-2} \\ \vdots \\ x_2 \\ x_1 \end{bmatrix}$$

(b) Best I can do is tell you that since QFT_N is the Nth root of I_N its eigenvalues are the Nth roots of unity (e.g. for $N = 4$, the eigenvalues are $1, -1, i$ and $-i$). There's probably a more general way to state that - and include the multiplicity of each eigenvalue - but I can't figure out what it is.

$\square$

Problem 7.1.5. Prove

$$\text{QFT}_{mr}^{-1}|\phi_{r,b}\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i \frac{b}{r} k}|mk\rangle.$$

Solution.
Starting with the definition of QFT_m^{-1}:

$$\text{QFT}_n^{-1}|x\rangle = \frac{1}{\sqrt{n}} \sum_{y=0}^{n-1} \left[e^{-2\pi i xy/n}|y\rangle\right]$$

Now simply let $|x\rangle = |\phi_{r,b}\rangle$, which itself is described by

$$|\phi_{r,b}\rangle = \frac{1}{\sqrt{m}} \sum_{z=0}^{m-1} \left[|zr + b\rangle\right]$$

and $n = mr$. This is most easily accomplished by recognizing that inner multiplication is distributive over addition. In other words:

$$\text{QFT}_{mr}^{-1}|\phi_{r,b}\rangle = \frac{1}{\sqrt{m}} \sum_{z=0}^{m-1} \left[\text{QFT}_{mr}^{-1}|zr + b\rangle\right] = \frac{1}{\sqrt{m}} \sum_{z=0}^{m-1} \left[\frac{1}{\sqrt{mr}} \sum_{y=0}^{mr-1} \left[e^{-2\pi i(zr+b)/mr}|y\rangle\right]\right]$$

3

Don't worry if that looks terrifying, that's only because it's terrifying. First of all, $\frac{1}{\sqrt{mr}}$ is constant, so it can be factored out to make this a slightly less-terrifying double sum. Of course, since the indices of summation aren't dependent on one another, we're free to exchange them. Doing so is helpful, because it makes it obvious that parts of the summand don't depend on z at all, and therefore can be factored out of the sum in z.

$$= \frac{1}{m\sqrt{r}} \sum_{y=0}^{mr-1} \left[e^{-2\pi i y b/mr} \sum_{z=0}^{m-1} \left[e^{-2\pi i y z/m} \right] |y\rangle \right]$$

Let's just consider that innermost sum for a second; $\sum_{z=0}^{m-1} [e^{-2\pi i y z/m}]$. First, I found it easier to work with using only the Sine function.

$$\sum_{z=0}^{m-1} [e^{-2\pi i y z/m}] = \sum_{z=0}^{m-1} \left[\mathtt{Cos} \left[\frac{2\pi y z}{m} \right] \right] - i \sum_{z=0}^{m-1} \left[\mathtt{Sin} \left[\frac{2\pi y z}{m} \right] \right]$$

$$= \sum_{z=0}^{m-1} \left[\mathtt{Sin} \left[\frac{2\pi y z}{m} + \frac{\pi}{2} \right] \right] - i \sum_{z=0}^{m-1} \left[\mathtt{Sin} \left[\frac{2\pi y z}{m} \right] \right]$$

It's well-known* that

$$\sum_{a=0}^{n-1} \left[\mathtt{Sin} \left[\frac{2\pi a}{n} \right] \right] = \mathtt{Sin} \left[\frac{2\pi (0)}{n} \right] + \sum_{a=1}^{n-1} \left[\mathtt{Sin} \left[\frac{2\pi a}{n} \right] \right] = 0 + 0 = 0,$$

and

$$\sum_{j=0}^{n} [\mathtt{Sin} \left[\theta + cj \right]] = \frac{\mathtt{Sin} \left[\frac{(n+1)c}{2} \right] \mathtt{Sin} \left[\theta + \frac{nc}{2} \right]}{\mathtt{Sin} \left[\frac{c}{2} \right]}$$

So, applying our symbols for θ, c and n, this makes our inner sum

$$\frac{\mathtt{Sin} \left[m\frac{2\pi y}{m} \right] \mathtt{Sin} \left[\frac{\pi}{2} + \frac{(m-1)\frac{2\pi y}{m}}{2} \right]}{\mathtt{Sin} \left[\frac{2\pi y}{m} \right]} = \frac{\mathtt{Sin}[\pi y] \mathtt{Cos} \left[\pi y \left(1 - \frac{1}{m} \right) \right]}{\mathtt{Sin} \left[\frac{\pi y}{m} \right]}$$

Notice that if y is an integer multiple of m, the denominator approaches zero, while the $\mathtt{Sin}[\pi y]$ in the numerator approaches zero for any integer-valued y. So that means to get values for integer y - more specifically non-zero values - two things need to happen.

1. y needs to be an integer multiple of m; $y = mk$ for some $k \in \mathbb{I}$

2. Directly placing values in gives a $\frac{0}{0}$, so a limit must be taken.

---

*listed on Wikipedia

Since L'Hopital's Rule is The Single Best Way to Find Limits$^{\text{TM}}$, I'm going to go ahead and take some derivatives without worrying about what the limiting conditions actually are just yet.

$$\frac{\delta}{\delta y}[\text{numerator}] = \pi \left(\texttt{Cos}[y\pi]\texttt{Cos}\left[y\pi \left(1 - \frac{1}{m} \right) \right] + \left(1 - \frac{1}{m} \right) \texttt{Sin}[y\pi]\texttt{Sin}\left[\pi y \left(1 - \frac{1}{m} \right) \right] \right)$$

$$\frac{\delta}{\delta y}[\text{denominator}] = \frac{\pi}{m}\texttt{Cos}\left[\frac{y\pi}{m} \right]$$

Before combining these, note that since y is an integer, $\texttt{Sin}[y\pi] = 0$ (there's no conflicting zero in the denominator in this case) so the rightmost term from the numerator's derivative vanishes. Now, slam them together like this:

$$\frac{\pi\texttt{Cos}[y\pi]\texttt{Cos}\left[y\pi \left(1 - \frac{1}{m} \right) \right]}{\frac{\pi}{m}\texttt{Cos}\left[\frac{y\pi}{m} \right]}$$

Now take the limit where $y \to mk$ for some $k \in \mathbb{I}$, and you'll find that the Cosines reduce to simply one, and you're left with just m. So now the original double sum can be re-written as a single sum with restrictions on the summation index:

$$\texttt{QFT}^{-1}_{mr}|\phi_{r,b}\rangle = \frac{1}{m\sqrt{r}} \sum_{y=nm}^{mr-1} \left[me^{-2\pi iyb/mr}|y\rangle \right]$$

It would probably be convenient at this point to redefine the summation index to be over the integers multiple of m in a more concise way. As a completely random suggestion, not influenced at all by the notation used in the book or in particular the form of the expression I'm trying to reduce this to, let's choose k as a summation index.

$$= \frac{1}{\sqrt{r}} \sum_{r-1}^{k=0} \left[e^{-2\pi \frac{b}{r} k}|mk\rangle \right]$$

Wow look; exactly what it ought to be. Fancy that.

$\square$

Problem 7.2.2a. Recall in Section 4.5 it was shown how to implement a parity measurement using a quantum circuit. In Exercise 3.4.4, it was shown how the parity measurement is equivalent to measuring the observable $Z^{\otimes n}$. Describe an alternative algorithm (and draw the corresponding circuit diagram for measuring the observable $Z \otimes Z \otimes Z$ using one application of a c-$(Z \otimes Z \otimes Z)$ gate.
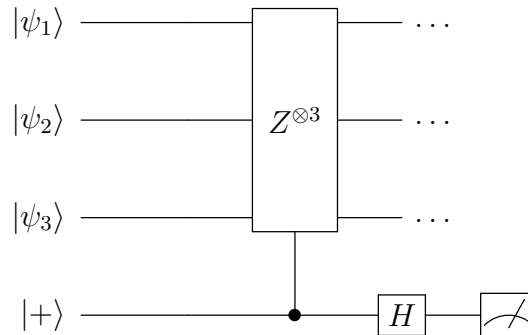
Solution.
First, let's examine the structure of $Z^{\otimes 3}$

$$Z^{\otimes 3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix}$$

I hope it's trivial to see that the eigenvalues of $Z^{\otimes 3}$ are ± 1. Obviously, the only eigenvectors that are interesting for phase kickback are those that have an eigenvalue of -1. It's also pretty trivial to find out what those vectors are, and subsequently not too difficult at all to express them as Kronecker Products of the computational basis vectors.

$$\begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |001\rangle, \quad \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |010\rangle, \quad \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |100\rangle, \quad \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = |111\rangle,$$

So in other words, 3-qubit inputs with odd parity have eigenvalue -1, whereas those with even parity have eigenvalue 1. This is easily exploited by controlling the Z-gate with a static $|+\rangle$, and then applying a Hadamard transformation before measurement. That way, a phase of -1 will signify odd parity, and no phase change signifies even parity. Here's the circuit:

6

Problem 7.3.1a. Compute 118 mod 5

Solution.
$118\%5 = 3$ □

Problem I1. TBS

Solution.
TBS □