**18.435/2.111 Homework 6 Solutions**

**1:** A similar example of this is discussed in Nielsen and Chuang on page 92. The solution is easier to see if we label our 3 results as 'I know $|0\rangle$ did NOT occur,' 'I know $-\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$ did NOT occur,' and 'I can't conclude anything.' Thought of in that way, we should be able to quickly right down scaled versions of $|e_1\rangle = \alpha|1\rangle$ and $|e_2\rangle = \beta(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle)$. We can then obtain $|e_3\rangle$ by remembering that the POVM must sum to the identity: $\sum_{i=1}^{3}|e_i\rangle\langle e_i| = I \Rightarrow |e_3\rangle\langle e_3| = I - |e_1\rangle\langle e_1| - |e_2\rangle\langle e_2|$. All that is left is to make a reasonable choice for $\alpha$ and $\beta$ and to calculate $|e_3\rangle$. (Many of you may jump right to the solution by noting the carefully chosen states. That's fine, but we are going to walk through a more methodical approach.)

There are many feasible choices for $\alpha$ and $\beta$, as the only criteria is that $I - |e_1\rangle\langle e_1| - |e_2\rangle\langle e_2|$ must be positive semidefinite. Let's choose $\alpha = \beta$ (kind of an 'equally likely' choice), and also assume that they are real. We will choose $\alpha$ to be as large as possible, essentially minimizing the probability we will have to answer 'I don't know.'

$$\begin{aligned} |e_1\rangle\langle e_1| + |e_2\rangle\langle e_2| &= \alpha^2|1\rangle\langle 1| + \alpha^2(\frac{3}{4}|0\rangle\langle 0| + \frac{\sqrt{3}}{4}|1\rangle\langle 0| + \frac{\sqrt{3}}{4}|0\rangle\langle 1| + \frac{1}{4}|1\rangle\langle 1|) \\ &= \alpha^2 \begin{bmatrix} \frac{3}{4} & \frac{\sqrt{3}}{4} \\ \frac{\sqrt{3}}{4} & \frac{5}{4} \end{bmatrix} \end{aligned}$$

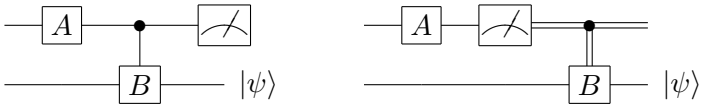
If we take the eigen-decomposition of the above matrix, we see that it has eigenvectors $\frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle$ and $\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$ associated with eigenvalues $\frac{3\alpha^2}{2}$ and $\frac{\alpha^2}{2}$. We want the larger of the eigenvalues to be 1, and so we choose $\alpha = \sqrt{\frac{2}{3}}$. From this, we can see that the proper choice of $|e_3\rangle$ is $\alpha(\frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle)$. This will complete the POVM such that $\sum_{i=1}^{3}|e_i\rangle\langle e_i| = I$. To summarize:

$$|e_1\rangle = \sqrt{\frac{2}{3}}|1\rangle \quad (1)$$

$$|e_2\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{6}}|1\rangle) \quad (2)$$

$$|e_3\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{6}}|1\rangle) \quad (3)$$

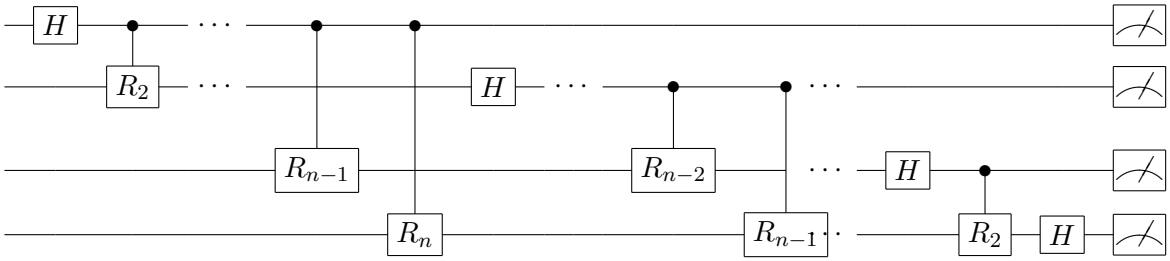
**2:** The first item of interest here is the 'principle of deferred measurement,' defined in Nielsen and Chuang section 4.4, which we will use in reverse. This states that the following two circuits are equivalent:



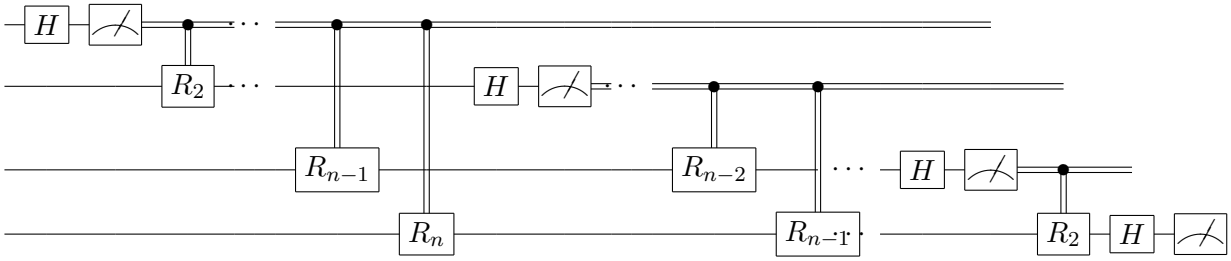

To make use of this equivalence in the measure QFT, we need to rearrange the QFT circuit derived in class and found in figure 5.1 of Nielsen and Chuang. We want to arrange the circuit so that for each qubit all of the single qubit gates and the control targets appear to the left and the controls appear to the right. This puts us in position to use the 'deferred measurement' equivalence. We can accomplish this by noting that the following two controlled gates are equivalent:


This means that it doesn't matter in our diagram which is the target and which is the control! We can understand this by noting that the control-$R_k$ gate applies the phase only when the observed state is $|11\rangle$.

Let's switch the control and target qubits for the circuit in 5.1 and add the measurement at the end.




Once we've done this, the deffered measurement equivalence gives us




This is circuit is now in the desired form.

**3:** We can show the probability of measuring a $|0\rangle$ by a straightforward analysis of the circuit. Beginning after the first Hadamard gate we have

$$\begin{aligned}
\frac{1}{\sqrt{2}}(|0\rangle|u\rangle + |1\rangle|u\rangle) &\rightarrow \frac{1}{\sqrt{2}}(|0\rangle|u\rangle + e^{2\pi i\phi}|1\rangle|u\rangle) \\
&\rightarrow \frac{1}{2}(|0\rangle|u\rangle + |1\rangle|u\rangle + e^{2\pi i\phi}|0\rangle|u\rangle - e^{2\pi i\phi}|1\rangle|u\rangle) \\
&= \frac{1}{2}((1+e^{2\pi i\phi})|0\rangle|u\rangle + (1-e^{2\pi i\phi})|1\rangle|u\rangle)
\end{aligned}$$

From this we can see that

$$\begin{aligned}
p &= \left|\frac{1+e^{2\pi i\phi}}{2}\right|^2 \\
&= \left|e^{\pi i\phi}\frac{e^{-\pi i\phi}+e^{\pi i\phi}}{2}\right|^2 \\
&= |e^{\pi i\phi}|^2 |cos\pi\phi|^2 \\
&= cos^2\pi\phi.
\end{aligned}$$

What does this tell us? Since $|u\rangle$ is still available, we can repeat the circuit as often as we want, and thus we can get an estimate for $p$ (*i.e.* the number of $|0\rangle$ divided by the number of trials). Are we done? No - we want to show an efficient method for obtaining $n$ bits of accuracy for $p$. That is to say, to learn $p$ to within $2^{-n}$ accuracy, we would need $O(2^n)$ trials.

This is where $\phi$ and the $U^k$ controlled gates come in. (I'm going to wave my hands at this argument, but you should get the idea.) Consider this - to know $p$ to $n$ bits, it is sufficient to know $\phi$ to $O(n)$ bits. Now notice that we can estimate the first bit of $\phi$ in a small number of trials learning $p$. How do we learn the $k^{th}$ bit of $\phi$? We replace $U$ with $U^{2^k}$. We are now estimating $p_k = cos^2\pi 2^k\phi$ and a small number of gates will get us a good estimate of the $k^{th}$ bit of $\phi$. This is a sketch of the algorithm to achieve $n$ bits of accuracy for estimating $p$ in polynomial time.