18.435/2.111 Homework # 5 Solutions

1:

We start with the system in the state

$$|\,0\rangle\,|\,u\rangle$$

After the Hadamard gate on the first bit, we obtain

$$\frac{1}{\sqrt{2}}(|\,0\rangle + |\,1\rangle)\,|\,u\rangle$$

After the control U gate, we get

$$\frac{1}{\sqrt{2}}(|\,0\rangle + e^{2i\pi\theta}\,|\,1\rangle)\,|\,u\rangle$$

Now, after the second Hadamard gate, we obtain

$$\frac{1}{2}[(|\,0\rangle + |\,1\rangle) + e^{2i\pi\theta}(|\,0\rangle - |\,1\rangle)]\,|\,u\rangle\,.$$

This is equal to

$$\frac{1}{2}[|\,0\rangle\,(1 + e^{2i\pi\theta}) + |\,1\rangle\,(1 - e^{2i\pi\theta})]\,|\,u\rangle\,.$$

which has probability of being measured as $|\,0\rangle$ of $|1 + e^{2i\pi\theta}|^2/4$, which is $\cos^2\pi\theta$.

For the second part, if you can approximate the fractional part of θ, 2θ, 4θ, 8θ, 16θ, etc., to within (say) one decimal place, you can combine all these observations to find θ exactly. Knowing $\cos^2\pi\theta$ doesn't quite let you do that — you can't tell the difference between θ and $1-\theta$. But this doesn't matter in approximating p, since $\cos^2\pi\theta = \cos^2\pi(1-\theta)$. So the idea is to approximate $p = \cos^2\pi\theta$ to (say) one decimal place by repeated observation, then approximate $cos^2\pi 2\theta$ by using U^2 in the circuit rather than U, and $\cos^2\pi 4\theta$ by using U^4, etc. This needs only a constant number of observations for U, U^2, U^4, etc, and so we get an efficient algorithm for approximating phase. Kitaev discovered this algorithm after hearing that the quantum factorization algorithm, when he could not get ahold of the details.

2: We want to take

$$|\,x\rangle \rightarrow \frac{1}{pq^{1/2}}\sum_{y=0}^{pq-1} e^{2\pi ixy/pq}\,|\,y\rangle$$

We will write $x = x_1p + x_2$ and $y = y_1q + y_2$. Now,

$$\begin{aligned} e^{2\pi ixy/pq} &= e^{2\pi i(x_1p+x_2)(y_1q+y_2)} \\ &= e^{2\pi ix_1y_2/q}e^{2\pi ix_2y_1/p}e^{2\pi ix_2y_2/pq} \end{aligned}$$

The $x_1 y_1$ term goes away because $e^{2\pi i n}$ is 1 if n is an integer. The first term on the second line is a QFT mod q. The second one is a QFT mod p. This only leaves the third term to worry about. This is a phase change that depends only on x_2 and y_2. So if we want to be able to apply this phase change, we need to have x_2 and y_2 around at the same time. We start out with $|\, x_1\rangle\, |\, x_2\rangle$. Now, if we first apply the FT mod q, which takes

$$|\, x_1\rangle\, |\, x_2\rangle \rightarrow \frac{1}{q^{1/2}} \sum_{y_2=0}^{q} e^{2i\pi x_1 y_2/q}\, |\, y_2\rangle\, |\, x_2\rangle$$

we get $|\, y_2\rangle\, |\, x_2\rangle$. We can then apply the phase change

$$|\, y_2\rangle\, |\, x_2\rangle \rightarrow e^{2i\pi x_2 y_2/pq}\, |\, y_2\rangle\, |\, x_2\rangle$$

and finally apply the Fourier transform mod p, which is

$$|\, y_2\rangle\, |\, x_2\rangle \rightarrow \frac{1}{p^{1/2}}\, |\, y_2\rangle \sum_{y_1=0}^{p} e^{2i\pi x_1 y_2/p}\, |\, y_1\rangle\, .$$

Combining these three transformation gives the quantum Fourier transform mod pq.o