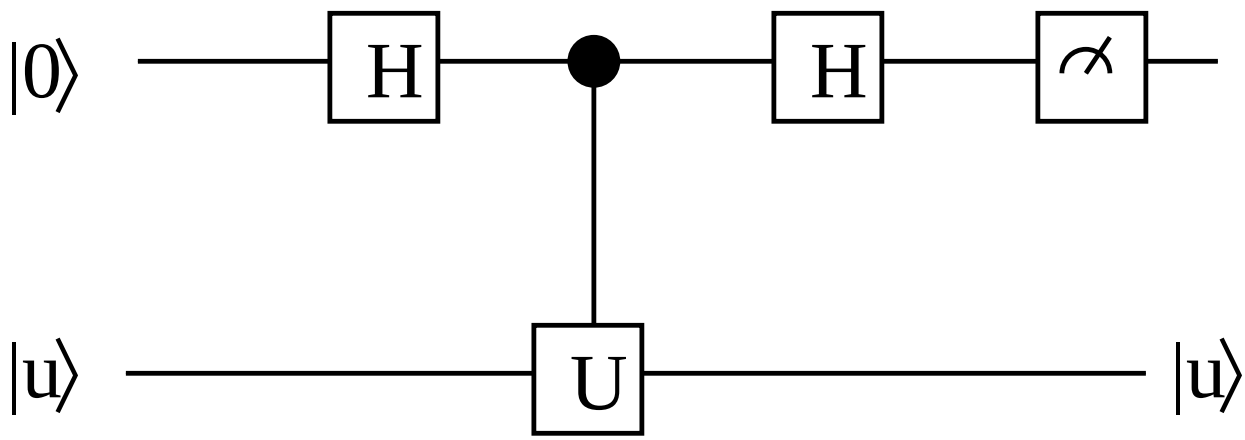
18.435/2.111 Homework # 5

Due Thursday, October 16.

1: Again, a problem from Nielsen and Chuang. This is Kitaev's algorithm for phase estimation. Consider the quantum circuit



where $|\,u\rangle$ is an eigenstate of U with eigenvalue $e^{2\pi i\theta}$. Show that the top qubit is measured to be 0 with probability $p = \cos^2 \pi\theta$. Since the state $|\,u\rangle$ is unaffected by the circuit, it may be reused. If U can be replaced by U^k, where k is an arbitrary integer, show that by repeating this circuit and increasing k appropriately, you can efficiently obtain as many bits of p as desired, and thus of ϕ.

2: Suppose that you have a quantum circuit for taking the quantum Fourier transform over Z_p and Z_q, where p and q are relatively prime. Show how you can combine these to take the Fourier transform over Z_{pq}. Specifically, you want to take

$$|\,x\rangle \to \frac{1}{\sqrt{pq}} \sum_{y=0}^{pq-1} e^{2\pi i xy/pq}\,|\,y\rangle\,.$$

Hint: try writing $x = x_1 p + x_2$ and $y = y_1 q + y_2$ where $0 \le x_1, y_2 \le q$ and $0 \le x_2, y_1 \le p$.