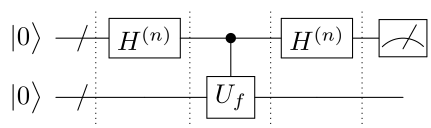
Dropbox submission folder link: https://www.dropbox.com/request/Xc4QIjV3LcbxbNBqD3gL

Problem Set 5: Periodicity

1. *Simon's Problem*— We are given a quantum black box which computes a 2-to-1 function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ on n bits. The function has an unknown periodicity a: $f(x) = f(y)$ if and only if $x = y \oplus a$ (bitwise mod 2 arithmetic). The following quantum circuit can be used to determine a efficiently:



   (a) Show the operation of the circuit by writing out the state $|\psi\rangle$ of the two registers at each time step shown by the dotted lines.

   (b) Show that the final measurement uniformly randomly produces an output y such that $y \cdot a = 0$.

   (c) Show that it requires at least exponentially many queries of $f(x)$ to find a by random classical sampling with a probability of failure less than ϵ.

2. Show that the quantum Fourier transform on an N-dimensional Hilbert space,

$$QFT : |x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i x y / N} |y\rangle \tag{1}$$

   is unitary.

3. Compute the QFT of the n-qubit state $|\psi\rangle = |0000\cdots 0\rangle$. How does this relate to the n-qubit Hadamard transform of $|\psi\rangle$?

4. Nielsen and Chuang, Exercise 5.7

5. Nielsen and Chuang, Exercise 5.18 (Factoring 91)

6. Nielsen and Chuang, Problem 5.3 (Kitaev's algorithm)