CS333 - Problem Set 8

See final page for hints.

1. Quantum Fourier Transform and Period Finding. For a standard basis states $|x\rangle \in \mathbb{C}^t$,

$$QFT_t|x\rangle = \frac{1}{\sqrt{t}}\sum_{y=0}^{t-1} e^{2\pi ixy/t}|y\rangle; \qquad QFT_t^{-1}|x\rangle = \frac{1}{\sqrt{t}}\sum_{y=0}^{t-1} e^{-2\pi ixy/t}|y\rangle \tag{1}$$

   (a) Show that

$$QFT_t|0\rangle = \frac{1}{\sqrt{t}}\sum_{y=0}^{t-1}|y\rangle. \tag{2}$$

   (b) Show that QFT_t^{-1} really is the inverse of QFT. In other words, show:

$$QFT_t^{-1}QFT_t = I. \tag{3}$$

   (c) Given a function f, let $P_k(f(x)) = f(x+k)$. What is a connection between P_k and period finding? (There is nothing quantum in this problem.)

   (d) Let P denote the unitary operation that adds 1 modulo t. In other words, for any $x \in \{0, 1, \ldots, t-1\}$, $P|x\rangle = |x + 1 \bmod t\rangle$. Show that the states that result from applying QFT_t to standard basis states are eigenvectors of P. That is, show

$$P\frac{1}{\sqrt{t}}\sum_{y=0}^{t-1} e^{2\pi ixy/t}|y\rangle = \lambda_y \frac{1}{\sqrt{t}}\sum_{y=0}^{t-1} e^{2\pi ixy/t}|y\rangle \tag{4}$$

   where λ_y is a complex number. What is λ_y? (This problem is meant to show you that there is some relationship between periodic functions and Fourier states.)

2. Let p be a prime number. Suppose you are given a black-box function $f\colon \{0,1,\ldots,p-1\} \times \{0,1,\ldots,p-1\} \to \{0,1,\ldots,p-1\}$ such that $f(x,y) = f(x',y')$ if and only if $y' - y = m(x'-x) \bmod p$ for some unknown integer m. In other words $f(x, mx+b) = C_b$, where C_b is a constant that depends on b. This means that for all points on the line $y = mx + b$, f has the same value. However, for different values of b, the function takes different values. Your goal is to determine $m \bmod p$ using as few queries as possible to f, which is given by a unitary operation U_f satisfying $U_f|x\rangle_A|y\rangle_B|z\rangle_C = |x\rangle_A|y\rangle_B|(z + f(x,y)) \bmod p\rangle_C$ for all $x, y, z \in \{0,1,\ldots,p-1\}$. (Note that each of the three registers is a p-dimensional state.)

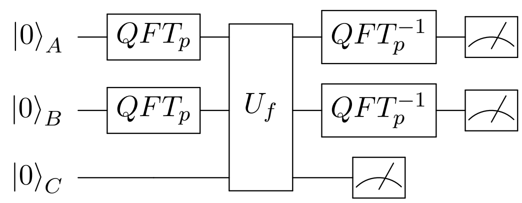
(a) **[3 points]** Consider the case that $p = 3$. Here is a truth table for a function of the above form. What is m?

x	y	$f(x,y)$
0	0	1
0	1	2
0	2	0
1	0	2
1	1	0
1	2	1
2	0	0
2	1	1
2	2	2

(5)

(b) What is the classical query complexity of this problem?

(c) Consider the following circuit (which is very similar to the period finding circuit!!)



(6)

i. What is the state of the system after the first time step (the two parallel QFTs)?

ii. Show that the state after applying U_f is

$$\frac{1}{\sqrt{p}} \sum_{b=0}^{p-1} \left(\frac{1}{\sqrt{p}} \sum_{x=0}^{p-1} |x, mx + b\rangle_{AB} \right) |f(0,b)\rangle_C. \tag{7}$$

iii. Argue that when we measure register C, each outcome occurs with equal probability. If the outcome is $|f(0,b^*)\rangle$, what is the state of the system after measurement?

iv. If the outcome on register C is $|f(0,b^*)\rangle$, show that the final state after the last two inverse QFTs is

$$\frac{1}{\sqrt{p}^3} \sum_{j,l=0}^{p-1} e^{-2\pi i l b^*/p} \left(\sum_{x=0}^{p-1} e^{-2\pi i x(j+lm)/p} \right) |j\rangle|l\rangle \tag{8}$$

v. Explain why when you measure the remaining state in the standard basis, you will get an outcome $|j\rangle|l\rangle$ where $j \equiv -lm \mod p$.

vi. It is a fact from number theory that every number except 0 has a multiplicative inverse $\mod p$. In otherwords, if $j \not\equiv 0 \mod p$, there exists j^{-1} such that $jj^{-1} \equiv 1 \mod p$. Use this fact to explain how to learn m from the outcome of the final measurement.

Hints!

- $1b$: There are several ways to do this, but one way is to show that the operation takes every standard basis state to itself.
- $2ci$: Since $y = mx + b$, we can replace the variable y with the expression $mx + b$. Then $f(x, mx + b) = f(0, b)$ for all x because of the promise.