QIC710/CS768/CO681/PH767/AM871 Introduction to Quantum Information Processing (F19)

Assignment 3
Due date: October 24, 2019

1. **Quantum Fourier transform modulo 3^n on n qutrits [10 points]**. Assume that you have n *qutrit* registers (with computational basis $\{|0\rangle, |1\rangle, |2\rangle\}$). Give a circuit consisting of $O(n^2)$ one- and two-qutrit gates that computes F_{3^n}, the Fourier transform modulo 3^n. Explain why it works.

2. **Interpolating a linear function with a single quantum query [10 points, 5 each].** Let p be prime and $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be a function of the form $f(x) = ax + b \bmod p$, where $a, b \in \mathbb{Z}_p$ are unknown coefficients, and your goal is to determine the coefficient a with as few queries to f as possible (you do *not* have to determine coefficient b).

   (a) Suppose that you are given a black-box that reversibly computes f as $(x, y) \mapsto (x, y + f(x) \bmod p)$, for all $x, y \in \mathbb{Z}_p$. Show that two classical queries are necessary to deduce a.

   (b) Suppose that you are given a black-box unitary that reversibly computes f as $|x\rangle|y\rangle \mapsto |x\rangle|y + f(x) \bmod p\rangle$, for all $x, y \in \mathbb{Z}_p$. Show that one quantum query is sufficient to deduce a. (Hint: you may use the quantum Fourier transform F_p and/or $F_p^\dagger$.)

3. **Distinguishing states by local measurements [12 points, 3 each].** In this question, we suppose Alice and Bob (who are physically separated from each other, say, in separate labs) are each given one of the qubits of some two-qubit state. Working as a team, they are required to distinguish between State I and State II with only *local* measurements. We will take this to mean that they can each perform a one-qubit unitary operation and then a measurement (in the computational basis) on their own qubit. After their measurements, they can send only *classical* bits to each other.

   In each case below, either give a perfect distinguishing procedure (that never errs) or explain why there is no perfect distinguishing procedure (i.e., that for any procedure the success probability must be less than 1).

   (a) State I: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
   State II: $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$

   (b) State I: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
   State II: $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$

   (c) State I: $\frac{1}{\sqrt{2}}(|00\rangle + i|11\rangle)$ $\quad (i = \sqrt{-1})$
   State II: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

   (d) State I: $\frac{1}{\sqrt{2}}(|00\rangle + i|11\rangle)$
   State II: $\frac{1}{\sqrt{2}}(|00\rangle - i|11\rangle)$

CONTINUED ON NEXT PAGE

4. **Period-finding algorithm in an idealized setting [16 points].** Suppose that $m = pq$, where p and q are n-bit primes. Define $f : \mathbb{Z}_m \to \mathbb{Z}_m$ to be a *strictly p-periodic* if it has the property that $f(x) = f(y)$ if and only if $x - y$ is a multiple of p.

   Assume we are given m but not its factorization, and our goal is to efficiently determine p. Suppose that we have an efficient implementation of m-dimensional registers and also the unitary U_f for some strictly p-periodic $f : \mathbb{Z}_m \to \mathbb{Z}_m$, where $U_f|x\rangle|y\rangle = |x\rangle|y + f(x) \bmod m\rangle$ (for all $x, y \in \mathbb{Z}_m$). In addition, suppose that we have an efficient implementation of F_m, the quantum Fourier transform modulo m. We will show how to efficiently determine p. The first step is to apply F_m and U_f once to construct the state

$$U_f(F_m \otimes I)|0\rangle|0\rangle = \frac{1}{\sqrt{m}} \sum_{x \in \mathbb{Z}_m} |x\rangle|f(x)\rangle. \tag{1}$$

   (a) [2 points] Explain why, if the second register of the above state is measured, then the state of the first register is of the form

$$|\psi_s\rangle = \frac{1}{\sqrt{q}}\Big(|s\rangle + |s+p\rangle + |s+2p\rangle + \cdots + |s+(q-1)p\rangle \Big) = \frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |s + xp\rangle \tag{2}$$

   for some $s \in \mathbb{Z}_p$.

   (b) [5] Show that, if F_m is applied to the state

$$|\psi_0\rangle = \frac{1}{\sqrt{q}}\Big(|0\rangle + |p\rangle + |2p\rangle + \cdots + |(q-1)p\rangle \Big) = \frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |xp\rangle \tag{3}$$

   then the result is

$$F_m|\psi_0\rangle = \frac{1}{\sqrt{p}}\Big(|0\rangle + |q\rangle + |2q\rangle + \cdots + |(p-1)q\rangle \Big) = \frac{1}{\sqrt{p}} \sum_{x=0}^{p-1} |xq\rangle. \tag{4}$$

   (c) [5] In part (b), we have an expression for $F_m|\psi_0\rangle$. What is $F_m|\psi_s\rangle$, for an arbitrary $s \in \mathbb{Z}_p$? (Hint: expressed in the computational basis, the amplitudes have the same absolute value as those for $F_m|\psi_0\rangle$.)

   (d) [4] Suppose that $F_m|\psi_s\rangle$ is measured in the computational basis, yielding result z. For the case where $z \neq 0$, explain how to efficiently compute the periodicity p from z. You can assume that there is an efficient algorithm for computing the greatest common divisor of two integers, which can be called as a subroutine.

CONTINUED ON NEXT PAGE

5. **Entanglement among three qubits [12 points, 4 each].** Suppose that Alice, Bob and Carol each possess a qubit and that the joint state of their three qubits is $|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$.

   (a) Suppose that Carol leaves the scene, taking her qubit with her, and without communicating with either Alice or Bob. Consider the two-qubit state of Alice and Bob's qubits. Is this state equivalent to $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$? Justify your answer.

   (b) Suppose again that Carol leaves the scene, taking her qubit with her, but she is allowed to send one classical bit to Alice. Carol wants to help Alice and Bob transform their state into the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ (and without Alice and Bob having to send any messages between each other). The framework is as follows:

      i. Carol applies some unitary operation U to her qubit, and then measures the qubit, yielding the classical bit b.

      ii. Carol sends just the classical bit b to Alice.

      iii. Alice applies a unitary operation, depending on b, to her qubit. In other words, Alice has two unitary operations V_0 and V_1, and she applies V_b to her qubit.

      At the end of this procedure, the two-qubit state of state of Alice and Bob's qubits should be $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Explain how to make this procedure work.

   (c) Is it possible for Alice, Bob and Carol to each possess a qubit such that the joint state of the three qubits has both of the following properties at the same time?

      Property 1: The two-qubit state of Alice and Bob's qubits is $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

      Property 2: The two-qubit state of Bob and Carol's qubits is $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

      Either give an example of a three-qubit state with these properties or show that such a state does not exist.