QIC710/CS678/CO681/PH767/AM871 Introduction to Quantum Information Processing (F13)

Assignment 3
Due date: October 24, 2013

1. **A version of Simon's problem modulo m (quantum part of the algorithm).** Let m be some n-bit number ($2^{n-1} < m < 2^n$) and assume that we are given a black box computing $f : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$ that is promised to have the property: $f(a_1, a_2) = f(b_1, b_2)$ if and only if $(a_1, a_2) - (b_1, b_2) \in S$, where $S = \{k(r, 1) : k \in \mathbb{Z}_m\}$ for some unknown $r \in \mathbb{Z}_m$. Let the goal be to compute r.

   Also, assume that we have a good implementation of F_m, the quantum Fourier transform modulo m, and its inverse $F_m^\dagger$. (Technically, F_m can be defined in a qubit setting as an n-qubit unitary operation, where on the basis states that are out of range, namely $|a\rangle$ with $a \in \{m, \ldots, 2^n - 1\}$, some other arbitrary unitary operation is applied.)

   In class, we considered a quantum algorithm that proceeds as follows.

   1. Initialize three quantum $\mathbb{Z}_m$-registers, each to state $|0\rangle$.
   2. Apply F_m to the first and second register.
   3. Compute f (with inputs from registers 1 and 2 and output added to register 3).
   4. Apply $F_m^\dagger$ to the first and second register.
   5. Measure the first and second register (and ignore the third register).

   Let the two outcome values of the measurement be $(s_1, s_2) \in \mathbb{Z}_m \times \mathbb{Z}_m$. Begin by convincing yourself that the state of the system just after step 3 is completed is

$$\frac{1}{m} \sum_{x_1=0}^{m-1} \sum_{x_2=0}^{m-1} |x_1\rangle |x_2\rangle |f(x_1, x_2)\rangle.$$

   In this question, we will show that, after step 5 is completed, for each $(s_1, s_2) \in \mathbb{Z}_m \times \mathbb{Z}_m$,

$$\text{Prob}[\,\text{outcome is } (s_1, s_2)] = \begin{cases} \frac{1}{m} & \text{if } (s_1, s_2) \cdot (r, 1) = 0 \\ 0 & \text{if } (s_1, s_2) \cdot (r, 1) \neq 0. \end{cases} \tag{1}$$

   (a) For each $a \in \mathbb{Z}_m$, define $S_a = S + (a, 0)$ (meaning that $(a, 0)$ is added to every element of S, modulo m). Prove that $S_0, S_1, \ldots, S_{m-1}$ form a *partition* of $\mathbb{Z}_m \times \mathbb{Z}_m$, in the sense that:

      i. For all $a \neq b$, $S_a \cap S_b = \emptyset$

      ii. $S_0 \cup S_1 \cup \cdots \cup S_{m-1} = \mathbb{Z}_m \times \mathbb{Z}_m$.

   (b) Prove that $f(x_1, x_2) = f(y_1, y_2)$ if and only if (x_1, x_2) and (y_1, y_2) are in the same element of the above partition (in other words, $(x_1, x_2), (y_1, y_2) \in S_a$, for some a).

   (c) Prove that Equation (1) holds. (Hint: you may use the results of parts (a) and (b).)

2. **Determining the leading coefficient of a "linear" function.** Let m be any integer greater than 1. Consider the problem where one is given black-box access to a function $f : \mathbb{Z}_m \to \mathbb{Z}_m$ such that $f(x) = ax + b$ (arithmetic modulo m), for unknown parameters $a, b \in \mathbb{Z}_m$, and the goal is to determine the coefficient a. The reversible form of the black box is: $(x, y) \mapsto (x, y + f(x))$ (addition modulo m).

   (a) Show that there is a classical algorithm solving this problem with 2 queries, and that 2 queries are *required* classically.

   (b) Show that there is a quantum algorithm that solves this problem with 1 query to the reversible black box for f. (Hint: you may use the quantum Fourier transform F_m and/or $F_m^\dagger$ and consider setting the target register to the state $F_m^\dagger|1\rangle$.)

   (c) **Optional for bonus credit:** Consider the extension of the above where the function is quadratic, $f(x) = ax^2 + bx + c$ (arithmetic modulo m), for unknown parameters $a, b, c \in \mathbb{Z}_m$, and the goal is to determine the coefficient a. For this part, assume that m is prime and $m > 2$. Show that: (i) any classical algorithm solving this problem requires 3 queries to f; (ii) there is a quantum algorithm that solves this problem with 2 queries to f (the reversible black box for f).

3. **Period inversion.** Let p and q be integers greater than 1, and pq denote their product. Recall that the quantum Fourier transform modulo pq is the pq-dimensional unitary operation F_{pq} such that

$$F_{pq}|x\rangle = \frac{1}{\sqrt{pq}} \sum_{y=0}^{pq-1} \left(e^{2\pi i/pq}\right)^{xy} |y\rangle$$

   for each $x \in \mathbb{Z}_{pq}$.

   (a) Define two quantum states $|\psi_1\rangle$ and $|\psi_2\rangle$ as

$$|\psi_1\rangle = \frac{1}{\sqrt{q}} (\,|0\rangle + |p\rangle + |2p\rangle + \cdots + |(q-1)p\rangle\,) = \frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |xp\rangle$$

   and

$$|\psi_2\rangle = \frac{1}{\sqrt{p}} (\,|0\rangle + |q\rangle + |2q\rangle + \cdots + |(p-1)q\rangle\,) = \frac{1}{\sqrt{p}} \sum_{x=0}^{p-1} |xq\rangle.$$

   Show that $F_{pq}|\psi_1\rangle = |\psi_2\rangle$.

   (b) Let $s \in \{0, 1, \ldots, p-1\}$, and define $|\psi_3\rangle$ (a "shifted" version of $|\psi_1\rangle$) as

$$\begin{aligned} |\psi_3\rangle &= \frac{1}{\sqrt{q}} (\,|s\rangle + |s+p\rangle + |s+2p\rangle + \cdots + |s+(q-1)p\rangle\,) \\ &= \frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |s + xp\rangle. \end{aligned}$$

   What is $F_{pq}|\psi_3\rangle$? Find a simple expression for this quantity. If $F_{pq}|\psi_3\rangle$ is measured in the computational basis, what is the probability distribution describing the outcome?

4. **Some consequences of putting inputs to unitaries in superposition.**

   (a) Let U be any n-qubit unitary, $|\psi_1\rangle$, $|\psi_2\rangle$ be orthogonal n-qubit states, and $a_1, a_2 \in \{0,1\}^n$ such that the following property holds. For each $j \in \{1,2\}$, if $U|\psi_j\rangle$ is measured in the computational basis then the outcome is a_j for sure (i.e., with probability 1). Let α_1, α_2 be such that $|\alpha_1|^2 + |\alpha_2|^2 = 1$. Does it follow that, if $U(\alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle)$ is measured in the computational basis, then the outcome is

   $$\begin{cases} a_1 & \text{with probability } |\alpha_1|^2 \\ a_2 & \text{with probability } |\alpha_2|^2? \end{cases}$$

   Either prove it or give a counterexample.

   (b) Let U be any n-qubit unitary, $|\psi_1\rangle$ and $|\psi_2\rangle$ be orthogonal n-qubit states, and $a_1, b_1, a_2, b_2 \in \{0,1\}^n$ such that the following property holds. For each $j \in \{1,2\}$, if $U|\psi_j\rangle$ is measured in the computational basis then the outcome is

   $$\begin{cases} a_j & \text{with probability } p_j \\ b_j & \text{with probability } q_j \end{cases}$$

   (where $p_k + q_k = 1$). Let α_1, α_2 be such that $|\alpha_1|^2 + |\alpha_2|^2 = 1$. Does it follow that if $U(\alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle)$ is measured in the computational basis then the outcome is

   $$\begin{cases} a_1 & \text{with probability } p_1|\alpha_1|^2 \\ b_1 & \text{with probability } q_1|\alpha_1|^2 \\ a_2 & \text{with probability } p_2|\alpha_2|^2 \\ b_2 & \text{with probability } q_2|\alpha_2|^2. \end{cases}$$

   Either prove it or give a counterexample.

5. **More consequences of putting inputs to unitaries in superposition.** This question is sort of a continuation of question 4, and pertains to a detail that arose in the quantum algorithm for order-finding that was discussed in class. Let W denote a generalized n-qubit controlled-U gate (i.e., for all $x, y \in \{0,1\}^n$, $W|x\rangle|y\rangle = |x\rangle U^x|y\rangle$) and let $|\psi_1\rangle$, $|\psi_2\rangle$ be two orthogonal eigenvectors of U. Let V be any n-qubit unitary (for order-finding, this was the inverse QFT $F^\dagger$). Also, let $|\phi\rangle$ be any n-qubit state initial state for the control-qubits of W (for order-finding, this was $\frac{1}{2^{n/2}}\sum_x |x\rangle$). Suppose that the following property holds. For each $j \in \{1,2\}$, if *the first register (i.e., the first n qubits)* of $(V \otimes I)W|\phi\rangle|\psi_j\rangle$ is measured in the computational basis then the outcome is

   $$\begin{cases} a_j & \text{with probability } p_j \\ b_j & \text{with probability } q_j \end{cases}$$

   (where $p_k + q_k = 1$). Prove that then, if *the first register of* $(V \otimes I)W|\phi\rangle(\alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle)$ is measured in the computational basis, the outcome is

   $$\begin{cases} a_1 & \text{with probability } p_1|\alpha_1|^2 \\ b_1 & \text{with probability } q_1|\alpha_1|^2 \\ a_2 & \text{with probability } p_2|\alpha_2|^2 \\ b_2 & \text{with probability } q_2|\alpha_2|^2. \end{cases}$$