QIC710/CS667/CO681/PH767/AM871 Introduction to Quantum Information Processing (F12)

Assignment 3
Due date: October 23, 2012

1. **Quantum Fourier transform.** Let F_m denote the m-dimensional Fourier transform

$$F_m = \frac{1}{\sqrt{m}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{m-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(m-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{m-1} & \omega^{2(m-1)} & \cdots & \omega^{(m-1)^2} \end{pmatrix}, \quad \text{where } \omega = e^{2\pi i/m} \ (i = \sqrt{-1})$$

(an $m \times m$ matrix, whose entry in position jk is $\frac{1}{\sqrt{m}}(e^{2\pi i/m})^{jk}$ for $j, k \in \{0, 1, \ldots, m-1\}$).

   (a) As a warm-up exercise, show that, for all $j \in \{1, 2, \ldots, m-1\}$, $\sum_{k=0}^{m-1} \omega^{jk} = 0$.

   (b) Show that any two rows of F_m are orthonormal.

   (c) What is $(F_m)^2$? The matrix has a very simple form.

2. **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 $(s_1, s_2) \in \mathbb{Z}_m \times \mathbb{Z}_m$,

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

(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).)

3. **A version of Simon's problem modulo m (classical post-processing part of the algorithm).**

   Once we obtain the outcome of the measurement in the procedure for Simon's algorithm mod m, we still need to compute r. Assume from Question 2 that we obtain (s_1, s_2) satisfying Equation (1). In class we saw that r can be computed whenever $\gcd(s_1, m) = 1$. Here we address the question of showing that the probability that s_1 satisfies $\gcd(s_1, m) = 1$ is not too small, resulting in overall polynomial efficiency.

   (a) Show that, whatever the value of r is, s_1 is uniformly distributed over the set $\mathbb{Z}_m$.

   (b) *Euler's totient function* $\phi(m)$ is defined as the size of the set of all numbers in $\{1, 2, \ldots, m-1\}$ that are relatively prime to m (that is, whose gcd with respect to m is 1). It is known that $\phi(m) \geq cm/\log\log(m)$ for some constant c (let us assume this fact for this question). Explain why this (and the result in part (a)) implies that the probability that $\gcd(s_1, m) = 1$ is at least a constant times $1/\log(n)$ (where n is the number of bits of m). If $\gcd(s_1, m) \neq 1$, the algorithm described in Question 2 can be run again, yielding a fresh pair (s_1, s_2); what is the expected number of repetitions required until $\gcd(s_1, m) = 1$ will occur?

   (Note: there is an even more efficient approach than re-running the algorithm whenever $\gcd(s_1, m) \neq 1$, but we omit this here.)

4. **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 $F_m^\dagger|1\rangle$.)

5. **Distinguishing states by local measurements.** 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: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

6. **Optional Bonus Question: leading coefficient of a "quadratic" function.**

   This is just like question 4, except $f(x) = ax^2+bx+c$ (arithmetic modulo m), for unknown parameters $a, b, c \in \mathbb{Z}_m$, and the goal is to determine the coefficient a. Unlike question 4, assume that m is prime and $m > 2$.

   (a) Show that there is a classical algorithm solving this problem with 3 queries, and that 3 queries are *required* classically.

   (b) Show that there is a quantum algorithm that solves this problem with 2 queries to the reversible black box for f.

   (c) **Extra challenge:** show that this problem cannot be solved with 1 quantum query. (Warning: this is meant to be a significant challenge; don't get bogged down by this question.)