QIC710/CS667/CO681/PH767/AM871 Introduction to Quantum Information Processing (F11)

Assignment 3 (slightly **re-**revised in question 1)
Due date: October 27, 2011

1. **A version of Simon's problem modulo p.** Let p be some large prime number ($2^{n-1} < p < 2^n$) and assume that we are given a black box computing $f : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$ 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 $S = \{k(r_1, r_2) : k \in \mathbb{Z}_p\}$ for some unknown $(r_1, r_2) \in \mathbb{Z}_p \times \mathbb{Z}_p$. Note that S does not uniquely determine (r_1, r_2), because any non-zero multiple of (r_1, r_2) also generates S.

   Also, assume that we have a good implementation of F_p, the quantum Fourier transform modulo p, and its inverse $(F_p)^\dagger$. Technically, F_p 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 $a \in \{p, \ldots, 2^n - 1\}$, some other arbitrary unitary operation is applied).

   (a) Describe and analyze a quantum algorithm that makes a single query to the black box for f and produces an $(s_1, s_2) \in \mathbb{Z}_p \times \mathbb{Z}_p$ with uniform probability conditioned on $(s_1, s_2) \cdot (r_1, r_2) = 0$.

   (b) Show how, after one instances of the process in part (a), a non-zero multiple of (r_1, r_2) can be efficiently determined with high probabilitry.

2. **Parity of three bits?** Recall the quantum algorithm for computing $f(0) \oplus f(1)$ with a single query to $f : \{0, 1\} \to \{0, 1\}$. This algorithm first constructs the state

$$\tfrac{1}{\sqrt{2}}(-1)^{f(0)}|0\rangle + \tfrac{1}{\sqrt{2}}(-1)^{f(1)}|1\rangle$$

   with a single query to f and then performs a measurement on this state to exactly determine $f(0) \oplus f(1)$.

   Consider the possibility of generalizing this approach to computing $g(0) \oplus g(1) \oplus g(2)$ with a single query to $g : \{0, 1, 2\} \to \{0, 1\}$. It is straightforward to construct the state

$$\tfrac{1}{\sqrt{3}}(-1)^{g(0)}|0\rangle + \tfrac{1}{\sqrt{3}}(-1)^{g(1)}|1\rangle + \tfrac{1}{\sqrt{3}}(-1)^{g(2)}|2\rangle$$

   with a single query to g.

   Is there a measurement of this state that deduces the value of $g(0) \oplus g(1) \oplus g(2)$? Either give the measurement or explain why such a measurement is impossible.

3. **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: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

4. **Generalized form of period-finding by quantum algorithms.** Let $\sigma : \{0,1\}^n \to \{0,1\}^n$ be a bijection (hence a permutation on the set $\{0,1\}^n$). Let $z \in \{0,1\}^n$. Then the sequence

$$z, \sigma(z), \sigma(\sigma(z)), \sigma(\sigma(\sigma(z))), \ldots \quad = \quad \sigma^{(0)}(z), \sigma^{(1)}(z), \sigma^{(2)}(z), \sigma^{(3)}(z), \ldots$$

eventually comes back to z. Consider the size of this cycle: that is, the minimum $r > 0$ such that $\sigma^{(r)}(z) = z$. Suppose that we are given a black box for the mapping

$$|x\rangle|y\rangle \mapsto |x\rangle|\sigma^{(x)}(y)\rangle,$$

where $x, y \in \{0,1\}^n \equiv \{0, 1, 2, \ldots, 2^n - 1\}$. Suppose that we are also promised that $r \leq 2^{n/2}$, but that otherwise r is unknown to us, and our goal is to determine r. Let $\omega = e^{2\pi i/r}$, and $|\phi\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \omega^s |\sigma^{(s)}(z)\rangle$.

Show that there is a quantum circuit that, given the additional help of one copy of $|\phi\rangle$, determines r with a single query to the black box, plus an additional number of 1- and 2-qubits gates that is polynomial in n.

(Note: r can also be determined with a constant number of queries to the black box *without* being provided with any special quantum state; however, you are not asked to show this here.)

5. **Classical and quantum algorithms for the AND problem.** Recall that, for Deutsch's problem, there is a function $f : \{0,1\} \to \{0,1\}$ and the goal is to determine $f(0) \oplus f(1)$ with a *single* query to f. There is no classical algorithm that succeeds with probability more than $1/2$, whereas there is a quantum algorithm that succeeds with probability 1. This question pertains to a variation of Deutsch's problem, which we'll call the AND problem, where the goal is to determine $f(0) \wedge f(1)$ with a single query to f. ($\wedge$ denotes the logical AND operation.)

(a) Give a classical probabilistic algorithm that makes a single query to f and predicts $f(0) \wedge f(1)$ with probability at least $2/3$. (The probability is respect to the random choices of the algorithm; the input instance of f is assumed to be *worst-case*.)

It turns out that no classical algorithm can succeed with probability greater than $2/3$ (but you are not asked to show this here).

(b) Give a quantum circuit that, with a single query to f, constructs the two-qubit state

$$\tfrac{1}{\sqrt{3}}\left((-1)^{f(0)}|00\rangle + (-1)^{f(1)}|01\rangle + |11\rangle\right).$$

(c) The quantum states of the form in part (a) are three-dimensional and have real-valued amplitudes. This makes it easy for us to visualize the geometry of these states (as vectors or lines in $\mathbb{R}^3$). Consider the four possible states that can arise from part (a), depending on which of the four possible functions f is. What is the absolute value of the inner product between each pair of those four states?

(d) Based on parts (b) and (c), give a quantum algorithm for the AND problem that makes a single query to f and: succeeds with probability 1 whenever $f(0) \wedge f(1) = 1$; succeeds with probability 8/9 whenever $f(0) \wedge f(1) = 0$.

(e) Note that the error probability of the algorithm from part (d) is one-sided in the sense that it is always correct in the case where $f(0) \wedge f(1) = 1$. Give a quantum algorithm for the AND problem that makes a single query to f and succeeds with probability 9/10. (Hint: take the output of the one-sided error algorithm from part (d) and do some classical post-processing on it, in order to turn it into a two-sided error algorithm with higher success probability.)

6. **Optional bonus question: leading coefficients of quadratic polynomials.** Consider the problem where one is given black-box access to a function $f : \mathbb{Z}_3 \to \mathbb{Z}_3$ such that $f(x) = ax^2 + bx + c$ (arithmetic here is modulo 3), where $a, b, c \in \mathbb{Z}_3$ are unknown coefficients. The goal is to determine the coefficient a.

(a) Show that any classical algorithm for this problem must make 3 queries.

(b) Give a quantum algorithm for this problem that makes only 2 queries.