CS667/CO681/PH767/AM871 Quantum Information Processing (Fall 09)

Assignment 3

Due date: October 27, 2009

1. **Simon's problem modulo p.** Let p be some large prime number and assume that we are given a black box computing $f : \mathbb{Z}_p \times \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ that is promised to have the following property. There exists $(r_1, r_2) \in \mathbb{Z}_p \times \mathbb{Z}_p$ such that $(r_1, r_2) \neq (0, 0)$ and $f(a_1, a_2) = f(b_1, b_2)$ if and only if $(a_1, a_2) - (b_1, b_2)$ is a multiple of (r_1, r_2) (the multiples of (r_1, r_2) are $\{k(r_1, r_2) : k \in \mathbb{Z}_p\}$).

   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 $2^{n-1} < p \leq 2^n$. On the basis states that are out of range ($|a\rangle$ with $a \in \{p, \ldots, 2^n - 1\}$) some other arbitrary unitary operation is applied. For any state in range, F_p is applied to it.

   Describe a quantum algorithm that determines (r_1, r_2) with high probability after only two queries to f.

2. **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 A and State B 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 A: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
   State B: $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$

   (b) State A: $|00\rangle$
   State B: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

   (c) State A: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
   State B: $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$

3. **Approximating unitary transformations.** There are frequent situations where it is much easier to approximate a unitary transformation than to compute it exactly. For a vector $v = (v_0, \ldots, v_{m-1})$, let $||v|| = \sqrt{\sum_{j=0}^{m-1} |v_j|^2}$, which is the usual Euclidean length of v. For an arbitrary $m \times m$ matrix M, define its *norm* $||M||$ as

$$||M|| = \max_{|\psi\rangle} ||M|\psi\rangle||,$$

   where the maximum is taken over quantum states (i.e., vectors $|\psi\rangle$ such that $|||\psi\rangle|| = 1$). We can now define the *distance* between to $m \times m$ unitary matrices U_1 and U_2 as $||U_1 - U_2||$.

(a) Show that if $||U_1 - U_2|| \leq \epsilon$ then, for any quantum state $|\psi\rangle$, $||U_1|\psi\rangle - U_2|\psi\rangle|| \leq \epsilon$.

(b) Show that $||A - B|| \leq ||A - C|| + ||C - B||$, for any three $m \times m$ matrices A, B, and C. (Thus, this distance measure satisfies the *triangle inequality.*)

(c) Show that $||A \otimes I|| = ||A||$ for any $m \times m$ matrix A and the $l \times l$ identity matrix I.

(d) Show that $||U_1 A U_2|| = ||A||$, for any $m \times m$ matrix A and any two $m \times m$ unitary matrices U_1 and U_2.

4. **Approximate quantum Fourier transform modulo** 2^n. Recall that in class we saw how to compute the QFT modulo 2^n by a quantum circuit of size $O(n^2)$. Here, we consider how to compute an approximation of this QFT within ϵ by a quantum circuit of size $O(n \log(n/\epsilon))$.

(a) Recall that the $O(n^2)$ size QFT quantum circuit uses gates of the form

$$P_k = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{2\pi i/2^k} \end{pmatrix},$$

for values of k that range between 2 and n. Show that $||P_k - I|| \leq 2\pi/2^k$, where I is the 4×4 identity matrix. (Thus, P_k gets very close to I when k increases.)

(b) The idea behind the approximate QFT circuit is to start with the $O(n^2)$ circuit and then remove some of its P_k gates. Removing a P_k gate is equivalent to replacing it with an I gate. Removing a P_k gate makes the circuit smaller but it also changes the unitary transformation. From part (a) and the general properties of our measure of distance between unitary transformations in the previous question, we can deduce that if k is large enough then removing a P_k gate changes the unitary transformation by only a small amount. Show how to use this approach to obtain a quantum circuit of size $O(n \log(n/\epsilon))$ that computes a unitary transformation $\tilde{F}_{2^n}$ such that

$$||\tilde{F}_{2^n} - F_{2^n}|| \leq \epsilon.$$

(Hint: Try removing all P_k gates where $k \geq t$, for some carefully chosen threshold t. The properties of our distance measure from the previous question should be useful for your analysis 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) Consider how well a *classical* algorithm can predict $f(0) \wedge f(1)$ with a single query to $f : \{0,1\} \rightarrow \{0,1\}$. 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 arbitrary.)

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 $f : \{0,1,2\} \rightarrow \{0,1,2\}$ such that $f(x) = ax^2 + bx + c$ (arithmetic here is modulo 3), where $a, b, c \in \{0,1,2\}$ 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.