CS667/CO681/PH767 Quantum Information Processing (Fall 06)

Assignment 3

Due date: November 7, 2006

1. **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

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

and

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

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

(b) Let $s \in \{0, 1, \ldots, p-1\}$, and define $|\psi_3\rangle$ as

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

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?

2. **Detail from the analysis of the order-finding algorithm.** Suppose that U is a unitary operation on n qubits and C_m-U is a controlled-U with an m-qubit control. Thus, $C_m\text{-}U|a\rangle|b\rangle = |a\rangle(U^a|b\rangle)$, where $U^a|b\rangle$ means apply U to $|b\rangle$ a times.

   Let $|\psi_1\rangle$ and $|\psi_2\rangle$ be any two distinct eigenvectors of U (with different eigenvalues), $|\phi\rangle$ be any m-qubit state, and $\alpha_1, \alpha_2 \in \mathbb{C}$ such that $|\alpha_1|^2 + |\alpha_2|^2 = 1$.

   (a) Show that the final states of resulting from the following two procedures are identical.

   Procedure I: With probability $|\alpha_1|^2$ create the state $|\phi\rangle|\psi_1\rangle$ and with probability $|\alpha_2|^2$ create the state $|\phi\rangle|\psi_2\rangle$. Apply C_m-U to the created state and measure the second register (the last n qubits).

   Procedure II: Create the state $|\phi\rangle(\alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle)$, apply C_m-U to it and and measure the second register.

   (b) Show by a counterexample that the two final states in part (a) might *not* be identical if the condition that $|\psi_1\rangle$ and $|\psi_2\rangle$ are eigenvectors of U is dropped. (You should still assume $|\psi_1\rangle$ and $|\psi_2\rangle$ are orthonormal.)

3. **Fractional queries.** Recall that, for a function $f : \{0,1\} \to \{0,1\}$, an f-query is defined as the unitary operation U_f such that, for all $a, b \in \{0,1\}$, $U_f|a\rangle|b\rangle = |a\rangle|b \oplus f(a)\rangle = |a\rangle(X^{f(a)}|b\rangle)$. Define a *half f-query* as the unitary operation $U_f^{1/2}$ such that $U_f^{1/2}|a\rangle|b\rangle = |a\rangle(W^{f(a)}|b\rangle)$, where

   $$W = \frac{1}{\sqrt{2}}\begin{pmatrix} \omega & \omega^* \\ \omega^* & \omega \end{pmatrix} \quad \text{and} \quad \omega = e^{\pi i/4} \text{ (hence } \omega^* = e^{-\pi i/4}).$$

   Note that W is unitary and $W^2 = X$.

   (a) Show that two half f-queries amount to a full f-query in the sense that $U_f^{1/2} U_f^{1/2} = U_f$.

   (b) What can a half f-query do? Define the *one-out-of-two search problem* as follows. One is given black-box access to $f : \{0,1\} \to \{0,1\}$, that is promised to be uniquely satisfiable in the sense that either $(f(0), f(1)) = (1,0)$ or $(f(0), f(1)) = (0,1)$. The goal is to determine the unique $a \in \{0,1\}$ for which $f(a) = 1$. Classically, one query suffices to do this.

Show that there is a quantum algorithm that performs one half f-query and exactly solve the one-out-of-two search problem.

(c) What *can't* a half f-query do? Prove that one half f-query cannot exactly solve the *evaluate-at-zero* problem, where the input is an arbitrary $f : \{0,1\} \to \{0,1\}$ (there are four possibilities) and the goal is just to determine $f(0)$.

4. **Differences between unitary operations.** One distance measure between two unitary operations is based on the Euclidean norm of vectors, defined as $||v||_2 = \sqrt{|v_1|^2 + |v_2|^2 + \cdots + |v_d|^2}$. For any matrix M, define

$$||M|| = \max_{|\psi\rangle} ||M|\psi\rangle||_2,$$

where it is understood that $|\psi\rangle$ ranges over quantum state so that $|||\psi\rangle||_2 = 1$. Then one can define the distance between two unitaries U and V as $||U - V||_2$.

This isn't the only or best distance measure, but it's good for many purposes; if this distance measure between U and V is small then the effect of changing U with V in the context of any computation will also be small—the final outcome probability will be almost the same.

This question is about a sort of converse of the above property. Suppose that $f : \{0,1\}^n \to \{0,1\}$ and that V approximates U_f in the weak sense that, for all $x \in \{0,1\}^n$, if the last qubit of $V|x\rangle|0\rangle$ measured then, with probability $1-\epsilon$, the result will be $f(x)$. This does not imply that $||V - U_f||$ is small—for example, the first n qubits of $V|x\rangle|0\rangle$ need not be in state $|x\rangle$; they could even be entangled with the last qubit.

Show how to make one query to V and one query to $V^\dagger$ to produce a unitary transformation that is close to U_f (and quantify the closeness in terms of ϵ).

You may use ancilla qubits and produce a unitary transformation that is close to $U_f \otimes I$ (where I is the identity acting on the ancilla qubits).