QIC710/CS768/CO681/PH767/AM871 Introduction to Quantum Information Processing (F14)

**Assignment 2**
**Due date: October 9, 2014**

1. **The "all-one-or-one-in-three" search problem.** Consider the query problem defined as follows. One is given a black box computing a function $f : \{0, 1, 2\} \to \{0, 1\}$ such that either $f$ is 1 on all inputs (i.e., $f(0) = f(1) = f(2) = 1$) or $f$ takes on the value 1 at a single input from $\{0, 1, 2\}$. The goal is to determine which of these four possibilities $f$ is. The four possibilities are shown by the following tables (where we are using a binary encoding of $\{0, 1, 2\}$ as $\{00, 01, 10\}$):

| $x$ | $f_{\text{all}}(x)$ |
|---|---|
| 00 | 1 |
| 01 | 1 |
| 10 | 1 |
| 11 | 1 |

| $x$ | $f_0(x)$ |
|---|---|
| 00 | 1 |
| 01 | 0 |
| 10 | 0 |
| 11 | 1 |

| $x$ | $f_1(x)$ |
|---|---|
| 00 | 0 |
| 01 | 1 |
| 10 | 0 |
| 11 | 1 |

| $x$ | $f_2(x)$ |
|---|---|
| 00 | 0 |
| 01 | 0 |
| 10 | 1 |
| 11 | 1 |

What is the last row, with the "out of range" input 11? It arises because of the binary encoding: 2-bit strings can also take on this value. We'll allow $f$ to be queried at 11 and we'll set $f(11) = 1$ (though we could have chosen 0). Note that one obtains no information about which function $f$ is by learning the value of $f(11)$ (since it's always 1).

   (a) How many queries are necessary and sufficient to solve this problem by a classical algorithm? Your answer should consist of an optimal classical algorithm as well as a proof that the problem cannot be solved with fewer queries.

   (b) Give a quantum algorithm that solves the problem with a single query to $f$.

   (c) What if we changed the out-of-range value from 1 to 0? In other words, if we changed each of the above functions $f$ so that $f(11) = 0$. Is it possible to adapt your 1-query algorithm in part (b) to work in this case? Why or why not?

2. **Quantum Fourier transform.** Let $F_N$ denote the $N$-dimensional Fourier transform

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

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

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

   (b) Show that, for $F_N$, all rows are vectors of length 1, and any two rows are orthogonal.

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

3. **Distinguishing between pairs of unitaries.** In each case, you are given a black box gate that computes one of the two given unitaries, but you are not told which one. It is chosen uniformly: each is selected with probability $\frac{1}{2}$. Your goal is to guess which of the two unitaries it is with as high a probability as you can. To help you do this, you can create any one-qubit quantum state, apply the black box gate to this qubit, and then measure the answer in some basis (that is, you can apply a unitary of your choosing and then measure in the computational basis). You can only use the black-box gate once.

   For example, consider the case where the two unitaries are $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. In this case, setting the initial state to $|+\rangle$, applying the black-box unitary, followed by $H$ and measuring yields 0 in the first case and 1 in the second case. So this is a perfect distinguishing procedure (it succeeds with probability 1).

   Give the best distinguishing procedure (i.e., highest success probability) you can find in each case below. You do not have to prove optimality.

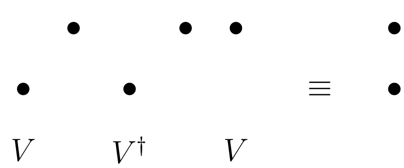
   (a) $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ (the latter is a rotation by $\pi/4$).

   (b) $I$ and $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$.

   (c) $I$ and $H$.

   (Hint: in two out of the above three cases there is a perfect distinguishing procedure.)

4. **Constructing a Toffoli gate out of two-qubit gates.** The Toffoli gate (controlled-controlled-NOT) is a 3-qubit gate, and here we show how to implement it with 2-qubit gates. The construction is given by the following quantum circuit




   where
$$V = \frac{1}{\sqrt{2}}\begin{pmatrix} \omega & \overline{\omega} \\ \overline{\omega} & \omega \end{pmatrix}, \quad \text{with } \omega = e^{i\pi/4} \text{ and } \overline{\omega} = e^{-i\pi/4} \text{ ($\omega$'s conjugate).}$$

   We *could* verify this by multiplying $8 \times 8$ matrices; however, we take a simpler approach.

   (a) Show that $V^2 = X$ (this means $V$ is a square root of NOT).

   (b) Prove each of the following, where $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is an arbitrary 1-qubit state:

      i. The circuit maps $|00\rangle|\psi\rangle$ maps to $|00\rangle|\psi\rangle$.

      ii. The circuit maps $|01\rangle|\psi\rangle$ maps to $|01\rangle|\psi\rangle$.

      iii. The circuit maps $|10\rangle|\psi\rangle$ maps to $|10\rangle|\psi\rangle$.

      iv. The circuit maps $|11\rangle|\psi\rangle$ maps to $|11\rangle V^2|\psi\rangle$.

   (c) Based on parts (a) and (b), write down the $8 \times 8$ unitary matrix that the above circuit computes.

5. **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 (for example) $(2r_1, 2r_2)$ also generates $S$.

   **Note:** for this question, assume that $(r_1, r_2) \neq (0, 0)$.

   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 instance of the process in part (a), a non-zero multiple of $(r_1, r_2)$ can be efficiently determined with high probability.