QIC710/CS768/CO681/PH767/AM871 Introduction to Quantum Information Processing (F16)

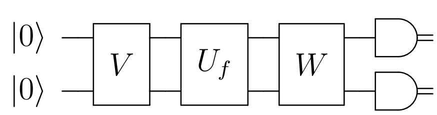
Assignment 2
Due date: October 13, 2016

1. **The 2-out-of-4 and 3-out-of-4 search problems [12 points; 6 each].** Recall the 1-out-of-4 search problem, where one is given a function $f : \{0,1\}^2 \to \{0,1\}$ with the property that there is a unique $x \in \{0,1\}^2$ such that $f(x) = 1$ and the goal is to determine x. We saw that 3 queries are necessary to solve this problem, whereas 1 quantum query is sufficient. In the context of this question, we are only interested in exact solutions (with failure probability zero).

   (a) Consider the 2-out-of-4 search problem, where one is given a black box for a function $f : \{0,1\}^2 \to \{0,1\}$ with the property that there are exactly two $x \in \{0,1\}^2$ such that $f(x) = 1$ and the goal is to determine both such x's. Prove that 3 classical queries are necessary to solve this problem *and* that 2 quantum queries are sufficient to solve this problem.

   (b) Consider the 3-out-of-4 search problem, where one is given a black box for a function $f : \{0,1\}^2 \to \{0,1\}$ with the property that there are exactly three $x \in \{0,1\}^2$ such that $f(x) = 1$ and the goal is to determine all three such x's. Prove that 3 classical queries are necessary to solve this problem *and* that 1 quantum queries is sufficient to solve this problem.

2. **Can a function be evaluated at two points with one quantum query? [12 points; 4 each].** Here we consider the problem where we have a query oracle for a function $f : \{0,1\} \to \{0,1\}$ and the goal is to obtain information about both $f(0)$ and $f(1)$ with a single query. We assume that the query oracle is in the usual form of a unitary operator U_f that, for all $a, b \in \{0,1\}$, maps $|a\rangle|b\rangle$ to $|a\rangle|b \oplus f(a)\rangle$. For simplicity, we consider methods that employ only two qubits in all and are expressible by a circuit of the form



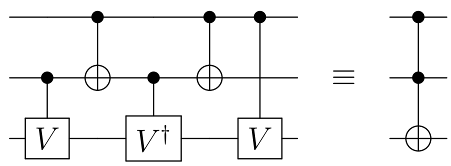
   where V and W are two-qubit unitaries and the D-shaped gates are measurements in the computational basis. Therefore, it can be assumed that the input state to the query is a two-qubit state of the form $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$.

   (a) For each of the four functions of the form $f : \{0,1\} \to \{0,1\}$, give the quantum state right after the query has been performed.

   (b) If there is a measurement procedure that perfectly distinguishes between the four states in part (a) then they must be mutually orthogonal. Show that, for a measurement to be able to perfectly determine the value of $f(0)$, it must be the case that $\alpha_{10} = \alpha_{11}$. (Hint: think of the orthogonality relationships that need to hold.)

   (c) Show that, if the states are such that $f(0)$ can be determined perfectly from them, then $f(1)$ cannot be determined with probability better than $1/2$ (which is no better than random guessing). (Hint: You may use the result in part (b) for this.)

3. **Constructing a Toffoli gate out of two-qubit gates [12 points].** 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

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

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

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

(b) [8 points] 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) [2 points] Based on parts (a) and (b), write down the 8×8 unitary matrix that the above circuit computes.

4. **Quantum Fourier transform [12 points; 4 each].** 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.

5. **Period inversion [12 points].** Recall the 2-dimensional mod m generalization of Simon's problem, where $f : \mathbb{Z}_m^2 \to \mathbb{Z}$ has the property that $f(x) = f(y)$ iff $x - y$ is a multiple of some nonzero $r \in \mathbb{Z}_m^2$. The first part of the quantum algorithm for this (discussed in class) generates a state of the form

$$\frac{1}{\sqrt{m^2}} \sum_{k=0}^{m-1} |x + kr\rangle = \frac{1}{\sqrt{m^2}} \left(|x\rangle + |x + r\rangle + |x + 2r\rangle + \cdots + |x + (m-1)r\rangle \right),$$

for some arbitrary $x \in \mathbb{Z}_m^2$ (all arithmetic expressions are mod m). Informally, we can think of this as a periodic superposition of basis states with period r and offset x. Measuring this state in the computational basis is useless, because of the offset x. However, applying a suitable quantum Fourier transform to this state produces a an equally weighted superposition of all $s \in \mathbb{Z}^2$ such that $s \cdot r = 0$. We proved this in the context of Simon's algorithm and asserted it without proof in the mod m case.

Here we consider a *different* problem somewhat related to the above. Let $m = qr$ for positive integers q and r (juxtaposition means multiplication) and suppose we are given a state of the form

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

where $r, x \in \mathbb{Z}_m$, and with arithmetic mod m. Informally, we can think of this state as periodic with periodicity r and an offset of x.

(a) [8 points] Prove that, if we apply the quantum Fourier transform F_m to $|\psi_1\rangle$, we obtain the state

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} (\omega^{qx})^{\ell} |\ell q\rangle \\ &= \frac{1}{\sqrt{r}} \left(|0\rangle + \omega^{qx}|q\rangle + (\omega^{qx})^2|2q\rangle + \cdots + (\omega^{qx})^{r-1}|(r-1)q\rangle \right), \end{aligned}$$

where $\omega = e^{2\pi i/m}$. Informally, the periodicity has changed from r to q—and there is no offset! The original offset x has become part of the phase.

Hint: Note that $\omega^r = e^{2\pi i/q}$ and $\omega^q = e^{2\pi i/r}$.

(b) [4 points] Explain why, if we measure the state $|\psi_2\rangle$ (in the computational basis), the result is a uniformly sampled element from the set $\{s \in \mathbb{Z}_m : sr = 0\}$ (where the arithmetic is mod m).

(Informally, this is analogous to the measured outcome s in the quantum part of Simon's algorithm satisfying $s \cdot r = 0$.)