Introduction to Quantum Information Processing

(CS 467/667, C&0 481/681, PHYS 467/767)

Fall 2005

Assignment 2

Due date: October 28, 2005

1. **Distinguishing between 3-to-1 balanced and zero.** For $n \geq 2$, call a function $f : \{0,1\}^n \rightarrow \{0,1\}$ *3-to-1 balanced*, if for $3 \cdot 2^{n-2}$ values of x, $f(x) = 1$ and, for the remaining 2^{n-2} values of x, $f(x) = 0$. (Thus the ratio of 1s to 0s for such an f is 3 to 1.) Call a function $f : \{0,1\}^n \rightarrow \{0,1\}$ *zero* if, for all x, $f(x) = 0$. Consider the *3-to-1 vs. zero* problem, where the input is a black-box computing a function $f : \{0,1\}^n \rightarrow \{0,1\}$ that is promised to be either 3-to-1 balanced or zero and the goal is to determine which of the two types f is.

   (a) How many queries to f must a classical algorithm make to solve 3-to-1 vs. zero with certainty on a worst-case input?

   (b) Give a quantum algorithm that solves 3-to-1 vs. zero with a single query to f, with certainty on a worst-case input. (As usual for quantum algorithms, a query to f means an application of the unitary transformation $U_f : |x, y\rangle \mapsto |x, y \oplus f(x)\rangle$.)

2. **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 $||v|| = \sqrt{\sum_{x=0}^{m-1} |v_x|^2}$, 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 two $m \times m$ 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, 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.

3. **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 is very close to I when k is close to n.)

(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 $\tilde{F}_m$ such that $||\tilde{F}_m - F_m|| \leq \epsilon$.

(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.)

4. **More generalizations of Toffoli gates.** Let U be any 2×2 unitary operation. Recall the generalized n-qubit Toffoli gate that maps $|x_1, \ldots, x_{n-1}\rangle|y\rangle$ to

$$\begin{cases} |x_1, \ldots, x_{n-1}\rangle|y\rangle & \text{if } x_1 \wedge \cdots \wedge x_{n-1} = 0 \\ |x_1, \ldots, x_{n-1}\rangle U|y\rangle & \text{if } x_1 \wedge \cdots \wedge x_{n-1} = 1, \end{cases}$$

for all $x_1, \ldots, x_{n-1}, y \in \{0,1\}$. The unitary matrix corresponding to this is of the form

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & u_{00} & u_{01} \\ 0 & 0 & \cdots & u_{10} & u_{11} \end{pmatrix},$$

though the gate can be oriented in different ways (ie, the target qubit can be any one of the n qubits). Consider the more general operations of the form

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & u_{00} & 0 & \cdots & u_{01} & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 1 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & u_{10} & 0 & \cdots & u_{11} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix},$$

where the entries of U are placed in positions (x,x), (x,y), (y,x), and (y,y) of this matrix (for *arbitrary* $x, y \in \{0,1\}^n$ such that $x \neq y$). Show that any such operation can be simulated with one generalized n-qubit Toffoli gate (in one of its n orientations) plus $O(n)$ two-qubit CNOT gates plus $O(n)$ one-qubit NOT gates.

5. **Entanglement among three qubits.** Suppose that Alice, Bob and Carol each possess a qubit and that the joint state of their three qubits is

$$|\psi\rangle_{ABC} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle).$$

   (a) Suppose that Carol leaves the scene, taking her qubit with her, and without communicating with either Alice or Bob. Consider the two-qubit state of Alice and Bob's qubits. Is this state equivalent to $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$? Justify your answer.

   (b) Suppose that Carol leaves the scene, again taking her qubit with her, but she is allowed to send *one classical bit* to Alice. Carol wants to help Alice and Bob transform their state into the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ (and without Alice and Bob having to send any messages between each other). The framework is as follows:

      i. Carol applies some unitary operation U to her qubit, and then measures the qubit, yielding the classical bit b.

      ii. Carol sends b to Alice.

      iii. Alice applies a unitary operation, depending on b, to her qubit. In other words, Alice has two unitary operations V_0 and V_1, and she applies V_b to her qubit.

   At the end of this procedure, the two-qubit state of state of Alice and Bob's qubits should be $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

   Explain how to make this procedure work.

   (c) Is it possible for Alice, Bob and Carol to each possess a qubit such that the joint state of the three qubits has both of the following properties at the same time?

   Property 1: The two-qubit state of Alice and Bob's qubits is $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

   Property 2: The two-qubit state of Bob and Carol's qubits is $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

   Either give an example of a three-qubit state with these properties or show that such a state does not exist.

6. Let F be the quantum Fourier transform modulo 2^n. That is, $F|x\rangle = \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} \omega^{xy}|y\rangle$, for all $x \in \{0,1\}^n = \{0, 1, \ldots, 2^n - 1\}$, where $\omega = e^{2\pi i/2^n}$. Also, define the "phase gate" U acting on n qubits as $U|x\rangle = \omega^x|x\rangle$, for all $x \in \{0, 1, \ldots, 2^n - 1\}$.

   (a) Show how to implement U with $O(n)$ one-qubit gates.

   (b) What is the effect of $F^\dagger UF$ on basis states? (Ie, what is $F^\dagger UF|x\rangle$, for $x \in \{0, 1, \ldots, 2^n - 1\}$?) Give your answer in as simple terms as possible.