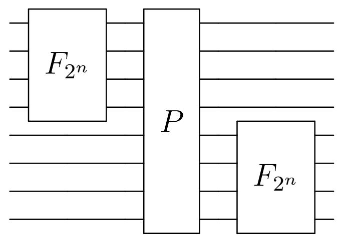
QIC710/CS768/CO681/PH767/AM871 Introduction to Quantum Information Processing (F15)

Assignment 3
Due date: October 27, 2015

1. **Another construction of the quantum Fourier transform [12 points; 6 each].** Here we consider another, recursive, construction of F_{2^n}, the quantum Fourier transform on n qubits. This construction works if n is a power of 2. Suppose that we have an implementation of F_{2^n} and want to implement $F_{2^{2n}}$. Divide the $2n$ qubits into two registers: the first n qubits, and the last n qubits. Define the unitary P on two registers such that

$$P|x\rangle|y\rangle = \left(e^{2\pi i/2^{2n}}\right)^{m(x,y)}|x\rangle|y\rangle, \tag{1}$$

for all $x, y \in \{0,1\}^n$, and where $m(x,y)$ denotes the product of x and y as n-bit integers (e.g., 1101 denotes 13, and 0100 denotes 4, so $m(1101, 0100) = 13 \times 4 = 52$).



   (a) Show that the above circuit followed by a swap of the two n-bit registers computes $F_{2^{2n}}$. (This swap is the unitary such that $|x\rangle|y\rangle \mapsto |y\rangle|x\rangle$ for $x, y \in \{0,1\}^n$.)

   (b) You may assume without proof that the operation P can be implemented at the asymptotic cost of multiplying two n-bit integers, which is $O(n \log n \log\log n)$. Based on this, what is the resulting cost of computing F_{2^n}? (Hint: express the cost as a recurrence and then solve it.)

2. **Generalized form of period-finding by quantum algorithms [12 points].** Let $\sigma : \{0,1\}^n \to \{0,1\}^n$ be a bijection (hence a permutation on the set $\{0,1\}^n$). Let $z \in \{0,1\}^n$. Then the sequence

$$z, \sigma(z), \sigma(\sigma(z)), \sigma(\sigma(\sigma(z))), \ldots \quad = \quad \sigma^{(0)}(z), \sigma^{(1)}(z), \sigma^{(2)}(z), \sigma^{(3)}(z), \ldots$$

eventually comes back to z. Consider the size of this cycle: that is, the minimum $r > 0$ such that $\sigma^{(r)}(z) = z$. Suppose that we are given a black box for the mapping

$$|x\rangle|y\rangle \mapsto |x\rangle|\sigma^{(x)}(y)\rangle,$$

where $x, y \in \{0,1\}^n \equiv \{0, 1, 2, \ldots, 2^n - 1\}$. Suppose that we are also promised that $r \leq 2^{n/2}$, but that otherwise r is unknown to us, and our goal is to determine r. Let $\omega = e^{2\pi i/r}$, and $|\phi\rangle = \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\omega^{-s}|\sigma^{(s)}(z)\rangle$.

Show that there is a quantum circuit that, given the additional help of one copy of $|\phi\rangle$, determines r with a single query to the black box, plus an additional number of 1- and 2-qubits gates that is polynomial in n. It suffices for the success probability $\geq 1/4$.

(Note: r can also be determined with a constant number of queries to the black box *without* being provided with any special quantum state; however, you are not asked to show this here.)

3. **Classical and quantum algorithms for the AND problem [15 points; 3 each].** 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) 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. (**Note:** the probability should be respect to the random choices of the algorithm; the input instance of f is assumed to be *worst-case*.)

   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.)

4. **Questions about unitaries with inputs in superposition [10 points; 5 each].**

   (a) Let U be any n-qubit unitary, $|\psi_1\rangle$, $|\psi_2\rangle$ be orthogonal n-qubit states, and $a_1, a_2 \in \{0,1\}^n$ such that the following property holds. For each $j \in \{1,2\}$, if $U|\psi_j\rangle$ is measured in the computational basis then the outcome is a_j for sure (i.e., with probability 1). Let α_1, α_2 be such that $|\alpha_1|^2 + |\alpha_2|^2 = 1$. Does it follow that, if $U(\alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle)$ is measured in the computational basis, then the outcome is

   $$\begin{cases} a_1 & \text{with probability } |\alpha_1|^2 \\ a_2 & \text{with probability } |\alpha_2|^2? \end{cases}$$

   Either prove it or give a counterexample.

(b) Let U be any n-qubit unitary, $|\psi_1\rangle$ and $|\psi_2\rangle$ be orthogonal n-qubit states, and $a_1, b_1, a_2, b_2 \in \{0,1\}^n$ such that the following property holds. For each $j \in \{1,2\}$, if $U|\psi_j\rangle$ is measured in the computational basis then the outcome is

$$\begin{cases} a_j & \text{with probability } p_j \\ b_j & \text{with probability } q_j \end{cases}$$

(where $p_k + q_k = 1$). Let α_1, α_2 be such that $|\alpha_1|^2 + |\alpha_2|^2 = 1$. Does it follow that if $U(\alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle)$ is measured in the computational basis then the outcome is

$$\begin{cases} a_1 & \text{with probability } p_1|\alpha_1|^2 \\ b_1 & \text{with probability } q_1|\alpha_1|^2 \\ a_2 & \text{with probability } p_2|\alpha_2|^2 \\ b_2 & \text{with probability } q_2|\alpha_2|^2. \end{cases}$$

Either prove it or give a counterexample.

5. **More questions about unitaries with inputs in superposition [11 points].** This question is sort of a continuation of question 4, and is related to a detail that arose in the quantum algorithm for order-finding that was discussed in class. Let W denote a generalized n-qubit controlled-U gate (i.e., for all $x, y \in \{0,1\}^n$, $W|x\rangle|y\rangle = |x\rangle U^x|y\rangle$) and let $|\psi_1\rangle$, $|\psi_2\rangle$ be two orthogonal eigenvectors of U. Let V be any n-qubit unitary (for order-finding, this was the inverse QFT $F^\dagger$). Also, let $|\phi\rangle$ be any n-qubit state initial state for the control-qubits of W (for order-finding, this was $\frac{1}{2^{n/2}}\sum_x |x\rangle$). Suppose that the following property holds. For each $j \in \{1,2\}$, if *the first register (i.e., the first n qubits)* of $(V \otimes I)W|\phi\rangle|\psi_j\rangle$ is measured in the computational basis then the outcome is

$$\begin{cases} a_j & \text{with probability } p_j \\ b_j & \text{with probability } q_j \end{cases}$$

(where $p_k + q_k = 1$). Prove that then, if *the first register of* $(V \otimes I)W|\phi\rangle(\alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle)$ is measured in the computational basis, the outcome is

$$\begin{cases} a_1 & \text{with probability } p_1|\alpha_1|^2 \\ b_1 & \text{with probability } q_1|\alpha_1|^2 \\ a_2 & \text{with probability } p_2|\alpha_2|^2 \\ b_2 & \text{with probability } q_2|\alpha_2|^2. \end{cases}$$