ASSIGNMENT 3 CO 481/CS 467/PHYS 467 (Winter 2010)

Due in class on Wednesday, February 24.

1. *Fourier transforms and composite systems.* Recall that the quantum Fourier transform on n qubits is defined as the transformation

$$|x\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi ixy/2^n} |y\rangle$$

where we identify n-bit strings and the integers they represent in binary. More generally, for any nonnegative integer N, we can define the quantum Fourier transform modulo N as the transformation

$$|x\rangle \overset{F_N}{\mapsto} \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi ixy/N} |y\rangle$$

where the state space is $\mathbb{C}^N$, with orthonormal basis $\{|0\rangle, |1\rangle, \ldots, |N-1\rangle\}$.

   (a) [1 point] Write F_5 in matrix form.

   (b) [3 points] Show that F_N is a unitary transformation.

   (c) [3 points] Show that $F_2 \otimes F_3 \cong F_6$, where $\cong$ denotes equivalence up to a permutation of the rows and columns (not necessarily the same permutation for the rows as for the columns).

   (d) [2 points] Show that $F_N \otimes F_M \cong F_{NM}$ does not hold in general.

   (e) [5 bonus points] Show that if N and M are relatively prime, then $F_N \otimes F_M \cong F_{NM}$.

2. *A fast approximate QFT*

   (a) [2 points] In class, we saw a circuit implementing the n-qubit QFT using Hadamard and controlled-R_k gates, where $R_k|x\rangle = e^{2\pi ix/2^k}|x\rangle$ for $x \in \{0,1\}$. How many gates in total does that circuit use? Express your answer both exactly and using Θ notation.

   (b) [3 points] Let $\mathrm{C}R_k$ denote the controlled-R_k gate, $\mathrm{C}R_k|x,y\rangle = e^{2\pi ixy/2^k}|x,y\rangle$ for $x, y \in \{0,1\}$. Show that $E(\mathrm{C}R_k, I) \leq 2\pi/2^k$, where I denotes the 4×4 identity matrix, and where $E(U,V) = \max_{|\psi\rangle} \||U|\psi\rangle - V|\psi\rangle\|$. You may use the fact that $\sin x \leq x$ for any $x \geq 0$.

   (c) [5 points] Let F denote the exact QFT on n qubits. Suppose that for some constant c, we delete all the controlled-R_k gates with $k > \log_2(n)+c$ from the QFT circuit, giving a circuit for another unitary operation, $\tilde{F}$. Show that $E(F,\tilde{F}) \leq \epsilon$ for some ϵ that is independent of n, where ϵ can be made arbitrarily small by choosing c arbitrarily large. (You may use equation 4.3.3 of KLM.)

   (d) [2 points] For a fixed c, how many gates are used by the circuit implementing $\tilde{F}$? It is sufficient to give your answer using Θ notation.

3. *Translation invariance.* Let P denote the unitary operation that adds 1 modulo 2^n: for any $x \in \{0,1,\ldots,2^n-1\}$, $P|x\rangle = |x+1 \bmod 2^n\rangle$.

   (a) [5 points] Show that the Fourier basis states are eigenvectors of P. What are their eigenvalues? (Equivalently, show that $F^{-1}PF$ is diagonal, and find its diagonal entries.)

(b) [3 points] Let $|\psi\rangle$ be a state of n qubits. Show that if $P|\psi\rangle$ is measured in the Fourier basis (or equivalently, if we apply the inverse Fourier transform and then measure in the computational basis), the probabilities of all measurement outcomes are the same as if the state had been $|\psi\rangle$.

4. *Finding a hidden slope.* Let p be a prime number. Suppose you are given a black-box function $f : \{0, 1, \ldots, p-1\} \times \{0, 1, \ldots, p-1\} \to \{0, 1, \ldots, p-1\}$ such that $f(x, y) = f(x', y')$ if and only if $y' - y = m(x' - x) \bmod p$ for some unknown integer m. In other words, the function is constant on lines of slope m, and distinct on different parallel lines of that slope. Your goal is to determine $m \bmod p$ using as few queries as possible to f, which is given by a unitary operation U_f satisfying $U_f|x\rangle|y\rangle|z\rangle = |x\rangle|y\rangle|z + f(x, y) \bmod p\rangle$ for all $x, y, z \in \{0, 1, \ldots, p-1\}$. (Note that each of the three registers stores an integer modulo p, which we do not explicitly represent using qubits.)

   (a) [2 points] Suppose we begin with three registers in the state $|0\rangle|0\rangle|0\rangle$. If we apply $F_p \otimes F_p \otimes I$, where F_p is the Fourier transform modulo p defined in question 1, what is the resulting state?

   (b) [3 points] Now suppose we apply U_f and measure the state of the third register in the computational basis (i.e., the basis $\{|0\rangle, |1\rangle, \ldots, |p-1\rangle\}$). What are the probabilities of the different possible measurement outcomes, and what are the resulting post-measurement states of the first two registers?

   (c) [5 points] Show that by applying $F_p^{-1} \otimes F_p^{-1}$ to the post-measurement state of the first two registers and then measuring in the computational basis, one can learn $m \bmod p$ with certainty.