ASSIGNMENT 4 CO 481/CS 467/PHYS 467 (Winter 2012)

Due in class on Thursday, March 8.

1. *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 $R_k|x\rangle = e^{2\pi i x/2^k}|x\rangle$ 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, $\mathrm{C}R_k|x,y\rangle = e^{2\pi i xy/2^k}|x,y\rangle$ for $x, y \in \{0,1\}$. Show that $E(\mathrm{C}R_k, I) \le 2\pi/2^k$, 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 $\sin x \le x$ for any $x \ge 0$.

   (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 $E(F, \tilde{F}) \le \epsilon$ for some ϵ that is independent of n, where ϵ can be made arbitrarily small by choosing c arbitrarily large. (Hint: Use equation 4.3.3 of KLM.)

   (d) [1 point] 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.

2. *Implementing the square root of a unitary.*

   (a) [1 point] Let U be a unitary operation with eigenvalues ± 1. Let P_0 be the projection onto the $+1$ eigenspace of U and let P_1 be the projection onto the -1 eigenspace of U. Let $V = P_0 + iP_1$. Show that $V^2 = U$.

   (b) [2 points] Give a circuit of 1- and 2-qubit gates and controlled-U gates with the following behavior (where the first register is a single qubit):

$$|0\rangle|\psi\rangle \mapsto \begin{cases} |0\rangle|\psi\rangle & \text{if } U|\psi\rangle = |\psi\rangle \\ |1\rangle|\psi\rangle & \text{if } U|\psi\rangle = -|\psi\rangle. \end{cases}$$

   (c) [3 points] Give a circuit of 1- and 2-qubit gates and controlled-U gates that implements V. Your circuit may use ancilla qubits that begin and end in the $|0\rangle$ state.

3. *Finding a hidden slope.* Let p be a prime number. Suppose you are given a black-box function $f\colon \{0,1,\ldots,p-1\} \times \{0,1,\ldots,p-1\} \to \{0,1,\ldots,p-1\}$ 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 probability $1 - 1/p$.

4. *Continuous-time quantum search.*

   In this problem we will see how Grover's algorithm can be formulated as a continuous-time process. In quantum mechanics, time evolution is determined by the Schrödinger equation, $i\frac{\mathrm{d}}{\mathrm{d}t}|\phi(t)\rangle = H|\phi(t)\rangle$, where H is a Hermitian operator (i.e., $H = H^\dagger$) called the *Hamiltonian* of the quantum system. When H is time-independent, the solution of this equation is $|\phi(t)\rangle = e^{-iHt}|\phi(0)\rangle$, where $|\phi(0)\rangle$ is the state at time $t = 0$.

   (a) [3 points] Let $|w\rangle$ be the computational basis state corresponding to the marked item $w \in \{1, 2, \ldots, N\}$, and let $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=1}^{N} |x\rangle$ denote the uniform superposition. Find an orthonormal basis $\{|w\rangle, |w^\perp\rangle\}$ for the two-dimensional subspace of $\mathbb{C}^N$ spanned by $|w\rangle$ and $|\psi\rangle$, and express $|\psi\rangle$ in this basis.

   (b) [3 points] Let the Hamiltonian of the quantum system be $H = |w\rangle\langle w| + |\psi\rangle\langle\psi|$. Write H in terms of the basis $\{|w\rangle, |w^\perp\rangle\}$.

   (c) [3 points] Suppose the system is prepared in the state $|\psi\rangle$ at time $t = 0$ and evolved under the Hamiltonian H for a total time T. What is the resulting state at time $t = T$?

   (d) [2 points] Suppose the state is measured in the computational basis at time T. What is the probability of observing the marked item, w? How should you choose T in order to make this probability high?

5. *The collision problem.*

   Recall that the quantum search algorithm can find a marked item in a search space of size N using $O(\sqrt{N/M})$ queries, where M is the total number of marked items.

   In the collision problem, you are given a black-box function $f\colon \{1, 2, \ldots, N\} \to S$ (for some set S) with the promise that f is two-to-one. In other words, for any $x \in \{1, 2, \ldots, N\}$, there is a unique $x' \in \{1, 2, \ldots, N\}$ such that $x \neq x'$ and $f(x) = f(x')$. The goal of the problem is to find such a pair (x, x') (called a collision).

   (a) [3 points] For any $K \in \{1, 2, \ldots, N\}$, consider a quantum algorithm for the collision problem that works as follows:

      - Query $f(1), f(2), \ldots, f(K)$.
      - If a collision is found, output it.
      - Otherwise, search for a value $x \in \{K + 1, K + 2, \ldots, N\}$ such that $f(x) = f(x')$ for some $x' \in \{1, 2, \ldots, K\}$.

      How many quantum queries does this algorithm need to make in order to find a collision? Your answer should depend on N and K, and can be expressed using big-O notation.

   (b) [3 points] How should you choose K in part (a) to minimize the number of queries used?

   (c) [2 points] It turns out that the algorithm you found in part (b) is essentially optimal (although proving this is nontrivial). Discuss the relationship between the collision problem and Simon's problem in light of this fact.