ASSIGNMENT 4 CO 481/CS 467/PHYS 467 (Winter 2010)

Due in class on Wednesday, March 10.

1. *Success probability of period finding.* [10 points]

   Let $f : \{0, 1, \ldots, 2^n - 1\} \to \{0, 1\}^m$ be a periodic function with period r (i.e., $f(x) = f(y)$ if and only if $x - y$ is an integer multiple of r), where r does not necessarily divide 2^n. Prove that for any $j \in \{0, 1, \ldots, r - 1\}$, the quantum algorithm for period finding outputs the closest integer to $j2^n/r$ with probability at least c/r, for some constant c. (You may find it helpful to refer to the strategy discussed in KLM, Lemma 7.1.3 and Theorem 7.1.6, but your proof should be self-contained. Also, note that Lemma 7.1.3 contains a typo: the condition on θ should be $|\theta| \leq \frac{\pi}{2M}$.)

2. *Factoring 21.*

   (a) [2 points] Suppose that, when running Shor's algorithm to factor the number 21, you choose the value $a = 2$. What is the order r of a mod 21?

   (b) [3 points] Suppose that, in executing the algorithm, you use $n = 7$ qubits for the first register. Plot the probabilities of the possible measurement outcomes obtained by the algorithm. You may assume for simplicity that the result of measuring the second register is $a^0 = 1$ (recall that the distribution for the first register does not depend much on which outcome is obtained for the second register). You are welcome to use software to produce your plot.

   (c) [3 points] Compute $\gcd(21, a^{r/2} - 1)$ and $\gcd(21, a^{r/2} + 1)$. How do they relate to the prime factors of 21?

   (d) [3 points] How would your above answers change if instead of taking $a = 2$, you had taken $a = 5$?

3. *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, $i\frac{\mathrm{d}}{\mathrm{d}t}|\phi(t)\rangle = H|\phi(t)\rangle$ (in units where $\hbar = 1$), where H is a Hermitian operator 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?

(continued on next page)

4. *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 $f : \{0, 1, \dots, N-1\} \to S$ (for some set S) with the promise that f is two-to-one. In other words, for any $x \in \{0, 1, \dots, N-1\}$, there is a unique $x' \in \{0, 1, \dots, N-1\}$ 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 $K \in \{1, 2, \dots, N\}$, consider a quantum algorithm for the collision problem that works as follows:

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

   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.