ASSIGNMENT 4 CO 481/CS 467/PHYS 467 (Winter 2014)

Due in class on Tuesday, March 11.

1. *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 need to explicitly represent using qubits.)

   (a) [2 points] Let F_p denote the Fourier transform modulo p, the unitary operator
   $$F_p = \frac{1}{\sqrt{p}} \sum_{x,y=0}^{p-1} e^{2\pi i xy/p} |x\rangle\langle y|.$$
   Suppose we begin with three registers in the state $|0\rangle|0\rangle|0\rangle$. If we apply $F_p \otimes F_p \otimes I$, 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 $1 - 1/p$.

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 $a \bmod 21$?

   (b) [3 points] Give an expression for the probabilities of the possible measurement outcomes when performing phase estimation with n bits of precision in Shor's algorithm.

   (c) [2 points] In the execution of Shor's algorithm considered in part (a), suppose you perform phase estimation with $n = 7$ bits of precision. Plot the probabilities of the possible measurement outcomes obtained by the algorithm. You are encouraged to use software to produce your plot.

   (d) [2 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?

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

3. *Searching for a quantum state.*

   Suppose you are given a black box U_ϕ that identifies an unknown quantum state $|\phi\rangle$ (which may not be a computational basis state). Specifically, $U_\phi|\phi\rangle = -|\phi\rangle$, and $U_\phi|\xi\rangle = |\xi\rangle$ for any state $|\xi\rangle$ satisfying $\langle\phi|\xi\rangle = 0$.

   Consider an algorithm for preparing $|\phi\rangle$ that starts from some fixed state $|\psi\rangle$ and repeatedly applies the unitary transformation VU_ϕ, where $V = 2|\psi\rangle\langle\psi| - I$ is a reflection about $|\psi\rangle$.

   Let $|\phi^\perp\rangle = \frac{e^{-i\lambda}|\psi\rangle - \sin(\theta)|\phi\rangle}{\cos(\theta)}$ denote a state orthogonal to $|\phi\rangle$ in $\mathrm{span}\{|\phi\rangle, |\psi\rangle\}$, where $\langle\phi|\psi\rangle = e^{i\lambda}\sin(\theta)$ for some $\lambda, \theta \in \mathbb{R}$.

   (a) [1 point] Write the initial state $|\psi\rangle$ in the basis $\{|\phi\rangle, |\phi^\perp\rangle\}$.

   (b) [3 points] Write U_ϕ and V as matrices in the basis $\{|\phi\rangle, |\phi^\perp\rangle\}$.

   (c) [3 points] Let k be a positive integer. Compute $(VU_\phi)^k$.

   (d) [2 points] Compute $\langle\phi|(VU_\phi)^k|\psi\rangle$.

   (e) [2 points] Suppose that $|\langle\phi|\psi\rangle|$ is small. Approximately what value of k should you choose in order for the algorithm to prepare a state close to $|\phi\rangle$, up to a global phase? Express your answer in terms of $|\langle\phi|\psi\rangle|$.

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 $f\colon \{1, 2, \ldots, N\} \to S$ (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.