ASSIGNMENT 3 CMSC 858K (Fall 2016)

Due in class on Thursday, October 20.

1. *The Fourier transform and translation invariance.* The quantum Fourier transform on n qubits is defined as the transformation

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

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

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

where the state space is $\mathbb{C}^N$, with orthonormal basis $\{|0\rangle, |1\rangle, \ldots, |N-1\rangle\}$. Let P denote the unitary operation that adds 1 modulo N: for any $x \in \{0, 1, \ldots, N-1\}$, $P|x\rangle = |x+1 \bmod N\rangle$.

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

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

   (c) [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 $|\psi\rangle$.

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 need to explicitly represent using qubits.)

(a) [2 points] Let F_p denote the Fourier transform modulo p, the unitary operator

$$F_p = \frac{1}{\sqrt{p}} \sum_{x,y=0}^{p-1} e^{2\pi i x y/p} |x\rangle\langle y|.$$

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 $1 - 1/p$.

4. *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] 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 $a = 5$?

5. *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 to make this probability high?

6. *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.