Due: March 27th, 2020
Date: March 7, 2020

Assignment 4

Please submit it electronically to ELMS. This assignment is 7% in your final grade. For the simplicity of the grading, the total number of points for the assignment is 70.

Problem 1. *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).

1. *(6 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.

2. *(6 points)* How should you choose K in part (a) to minimize the number of queries used?

3. *(8 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.

Problem 2. *Simon's algorithm and its extension.* In Simon's problem, recall that we're given oracle access to a function $f : \{0,1\}^n \to \{0,1\}^n$ with the promise that there exists a secret string $s \neq 0^n$ such that $f(x) = f(y)$ if and only if $y = x \oplus s$ for all different $x, y \in \{0,1\}^n$.

1. *(5 points)* Recall the algorithm described during the lecture. Rigorously prove that $O(n)$ repetitions of Simon's algorithm are enough, if we want to succeed with $1 - e^{-n}$ probability.

2. *(15 points)* Suppose instead that there are two nonzero secret strings, $s \neq t$, such that $f(x) = f(x \oplus s) = f(x \oplus t) = f(x \oplus s \oplus t)$ for all x. Describe a variation of Simon's algorithm that finds the entire set $s, t, s \oplus t$ in time polynomial in n. When you measure a state in your algorithm, what are the possible results of the measurement? How do you use those measurement results to reconstruct the set $s, t, s \oplus t$?

Problem 3. *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 $\mathcal{C}^N$, with orthonormal basis $\{|0\rangle, |1\rangle, \ldots, |N-1\rangle\}$. Let P denote the unitary operation that adds 1 modulo N: for any $x \in \{0, 1, \ldots, N-1\}$, $P|x\rangle = |x+1 \bmod N\rangle$.

1. *(4 points)* Show that F_N is a unitary transformation.
2. *(7 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.)
3. *(4 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 $|\psi\rangle$.

Problem 4. *Factoring 21.*

1. *(3 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?
2. *(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.
3. *(3 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.
4. *(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?
5. *(3 points)* How would your above answers change if instead of taking $a = 2$, you had taken $a = 5$?
