Homework 2

1 Problem 1

In class, we saw how to use Grover's algorithm to find a collision in a function $f : \{0,1\}^m \to \{0,1\}^n$ for $m \gg n$ in time $O(2^{n/3})$ if we treat each evaluation of f as unit time. A collision can be thought of as follows: two distinct inputs x_0, x_1 such that $f(x_0) \oplus f(x_1) = 0^n$.

Consider the following generalization: given $f : \{0,1\}^m \to \{0,1\}^n$ for $m \gg n$, find 3 distinct inputs x_0, x_1, x_2 such that $f(x_0) \oplus f(x_1) \oplus f(x_2) = 0^n$. Explain how to solve this problem using time $O(2^{n/4})$ using Grover's algorithm.

2 Problem 2

A 3-collision is a triple of inputs x_0, x_1, x_2 that are all distinct such that $f(x_0) = f(x_1) = f(x_2)$. Explain how to use Grover's algorithm to find a 3-collision in time $O(2^{3n/7})$.

Hint: the BHT algorithm for finding collisions can be seen as the following: take an algorithm for 1-collisions (which are just arbitrary single points) and extending it to an algorithm for 2-collisions using Grover's algorithm. Extend this idea to find a 3-collision using time $O(2^{4n/9})$. Then show how to optimize the algorithm to obtain a 3-collision in time $O(2^{3n/7})$

3 Problem 3

Let p be a prime, and consider functions of the form $f_{a,b}(x) = ax + b \bmod p$ for $a, b \in \mathbb{Z}_p$. a, b will be chosen uniformly at random in $\mathbb{Z}_p$.

(a) Suppose you are given just a single *classical* query to $f_{a,b}$. Explain why it is impossible to recover both a, b.

(b) Suppose you are given just a single *quantum* query to $f_{a,b}$. Explain how to recover a, b with high probability, namely $1 - O(p)$. Here, the success probability is allowed to be over any randomness of the algorithm (such as the randomness inherent to measurement), and well as the random choice of a, b.

You may assume you can perfectly compute the *multi-dimensional* quantum Fourier transform mod p, as well as its inverse. That is, the map

$$|\mathbf{x}\rangle \mapsto \frac{1}{p^{n/2}} \sum_{\mathbf{y} \in \mathbb{Z}_p^n} \omega_p^{\mathbf{x}\cdot\mathbf{y}} |\mathbf{y}\rangle$$

The n-dimensional QFT mod p is just the 1-dimensional QFT mod p applied separately to each component of $\mathbf{x}$.

Hint: The QFT has the following effect for full rank $\mathbf{A} \in \mathbb{Z}_p^{m\times n}$:

$$\frac{1}{p^{(n-m)/2}} \sum_{\mathbf{u}\in\mathbb{Z}_p^n \text{ s.t. } \mathbf{A}\cdot\mathbf{u}=0} |\mathbf{u}\rangle \mapsto \frac{1}{p^{m/2}} \sum_{\mathbf{v}\in\mathbb{Z}_p^m} |\mathbf{A}^T \cdot \mathbf{v}\rangle$$
$$\frac{1}{p^{m/2}} \sum_{\mathbf{v}\in\mathbb{Z}_p^m} |\mathbf{A}^T \cdot \mathbf{v}\rangle \mapsto \frac{1}{p^{(n-m)/2}} \sum_{\mathbf{u}\in\mathbb{Z}_p^n \text{ s.t. } \mathbf{A}\cdot\mathbf{u}=0} |\mathbf{u}\rangle$$

That is, if the input state is the uniform superposition over the kernel of $\mathbf{A}$, then the QFT is the uniform superposition over the row-space of $\mathbf{A}$.

Also, suppose you know that the QFT maps

$$\sum \alpha_{\mathbf{x}} |\mathbf{x}\rangle \mapsto \sum \beta_{\mathbf{y}} |\mathbf{y}\rangle$$

Then, the QFT has the following effects on related states

$$\sum \alpha_{\mathbf{x}} |\mathbf{x}+\mathbf{r}\rangle \mapsto \sum \beta_{\mathbf{y}} \omega_p^{\mathbf{r}\cdot\mathbf{y}} |\mathbf{y}\rangle$$
$$\sum \alpha_{\mathbf{x}} \omega_p^{\mathbf{r}\cdot\mathbf{x}} |\mathbf{x}\rangle \mapsto \sum \beta_{\mathbf{y}} |\mathbf{y}-\mathbf{r}\rangle$$
$$\sum \alpha_{\mathbf{x}} |t\mathbf{x}\rangle\rangle \mapsto \sum \beta_{\mathbf{y}} |t^{-1}\mathbf{y}\rangle$$

4 Problem 4

Let $P : \{0,1\}^n \to \{0,1\}^n$ be a permutation; that is, a function without any collisions. Let $Q(x) = P(x \oplus k_0) \oplus k_1$ for some secret keys k_0, k_1.

It is known that if you can only make classical queries to these two functions, then you cannot recover k_0, k_1. This fact is used in the design of encryption schemes: basically P is a public permutation that everyone knows, and you turn it into a private permutation Q as above. Then Q can be used to encrypt messages (decryption will require the ability to compute P^{-1}, but we will ignore it for this problem).

Show that quantum queries to both P and Q allow for the recovery of k_0, k_1.

Hint: try defining a function f based on P and Q such that f is an instance of Simon's problem. Then solve Simon's problem on f as we saw in class.