CS 593/MA 595 - Intro to Quantum Computation
Theoretical Homework 5

Due Wednesday, October 22 at 11:59PM (upload to Brightspace)

1. Prove that $\mathsf{BQP} \subseteq \mathsf{PSPACE}$.

   Here, BQP was defined in the class, and PSPACE is all decision problems that can be solved using a classical Turing machine with polynomial space (although you do not need to argue formally with Turing machines for this problem—just show that any problem in BQP admits an algorithm that solves it using only polynomial space).

2. Consider a 2-to-1 function $f : \{0,1\}^n \to \{0,1\}^m$ provided as an oracle U_f satisfying

   $$U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle .$$

   By "2-to-1", we mean that for each $z \in \{0,1\}^m$, there are either 0 or 2 inputs that map to z, i.e., $|f^{-1}(z)| \in \{0,2\}$ for all $z \in \{0,1\}^m$. We want to find a collision of f, which is a pair $x \neq y$ such that $f(x) = f(y)$.

   Find a quantum algorithm that solves this problem. You need to analyze the number of queries to U_f to achieve a high success probability (i.e., greater than 2/3). You may use anything we covered in classes as known priors.

   A baseline algorithm is a classical algorithm: Query f with randomly generated x until a collision is found. This algorithm succeed with high probability with $O(2^{n/2})$ queries due to the birthday paradox. Your quantum algorithm should have a lower query complexity than $O(2^{n/2})$ (i.e., $O(2^{n/3})$).

   Hint:

   The algorithm roughly contains two steps:

   (a) Select a set X of size K and query $f(X) = \{f(x) : x \in X\}$.
   (b) Search for $y \in \{0,1\}^m \backslash X$ such that $f(y) \in f(X)$.

   Analyze the query complexities of both steps with K, and choose the optimal K.