Problem Set #3
CMSC 858L
Instructor: Daniel Gottesman
Due on Gradescope Mar. 16, 2023, noon

The late deadline to turn the problem set in without penalty is Mar. 19, 2023, noon.

Problem #1. Phase vs. Bit Flip Oracles (25 pts.)
In class, we have seen two different ways to convert a classical oracle \(O(x)\) into a quantum one. (In this problem, restrict attention to oracles with a one-bit output.) The “standard” answer is the bit flip oracle \(O_b|\!\!x\rangle|c\rangle = |\!\!x\rangle|c \oplus O(x)\rangle\). The phase oracle is \(O_p|\!\!x\rangle = (-1)^{O(x)}|\!\!x\rangle\) is simpler since it doesn’t require an ancilla. We saw in class that you can implement \(O_p\) given one use of \(O_b\) by using the ancilla \(|-\rangle = |0\rangle - |1\rangle\).

In this problem, we will investigate the opposite direction.

a) (10 pts.) Show that with any number of queries to \(O_p\), it is not possible to distinguish \(O(x)\) from its complement \(\overline{O}(x)\), for which \(\overline{O}(x) = 1 \oplus O(x)\).

b) (15 pts.) Assume we know that \(O(00\ldots0) = 1\). Find a way to implement \(O_b\) using one query to \(O_p\).

Problem #2. Query Complexity Problems (75 pts.)
A marked element for an oracle \(O\) is an input \(x\) such that \(O(x) = 1\).

a) (25 pts.) Consider the following problem: Given an oracle \(O\) with \(N\) possible inputs, return 1 if there are either 0 or exactly 2 marked elements; otherwise return 0.

Find an algorithm to solve this problem using \(O(\sqrt{N})\) queries. Then use the method of polynomials to prove that the query complexity is \(\Omega(\sqrt{N})\).

b) (25 pts.) Consider the following problem: Given an oracle \(O\) with \(N\) possible inputs (\(N\) a multiple of 4), return 1 if there are at most \(N/4\) marked elements and 0 otherwise. Note that the threshold \(N/4\) is sharp: If there are \(N/4\) marked elements, the algorithm should return 1 with probability at least 2/3, and if there are \(N/4 + 1\) marked elements, the algorithm should return 0 with probability at least 2/3. Find the quantum query complexity (upper and lower bounds, up to a constant factor) of this problem.

c) (25 pts.) Consider the following problem: Given an oracle \(O(x, y)\) which takes two inputs, each with \(N\) possible values. There exist \(x_0\) and \(y_0\) such that \(O(x, y) = 1\) iff exactly one of \(x = x_0\) and \(y = y_0\), otherwise \(O(x, y) = 0\). That is, \(O(x_0, y) = 1\) if \(y \neq y_0\), \(O(x, y_0) = 1\) if \(x \neq x_0\), \(O(x, y) = 0\) if \(x \neq x_0\) and \(y \neq y_0\), and \(O(x_0, y_0) = 0\). The algorithm should return \((x_0, y_0)\).

Find an algorithm to solve this problem using \(O(\sqrt{N})\) queries. Then prove that the query complexity is \(\Omega(\sqrt{N})\).

Hint: There are probably many ways to prove a lower bound, but my solution involves a reduction.