1. Exactly one out of the four values $O_1, O_2, O_3, O_4$ is one. Show that with two queries you can find with success probability one, the index $i$ such that $O_i = 1$.

2. • Let $f : \{0, 1\}^N \rightarrow \{0, 1\}$ be a symmetric function. Prove that if there exists a degree $k$ multi-variate polynomial $p : \mathbb{R}^N \rightarrow \mathbb{R}$ that $\varepsilon$–approximates $f$, then there exists a degree $k$ symmetric, multi-variate polynomial $p' : \mathbb{R}^N \rightarrow \mathbb{R}$ that $\varepsilon$–approximates $f$.

• Let $p : \mathbb{R}^N \rightarrow \mathbb{R}$ be a degree $k$ symmetric polynomial. Prove that there exists a degree $k$ univariate polynomial $q : \mathbb{R} \rightarrow \mathbb{R}$ such that for every $x_1, \ldots, x_N \in \{0, 1\}^N$, $p(x_1, \ldots, x_N) = q(\sum x_i)$.

• Prove that $\deg(OR_N) = N$ and conclude that $Q_E(OR_N) \geq \frac{N}{2}$.

• Prove that for any symmetric, non-trivial function $f : \{0, 1\}^N \rightarrow \{0, 1\}$ we have $\deg(f) \geq \frac{N}{2}$ and conclude that $Q_E(f) \geq \frac{N}{4}$.

3. A quantum black-box algorithm solves the $OR$ function with one-sided unbounded error, if

• On input $O_1 = O_2, \ldots = O_N = 0$ there is some positive probability of answering 0.

• On input $O_1, O_2, \ldots, O_N$ such that $OR(O_1, \ldots, O_N) = 1$ the answer is always 1. In other words, whenever the answer is zero, $OR(O_1, \ldots, O_N) = 0$.

Let us denote by $Q_1(OR)$ the minimal number of queries such an algorithm should make. Prove that $Q_1(OR) \geq \frac{N}{2}$.

4. (a) We are given $O_1, \ldots, O_N$ with the promise that there are exactly $R$ elements with $O_i = 1$. Show an algorithm that finds (with a constant probability) such an $i$ using only $O(\sqrt{\frac{N}{R}})$ queries.

(b) Now we are given $O : [N] \rightarrow [N]$ with the promise that $O$ is two-to-one (i.e., for every $i$ there is exactly one other element having the same value $O_i$). Devise a quantum black-box algorithm that finds (with a constant probability) a collision (a pair $\{i, j\}$ such that $O_i = O_j$) using only $O(N^{1/3})$ queries.

(c) Compare with Simon’s algorithm.

(d) Compare with classical algorithms.

5. Let $R_0(f)$ denote the query complexity of a probabilistic black-box algorithm that for every input $x \in \{0, 1\}^N$ outputs ‘quit’ with probability at most half and $f(x)$ otherwise (such an algorithm is called a zero-error algorithm).

The majority function $MAJ(x_1, x_2, x_3)$ returns 1 if two or three of its inputs are 1, and zero otherwise. The recursive-majority function is defined recursively as follows:

$$f(x_1, x_2, x_3) = MAJ(x_1, x_2, x_3)$$

$$f(x_1, \ldots, x_{3n}) = f(f(x_1, \ldots, x_{3n-1}), f(x_{3n-1+1}, \ldots, x_{2\cdot3n-1}), f(x_{2\cdot3n-1+1}, \ldots, x_{3n}))$$
Let $N = 3^n$.

Prove that $R_0(f) \leq O(N^{\log_3 8 - 1}) \approx O(N^{0.892})$. 