1. You are given the promise that 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 \(k\) multivariate polynomial \(p : \mathbb{R}^N \rightarrow \mathbb{R}\) that \(\varepsilon\)-approximates \(f\), then there exists a degree \(k\) symmetric, multivariate 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 \(x_1, \ldots, x_N \in \{0, 1\}\), \(p(x_1, \ldots, x_N) = q(\sum x_i)\).

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

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

\[
\begin{align*}
f(x_1, x_2, x_3) &= \text{MAJ}(x_1, x_2, x_3) \\
\end{align*}
\]

We also denote \(N = 3^n\).

Prove that \(R_0(f) \leq O(N^{\log_3 8 - 1}) \approx O(N^{0.892})\).
6. (the deterministic communication complexity of the median) Alice holds $n$ elements $x_1, \ldots, x_n$ each from $[m]$ and Bob holds $n$ elements $y_1, \ldots, y_n$ also from $[m]$. Their goal is to compute the median element of $\{x_1, \ldots, x_n, y_1, \ldots, y_n\}$. More generally, they both know some $1 \leq k \leq 2n$, and their goal is to compute the $k$'th largest element in the set $\{x_1, \ldots, x_n, y_1, \ldots, y_n\}$.

- Show a deterministic protocol using only $O(\log(m) \cdot \log(n))$ communication bits.
- Improve that to show a deterministic protocol using only $O(\log(m) + \log(n))$ communication bits.

7. (Order finding as phase estimation) We saw in class the order finding problem:

**Input**: $n$ and an element $x \in \mathbb{Z}_n^*$. 

**Output**: The minimal $r$ such that $x^r = 1 \pmod{n}$.

The algorithm we saw in class (a few weeks ago) can be described as follows. We define $U_x(y) = |xy \pmod{n}\rangle$ and apply the following circuit:

![Order finding circuit](image)

Figure 1: Order finding

The circuit is then followed by the continued fraction algorithm. As you see this circuit is almost identical to the phase estimation circuit for $U_x$. We now want to analyze the above circuit using phase estimation.

- Define $W = \text{Span} \{ |x^0\rangle, |x^1\rangle, \ldots, |x^{r-1}\rangle \}$. Prove the $W$ is invariant under $U_x$ (i.e., $U_xW = W$) and that $U_x$ is unitary over $W$.
- Find the matrix $M$ describing the unitary transformation $U_x$ in the basis $\{ |x^0\rangle, |x^1\rangle, \ldots, |x^{r-1}\rangle \}$ of $W$.
- Prove that the eigenvectors of $M$ are $v_0, \ldots, v_{r-1}$ where $v_k = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} w^{kj} |x^j\rangle$, and where $w_r$ is a primitive $r$'th root of unity. (This follows from a general principle, but if you don’t know it you can do a direct check). What are the eigenvalues?
- Prove that $|1\rangle = |x^0\rangle$ is the sum of all the eigenvectors $|v_k\rangle$. (This again follows from a general principle, and again if you don’t know it simply do a direct check).
- Analyze the circuit above.