Problem Session 2

The polynomial method

Problem 1 (Miscellaneous)

Question 1. What is the exact degree $\deg(f)$ of the functions OR, Parity and Majority?

Question 2. Recall the definition of the block sensitivity $bs(f)$ from the last problem session. Give an example of a function $f$ such that $bs(f) \neq \deg(f)$.

Question 3. Show that $D(f) \geq \deg(f)$ and $R(f) \geq g \deg(f)$ for all $f : \{0, 1\}^n \to \{0, 1\}$.

Problem 2 (Symmetrization)

This problem studies some applications to the symmetrization technique.

Question 1. We showed in the course that any $T$-query quantum algorithm computing the OR function gives rise to a univariate polynomial $P_{\text{sym}}$ such that $\deg(P_{\text{sym}}) \leq 2T$, $P_{\text{sym}}(0) \in [0, 1/3]$ and $P_{\text{sym}}(k) \in [2/3, 1]$ for all $k \in \{1, \ldots, n\}$. Show that any such polynomial must be of degree $\Omega(\sqrt{n})$ by using the next inequality due to Ehlich, Zeller and Rivlin, Cheney:

Let $a, b, c \in \mathbb{R}_{\geq 0}$, $k \in \mathbb{N}$ and $P : \mathbb{R} \to \mathbb{R}$ be a polynomial such that $P(i) \in [a, b]$ for all integers $i \in \{0, 1, \ldots, k\}$ and $|P(x)| \geq c$ for some real $x \in [0, k]$. Then, $\deg(P) \geq \sqrt{ck/(b-a)}$.

Recall the definition of the Parity function: $\text{Parity}(x_1, \ldots, x_n) = x_1 \oplus \cdots \oplus x_n$ and the upper bound $Q(\text{Parity}) \leq n/2$ proved in the last problem session. We aim at showing a matching lower bound.

Question 2.1. Consider the Sign function defined as $\text{Sign}(k) = (-1)^k$. Show that any multilinear polynomial $P$ approximating Parity gives rise to some univariate polynomial $Q$ such that $\deg(Q) \leq \deg(P)$ and $|Q(k) - \text{Sign}(k)| \leq 1/3$ for all $k \in \{0, \ldots, n\}$.

Question 2.2. Show that any polynomial $Q$ satisfying the above constraints must be of degree at least $n$. Conclude that $\overline{\deg(\text{Parity})} = n$ and $Q(f) = n/2$.

For the next two questions, try to reuse the result $\overline{\deg(\text{OR})} = \Omega(\sqrt{n})$ shown in question 1.

Question 3.1. Consider the Palindrome function that evaluates to 1 if and only if $x_i = x_{n-i}$ for all $i$. Show that $\overline{\deg(\text{Palindrome})} = \Omega(\sqrt{n})$.

Question 3.2. Show that $\overline{\deg(f)} = \Omega(\sqrt{bs(f)})$ for any $f : \{0, 1\}^n \to \{0, 1\}$.
Problem 3 (Dual polynomial)

Recall the primal-dual programs introduced in the course:

\[
\begin{align*}
\min_{\epsilon, P} & \quad \epsilon \\
\text{s.t.} & \quad |P(x) - f(x)| \leq \epsilon \quad \forall x \in \{-1, 1\}^n \\
& \quad \deg(P) < d
\end{align*}
\]

\[
\begin{align*}
\max_{\phi} & \quad \sum_{x \in \{-1,1\}^n} \phi(x) \cdot f(x) \\
\text{s.t.} & \quad \sum_{x} \phi(x) = 1 \\
& \quad \sum_{x} \phi(x) \cdot P(x) = 0 \quad \forall P, \deg(P) < d
\end{align*}
\]

**Question 1.** Show that the two programs are indeed linear by converting them into standard form.

**Question 2.** Give a dual polynomial for PARITY witnessing that deg(PARITY) = n.

Problem 4 (Distinguishing distributions)

In this problem, we look at the task of distinguishing between two distributions over \( \{0, 1\}^n \) given queries to an input \( x \) drawn from one of the two distributions. We let \( \mathcal{U} \) denote the uniform distribution over \( \{0, 1\}^n \). We say that a distribution \( D \) over \( \{0, 1\}^n \) is \( k \)-wise independent if for all subsets \( S \subseteq \{1, \ldots, n\} \) of size \( |S| \leq k \), the marginal distribution \( D|_S \) is uniform over \( \{0, 1\}^{|S|} \).

**Question 1.** Show that no randomized query algorithm can distinguish between \( \mathcal{U} \) and a \( k \)-wise independent distribution \( D \) if it makes less than \( k + 1 \) queries.

**Question 2.** By using the polynomial method, show that no quantum query algorithm can distinguish between \( \mathcal{U} \) and a \( 2k \)-wise independent distribution \( D \) if it makes less than \( k + 1 \) queries.

This type of application of the polynomial method can be generalized to other problems that are relevant in cryptography, such as Polynomial Interpolation\(^1\).

---