Quantum Query Complexity
PCMI Graduate Summer School 2023
Instructor: Yassine Hamoudi. Teaching assistant: Angelos Pelecanos.
Course page: `https://yassine-hamoudi.github.io/pcmi2023/`

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* $\mathrm{bs}(f)$ from the last problem session. Give an example of a function f such that $\mathrm{bs}(f) \neq \deg(f)$.

Question 3. Show that $D(f) \geq \deg(f)$ and $R(f) \geq \widetilde{\deg}(f)$ 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_{sym} such that $\deg(P_{\mathrm{sym}}) \leq 2T$, $P_{\mathrm{sym}}(0) \in [0, 1/3]$ and $P_{\mathrm{sym}}(k) \in [2/3, 1]$ for all $k \in \{1, \dots, n\}$. 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 $i \in \{0, 1, \dots, k\}$ 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: $\textsc{Parity}(x_1, \dots, x_n) = x_1 \oplus \cdots \oplus x_n$ and the upper bound $Q(\textsc{Parity}) \leq n/2$ proved in the last problem session. We aim at showing a matching lower bound.

Question 2.1. Consider the $\textsc{Sign} : \mathbb{N} \to \{0,1\}$ function defined as $\textsc{Sign}(k) = (-1)^k$. Show that any multilinear polynomial P approximating Parity gives rise to some univariate polynomial Q such that $\deg(Q) \leq \deg(P)$ and $|Q(k) - \textsc{Sign}(k)| \leq 2/3$ for all $k \in \{0, \dots, n\}$.

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

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

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

Question 3.2. Show that $\widetilde{\deg}(f) = \Omega(\sqrt{\mathrm{bs}(f)})$ for any $f : \{0,1\}^n \to \{0,1\}$.

Problem 3 (Dual polynomial)

Recall the primal-dual programs introduced in the course:

$$\begin{array}{lll} \min_{\epsilon,P} & \epsilon & \\ \text{s.t.} & |P(x)-f(x)| \le \epsilon & \forall x \in \{-1,1\}^n \\ & \deg(P) < d & \end{array}$$

$$\begin{array}{lll} \max_{\phi} & \sum_{x\in\{-1,1\}^n} \phi(x)\cdot f(x) & \\ \text{s.t.} & \sum_x |\phi(x)| = 1 & \\ & \sum_x \phi(x)\cdot P(x) = 0 & \forall P, \deg(P) < d \end{array}$$

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 $\widetilde{\deg}(\text{PARITY}) = n$.

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 $|S| \le k$, 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].

[1] "Quantum Interpolation of Polynomials". D. Kane, S. Kutin. *QIC.*, 2011.