July 25, 2023

Quantum Query Complexity Problem Session 2

Instructor: Yassine Hamoudi Teaching Assistant: Angelos Pelecanos

Problem 1

Question 1

We have seen that for any $f : \{0,1\}^n \to \mathbb{R}$, there exists a *unique* multilinear polynomial P_f such that $P_f(x) = f(x)$ for all $x \in \{0,1\}^n$. Thus it suffices to give a multilinear polynomial that computes each function exactly.

- OR. We can write $x_1 \vee \ldots \vee x_n$ as $\neg(\bar{x_1} \wedge \ldots \wedge \bar{x_n})$. Hence we will use the multilinear polynomial of AND to obtain

$$P_{OR}(x) = 1 - (1 - x_1)(1 - x_2) \ldots (1 - x_n).$$

  Thus the exact degree of OR is n.

- PARITY. If our variables were ± 1, then the product of the variables captures the parity exactly. Hence we will use the transformation $x \to 1 - 2x$ that maps $0 \to 1$ and $1 \to -1$ to obtain

$$P_{PARITY}(x) = (1 - 2x_1)(1 - 2x_2) \ldots (1 - 2x_n).$$

  Thus the exact degree of PARITY is n.

- MAJORITY. We will write the multilinear polynomial by considering all possible inputs. First, define the linear function

$$\mathbf{1}_{z_i}(x_i) = \begin{cases} 1 - x_i & z_i = 0 \\ x_i & z_i = 1 \end{cases}$$

  that outputs 1 if the bits z_i, x_i are equal and 0 otherwise. Now we can easily write P_{MAJ} as a sum of 'indicators' as follows:

$$P_{MAJ}(x) = \sum_{\substack{z \in \{0,1\}^n \\ \mathrm{MAJ}(z)=1}} \prod_{i=1}^{n} \mathbf{1}_{z_i}(x_i).$$

Now we should show that P_{MAJ} has degree n. We just have to consider the coefficient of $x_1 x_2 \ldots x_n$. It is easy to see that its coefficient is $\sum_{k=\lceil n/2 \rceil}^{n} (-1)^{n-k}\binom{n}{k}$, which is never equal to 0.

Question 2

The majority, as we have seen, is a function whose block sensitivity is not equal to its exact degree. Recall that its block sensitivity was $\lceil n/2 \rceil$, whereas its degree is equal to n.

Question 3

We have seen how we can represent a classical query algorithm $\mathcal{A}$ (deterministic or randomized) via a decision tree. If this algorithm makes q queries to its input, then this decision tree has depth at most q. Every leaf of the decision tree v is assigned the value $\mathcal{A}(v)$, which is the output of the algorithm in that branch.

For simplicity, we will use the following linear function

$$\mathbf{1}_{z_i}(x_i) = \begin{cases} 1 - x_i & z_i = 0 \\ x_i & z_i = 1 \end{cases}.$$

Note that $\mathbf{1}_{z_i}(x_i) = 1$ iff $x_i = z_i$. We can then write down a polynomial that has a term for every such leaf. We will represent with $\text{path}(v)$ the set of variables and their values in the path to leaf v. Then the polynomial is

$$P(x) = \sum_{\text{leaf } v} \mathcal{A}(v) \prod_{(x_i, b_i) \in \text{path}(v)} \mathbf{1}_{b_i}(x_i).$$

Since the path to each leaf contains at most q variables, $P(x)$ is a multilinear polynomial with degree at most q.

Now, if $\mathcal{A}$ is a deterministic algorithm, then the number of queries is at most $D(f)$ and the algorithm always succeeds, hence $P(x) = f(x)$. We conclude that $\deg(f) \leq D(f)$. For a randomized $\mathcal{A}$, the number of queries is at most $R(f)$ and the algorithm succeeds with probability at least $\frac{2}{3}$, thus the same polynomial is actually an approximation $\tilde{P}(x)$ to $f(x)$ that satisfies $|\tilde{P}(x) - f(x)| \leq \frac{1}{3}$. We conclude that $R(f) \leq \widetilde{\deg}(f)$.

Problem 2

Question 1

Consider the multivariate polynomial $P(x_1, \ldots, x_n)$ that approximates OR of minimal degree. As in the lecture, we define with B_k to be the set of inputs with Hamming weight k. We will define

$$P_{sym}(k) = \mathop{\mathbb{E}}_{x_1,\ldots,x_n \sim B_k} P(x_1, \ldots, x_n).$$

Since P approximates OR, it should hold that

$$\begin{cases} P_{sym}(0) \in \left[0, \frac{1}{3}\right] \\ P_{sym}(k) \in \left[\frac{2}{3}, 1\right] \quad k \in \{1, \ldots, n\}. \end{cases}$$

Also note that P_{sym} 'jumps' from at most $\frac{1}{3}$ to at least $\frac{2}{3}$ from 0 to 1. Hence there must exist some $x \in [0, 1]$ such that $P'_{sym}(x) \geq \frac{1}{3}$ by the mean value theorem. This allows us to use the Ehlich, Zeller and Rivlin, Cheney inequality with $a = 0, b = 1, c = \frac{1}{3}, k = n$. This implies that $\deg(P_{sym}) \geq \sqrt{\frac{n}{3}}$.

This already implies that

$$Q(OR) \geq \frac{\tilde{\deg}(OR)}{2} = \frac{\deg(P)}{2} \geq \frac{\deg(P_{sym})}{2} \geq \Omega(\sqrt{n}).$$

Question 2.1

Let P be a multilinear polynomial that approximates PARITY. We will define the univariate polynomial Q to be as follows:

$$Q(k) = \mathbb{E}_{\substack{x \in \{0,1\}^n \\ \sum_i x_i = k}} [1 - 2P(x)].$$

Note that $\deg(Q) \leq \deg(P)$ and for any x with odd Hamming weight k we have that $|P(x) - 1| \leq \frac{1}{3} \implies |Q(k) - (-1)| \leq \frac{2}{3}$, and for any x with even Hamming weight k $|P(x) - 0| \leq \frac{1}{3} \implies |Q(k) - 1| \leq \frac{2}{3}$. Thus $Q(k)$ approximates Sign(k) up to $\frac{2}{3}$ additive error.

Question 2.2

This polynomial $Q(k)$ is positive when k is even and negative and k is odd for all $k \in \{0, \ldots, n\}$. This means that it has at least n distinct roots from the mean value theorem, which implies that the degree of Q must be at least n.

Combining with the previous question we conclude that $\tilde{\deg}(\text{PARITY}) = n$ and thus $Q(f) \geq \frac{n}{2}$.

Question 3

Let $\tilde{P}_n$ be the polynomial that achieves the $\tilde{\deg}$ for PALINDROME with n inputs (n is even). Consider the following polynomial

$$P_{sym}(x_1, \ldots, x_n) = 1 - \tilde{P}_{2n}(0, \ldots, 0, x_n, \ldots, x_1)].$$

One can verify that $0 \ldots 0 x_n \ldots x_1$ is a palindrome iff $OR(x_1, \ldots, x_n) = 0$, thus $P_{sym}(x)$ approximates the OR function. now note that the degree of P_{sym} is at most the approximate degree of PALINDROME on $2n$ inputs. Since the approximate degree of OR is $\Omega(\sqrt{n})$, we deduce that $\tilde{\deg}(PAL) = \Omega(\sqrt{n})$ as well.

Question 4

Similar to the previous question, we will embed OR inside the polynomial that approximates f. Let $\tilde{P}_n$ be the polynomial that achieves the $\tilde{\deg}$ for f with n inputs and let y be an input that achieves the maximal number of sensitive blocks $B_1, \ldots, B_k$. For simplicity let $k = bs(f)$. Consider the following polynomial

$$P_{sym}(x_1, \ldots, x_k) = 1 - \tilde{P}_n(y^x).$$

Here we define y^x to be equal to y with the coordinates in B_i flipped if $x_i = 1$. This can be represented as $x_i(1 - y_j) + (1 - x_i)y_j$ if coordinate $j \in B_i$.

Now note that P_{sym} can distinguish between the all-zeros input $\mathbf{0}$ and the inputs with hamming weight exactly one $\mathbf{i}$ from Lecture 1. Using a symmetrization argument, no matter the values of P_{sym} for the rest of the inputs, it must hold that the degree of P_{sym} is at least $\Omega(\sqrt{k}) = \Omega(\sqrt{bs(f)})$. Since $\tilde{P}_n(y^x)$ has the same degree as $\tilde{P}_n(y)$, it must hold

Problem 3

Question 1

Primal. We will represent the degree-($< d$) polynomial using its coefficients $\{\alpha_S\}_{S \subseteq [n]}$ as:

$$P(x) = \sum_{\substack{S \subseteq [n] \\ |S| < d}} \alpha_S x^S,$$

where we define $x^S = \prod_{i \in S} x_i$. Hence the primal becomes:

$$\begin{aligned}
\min_{\epsilon, \{\alpha_S\}_S} \quad & \epsilon \\
\text{s.t.} \quad & \sum_S \alpha_S x^S - f(x) \leq \epsilon && \forall\, x \in \{-1,1\}^n \\
& \sum_S \alpha_S x^S - f(x) \geq -\epsilon && \forall\, x \in \{-1,1\}^n
\end{aligned}$$

We will convert it into standard form using some well-known tricks. First, we will replace the unconstrained coefficients with non-negative ones as follows:

$$\alpha_S := \alpha_S^+ - \alpha_S^-.$$

Additionally, we will change the right hand side variables to be non-negative by changing the sign of both sides. Finally, we change the inequalities to equalities by introducing slack variables, e.g.

$$\sum_S \alpha_S x^S - f(x) + \xi_x = \epsilon.$$

The final format is:

$$\begin{aligned}
\min \; & \epsilon \\
\text{s.t.} \; & \sum_S (\alpha_S^+ - \alpha_S^-) x^S - f(x) + \xi_x = \epsilon && \forall\, x \in \{-1,1\}^n \\
& \sum_S -(\alpha_S^+ - \alpha_S^-) x^S + f(x) + \psi_x = -\epsilon && \forall\, x \in \{-1,1\}^n \\
& \epsilon, \{\alpha_S^{\pm}\}_S, \{\xi_x\}_x, \{\psi_x\}_x \geq 0
\end{aligned}$$

Dual. We will first show that we can 'relax' the second condition to $\sum_x |\phi(x)| \leq 1$, without changing the optimal value. This is because if there exists some ϕ with $\sum_x |\phi(x)| < 1$, then we can obtain $\phi'(x)$, which is scaled up to make the inequality tight. By scaling up to $\phi'(x)$, we are also scaling the objective value, which will give us something larger. This is because the optimal of the dual is always non-negative. Thus we will convert the following program into standard form:

$$\begin{aligned}
\max_{\phi} \quad & \sum_x \phi(x) \cdot f(x) \\
\text{s.t.} \quad & \sum_x |\phi(x)| \leq 1 \\
& \sum_x \phi(x) \cdot P(x) = 0 \qquad\qquad \forall\ P, \deg(P) < d
\end{aligned}$$

We will follow the same recipe as the primal. Write the polynomial ϕ as

$$\phi(x) = \sum_{\substack{S \subseteq [n] \\ |S| \geq d}} (\beta_S^+ - \beta_S^-) x^S.$$

Now we will write the $\sum_x |\phi(x)| \leq 1$ by bounding each term separately, i.e.

$$|\phi(x)| \leq \gamma_x \implies -\gamma_x \leq \phi(x) \leq \gamma_x,\ \forall\ x \in \{\pm 1\}^n,$$

and imposing the condition that $\sum_x \gamma_x = 1$.

The final format is:

$$
\begin{aligned}
\max \quad & \sum_{x} \left[\sum_{\substack{S \subseteq [n] \\ |S| \geq d}} (\beta_S^+ - \beta_S^-) x^S \right] \cdot f(x) \\
\text{s.t.} \quad & \sum_{\substack{S \subseteq [n] \\ |S| \geq d}} (\beta_S^+ - \beta_S^-) x^S + \xi_x = \gamma_x && \forall\, x \in \{\pm 1\}^n \\
& - \sum_{\substack{S \subseteq [n] \\ |S| \geq d}} (\beta_S^+ - \beta_S^-) x^S + \phi_x = \gamma_x && \forall\, x \in \{\pm 1\}^n \\
& \sum_{x} \gamma_x = 1 \\
& \{\beta_S^{\pm}\}_S \geq 0, \{\xi_x\}_x \geq 0, \{\phi_x\}_x \geq 0, \{\gamma_x\}_x \geq 0
\end{aligned}
$$

Question 2

The dual polynomial certificate is $\phi(x) = \frac{1}{2^n} x_1 \ldots x_n$. It is easy to see that $\phi(x) = \frac{1}{2^n} f(x)$, and thus

$$\sum_{x \in \{\pm 1\}^n} \phi(x) \cdot f(x) = 1.$$

Additionally, we can check that $\sum_x |\phi(x)| = 2^n \cdot \frac{1}{2^n} = 1$, and ϕ has no monomial of degree $< n$. Thus, by weak duality $\widetilde{\mathrm{PARITY}} = n$.

Problem 4

Question 1

Since the marginal distribution $D_{|S}$ is uniform over $\{0,1\}^{|S|}$ for any k-wise independent distribution D, any randomized algorithm that makes less than $k+1$ queries will just see a uniform set of bits.

Hence the view of the algorithm is the same for both distributions. Thus the algorithm cannot distinguish between the two distributions.

Question 2

Consider a quantum query algorithm $\mathcal{A}$ that makes less than $k+1$ queries and outputs 1 if it thinks its input $x \in \{0,1\}^n$ was drawn from D and 0 otherwise.

We construct the polynomial $p(x)$ that captures the probability that $\mathcal{A}$ outputs 1 on input x. Since $\mathcal{A}$ makes $\leq k$ queries, then $p(x)$ has degree at most $2k$. Write $p(x)$ as:

$$p(x) = \sum_{\substack{S \subseteq [n] \\ |S| \leq 2k}} \alpha_S x^S.$$

Then the expected behavior of $\mathcal{A}$ for x drawn from D is

$$\begin{aligned} \mathop{\mathbb{E}}_{x \sim D}[\mathcal{A}(x)] &= \mathop{\mathbb{E}}_{x \sim D}[p(x)] \\ &= \mathop{\mathbb{E}}_{x \sim D}\left[\sum_{\substack{S \subseteq [n] \\ |S| \leq 2k}} \alpha_S x^S\right] \\ &= \sum_{\substack{S \subseteq [n] \\ |S| \leq 2k}} \alpha_S \mathop{\mathbb{E}}_{x \sim D}[x^S] \end{aligned}$$

Now note that since D is a $2k$-wise independent distribution, it means that the distribution of any $\leq 2k$ bits is equal to the uniform distribution. Thus we can write

$$\begin{aligned}\mathop{\mathbb{E}}_{x\sim D}[\mathcal{A}(x)] &= \sum_{\substack{S\subseteq[n]\\|S|\leq 2k}} \alpha_S \mathop{\mathbb{E}}_{x\sim\mathcal{U}}[x^S]\\ &= \mathop{\mathbb{E}}_{x\sim\mathcal{U}}[p(x)]\\ &= \mathop{\mathbb{E}}_{x\sim\mathcal{U}}[\mathcal{A}(x)].\end{aligned}$$

As a result, $\mathcal{A}$'s output distribution is the same when given input from D or $\mathcal{U}$. Thus no quantum query algorithm can distinguish between $\mathcal{U}$ and D.