Quantum query complexity

Lecture 2

The polynomial method

Materials: https://yassine-hamoudi.github.io/pcmi2023/

Focus of this lecture

Lower bounds based on the analysis of Boolean functions

- Any quantum algorithm computing f can be transformed into a bounded degree polynomial P such that $P(x) \approx f(x)$.
- Lower bounds on the degree of polynomials

Boolean analysis

<u>Multilinear polynomial:</u> $P(x_1, \ldots, x_n) = \sum_{S \subseteq \{1,\ldots,n\}} a_S \prod_{i \in S} x_i$ where a_S are real coefficients

<u>Degree:</u> $\deg(P) = \max_{a_S \neq 0} |S|$

We are interested in the approximation of Boolean functions $f : \{0,1\}^n \to \mathbb{R}$ by multilinear polynomials

Boolean analysis

Fact: For any $f : \{0,1\}^n \to \mathbb{R}$, there exists a unique multilinear polynomial P_f such that

$$P_f(x) = f(x) \qquad \text{for all } x \in \{0,1\}^n.$$

We denote $\deg(f) = \deg(P_f)$.

relax this condition

Definition: A multilinear polynomial P approximates f if

$$|P(x) - f(x)| \leq 1/3 \quad \text{and} \quad P(x) \in [0,1] \qquad \text{for all } x \in \{0,1\}^n.$$

Definition: The approximate degree of f is $\widetilde{\deg}(f) = \min_{P \text{ approx. } f} \deg(P)$

Boolean analysis

<u>Example:</u> $f = \mathrm{AND}$

(Exact) degree

$$P_f(x) = x_1 x_2 \cdots x_n$$

$$\deg(f) = n$$

Approximate degree

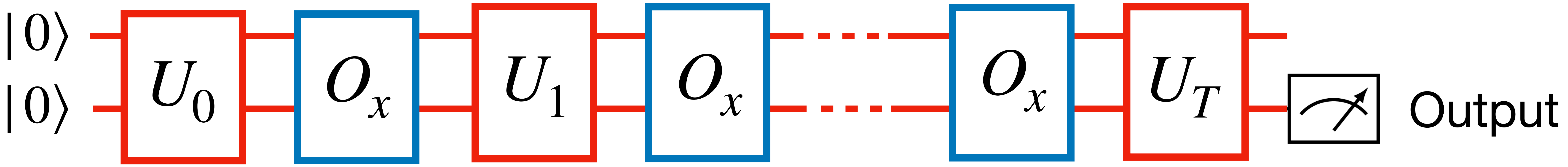
$$\widetilde{\deg}(f) = O(\sqrt{n})$$

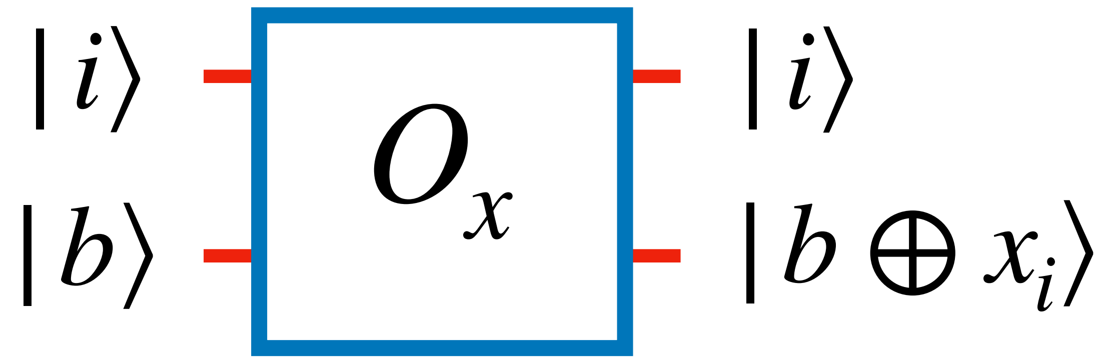
Plug $z = x_1 + \ldots + x_n$ into the (univariate) Chebyshev polynomial $T_d(z)$ of degree $d \approx \sqrt{n}$

Fundamental theorem

Theorem: $Q(f) \geq \widetilde{\deg}(f)/2$

<u>Proposition:</u> Fix a quantum algorithm making T queries. Let $p(x) \in [0,1]$ denote the probability that it outputs 1 on input x. Then $\deg(p) \leq 2T$.





$$|\psi_x^t\rangle = U_t O_x U_{t-1} O_x \ldots U_0 |0,0\rangle$$

Symmetrization

- Reduced the problem of lower bounding the query cpx $Q(f)$ to lower bounding the approximate degree $\widetilde{\deg}(f)$ of n-variable functions.

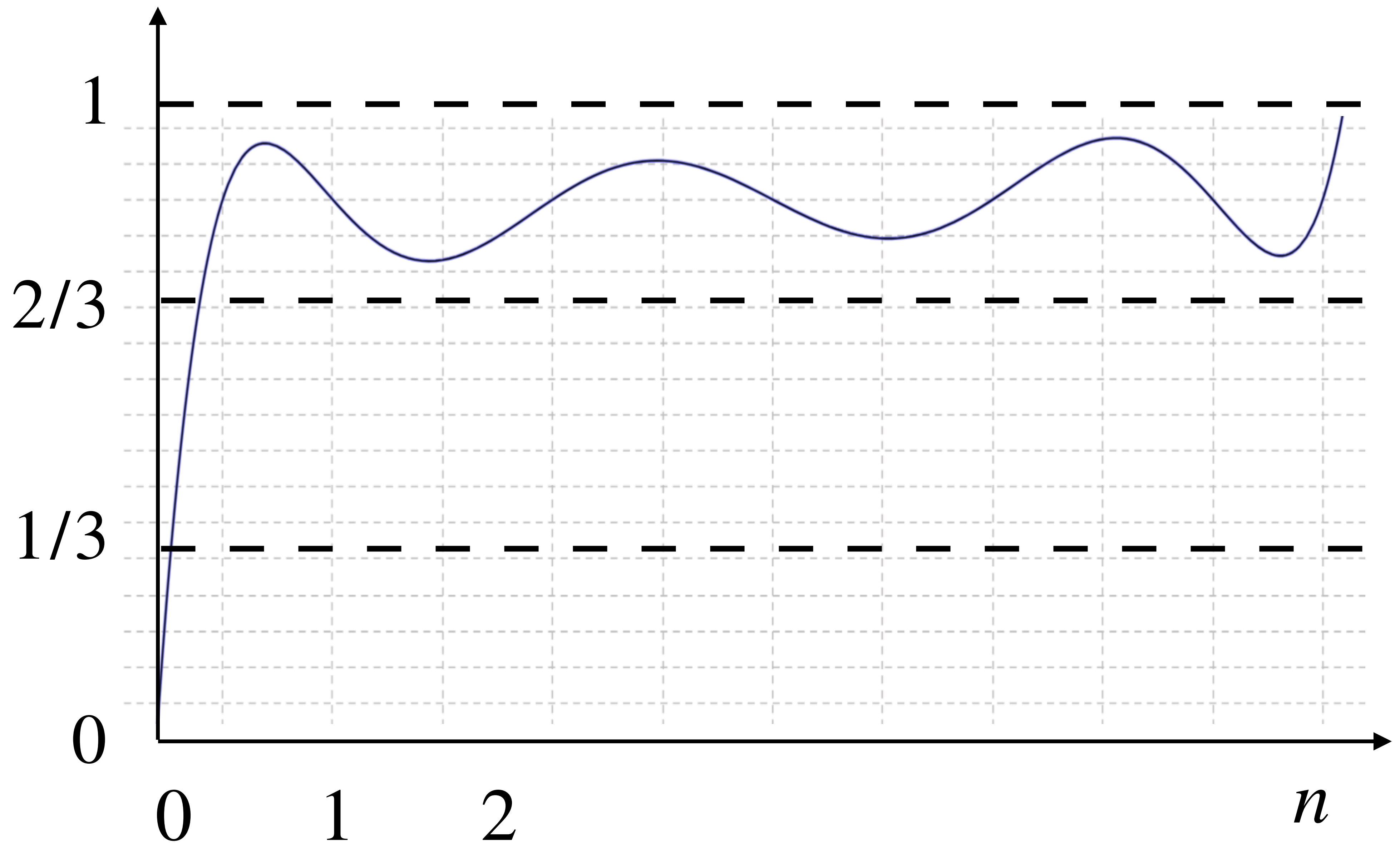
- Multivariate polynomials are often hard to analyze directly.

- Symmetrization is a technique to reduce the number of variables, without increasing the degree ($\widetilde{\deg}(f_{\text{sym}}) \leq \widetilde{\deg}(f)$).

OR function: $f(x) = 0$ if and only if $x = (0,0,\ldots,0)$

- Partition $\{0,1\}^n$ into $n+1$ buckets: $B_k = \{x : x_1 + \ldots + x_n = k\}$
- Fix any polynomial P approximating f and define $P_{\text{sym}}(k) = E_{x \sim B_k} P(x)$

Lemma 1: P_{sym} is a polynomial in k of degree $\deg(P_{\text{sym}}) \le \deg(P)$

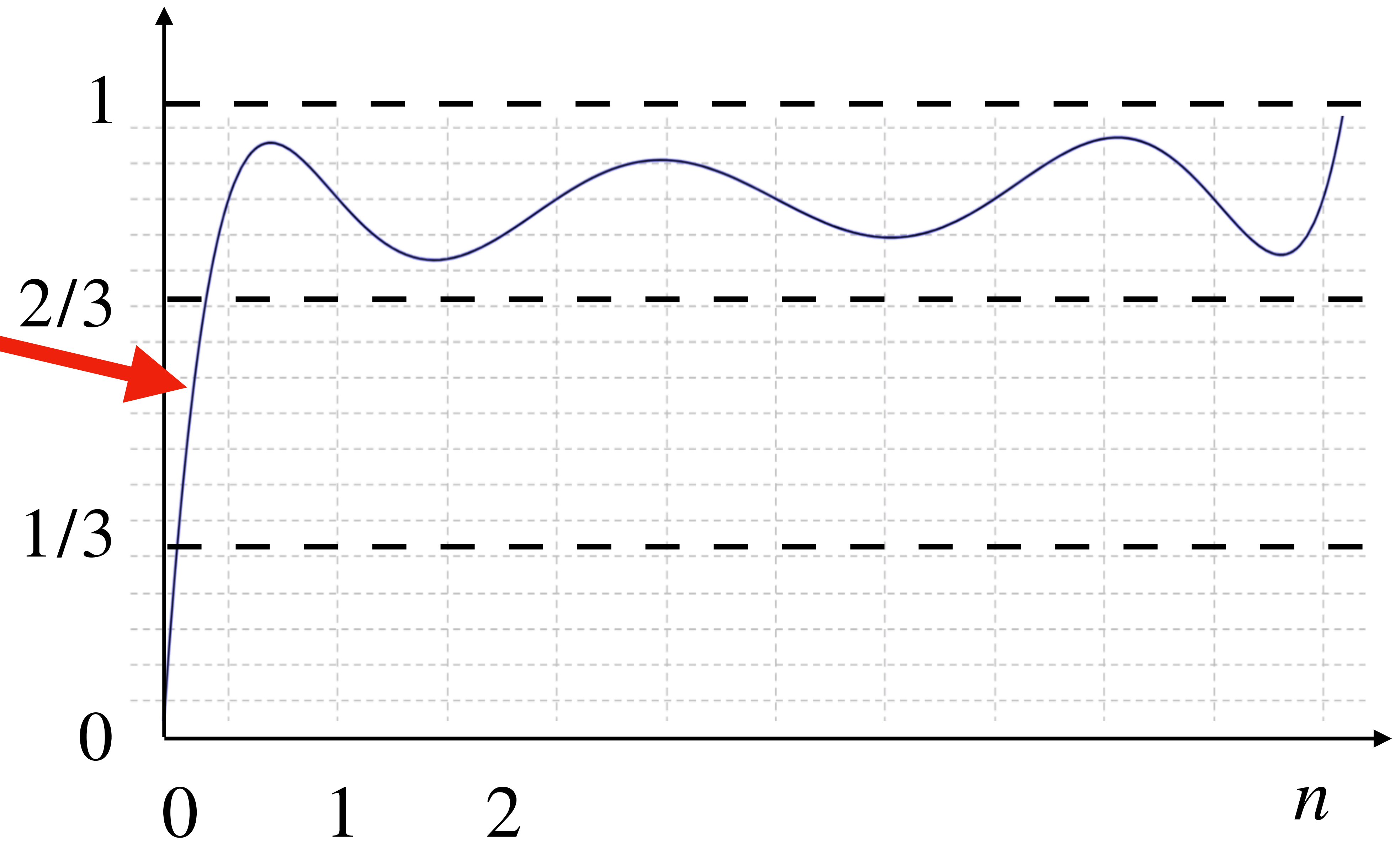


Lemma 2: $P_{\text{sym}}(0) \in [0,1/3]$ and $P_{\text{sym}}(k) \in [2/3,1]$ for $k \ge 1$

<u>OR function:</u> $f(x) = 0$ if and only if $x = (0,0,\ldots,0)$

- Partition $\{0,1\}^n$ into $n+1$ buckets: $B_k = \{x : x_1 + \ldots + x_n = k\}$
- Fix any polynomial P approximating f and define $P_{\text{sym}}(k) = E_{x \sim B_k} P(x)$

Any polynomial that "jumps" this way must have degree $\Omega(\sqrt{n})$



$\Rightarrow Q(\text{OR}) \geq \widetilde{\deg}(\text{OR})/2 = \Omega(\sqrt{n})$

Dual polynomials

For convenience, we express Boolean functions as

$$f : \{-1,1\}^n \to \{-1,1\}$$

$$\min_{\epsilon, P} \ \epsilon$$

s.t. $|P(x) - f(x)| \le \epsilon, \ \forall x \in \{-1,1\}^n$

$\deg(P) < d$

$\epsilon \ge 0$

LP duality $\longrightarrow$

$$\max_{\phi} \ \sum_x \phi(x) \cdot f(x)$$

s.t. $\sum_x |\phi(x)| = 1$

$\sum_x \phi(x) \cdot P(x) = 0, \ \forall P, \deg(P) < d$

"Best approximation of f by a polynomial of degree $< d$"

"Best correlation of f with a polynomial having no monomial of degree $< d$"

By weak duality:

$\exists \phi : \{-1,1\}^n \to \{-1,1\}$ such that

(correlation) $\sum_x \phi(x) \cdot f(x) > 1/3$

(normalization) $\sum_x |\phi(x)| = 1$

(pure high degree) $\sum_x \phi(x) \cdot P(x) = 0, \forall P, \deg(P) < d$

$\Rightarrow \widetilde{\deg}(f) \geq d$

It suffices to exhibit any such ϕ to deduce that $Q(f) \geq d/2$