CS 6810: Theory of Computing	**Fall 2023**

Lecture 12: Sep 28, 2023

Lecturer: Eshan Chattopadhyay — *Scribe: Yunya Zhao*

1 Last class

$\mathbf{AC^0}$ has low degree approximators, more formally, let C be an $\mathbf{AC^0}$ circuit of size s and depth t, then

1. $\exists$ prob. polynomial P of degree $d \leq O(\log^t(s/\varepsilon)$ such that $\forall$ x, $\mathbf{Pr}_{p\sim P}[p(x) = C(x)] \geq 1 - \varepsilon$
2. $\exists$ $p \in P_{n,d}$, $d \leq O(\log^t(s/\varepsilon))$ such that $\mathbf{Pr}_x[p(x) = C(x)] \geq 1 - \varepsilon$,

where $P_{n,d}$ is family of n-variate polynomials of degree at most d (over $\mathbb{F}_2$).

2 Maj does not have low degree approximator

Theorem 2.1. *For any $p \in P_{n,d}$,*

$$\mathbf{Pr}_{x\sim U_n}[p(x) = Maj(x)] \leq \frac{1}{2} + O\left(\frac{d}{\sqrt{n}}\right)$$

This will give us the following:

Theorem 2.2. *For any $C \in \mathbf{AC^0}$ of size s and depth d,*

$$\mathbf{Pr}[C(x) = Maj(x)] \leq \frac{1}{2} + O\left(\frac{\log^t(s/\varepsilon)}{\sqrt{n}}\right) + \varepsilon$$

Suppose circuit C has size s, depth t. Then by last lecture's theorem, there is a probabilistic polynomial P of degree $O(\log^t(s/\varepsilon))$ with error probability $\leq \varepsilon$. This implies that there exists a fixed polynomial p such that $\mathbf{Pr}_{x\sim U_m}[p(x) = Maj(x)] \geq 1 - \varepsilon$.

Setting ε to be a small constant $\varepsilon = 0.1$, we get $s = 2^{\Omega(n^{1/2t})}$

Remark 2.3. *This not only proves against approximation of Maj with polynomial size $\mathbf{AC^0}$ circuits, but also subexponential size.*

Proof of Theorem 2.1. Let p be a polynomial in $P_{n,d}$. Define the following set:

$$A = \{x : Maj(x) = p(x)\}$$

Let $\mathcal{F}_A$ be the family of functions $f : A \to \mathbb{F}_2$. $\mathcal{F}_A$ can be interpretated as a vector space. We make the following observations:

1. $\dim(\mathcal{F}_A) = |A|$, this is because the vector space contains the standard basis.
2. Any $f : \mathbb{F}_2^n \to \mathbb{F}_2$ can be written as $f(x) = Maj(x)f_1(x) + (1 - Maj(x))f_2(x)$ for some f_1, f_2.

Claim 2.4. *There exists f_1 and f_2 with degree no greater than $n/2$.*

Assuming Claim 2.4, any $f \in \mathcal{F}_A$ can be computed by a polynomial with degree no more than $n/2 + d$ since for $x \in A$, $Maj(x) = p(x)$ where $p \in P_{n,d}$. Therefore,

$$|A| = \dim(\mathcal{F}_1) \leq \dim(P_{n,\frac{n}{2}+d})$$

Now we show that $\dim(P_{n,\frac{n}{2}+d}) \leq 2^n(\frac{1}{2} + \frac{c \cdot d}{\sqrt{n}})$ by observing that monomials of degree $\leq (\frac{n}{2} + d)$ form a basis and counting the number of such monomials:

$$\sum_{j=1}^{\frac{n}{2}+d} \binom{n}{j} = (2^{n-1}) + \sum_{j=\frac{n}{2}+1}^{\frac{n}{2}+d} \binom{n}{j} \leq 2^{n-1} d \binom{n}{n/2} = 2^{n-1} + cd\frac{2^n}{\sqrt{n}}$$

Therefore, for $p \in P_{n,d}$

$$\Pr_{x \sim U_n}[Maj(x) = p(x)] = \frac{|A|}{2^n} \leq \frac{1}{2} + \frac{c \cdot d}{\sqrt{n}}$$

□

It remains to prove Claim 2.4. We will prove the following stronger result that will imply Claim 2.4.

Definition 2.5 (Interpolating sets for polynomials)**.** *$S \subset \mathbb{F}_2^n$ is an interpolating set for $P_{n,d}$ if for any $f : S \to \mathbb{F}_2$, $\exists$ unique $p \in P_{n,d}$ such that $\forall x \in S$, $f(x) = p(x)$*

Definition 2.6. *$Ball(x, r) = \{y \in \{0, 1\}^n : \triangle(x, y) \leq r\}$*

Claim 2.7. *$Ball(0^n, d)$ and $Ball(1^n, d)$ are both interpolating sets for $P_{n,d}$.*

Note that this will give us Claim 2.4 by considering $Ball(0^n, n/2)$ which covers all points on which Majority evaluates to 0, and $Ball(1^n, n/2)$ which covers all points on which Majority evaluates to 1.

Proof. The proof for $Ball(0^n, d)$ and $Ball(1^n, d)$ are symmetric, here we only show by induction that $Ball(0^n, d)$ is an interpolating set for $P_{n,d}$.

It's easy to verify the base case holds when $d = 0$.

Now assume claim holds for radius from 0 up to $d - 1$, i.e. for any $f : Ball(0^n, < d) \to \mathbb{F}_2$, $p_{<d}$ is the unique polynomial such that $f(x) = p_{<d}(x)$. Then we show

$$p(x) = \sum_{S \in [n], |S| = d} \alpha_S x^S + p_{<d}(x)$$

computes $f : Ball(0^n, d) \to \mathbb{F}_2$. Let $T = \{i : |y| = d, y_i = 1\}$. For y such that $|y| < d$, $p(y) = p_{<d}(y)$; for y such that $|y| = d$, $p(y) = \alpha_T + p_{<d}(y)$. □