**CS221: Computational Complexity** Prof. Salil Vadhan

# Lecture 22: Parity is not in $\mathbf{AC_0}$

*11/18* *Scribe: Nicholas Shiftan*

**Note:** This lecture was delivered by Emanuele Viola.

Before we begin today's proof, we need to offer somes definitions and notations.

**Definition 1** $\mathbf{AC_0}$ *is the class of languages that can be decided by circuits with constant depth and unbounded fan-in.*

Recall that $\bar{X} := X_1, ...X_n$. Then we can define the Parity ($\oplus$) function as follows:

$$\oplus(\bar{X}) = \sum_i X_i \mod 2$$

In other words, the Parity function on a binary string returns true if the string has an odd number of 1s, and false otherwise.

For the purpose of this lecture, all circuits discussed will be over the basis $\{\vee, \neg\}$. We can still express an AND relationship, though, using DeMorgan's Law:

$$\alpha \wedge \beta = \neg(\neg\alpha \vee \neg\beta)$$

Thus our decision to use this basis will increase our circuit depth by at most a constant factor.

We can now offer the actual theorem:

**Theorem 2** $\oplus$ *cannot be computed by circuits of depth $d$ and size* $2^{n^{o\left(\frac{1}{d}\right)}}$

**Proof:** This proof is attributed to Smolensky. It uses a number of tools, including arithmetization, algebra, and the probabilistic method. The basic idea is simple; we will prove two facts:

- If $f \in \mathbf{AC_0}$, then $f$ is well approximated by a low degree polynomial
- $\oplus$ cannot be approximated by a low degree polynomial

It is trivial to conclude that $\oplus \notin \mathbf{AC_0}$ once we have proved these two facts.

**Claim 3** *Let $C$ have size $s$ and depth $d$. $C$ is 99% approximated by a polynomial of degree* $\log(s)^{O(d)}$ *over* $\mathbb{Z}_3 = \{0, 1, 2\} = \{0, 1, -1\}$

**Proof:** By construction. We will show to how map OR gates and NOT gates to such polynomials. Consider first an OR gate with input $X = \{X_1, ..., X_n\}$. Then,

$$OR(X) = 1 - \prod_i (1 - X_i)$$

Now, this polynomial returns the correct answer 100% of the time, but its degree ($n$) is too high. Before we can show how to lower its degree (at the cost of a slight probability of error), we need to offer another definition:

**Definition 4** *A probabilistic polynomial $p_R$ of degree $d$ is a distribution on polynomials of degree $d$ such that $p_R$ computes $f$ with error $\epsilon$ if $\forall x$,*

$$\underset{R}{P}\{p_R(x) \neq f(x)\} \leq \epsilon$$

Then, if we pick $a_1, ..., a_n \in \mathbb{Z}_3$ at random, we can offer such a probabilistic polynomial $p_{\bar{a}}$ for the OR function:

$$p_{\bar{a}}(\bar{X}) = \sum a_i x_i \qquad \text{where} \qquad \bar{a} \in \mathbb{Z}_3^n$$

Clearly, if $OR(\bar{x}) = 0$, then $p_{\bar{a}}(\bar{x}) = 0$ for every $\bar{a}$. So we just need to show that if $\bar{x} \neq 0$, then $p_{\bar{a}}(\bar{x}) \neq 0$ with high probability. This follows from the fact that $\sum_i a_i x_i$ is a nonzero polynomial of degree 1 *in* $\bar{a}$. Thus, by the Schwartz-Zippel Lemma (the lemma we used to analyze the randomized algorithm for Identity Testing), if we choose $\bar{a}$ randomly in $\mathbb{Z}_3^n$, we have

$$\underset{\bar{a}}{P}\{p_{\bar{a}}(\bar{x}) = 0\} \leq \frac{1}{3}$$

Now, a nice property of $\mathbb{Z}_3$ is that the only nonzero elements are $\{1, 2\} = \{1, -1\}$, both of whose squares are 1. Thus $p_{\bar{a}}^2(X)$ computes OR with probability $\frac{2}{3}$, and has degree 2. But, of course, we can amplify this probability, by taking the OR of $k$ probabilistic polynomials:

$$p_R(\bar{X}) = OR\left(p_{\bar{a}_1}^2(\bar{X}), p_{\bar{a}_2}^2(\bar{X}), ..., p_{\bar{a}_k}^2(\bar{X})\right)$$

The degree of this polynomial is $2k$, and it's error probability is $\left(\frac{1}{3}\right)^k$. So, if we let $k = \log_3 100s$, then our degree is $O(\log s)$, and our error probability is $\frac{1}{100s}$.

Now consider NOT gates. This is far simpler, as we need only one straightforward equation:

$$\neg x = 1 - x$$

Clearly, this arithmetization introduces no error into our equation. Now, let $\hat{p}$ be our "final polynomial", which we can obtain by composing together all the probabilistic polynomials associated with the circuit gates (using different random bits for each). Then $\hat{p}$ has degree $(\log s)^{O(d)}$. So what is the error of $\hat{p}$? For all $x$, the union bound tells us that:

$$\underset{R}{P}\{\hat{p}_R(x) \neq C(x)\} \leq s\left(\frac{1}{100s}\right) = 1\%$$

Furthermore,

$$\underset{x,R}{P}\{\hat{p}_R(x) = C(x)\} \geq 99\% \implies \exists p \text{ s.t. } \underset{x}{P}\{\hat{p}(x) = C(x)\} \geq 99\%$$

And so the proof is complete. ■

Now, we're ready to tackle the other half of this proof.

**Claim 5** *$\oplus$ cannot be 99% approximated by a polynomial of degree $\alpha\sqrt{n}$ (for some $\alpha$) over $\mathbb{Z}_3$.*

**Proof:** By contradiction. Suppose that $\oplus$ can be 99% approximated by a polynomial of degree $\alpha\sqrt{n}$ (for all values of $\alpha$). Thus it follows that there must exist some set $S$ such that $|S| = 99\% \cdot 2^n$ and such that there exists a polynomial $p$ of degree $\alpha\sqrt{n}$ such that $\oplus(x) = p(x)$, for all $x \in S$.

We will show that this implies that all functions on $S$ can be computed by a polynomial of degree $n/2 + \alpha\sqrt{n}$.

To do so, we need first define an alternative version of Parity over $\{-1, 1\}$ instead of $\{0, 1\}$. Clearly, the function $\phi$ maps this transformation $\{0, 1\} \mapsto \{-1, 1\}$:

$$\phi(x) = 2x - 1$$

$$\phi^{-1}(x) = \frac{x+1}{2}$$

Then, if $p(x)$ computes Parity on $\{0, 1\}$ and $p'(x)$ computes Parity on $\{-1, 1\}$, then it follows that we can define $p'(x)$ in terms of $p(x)$:

$$p'(x) = \phi^{-1}(p(\phi(x)))$$

(where by $\phi(x)$ we mean apply $\phi$ to each component of $x$). This is significant, since it tells us that the degree of $p'(x)$ is the same as the degree of $p(x)$; both must have degree $\alpha\sqrt{n}$. But why is $p'(\bar{X})$ important? It follows from the fact that over $\pm 1$, parity has the following unique formula:

$$\oplus'(\bar{X}) = \prod_i X_i,$$

so the low-degree polynomial $p'$ agrees with the high-degree monomial $\prod_i X_i$ on all points in $S$ (actually $\phi(S)$). We will see shortly why this is important.

Consider an arbitrary function $f$ on $S$. It follows that there must exist some polynomial $q$ (although it may be very long) such that $f(x) = q(x)$. Since we're considering only functions over $\{-1, 1\}$, we can assume, without loss of generality, that $q(x)$ is multilinear; that is, it contains only monomials. Thus,

$$q = \sum_{A \subseteq \{X_1, \ldots, X_n\}} c_i X_A,$$

where $X_A = \prod_{i \in A} X_i$. Of course, this polynomial has degree greater than $\frac{n}{2} + \alpha\sqrt{n}$. But we can fix that, using a clever trick which takes advantage of our assumption. Consider an arbitrary $A \subseteq \{X_1, ..., X_n\}$. We then have that

$$X_A \cdot X_{A^c} = X_1 \cdot X_2 \cdot \ldots \cdot X_n = \oplus' \bar{X}$$

But then since we're working over $\{\pm 1\}$ and since thus $X_i^2 = 1$ for all $i$, it follows that

$$X_A = \oplus' \bar{X} \cdot X_{A^c}$$

Now, we can break up our polynomial as follows:

$$\begin{aligned}
q &= \sum_{A \subseteq \{X_1, \ldots, X_n\}} c_i X_A \\
&= \sum_{\substack{A \subseteq \{X_1, \ldots, X_n\} \\ |A| \leq \frac{n}{2}}} c_i X_A + \sum_{\substack{A \subseteq \{X_1, \ldots, X_n\} \\ |A| > \frac{n}{2}}} c_i X_A \\
&= \sum_{\substack{A \subseteq \{X_1, \ldots, X_n\} \\ |A| \leq \frac{n}{2}}} c_i X_A + \sum_{\substack{A \subseteq \{X_1, \ldots, X_n\} \\ |A| > \frac{n}{2}}} c_i \oplus' \bar{X} \cdot X_{A^c} \\
&= \sum_{\substack{A \subseteq \{X_1, \ldots, X_n\} \\ |A| \leq \frac{n}{2}}} c_i X_A + \oplus' \bar{X} \sum_{\substack{A \subseteq \{X_1, \ldots, X_n\} \\ |A| > \frac{n}{2}}} c_i \cdot X_{A^c}
\end{aligned}$$

By assumption, if we replace the $\oplus' \bar{X}$ with $p'(\bar{X})$ without changing the function on $S$. Then the degree of the first sum is $\frac{n}{2}$ and the degree of the second is, after substitution, $n/2 + \alpha\sqrt{n}$. Thus it follows that the total degree is $\frac{n}{2} + \alpha\sqrt{n}$. Thus every function $f : S \mapsto \mathbb{Z}_3$ can be written as a polynomial of degree $\leq \alpha\sqrt{n} + \frac{n}{2}$.

This, however, leads us to a contradiction; a simple counting argument shows us that there are more functions on $S$ than polynomials of degree $\leq \alpha\sqrt{n} + \frac{n}{2}$. (We will do all our counting $\log_3$ for simplicity)

$$\log_3(\#\text{ functions on } S) = |S| = 99\%2^n$$

$$\begin{aligned}
\log_3(\#\text{ polynomials of degree } \alpha\sqrt{n} + \tfrac{n}{2}) &= \sum_{i=0}^{\frac{n}{2}+\alpha\sqrt{n}} \binom{n}{i} \\
&= \sum_{i=0}^{\frac{n}{2}} \binom{n}{i} + \sum_{i=\frac{n}{2}}^{\frac{n}{2}+\alpha\sqrt{n}} \binom{n}{i} \\
&= \frac{2^n}{2} + \sum_{i=\frac{n}{2}}^{\frac{n}{2}+\alpha\sqrt{n}} \binom{n}{i} \\
&< \frac{2^n}{2} + \sum_{i=\frac{n}{2}}^{\frac{n}{2}+\alpha\sqrt{n}} \frac{2^n}{\sqrt{n}} \\
&< \frac{2^n}{2} + \alpha 2^n
\end{aligned}$$

Thus there exist values of $\alpha$ (any value less than .49) such that there are more functions on $S$ than polynomials of degree $\frac{n}{2} + \alpha\sqrt{n}$. Since a contradiction has been forced, it follows that our assumption must have been false. Thus $\oplus$ cannot be 99% approximated by a polynomial of degree $\alpha\sqrt{n}$ for all values of $\alpha$. ∎

To conclude our proof, suppose we have a circuit computing $\oplus$ in degree $d$ and size $s$. From the first claim, we know that the circuit can be approximated by a poly. of degree $\log(s)^{O(d)}$. And from the second lemma, we know that the circuit cannot be approximated by a polynomial of degree $\alpha\sqrt{n}$. Thus, it follows that

$$\begin{aligned}
\log(s)^{O(d)} &\geq \alpha\sqrt{n} \\
\log(s) &\geq n^{\Omega(\frac{1}{d})} \\
s &\geq 2^{n^{\Omega(\frac{1}{d})}}
\end{aligned}$$

And our proof is complete. ∎