CS 6810: Theory of Computing **Fall 2021**

Lecture 23: Nov 16, 2021

Lecturer: Jyun-Jie Liao *Scribe: Ricky Shapley*

1 Circuit Lowerbounds

In studying circuits one of our ultimate goals is to show that $\mathbf{NP} \not\subseteq \mathbf{P}/\text{poly}$, as this implies that $\mathbf{P} \neq \mathbf{NP}$. To do this, ideally we want to find a function $f \in \mathbf{NP}$, that is not contained in $\mathbf{P}/\text{poly}$, or in other words, a function where $\text{size}(f)$ is superpolynomial.

But the best current result we know is that we can find $f \in \mathbf{P}$ where $\text{size}(f) \geq 5n - o(n)$ [3][2].

So instead of working on $\mathbf{P}/\text{poly}$, we will work on a simpler class of circuits: $\mathbf{AC}^0$. Today we will show that $\textsc{Parity} \notin \mathbf{AC}^0$.

Definition 1.1 ($\mathbf{AC}^0$)**.** *We say a circuit family is in $\mathbf{AC}^0$ if it has constant depth, has unbounded fan-in (and fan-out), and has polynomial size. We say a circuit family is in $\mathbf{AC}^0(s(n), d)$ if it has size $\leq s(n)$ and depth $\leq d$.*

For example, any CNF is in $\mathbf{AC}^0$, because it can be expressed as a depth 2 circuit.

Definition 1.2 (Parity)**.** *We define the parity function $\bigoplus$ as $\bigoplus(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i \mod 2$.*

The best result we know about Parity is that $\bigoplus \notin \mathbf{AC}^0(2^{O(n^{\frac{1}{d-1}})}, d)$ by Håstad[1]. But today, we will prove the slightly weaker result by Razborov[4] and Smolensky[5], that $\bigoplus \notin \mathbf{AC}^0(2^{O(n^{\frac{1}{2d}})}, d)$. Both of these results indicate that $\textsc{Parity} \notin \mathbf{AC}^0$, as any constant depth circuit calculating parity would require exponential size.

To prove this, we will prove the following two claims:

1. $\forall C \in \mathbf{AC}^0$ and $\forall n$, there is a degree k polynomial g over $\mathbb{F}_3$ satisfying
$$\Pr_{x \in \{0,1\}^n}[C_n(x) = g(x)] \geq 0.99$$
where we will later choose k to be $\sqrt{n}$.
2. $\bigoplus$ cannot be approximated by a degree $\sqrt{n}$ polynomial. Formally, $\forall$ degree k polynomials h over $\mathbb{F}_3$,
$$\Pr_x[\bigoplus(x) = h(x)] < 0.99.$$

To prove the first claim, we will construct a polynomial gadget (over $\mathbb{F}_3$) for every logical gate. Given a function $f(x)$ with boolean value, we can pass it through a NOT gate and the write the result as $1 - f(x)$. For an AND gate, we can take the product of the boolean valued input functions. And for an OR gate, we can use De Morgan's laws to express the output. But this formulation has the problem that in our AND and OR gadgets, the degree of our polynomial is too large. So instead, we will use randomness to create a good approximation.

We will describe how to represent an OR gate over input functions $f_1, \ldots, f_t$. Then, we randomly sample a set $S \subseteq [t]$, where each element of $[t]$ is chosen with probability $1/2$. Then,

$$\Pr_S\left[\sum_{i \in S} f_i \neq 0 \mod 3\right] \geq \frac{1}{2}$$

if any $f_i = 1$. To see this, we partition all subsets of $[t]$ into those containing i and those not containing i. Then there is a natural bijection between the two of pairs of subsets: a set $T \subseteq [t]$ not containing i and the set $T \cup \{i\}$. Since $f_i = 1$, $\sum_{j \in T} f_j$ and $\sum_{j \in T \cup \{i\}} f_j$ must differ by 1 and cannot both be 0. And since all subsets can be chosen with equal probability, the total probability that the sum is non-zero must be at least $1/2$.

By squaring, this statement becomes

$$\Pr_S \left[\left(\sum_{i \in S} f_i \right)^2 = 1 \mod 3 \right] \geq \frac{1}{2}.$$

Again, we can use De Morgan's laws to construct AND gates with the same degree.

Now, let $g_S = \left(\sum_{i \in S} f_i\right)^2$. Our above result indicates that

$$\forall x, \Pr_S \left[g_S(x) = \bigvee_i f_i(x) \right] \geq \frac{1}{2}$$

as if all $f_i(x)$ are 0, then g_S always outputs 0. But we want to minimize the error rate, which we can do by repetition. For r samples of S, (labeled $S_1, \ldots, S_r$), we will let

$$g = 1 - \prod_{i=1}^{r} (1 - g_{S_i}).$$

Then, if any g_{S_i} correctly outputs 1, then g will output 1. So this gives us a probability of error of 2^{-r} for an OR gate. And $\deg(g) \leq 2r \cdot \max(\deg(f_i))$.

So for a polynomial g_C that approximates the entire circuit C using the gadget we described above, $\deg(g_C) \leq (2r)^d$, since at each level in our circuit, the degree increases by at most a factor $2r$, and we begin on the first level with degree 1 polynomials $(x_1, \ldots, x_n)$.

By using a union bound over all the gates in the circuit C, we get that

$$\forall x, \Pr_{g_C}[g_C(x) = C(x)] \geq 1 - \frac{s(n)}{2^r}.$$

And we can take $r = O(\log(s(n))$ to achieve the desire 0.99 bound.

This means that

$$\begin{aligned} \mathop{\mathbb{E}}_{x, g_C}[\mathbb{1}\{g_C(x) = C(x)\}] &\geq 0.99 \\ \exists g_C \text{ s.t. } \mathop{\mathbb{E}}_{x}[\mathbb{1}\{g_C(x) = C(x)\}] &\geq 0.99 \\ \exists g_C \text{ s.t. } \Pr_{x}[g_C(x) = C(x)] &\geq 0.99 \end{aligned}$$

as desired.

And we have our $k = \deg(g_C) \leq O(\log(s(n)))^d$. So as long as we have $s(n) = 2^{O(n^{\frac{1}{2d}})}$, we have $k \leq \sqrt{n}$.

Now we will prove the second claim (that $\bigoplus$ cannot be approximated by a degree $\sqrt{n}$ polynomial in $\mathbb{F}_3$.

Let's suppose for a contradiction that there is some function h such that $\deg(h) \leq \sqrt{n}$ and $\Pr_x[\bigoplus(x) = h(x)] \geq 0.99$. We construct the set $G = \{x \in \{0,1\}^n : h(x) = \bigoplus(x)\}$. And by our supposition, $|G| \geq 0.99 \cdot 2^n$. Now we will show that this is impossible.

Consider the bijective mapping of $\{0,1\}$ to $\{1,-1\}$, where if $x_i = 0$, then $y_i = 1$, and if $x_i = 1$, then $y_i = -1$. Then if we call $\bigoplus'$ the parity function on our translated variables, we have

$$\bigoplus(x) = \bigoplus'(y) = \left(\prod_{i=1}^{n} y_i\right) - 1$$

We can also translate the function h on to the function h' on $\{1,-1\}$. Then $h(x) = h'(y)$, and the degree of h' should be no more than the degree of h, since $h(x)$ on $x_i = y_i - 1$ gives us $h'(y)$.

We will also convert G to $G' \subseteq \{1,-1\}$. Let $G' = \{y \in \{1,-1\}^n : h'(y) = \bigoplus'(y)\}$.

Consider an arbitrary function $F : G' \to \mathbb{F}_3$. We claim that there is a polynomial p such that for all $y \in G'$, $p(y) = F(y)$ and $\deg(p) \leq n/2 + \sqrt{n}$.

The first claim is that for any F, we can find some polynomial $f : \mathbb{F}_3^n \to \mathbb{F}_3$ such that $\forall y \in G'$, $f(y) = F(y)$. We can use a product of n degree 1 terms to check if our input matches a particular y and multiply by $F(y)$. Taking the sum over all such terms produces such a polynomial. Each monomial of this f could have up to degree n (each y_i appearing once). So to reduce the degree, if we see the monomial $y_1 y_2 \dots y_n$, we can replace it with $h'(y)$. And similarly if a monomial has degree more than $n/2$, we replace it with $h'(y) \prod_{i \in M} y_i$ where M is the set of indices missing from the monomial. (Remember that $y \in \{1,-1\}$, so multiplying by y_i is equivalent to factoring it out.) By doing this, since $h'(y)$ has degree at most $\sqrt{n}$, the degree of our resulting polynomial is no more than $n/2 + \sqrt{n}$.

There are $3^{|G'|}$ functions from G' to $\mathbb{F}_3$, and all of them can be represented by polynomials of degree at most $n/2 + \sqrt{n}$. So

$$3^{|G'|} \leq 3^{\sum_{i=0}^{n/2+\sqrt{n}} \binom{n}{i}}$$

where the right term is the number of such polynomials. For large enough n (which by my calculations is $n \geq 83$), we have $\sum_{i=0}^{n/2+\sqrt{n}} < 0.99 \cdot 2^n$, and hence $|G| = |G'| < 0.99 \cdot 2^n$, a contradiction.

This completes our proof.

References

[1] Johan Håstad. Computational limitations of small-depth circuits. 1987.

[2] Kazuo Iwama and Hiroki Morizumi. An explicit lower bound of 5n- o (n) for boolean circuits. In *International Symposium on Mathematical Foundations of Computer Science*, pages 353–364. Springer, 2002.

[3] Oded Lachish and Ran Raz. Explicit lower bound of 4.5 n-o (n) for boolena circuits. In *Proceedings of the thirty-third annual ACM symposium on Theory of computing*, pages 399–408, 2001.

[4] Alexander A Razborov. Lower bounds on the size of bounded depth circuits over a complete basis with logical addition. *Mathematical Notes of the Academy of Sciences of the USSR*, 41(4):333–338, 1987.

[5] Roman Smolensky. Algebraic methods in the theory of lower bounds for boolean circuit complexity. In *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, pages 77–82, 1987.