**Notes on Complexity Theory** Last updated: March, 2008

Lecture on Parity

*Jonathan Katz*

# 1 Parity is Not in $\mathsf{AC}^0$

Recall that $\mathsf{AC}^0$ is the set of languages/problems decided by *constant-depth* circuits (with unbounded fan-in) of polynomial size. (We allow circuits to have AND, OR, and NOT gates, and do not count NOT gates when measuring the depth or size of the circuit.) In this lecture we give the "polynomial proof" of the result that parity cannot be computed in $\mathsf{AC}^0$. We will actually prove something stronger:

**Theorem 1** *For sufficiently large $n$, any depth-$d$ circuit that computes parity on $n$-bit inputs must have at least $\frac{1}{50} \cdot 2^{0.5 \cdot n^{1/2d}}$ gates.*

Thus, for any fixed depth-bound $d$, any circuit family computing parity grows as $2^{n^\varepsilon}$ for some $\varepsilon > 0$.

**Proof** Fix a circuit $C$ of depth $d$ that computes parity on inputs of length $n$. Let $x_1, \ldots, x_n$ denote the inputs to the circuit. We will assume that $C$ has only OR gates and NOT gates; this assumption is without loss of generality since we may convert any AND gate to a combination of OR and NOT gates using De Morgan's laws (by setting $\bigwedge_i a_i = \neg \bigvee_i (\neg a_i)$) without affecting the size or depth of the circuit.

Let $\mathbb{F}_3 = \{-1, 0, 1\}$ be the field of size 3. Say a polynomial $p \in \mathbb{F}_3[x_1, \ldots, x_n]$ is *proper* if $p(x_1, \ldots, x_n) \in \{0, 1\}$ whenever $x_1, \ldots, x_n \in \{0, 1\}$. Note that any proper polynomial can be viewed as a boolean function in the natural way.

The proof hinges on two lemmas: we first show that any circuit in $\mathsf{AC}^0$ can be approximated fairly well by a (proper) low-degree polynomial, and then show that parity cannot be approximated well by any low-degree polynomial.

**Lemma 2** *For every integer $t > 0$, there exists a (proper) polynomial of total degree $(2t)^d$ that differs with $C$ on at most $\mathsf{size}(C) \cdot 2^{n-t}$ inputs.*

**Proof** We will associate a proper polynomial with each wire of the circuit, and then bound the error introduced. Begin at the input wires and associate the monomial $x_i$ to the input $x_i$. Now consider the output wire of some gate $g$, all of whose input wires have already been associated with polynomials. Then:

- If $g$ is a NOT gate, and its input wire is associated with the polynomial $p$, then associate its output wire with $1 - p$. Note that this does not increase the degree of the polynomial.
- If $g$ is an OR gate with $k$ input wires associated with the polynomials $p_1, \ldots, p_k$, then do the following:

> Choose sets $S_1, \ldots, S_t \subseteq [k]$ (see below for how these sets are chosen), and define $q_i = \left(\sum_{j \in S_i} p_j\right)^2$ for $i = 1, \ldots, t$. Then set $p = 1 - \prod_{i=1}^{t}(1 - q_i)$.
>
> (Note that $p$ is just the OR of the $q_i$.) If the maximum (total) degree of the $\{p_i\}$ is $b$, then the (total) degree of polynomial $p$ is at most $2tb$. Note further that if the $\{p_i\}$ are all proper then so is $p$.

For a given wire with associated polynomial $p$, an *error* is an input $x_1, \ldots, x_n$ on which the value of the wire and the value of $p$ differ. We now bound the fraction of errors in the polynomial $p^*$ associated with the output wire of the circuit. No errors are introduced at input wires or at NOT gates. Looking at any OR gate with $k$ input wires associated with the polynomials $p_1, \ldots, p_k$, we claim that there is *some* choice of subsets $S_1, \ldots, S_t \subseteq [k]$ that will not introduce too many errors. On any input where all the $p_i$'s evaluate to 0, the resulting polynomial $p$ will also evaluate to 0. Consider any input where at least one of the $p_i$'s evaluates to 1, and let $S_1, \ldots, S_t$ be random subsets of $[k]$. With probability at least half over choice of subset $S_j$, polynomial $q_j$ will evaluate to 1. If *any* of the $q_j$ evaluate to 1 then so does $p$. So the probability that $p$ does not evaluate to 1 is at most $2^{-t}$. By an averaging argument, this implies the *existence* of some collection of subsets which introduce errors on at most a $2^{-t}$ fraction of the inputs at this gate.

Taking a union bound, we conclude that $p^*$ is a polynomial of degree at most $(2t)^d$ having at most $\mathsf{size}(C) \cdot 2^{n-t}$ errors with respect to $C$. ■

Setting $t = n^{1/2d}/2$ we get a polynomial of degree at most $\sqrt{n}$ that differs from $C$ on at most $\mathsf{size}(C) \cdot 2^{n-t}$ inputs.

**Lemma 3** *Let $p \in \mathbb{F}_3[x_1, \ldots, x_n]$ be a proper polynomial of degree at most $\sqrt{n}$. Then for sufficiently large $n$ the polynomial $p$ differs from the parity function on at least $2^n/50$ inputs.*

**Proof** Consider the "translated" parity function $\mathsf{parity}' : \{-1, 1\}^n \to \{-1, 1\}$ defined as $\mathsf{parity}'(x_1, \ldots, x_n) = \prod_i x_i$. Since

$$\mathsf{parity}'(x_1, \ldots, x_n) = \mathsf{parity}(x_1 - 1, \ldots, x_n - 1) + 1\,,$$

we see that there exists a polynomial $p'$ of degree at most $\sqrt{n}$ that agrees with $\mathsf{parity}'$ on the same number of inputs for which $p$ agrees with $\mathsf{parity}$.

Let $S \subseteq \{-1, 1\}^n$ be the set of inputs on which $p'$ and $\mathsf{parity}'$ agree, and let $\mathcal{F}$ denote the set of *all* functions from $S$ to $\mathbb{F}_3$. Note that $|\mathcal{F}| = 3^{|S|}$. Now, for every function $f \in \mathcal{F}$ we can associate a polynomial $p_f \in \mathbb{F}_3[x_1, \ldots, x_n]$ that agrees with $f$ for all $\vec{x} \in S$: just set

$$p_f(x_1, \ldots, x_n) = \sum_{\vec{y} \in S} f(\vec{y}) \cdot \prod_{i=1}^{n}(-y_i x_i - 1)\,.$$

Although $p_f$, as constructed, has degree 1 in each input variable, the total degree of $p_f$ may be as large as $n$. We claim that, in fact, we can associate with each $f$ a polynomial $\hat{p}_f$ whose degree is at most $n/2 + \sqrt{n}$. To see this, fix $f$ and $p_f$ and look at some monomial

$\pm\prod_{i\in T} x_i$ appearing in $p_f$ where $|T| > n/2+\sqrt{n}$. For any $\vec{x} \in S \subset \{-1,1\}^n$ we have

$$\begin{aligned}\pm\prod_{i\in T} x_i &= \pm\prod_{i=1}^{n} x_i \cdot \prod_{i\notin T} x_i \\ &= \pm p'(\vec{x}) \cdot \prod_{i\notin T} x_i\,.\end{aligned}$$

Since $p'$ has degree at most $\sqrt{n}$, we see that we can re-write $p_f$ to a polynomial $\hat{p}_f$ that agrees with $p_f$ on $S$ and has degree at most $n/2+\sqrt{n}$.

The number of monomials whose total degree is at most $n/2+\sqrt{n}$ is $\sum_{i=0}^{n/2+\sqrt{n}} \binom{n}{i}$, which is less than $49 \cdot 2^n/50$ for large enough $n$. So the total number of polynomials whose degree is at most $n/2+\sqrt{n}$ is upper bounded by $3^{49\cdot 2^n/50}$. Given that $|\mathcal{F}| = 3^{|S|}$, this means we must have $|S| \leq 49 \cdot 2^n/50$ as claimed. ■

To complete the proof, we just combine the two lemmas. The first lemma gives a polynomial $p$ of degree at most $\sqrt{n}$ that differs from parity on at most $\mathsf{size}(C)\cdot 2^{n-n^{1/2d}/2}$ inputs. The second lemma tells us that, for large enough $n$, we must have $\mathsf{size}(C)\cdot 2^{n-n^{1/2d}/2} \geq 2^n/50$. We conclude that $\mathsf{size}(C) \geq \frac{1}{50}\cdot 2^{0.5\cdot n^{1/2d}}$, completing the proof. ■

## Bibliographic Notes

This proof approach is due to Razborov [2] and Smolensky [3] (who proves a more general result), though earlier proofs that parity was not in $\mathsf{AC}^0$ were given by Furst, Saxe, and Sipser, by Yao, and by Håstad. The article by Boppana and Sipser [1] contains a good write-up of this result and other circuit lower bounds.

## References

[1] R. Boppana and M. Sipser. The Complexity of Finite Functions. In *Handbook of Theoretical Computer Science, vol. A: Algorithms and Complexity*, J. van Leeuwen, ed., MIT Press, 1990.

[2] A. Razborov. Lower Bounds on the Size of Bounded Depth Networks Over a Complete Basis with Logical Addition. *Matematicheskie Zametki* 41:598–607, 1987.

[3] R. Smolensky. Algebraic Methods in the Theory of Lower Bounds for Boolean Circuit Complexity. STOC 1987.