18.405J/6.841J Advanced Complexity Theory	March 17, 1998
Lecture 11	
Lecturer: Daniel A. Spielman	*Scribe: Abby Knickerbocker*

This lecture presents a first proof that parity is not in AC^0. Recall that AC^0 is the class of languages decided by a logspace-uniform family of polynomial-size, constant-depth circuits. Each circuit is composed of inverters and AND and OR gates with an unbounded number of inputs. (Inverters are excluded when measuring the depth or size of a circuit.) Also recall that parity is the language of binary strings containing an odd number of ones. Parity can also be regarded as the boolean function which is 1 when an odd number of the inputs are 1.

The result is originally due to Furst-Saxe-Sipser and Ajtai. We will actually prove something stronger: that a parity circuit of constant depth must have exponential size. The proof given here is similar to that given in Beigel-Reingold-Spielman, which in turn uses an idea of Smolensky.

1 Approximating the OR function

Recall:

$$S_a = \sum_{i=1}^{N}\left[x_i \prod_{k=1}^{a}\left[1-\frac{1}{2}\left(1-\prod_{j=1}^{n}(1-2i_j r_j^{(k)})\right)\right]\right]$$

for the following:

- $1 \le a \le n+1$;
- $x_i : 1 \le i \le N$;
- $r_j^k : 1 \le j \le n$;
- $n = \lceil \log N \rceil$;
- $1 \le k \le n+1$;
- $x_i \in \{0,1\}$;
- $r_j \in \{0,1\}^n$

properties of S:

1. if $\sum x_i = 0$ then $S_a(x,r) = 0$
2. if $2^{a-2} \le \sum_{i=1}^{N} x_i \le 2^{a-1}$ then $S_a(x,r) = 1$, with probability $\ge \frac{1}{8}$ over the choice of r's.

We want a polynomial that approximates the OR function; in order to do so, make a polynomial V that is 1 if any of the S_a's are 1.

- $OR(y_1, ..., y_k) = 1 - \prod_{i=1}^{k}(1-y_i)$
- $degree(OR(x_1, ..., x_N)) = N$
- $V(x,r) = OR(S_1(x,r), ..., S_{n+1}(x,r)) = 1 - \prod_{a=1}^{n+1}(1-S_a(x,r))$

properties of V:

1. if $\sum x_i = 0$ then $V = 0$
2. if $\sum x_i \geq 0$ then $V(x, r) = 1$ with probability $\geq \frac{1}{8}$ over the choice of r.

In order to amplify the probability of correctness, repeat this many times, with different random variables:

$$1 - \prod_{b=1}^{m} (1 - V(x, r_b)) = V^m$$

this polynomial $= 0$ if $[OR(x_1, ..., x_N) = 0]$ and $= 1$ with probability $\geq 1 - (\frac{7}{8})^m$ if $[OR(x) = 1]$.

- in x_i's, *degree* $= O(m \log(N))$
- number of random variables $= O(m \log^2(N))$
- in random variables, *degree* $= O(m \log^3(N))$

2 Main Theorem and Proof Idea

AC^0 is the class of polynomial-sized circuits using AND, OR, and NOT gates, with constant depth and unbounded fanin. The parity function, given inputs $x_1, ..., x_n$ computes $\sum x_i \ mod \ 2$. The theorem proved in this lecture is that the parity function cannot be computed in AC^0.

Theorem 1 *parity* $\notin AC^0$.

Proof Take an AC^0 circuit, having $g = polynomial(N)$ gates (NOTE: We can just use OR and NOT gates to represent all gates in the circuit and still maintain its size). Replace all the bottom level gates with polynomials V^m. These have degree $\leq O(m \log(N))$. Now replace every single gate by a polynomial. Choose m such that $(\frac{7}{8})^m < \frac{1}{4g}$, so $m = O(g) = g$. Then with probability $\geq \frac{3}{4}$, this circuit of polynomials produces the correct answer.

We can use the same set of random variables for each polynomial. If the probability that a particular gate is wrong is $< \frac{1}{4g}$, then the probability that there exists a wrong gate is $< \frac{1}{4}$.

- degree of each polynomial $\leq O(m \log(g))$
- degree of entire polynomial (after composition) is $O((m \log(g))^d)$ in the x_i's
- degree in the random variables is $O((m \log^3(g))^d)$ using only $O(m \log^2(g))$ random variables.

Now we have a polynomial, let's call it $p(x_1, ..., x_N)$, having a degree of $O(\log(g)^{2d})$ that is supposed to compute the parity function with probability $\geq \frac{3}{4}$. As we will see, this implies that $\log(g) = \Omega(n^{\frac{1}{4d}})$. In other words, $g = 2^{\Omega(n^{\frac{1}{2d}})}$, which proves the theorem.

Fix the random variables so that p is correct on $\geq \frac{3}{4}$ of its inputs. Perform the linear transformation :

$$1 = true \rightarrow -1$$

$$0 = false \rightarrow 1$$

Now the parity function on inputs $(x_1, ..., x_N)$ is computed by $\prod_{i=1}^{N} x_i$.

Let T be the subset of $\{-1,1\}^N$ on which p computes parity. Consider the real functions over T. Every function over the reals on T can be expressed by a polynomial in $x_1, ..., x_N$. Since for all $x_i \in \{1,-1\}$, $x_i^2 = 1$, every real function on T can be expressed by a polynomial in which the degree of any $x_i \leq 1$, so the total degree $\leq N$.

Claim: Can do this in $degree \leq \frac{N}{2} + degree(p)$.

On T, $p(x) = \prod_{i=1}^{N} x_i$. Any monomial of degree $> \frac{N}{2}$ can be expressed as $p(x) \cdot monomial$, where the *monomial* is the product of the complement of the variables in the original. This gives us a basis of real functions on T of dimension

$$\sum_{i=0}^{\frac{N}{2}+degree(p)} \binom{N}{i}$$

However, the dimension of this space is $= |T|$ because the standard basis has elements that are 1 at one point of T and 0 elsewhere. So, $|T| \geq \frac{3}{4} \cdot 2^N$. If $degree(p) = o(\sqrt{N})$ then we arrive at a contradiction:

$$\sum_{i=0}^{\frac{N}{2}+degree(p)} \binom{N}{i} < (\frac{1}{2} + o(1)) \cdot 2^N, \qquad < |T| \quad \Rightarrow contradiction!$$

$\Rightarrow g \geq 2^{\Omega(n^{\frac{1}{4d}})}$, which is certainly super-polynomial.

■