18.405J/6.841J Advanced Complexity Theory	March 16, 2000
Lecture 13	
Lecturer: Dan Spielman	*Scribe: Andrew Glenn*

In lecture 10, we introduced the class AC_0 and showed that parity $\notin \mathrm{AC}_0$. This lecture presents a second proof of this assertion, published by Furst, Saxe and Sipser (1984).

1 Setup and Definitions

Definition 1 *A restriction is a function ρ such that:*

$$\rho(x_i) = \left\{ \begin{array}{ll} 0,1 & (fixed) \\ \star & (free) \end{array} \right\}$$

We designate the induced circuit obtained by applying the restriction ρ to the circuit C as $C\mid_\rho$. To show parity $\notin \mathrm{AC}_0$, we will apply random restrictions as follows:

$$\rho(x_i) = \left\{ \begin{array}{ll} \star & \text{with probability } \frac{1}{\sqrt{n}} \\ 0 & \text{with probability } \frac{1-\frac{1}{\sqrt{n}}}{2} \\ 1 & \text{with probability } \frac{1-\frac{1}{\sqrt{n}}}{2} \end{array} \right\}$$

There are two ideas that motivate this proof.
Idea 1: If we apply a restriction to a parity circuit, we will get parity, or parity on the remaining free variables.
Idea 2: If we apply two of these random restrictions on an AC_0 circuit of depth d, we will end up with a circuit of depth $d-1$ with high probability and at least $\frac{n^{\frac{1}{4}}}{4}$ of the variables will remain free. This results in a contradiction because we will need exponential size in a depth two circuit for computing parity. (After k restrictions, we will have approximately $n^{\frac{1}{4}^k}$ free variables.)

2 Parity $\notin \mathrm{AC}_0$

We will consider a depth d circuit which alternates AND and OR gates at every level, and we will make use of the following fact.

Fact 2 *Any function of c bits can be expressed as an AND of 2^c ORs or an OR of 2^c ANDs. This implies that switching from an AND of ORs to an OR of ANDs can result in a blowup in circuit size of at most 2^c, which is constant size.*

Lemma 3 *Let $c > 0$, G is an OR gate, and n is large. Then,*
$\Pr[G\mid_\rho$ *depends on more than c variables*$] < n^{-\frac{c}{3}}$

Proof of Lemma 3
Case 1 ("fat case" - the OR gate is large): $|G| > c \lg n$
$\Pr[G\mid_\rho \text{ is not fixed}] < (\frac{1+\frac{1}{\sqrt{n}}}{2})^{c \lg n} \sim \frac{1}{2}^{c \lg n} - n^{-c} < n^{-\frac{c}{3}}$

Case 2 ("thin case"): $|G| \leq c \lg n$
Pr[there are c free variables] $\leq \binom{c \lg n}{c} \cdot (\frac{1}{\sqrt{n}})^c \leq (c \lg n)^c \cdot (\frac{1}{\sqrt{n}})^c < n^{-\frac{c}{3}}$
■

Corollary 4 *Let C be a circuit with n^k gates. Then with high probability there exists a ρ with $\frac{\sqrt{n}}{2}$ free variables such that all bottom-level gates of C have fanin $\leq 4k$.*

Proof Apply lemma 3 with $c = 4k$:
Pr[any bottom gate depends on more than c variables] $\leq n^k \cdot n^{\frac{-4k}{3}} \ll 1$
Pr[there are fewer than $\frac{\sqrt{n}}{2}$ free variables] $\sim 2^{O(-\sqrt{n})}$ (by Chernoff) ■

Lemma 5 $\forall k, \forall c, \exists$ *a constant b_c such that for a sufficiently large n, if G is an AND of OR gates each having fanin at most c, then:* Pr[$G |_\rho$ *depends on more than* b_c *variables*] $< n^{-k}$

Definition 6 *Let M be a collection of the OR gates such that the ORs in the collection have disjoint sets of variables and every OR gate not in the collection M overlaps with an OR gate in M.*

Definition 7 *Let V be the set of variables in the OR gates of M.*

Proof of Lemma 7
This proof is an induction on c, the maximum fanin of the OR gates.
Base case: If $c = 1$, then the OR gates are unnecessary, and the circuit is really just an AND circuit. Thus, the base case holds by lemma 3.

Inductive step: Assume the lemma holds for $c - 1$ to prove it for c.

Case 1 ("Fat case"): $|V| > a \lg n$
We wish to find the probability that G is not fixed to 0. Given $\frac{a}{c} \lg n$ variables in M, then Pr[a particular OR gate outputs 0] $= (\frac{1-\sqrt{n}}{2})^c$, and thus
Pr[no OR gate outputs 0] = Pr[G is not fixed] =
$(1 - (\frac{1-\sqrt{n}}{2})^c)^{\frac{a}{c} \lg n} \sim (1 - 2^{-c})^{\frac{a}{c} \lg n} \sim e^{-\frac{a}{c 2^c} \lg n}$
Therefore, for the fat case, we need $a > 2^c \cdot k$

Case 2 ("Thin case"): $|V| \leq a \lg n$
Pr[V has i free variables] $\leq \binom{a \lg n}{i} \cdot (\frac{1}{\sqrt{n}})^i < n^{-\frac{i}{3}}$ (for sufficiently large n)
Therefore, we set $i = 4k$
Every OR gate not in M shares an input with an OR gate in M. Thus, if we fix those i free variables, then the other ORs will have a fanin of $c - 1$. (We can then apply the inductive hypothesis to complete the proof.)
Finally, since there are only 2^i ways to fix these variables, G will only depend on $i + 2^i b_{c-1} = b_c$ variables.
■