6.841 Advanced Complexity Theory	Feb 18, 2009
Lecture 5	
Lecturer: Madhu Sudan	*Scribe: Yang Cai*

1 Overview

- $PARITY \notin AC^0$.
- Random Restriction
- Switching Lemma $DNF \to CNF$

2 Introduction

We first introduce two sets of classes.

- AC^k: Class of functions computable by polynomial size and $O((\log n)^k)$ depth circuits over $\{\infty - AND, \infty - OR, NOT\}$ gates.
- NC^k: Class of functions computable by polynomial size and $O((\log n)^k)$ depth circuits over $\{2 - AND, 2 - OR, NOT\}$ gates.

We know that for any k, $AC^k \subseteq NC^{k+1} \subseteq AC^{k+1}$, so $\bigcup_k AC^k = \bigcup_k NC^k$.

Through this lecture, we assume all circuits in AC^k are organized to have alternating levels of AND and OR gates. Because all NOT gates can be moved to the first level, and since the AND and OR gates have infinite fan-in, we can combine any consecutive AND or OR levels. So we can consider the depth as the number of AND and OR levels.

The goal of this lecture is to prove the following theorem $PARITY \notin AC^0$. By $PARITY$ we mean

$$PARITY(x_1, x_2, \ldots, x_n) = \sum_i x_i \ (mod\ 2).$$

Theorem 1 *[Furst, Saxe, Sipser; Ajtai; Yao; Håstad; Razborov; Razborov-Smolensky]*

$$PARITY \notin AC^0.$$

3 Random Restriction

If $x_1, x_2, \ldots, x_n$ are variables, a random restriction on them is to randomly set values for most of the variables. Formally, we say a random restriction ρ with parameter p, if for every i, we leave x_i unset with probability p, restrict it as $x_i = 0$ or $x_i = 1$ with equal probability $\frac{1-p}{2}$.

$$x_i = \begin{cases} 0 \text{ with prob. } \frac{1-p}{2} \\ x_i \text{ with prob. } p \\ 1 \text{ with prob. } \frac{1-p}{2} \end{cases}$$

If a function f has n variables, after this restriction, we get the function $f|_\rho$ with about pn variables. Then

$$PARITY\ |_\rho\ (x_1, x_2, \ldots, x_n) = PARITY(x_{i_1}, x_{i_2}, \ldots, x_{i_t})(\oplus 1)\ (t \approx pn)$$

4 Switching Lemma

Lemma 2 *(Switching Lemma) Let F be a DNF formula on n variables with size $S \leq n^{c_1}$. Let ρ be a random restriction with $p = \frac{1}{\sqrt{n}}$,*

$$\Pr[F\mid_\rho \ \textit{depends on} \geq C \ \textit{variables}] \leq \frac{1}{n^{2c_1}}$$

C is a constant decided by c_1.

We will first use Switching Lemma to prove $PARITY \notin AC^0$, then prove the Switching Lemma. Notice that we can always set the circuit's bottom 2 levels to be DNF's, because if it's a CNF, we can just negate the circuit.

Theorem 1 $PARITY \notin AC^0$

Proof We prove this by induction. The base of induction is not hard to see that, if a circuit of depth 2 computes $PARITY$ then its size is $O(2^n)$.

If for every c and depth d, no depth d circuit of size $S = n^c$ computes $PARITY$. Now we prove this is also true for $d+1$.

Say G is a circuit with depth $d+1$ and size n^{c_1} that computes $PARITY(x_1, x_2, \ldots, x_n)$.

Hit G with random restriction ρ with parameter $p = \frac{1}{\sqrt{n}}$. We know the following:(a) According to Chernoff bound, we know with probability $(1 - 2^{-\sqrt{n}})$, there are at least $\frac{pn}{2} = \frac{\sqrt{n}}{2}$ variables are unset. (b) According to Switching Lemma, for every DNF formula, it depends on only C variables with probability $1 - \frac{1}{S^2}$. (c) Since there are at most S DNF formula at the bottom, all depth 2 gates depend on $\leq C$ variables with probabilty $1 - \frac{1}{S}$. When all depth 2 gates depend on $\leq C$ variables, we can replace the bottom levels by CNF of size 2^C, then G becomes $\widetilde{G}$. $\widetilde{G}$ computes PARITY of $\frac{\sqrt{n}}{2}$ unrestricted variables in a circuit with depth d and size $n^{c_1} 2^C = poly(\frac{\sqrt{n}}{2})$. Contradiction to the induction hypothesis. ■

5 Proof of Switching Lemma

Let the DNF $F = T_1 \vee T_2 \vee \ldots \vee T_m$. We restrict variables in two stages

Stage 1

Restrict variable with probability $\sqrt{p}$, i.e.

$$x_i = \begin{cases} 0 \text{ with prob. } \frac{1-\sqrt{p}}{2} \\ x_i \text{ with prob. } \sqrt{p} \\ 1 \text{ with prob. } \frac{1-\sqrt{p}}{2} \end{cases}$$

$$f \longrightarrow \ f|_{\rho_1}.$$

Stage 2

Restrict variables in $f|_{\rho_1}$ with probability $\sqrt{p}$, i.e.

$$x_i = \begin{cases} 0 \text{ with prob. } \frac{1-\sqrt{p}}{2} \\ x_i \text{ with prob. } \sqrt{p} \\ 1 \text{ with prob. } \frac{1-\sqrt{p}}{2} \end{cases}$$

$$f|_{\rho_1} \longrightarrow \ f|_{\rho_1 \cup \rho_2}.$$

Stage 1

- **Case 1**: Terms with fan-in $\geq 4 \log S$

$$\Pr[Any\ Term\ with\ fan-in \geq 4\log S \neq 0] \leq (\frac{1+\sqrt{p}}{2})^{4\log S} \leq (\frac{2}{3})^{4\log S} \leq \frac{1}{S^3}$$

Therefore,

$$\Pr[\exists\ Term\ with\ fan-in \geq 4\log S\ doesn't\ become\ 0] \leq \frac{1}{S^2}$$

- **Case 2**: Terms with fan-in$\leq 4\log S$

$$\Pr[T_i\ depends\ on\ c_0\ variables] \leq (4\log S)^{c_0}(\sqrt{p})^{c_0} \leq \frac{1}{S^3}$$

Therefore,

$$\Pr[\exists\ Term\ with\ fan-in \leq 4\log S,\ depends\ on \geq c_0\ variables] \leq \frac{1}{S^2}$$

. c_0 is a constant depend on c_1, so now the DNF is a c_0-DNF.

Stage 2

- **Case 1**: $\exists$ many disjoint Term $T_1, T_2, \ldots, T_l$, $l \geq 3^{c_0}4\log S$.

$$\Pr[T_i = 1] \geq (\frac{1}{3})^{c_0}$$

$$\Pr[T_i \neq 1] \leq (1-\frac{1}{3})^{c_0}$$

$$\Pr[\exists\ T_i = 1] \geq 1 - ((1-\frac{1}{3})^{c_0})^l = 1 - 2^{-l/3^{c_0}} \geq 1 - \frac{1}{S^2}$$

- **Case 2**: The max number of disjoint T_i's $\leq 4\log S$

  Claim: $\exists$ set H with $4c_0 3^{c_0}\log S$ variables, s.t. $\forall i\ H \cap T_i \neq \emptyset$.
  Proof Select disjoint T_i's greedily. When stop, variables in H hit all T_i's ■

  - **Part a**: First restrict variables of H; As in Case 2 of Stage 1, we can find a constant b, s.t. the number of unset variables in $H \leq b$.
  - **Part b**: Now we restrict variables not in H. And we use induction on c_0.
    Induction hypothesis: Any (c_0-1)-DNF under random restriction depends on only C' variables with high probability, C' is a constant.

    Now we want to prove that c_0-DNF under random restriction also only depends on constant many variables with high probability.

    Claim: With high probability c_0-DNF only depends on $C \leq b + 2^b C'$ variables.
    Proof After restricting variables in H, enumerate all possible assignments of the b unset variables. After assignning values to these variables, the c_0-DNF becomes a (c_0-1)-DNF. According to the induction hypothesis, we know this depends on C' variables under restriction. So the c_0-DNF depends on at most $b + 2^b C'$ variables. ■