U.C. Berkeley — CS278: Computational Complexity | Handout N21
Professor Luca Trevisan | 11/5/2002
Scribe: Kamalika Chaudhuri

Notes for Lecture 21

In today's lecture, we will talk about circuit lower bounds and take our first step towards proving a result about the lower bound on the size of a constant depth circuit which computes the XOR of n bits.

Before we talk about bounds on the size of a circuit, let us first clarify what we mean by circuit depth and circuit size. The depth of a circuit is defined as the length of the longest path from the input to output. The size of a circuit is the number of AND and OR gates in the circuit.Note that for our purpose, we assume all the gates have unlimited fan-in and fan-out. We define $\mathbf{AC_0}$ to be the class of decision problems solvable by circuits of polynomial size and constant depth. We want to prove the result that **PARITY** is not in $\mathbf{AC_0}$.

We will try to prove this result using two different techniques. In this class, we will talk about a proof which uses polynomials; in the next class we will look at a different proof which uses random restrictions.

1 Circuit Lower Bounds for PARITY

Before we go into our proof, let us first look at a circuit of constant depth d that computes **PARITY**.

Theorem 1 *If a circuit of size S and depth d computes* **PARITY** *then $S \geq 2^{\Omega(n^{\frac{1}{d-1}})}$*

This bound of $2^{\Omega(n^{\frac{1}{(d-1)}})}$ is actually tight, as the following example shows.

Consider the circuit C shown in Figure(1), which computes the **PARITY** of n variables. C comprises of a tree of XOR gates, each of which has fan-in $n^{\frac{1}{d-1}}$; the tree has a depth of $d-1$.

Now, since each XOR gate is a function of $n^{\frac{1}{d-1}}$ variables, it can be implemented by a CNF or a DNF of size $2^{n^{\frac{1}{d-1}}}$. Let us replace alternating layers of XOR gates in the tree by CNF's and DNF's - for example we replace gates in the first layer by their CNF implementation, gates in the second layer by their DNF implementation, and so on. This gives us a circuit of depth $2(d-1)$. Now we can use the associativity of OR to collapse consecutive layers of OR gates into a single layer. The same thing can be done for AND to get a circuit of depth d.

This gives us a circuit of depth d and size $O(n2^{n^{\frac{1}{d-1}}})$ which computes **PARITY**.

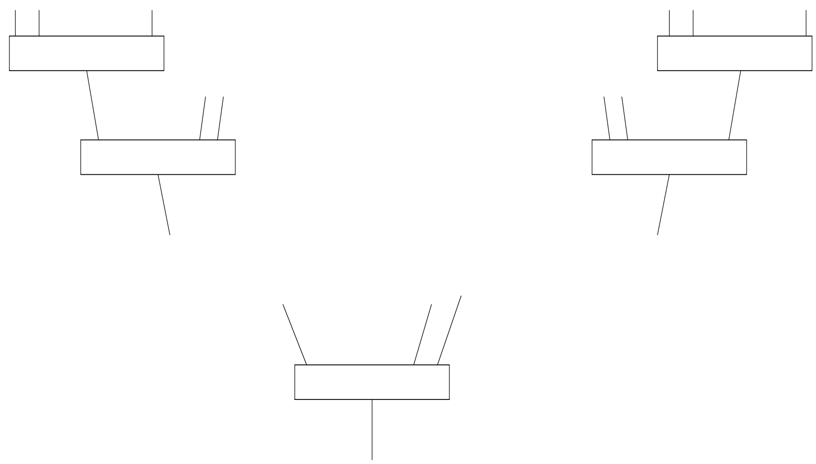

Figure 1: Circuit for Computing XOR of n variables; each small circuit in the tree computes the XOR of $k = n^{\frac{1}{d-1}}$ variables

2 Proof of Circuit Lower Bounds for PARITY using Polynomials

For our proof, we will utilise a property which is common to all circuits of small size and constant depth, which **PARITY** does not have. The property is that circuits of small size and constant depth can be represented by low degree polynomials, with high probability. More formally, we show that if a function $f : \{0,1\}^n \rightarrow \{0,1\}$ is computed by a circuit of size s and depth d, then there exists a function $g : \{0,1\}^n \rightarrow \Re$ such that $\Pr_x[f(x) = g(x)] \geq \frac{3}{4}$ and $\hat{g}_\alpha \neq 0$ only for $|\alpha| \leq O((\log S)^{2d})$.

Then we will show that if a function $g : \{0,1\}^n \rightarrow \Re$ agrees with **PARITY** on more than a fraction $\frac{3}{4}$ of its inputs, then $\hat{g}_\alpha = 0$ only for $|\alpha| = \Omega(\sqrt{n})$. That is, a function which agrees with **PARITY** on a large fraction of its inputs, has to have high degree. From these two results, it is easy to see that **PARITY** cannot be computed by circuits of constant depth and small size.

Lemma 2 *Suppose we can describe a distribution G_{OR} over functions $g : \{0,1\}^n \rightarrow \{0,1\}$ such that*

- *for every g in G_{OR}, $\hat{g}_\alpha \neq 0$ only for $|\alpha| \leq O\left((\log \frac{1}{\epsilon})(\log K)\right)$*
- *for every $x \in \{0,1\}^n$, $Pr_{g \sim G_{OR}}[g(x) = x_1 \vee x_2 \vee \cdots \vee x_k] \geq 1 - \epsilon$. Here K is the maximum fan-in of each gate.*

Also suppose we can describe a such a distribution G_{AND} for AND gates. Then, given a circuit C of size S and depth d, we can find a polynomial h of degree at most $O((\log S)^{2d})$, such that $\Pr_x[h(x) = C(x)] \geq \frac{3}{4}$

Proof: The way we do this is as follows. For every gate in a circuit C, we pick independently an approximating function g_i with parameter $\epsilon = \frac{1}{4S}$, and replace the gate by g_i.

Then, for a given input, probability that the new circuit computes $C(x)$ correctly, that is, the probability that the results of all the gates are correctly computed, is at least $\frac{3}{4}$. Let $G_i : \{1, -1\}^n \to \{1, -1\}$ be the Fourier transformed version of function g_i, so that

$$g_i(x_1, \cdots, x_n) = \frac{1}{2} + \frac{1}{2} G_i(1 - 2x_1, 1 - 2x_2, \cdots, 1 - 2x_n) \tag{1}$$

Then G_i can be written as

$$G_i = \sum_{\alpha} \hat{g}_{i,\alpha} \prod_{j \in \alpha} X_j \tag{2}$$

where $X_i = 1 - 2x_i$. Then G_i has degree at most $O((\log S)^2)$, as K, the fan-in of any gate, is at most S. Therefore, if we expand out the expression for $C(x)$, we will get a multilinear polynomial of degree at most $O((\log S)^{2d})$, as C has depth d. $\square$

Lemma 3 *Suppose there is a function $g : \{0, 1\}^n \to \Re$ such that*

- $\Pr_x[g(x) = x_1 \oplus x_2 \oplus \cdots \oplus x_n] \geq \frac{3}{4}$ *and*
- $\hat{g}_\alpha = 0$, *for all sets α such that $|\alpha| > d$.*

Then $d = \Omega(\sqrt{n})$

PROOF: Let $G : \{1, -1\}^n \to \{1, -1\}$ be the Fourier transformed version of the function g. That is,

$$G(x) = 1 - 2g(\frac{1}{2} - \frac{1}{2}x_1, \cdots, \frac{1}{2} - \frac{1}{2}x_n) \tag{3}$$

Then, $\Pr_x[G(X) = \prod_{i=1}^n X_i] \geq \frac{3}{4}$, where $X_i = 1 - 2x_i$. Define A to be the set of values over which g agrees with **PARITY**. In other words,

$$A = \{X : G(X) = \prod_{i=1}^{n} X_i\} \tag{4}$$

Then $|A| \geq \frac{3}{4} 2^n$, by our initial assumption. Now consider the set of all functions $S = \{f : A \to \Re\}$. These form a vector space of dimension $|A|$. Any function f in this set can be written as

$$f(X) = \sum_{\alpha} \hat{f}_\alpha \prod_{i \in \alpha} X_i \tag{5}$$

Over A, $G(X) = \prod_{i=1}^n X_i$. Therefore, for $X \in A$,

$$\prod_{i \in \alpha} X_i = G(X) \prod_{i \notin \alpha} X_i \tag{6}$$

By our initial assumption, $G(X)$ is a polynomial of degree at most d. Therefore, for every α, such that $|\alpha| \geq \frac{n}{2}$, we can replace $\prod_{i \in \alpha} X_i$ by a polynomial of degree less than or equal to $d + \frac{n}{2}$. Every such function f which belong to S can be written as a polynomial of degree at most $d + \frac{n}{2}$. Hence the set $\left\{\prod_{i \in \alpha} X_i\right\}_{|\alpha| \leq d + \frac{n}{2}}$ forms a basis for the set S. As there must be at least $|A|$ such monomials, this means that

$$\sum_{k=0}^{d+\frac{n}{2}} \binom{n}{k} \geq \frac{3}{4} 2^n \tag{7}$$

This holds when $d = \Omega(\sqrt{n})$. $\square$

Now we need to prove that we can indeed describe such distributions G_{OR} and G_{AND} over functions g_i for OR and AND. This we shall do in the next class.