Chapter 11

Circuit Lower Bounds

Chapter Outline: Razborov-Smolensky, Decision trees, Switching Lemma, Parity lower bounds, Non-approximability results for parity

11.1 Historical Notes

Discuss history of circuit lower bounds. Furst-Saxe-Sipser, Yao, Cai, Hastad.

11.2 Razborov-Smolensky Theorem

Constant depth size 2^{n^ϵ} boolean circuits together with Mod 3 gates cannot compute parity.

We will prove the above result in next two sections. We first show that constant depth circuit can be approximated by a low degree polynomial. Then we show that such polynomials cannot approximate parity function.

11.2.1 Approximating Constant Depth Circuits by Low Degree Polynomials

In this section, we show that constant depth circuits can be approximated by low degree polynomials over GF(3).

THEOREM 11.1 *We can approximate the function $F(x_1, x_2, \ldots, x_n) = x_1 \vee x_2 \vee \ldots \vee x_n$ with a low degree polynomial. More precisely, for any positive integer k, there is a degree $\leq 2k$ polynomial P in $x_1, \ldots, x_n$, over GF(3) that agrees with y on at least $2^n(1 - (\frac{1}{3})^k)$ of*

assignments. That is,

$$Pr_{\sigma\in\{0,1\}^n}[P(\sigma) = F(\sigma)] \geq 1 - \left(\frac{1}{3}\right)^k$$

The claim is also valid for the $\bigwedge, \neg and \mathrm{Mod}_3$ *functions.*

Proof. We use the probabilistic method to prove the lemma. Fix an assignment $\sigma_1 = (c_1, c_2, \ldots, c_n) \in \{0,1\}^n$. Choose $a_1, a_2, \ldots, a_n \in GF(3)$ uniformly at random. Consider the polynomial $\hat{F} = (\sum_{i=1}^n a_i x_i)^2)$. Note that, as we are working in GF(3)=$\{$-1,0,1$\}$, $\hat{F}$ evaluates to 0 or 1 for any input. What is the probability that $\hat{F}(\sigma_1) = F(\sigma_1)$? If $F(\sigma_1)$ evaluates to 0, then $\hat{F}$ also evaluates to 0 (regardless of the random values a_i). On the other hand, suppose $F(\sigma_1) = 1$. Let j be the largest index such that $c_j = 1$. Then

$$Pr[\hat{F}(\sigma_1) = 1] = Pr\left[\left(\sum_{i=1}^n a_i c_i\right)^2 = 1\right] = Pr\left[\left(\sum_{i=1}^j a_i c_i\right)^2 = 1\right] = Pr\left[\sum_{i=1}^j a_i c_i \neq 0\right]$$

The last equality is due to the fact that in GF(3), $x^2 = 1 \iff x \neq 0$. We evaluate the last quantity by conditioning on the first $j-1$ terms of the summation. These could sum up to 0,1 or -1. But regardless this value, we have 2/3 chance for the summation to be non-zero, because $c_j = 1$ and a_j is chosen at random from GF(3). To conclude, for any fixed $\sigma_1 \in \{0,1\}^n$,

$$Pr_{a_1,a_2,\ldots,a_n\in GF(3)}[\hat{F}(\sigma_1) = F(\sigma_1)] \geq \frac{2}{3}$$

There are 3^n ways to choose the coefficients a_i's of the polynomial and there are 2^n assignments for the variables $x_1, x_2, \ldots, x_n$. Consider the following table in which each row represents one possible vector of coefficients and each column represents a possible assignment.

	Assignment of the x_i				
	σ_1	σ_2	σ_3	$\cdots$	σ_{2^n}
$a^{(1)}$					
$a^{(2)}$					
$a^{(3)}$					
$\vdots$					
$a^{(3^n)}$					

Consider an assignment $\sigma_j = c_1, c_2, \ldots, c_n$ and a coefficient vector $a^{(i)} = (a_1, a_2, \ldots, a_n)$. Place a 1 in the cell $(a^{(i)}, \sigma_j)$ in the above table, if $(\sum_{j=1}^n a_i c_j^2 = F(c_1, c_2, \ldots, c_n,$ and place a 0 otherwise. By our probability calculation above, any column of the table has 1 in at least 2/3 of the cells. Thus, at least 2/3 of the entries in the entire table are 1. It follows that there is some row that has a 1 in at least 2/3 of its cells. Let this row be r_1 and let $\hat{F}_1$ be the polynomial corresponding to this row, i.e. $\hat{F}_1(x_1, x_2, \ldots, x_n) = \sum_{i=1}^n a_i^{(r_1)} x_i$. If we choose an

assignment σ at random, we have

$$Pr_{\sigma \in \{0,1\}^n}[\hat{F}_1(\sigma) = F(\sigma)] \geq \frac{2}{3}$$

Now ignore all the columns in which the row r_1 has 1. At most 1/3 of the columns remain. All these columns have 1 in at least 2/3 of their cells. Again by the same argument, there is some other row r_2 that has 1 in at least 2/3 of these remaining columns. We let F_2 be the polynomial corresponding to row r_2. Next ignore these columns. At most $(1/3)^2$ columns would remain. We continue like this for k iterations. At most $(1/3)^k$ columns would remain. We would have constructed polynomials $\hat{F}_1, \hat{F}_2, \ldots, \hat{F}_k$.

Being the OR function, F evaluates to 0 for only one assignment, namely $\sigma_0 = (x_1 = 0, x_2 = 0, \ldots, x_n = 0)$. All our k polynomials evaluate to 0 on this assignment and for any other input they all evaluate to 0 or 1. Consider the columns (or assignments) that were ignored. These are "covered"by our polynomials in the sense that if $F(\sigma) = 1$ then at least one of these polynomials F_i also evaluates to 1 on σ. So if we take OR of our polynomials $\hat{F} = \hat{F}_1 \vee \hat{F}_2 \vee \ldots \vee \hat{F}_k$, then for any "covered" assignment σ, $\hat{F}(\sigma) = F(\sigma)$. But $1 - (1/3)^k$ of the assignments are covered. So

$$Pr_{\sigma}[\hat{F}(\sigma) = F(\sigma)] \geq 1 - \left(\frac{1}{3}\right)^k$$

Only one problem remains. How do we OR two polynomials to get another polynomial? We use the trick mentioned in the beginning. We let $\hat{F}_1 \vee \hat{F}_2 = 1 - (1 - \hat{F}_1)(1 - \hat{F}_2)$. So we take OR of all the k polynomials this way and let the required polynomial P to be $\hat{F}_1 \vee \hat{F}_2 \vee \ldots \vee \hat{F}_k$. What is the degree of P? Each $\hat{F}_i$ has degree 2 (because of the squaring). Thus P has degree at most $2k$.

Thus we have constructed a polynomial of degree at most $2k$ that agrees with the OR function F on at least $1 - (1/3)^k$ assignments. Same way we can approximate AND and NOT functions.

Next we show that any depth d circuit C of size s over n inputs, can be approximated by a low degree polynomials. We use the above lemma to approximate each of the s gates by polynomials of degree $2k$. We construct a polynomial to approximate the circuit by combining these polynomials. For example, consider a two input $\vee$–gate g that receives its inputs from two other gates g_1 and g_2 (which are at lower depth). The polynomial for gate g constructed by Lemma 11.1 be $P(y_1, y_2)$. We substitute the polynomials for gates g_1 and g_2, say F_{g_1} and F_{g_2} for y_1 and y_2 in P to get the polynomial F_g for gate g. This way, we start at the input level and move upto the output level of the circuit to get the polynomial F_C to approximate the circuit. As the depth of the circuit is d and the polynomials for the gates (from Lemma 11.1 are of degree $2k$), the degree of F_C would be $(2k)^d$.

Choose an input $x_1, x_2, \ldots, x_n \in \{0, 1\}$ at random. What is the probability that F_C does not agree with circuit C on this input? F_C will fail to agree with the circuit C only when at

least one of the s polynomials (of the gates) fails. By the guarantee given by Lemma 11.1, for any specific gate, this happens with probability at most $\frac{s}{3^k}$. Thus probability that at least one gate fails is at most $\frac{1}{3^k}$. Thus,

$$Pr_{x_1,x_2,\ldots,x_n\in\{0,1\}}[F_C(x_1,x_2,\ldots,x_n) = C(x_1,x_2,\ldots,x_n)] \geq 1 - \frac{s}{3^k}$$

We have shown that

THEOREM 11.2 *For any circuit C of depth d and size s on n boolean variables, for any integer k, there is a polynomials $F(x_1,x_2,\ldots,x_n)$ of degree at most $(2k)^d$ over GF(3) whose value is equal to the output of the C on at least $2^n(1-s/3^k)$ inputs. The circuit is allowed to use AND, OR, NOT and* Mod_3 *gates.*

11.2.2 Low Degree Polynomials Cannot Approximate Parity

11.3 Switching Lemma and Parity Lower Bounds

11.3.1 Decision Trees

Decision trees are used to represent boolean functions.

DEFINITION 11.3 (DECISION TREES) *A* decision tree *is a rooted binary tree t with every leaf labeled as 0 or 1. Every internal node is labeled with an x_i. The two edges from an internal node are labeled with* 0 *and* 1 *respectively. We do not disallow variables to repeat along a path from the root to the leaf.*

DEFINITION 11.4 (DECISION TREE DEPTH) *The* depth *of a decision tree is defined to be the number of edges in the longest path from the root to a leaf.*

Figure 11.1 shows an example of a decision tree.

A decision tree T defines a boolean function as follows:

1. if $\mathrm{depth}(T) = 0$, then it is a constant function (either 0 or 1)
2. if $\mathrm{depth}(T) = d+1$ ($d \geq 0$): inductively assume that the left subtree and the right subtree respectively define a boolean function. Call the boolean function defined by the left subtree G and the right subtree as H. Also assume that the root is labeled as x_i and has the left edge labeled 0 and the right edge labeled 1. Then,

$$F(x_1,x_2,\ldots,x_n) = \begin{cases} G(x_1,x_2,\ldots,x_n) & \text{if } x_i = 0 \\ H(x_1,x_2,\ldots,x_n) & \text{if } x_i = 1 \end{cases}$$

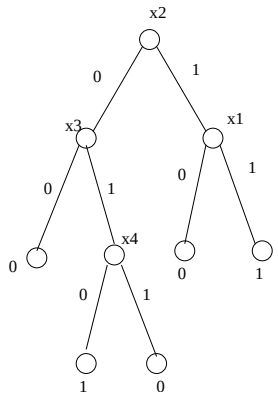

Figure 11.1: An example of a decision tree

Both G and H are also functions in x_i, but if we disallow x_i from repeating along any path from root to leaf in the decision tree, we can leave it out of the functions G and H. Then instead, we can write G as a function of $x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$, which is often written as $G(x_1, x_2, \ldots \hat{x_i}, \ldots, x_n)$

Hence, the function F is in fact:

$$F = (G \wedge \bar{x_i}) \vee (H \wedge x_i)$$

We can instead choose to write G as $F|_{x_i=0}$ and H as $F|_{x_i=1}$ and rewrite the above equation as:

$$F = (F|_{x_i=0} \wedge \bar{x_i}) \vee (F|_{x_i=1} \wedge x_i)$$

This expansion gives us a way to write the formula in DNF (i.e., $\vee$ of $\wedge$'s). If $F|_{x_i=0}$ and $F|_{x_i=1}$ can be written as a DNF where every conjunct has size at most t, then we get a formula F in DNF in which every conjunct is of size at most $t+1$.

Definition 11.5 (Decision tree complexity) *For boolean function f, the decision tree complexity, $DC(f)$, is the minimum depth of the decision trees that compute f.*

Lemma 11.6 $D(f) = D\left(\bar{f}\right)$

Proof: The set of boolean decision trees that compute f are in 1-1 correspondence with those that compute $\bar{f}$. (Just flip the bits at the leaves of the tree.) ♣

As demonstrated in the previous section, a boolean function computed by a decision tree of depth d can be expressed as a boolean formula in disjunctive normal form (DNF), where each conjunct has size at most d. Using that idea, we get the following corollary.

COROLLARY 11.7 *A boolean function f and its complement $\bar{f}$ can be expressed in DNF in which every conjunct has size $\leq DC(f)$. So f can be written as a DNF formula with conjuncts of size $\leq DC(f)$, and as a CNF formula with disjuncts of size $\leq DC(f)$.*

The above mentioned special case of DNF where every conjunct is bounded in size will be useful in our discussion. The following definition spells this out.

DEFINITION 11.8 (t-AND-OR) *Boolean formula G is a t-AND-OR if $G = G_1 \wedge G_2 \wedge \cdots \wedge G_w$, where each G_i is the OR of at most t literals. So $G_i = \tilde{x}_1 \vee \tilde{x}_2 \vee \cdots \vee \tilde{x}_s$, for $s \leq t$, and $\tilde{x}_i \in \{x_i, \bar{x}_i\}$. (Likewise, a t-OR-AND is a formula in disjunctive normal form with at most t terms in each conjunct.)*

11.3.2 Random Restrictions

DEFINITION 11.9 (RESTRICTION) *A restriction ρ is a partial assignment to variables of boolean formula G. Specifically, it is a mapping $\rho : \{1, 2, \cdots, n\} \mapsto \{0, 1, *\}$. The restriction of G by ρ, written $G|_\rho$, is the boolean function obtained by setting x_i to $\rho(i)$ if $\rho(i) \in \{0, 1\}$ and leaving x_i as a variable otherwise.*

A random p-restriction is a restriction ρ where, for each i, one independently assigns $\rho(i)$ such that:

$$\begin{aligned} \Pr[\rho(i) = *] &= p, \quad \text{and} \\ \Pr[\rho(i) = 0] = \Pr[\rho(i) = 1] &= \frac{1-p}{2} \end{aligned}$$

11.3.3 Proving Circuit Lower Bounds for Parity: Overview

Here we will present a high level overview of proving lower bounds relating depth and size of circuits computing parity. A formal proof will be presented in subsequent lectures.

Before proceeding, let us review some conventions. Suppose we have a circuit that uses negation gates. By using de Morgan's law, we can push down the negation gates until they reach the input level. Thus, any boolean circuit can be transformed to an equivalent one such that all the negation gates occur at the bottom level (i.e. any negation gate takes it input only from variables). This transformation can be accomplished increasing the size at most twice the original and without any increase in depth. We assume that the input consists of both the variables and their negations so that size of a circuit refers to the number of AND and OR gates. We do not restrict fan-in or fan-out of the gates. So, without loss of generality, we can assume that the circuit is "leveled": a circuit of depth d is made of d levels so that all gates in a level are of same type and edges are only between adjacent levels. Thus, AND and OR gates will alternate across levels. From now on, we consider

only circuits with above properties. By convention, output level (made of just one gate) is numbered 1 and the bottom level (where gates take their input from variables) is numbered d.

Now we are ready to state the the lower bound theorem.

THEOREM 11.10 *For sufficiently large n, Parity_n cannot be computed by a depth-d circuit of size $\leq 2^{cn^{1/d}}$, where $c > 0$ is some constant.*

One can prove the theorem with $c = 0.143781$. Here we will prove a weaker version where $c \approx 0.1$. The main ingredient of the proof is the switching lemma, which is as follows.

LEMMA 11.11 *[Switching Lemma] Let G be a t-And-Or formula. Let ρ be a random p-restriction. Then, for all $\Delta \geq 0$,*

$$\Pr[DC(G|_\rho) > \Delta] \leq (5pt)^\Delta. \tag{11.1}$$

Assuming the switching lemma, we sketch a proof of Theorem 11.10. Set $p = \gamma_0/t$, where $\gamma_0 > 0$ is a suitable constant fixed later. We will apply the lemma with $\Delta = t$. Then, the lemma says that when we apply a random p-restriction to a t-AND-OR formula G, with probability at least $1 - (5\gamma_0)^t$, the resultant formula $G|_\rho$ has DC $\leq t$. As we noted before, a formula with DC $\leq t$, can be expressed as a t-OR-AND formula. Thus, with high probability, the t-AND-OR formula $G|_\rho$ can be "switched" into an equivalent t-OR-AND formula. Using this ability to "switch", we can prove Theorem 11.10.

We first consider some restricted type of circuits. A circuit C of depth d is said to be of type $C^d(s,t)$ if it satisfies the two conditions: i) the gates at the bottom-most level (i.e. input level) have fan-in $\leq t$; ii) number of gates at levels above the bottom level $\leq s$. Thus, we have a bottom fan-in condition (bfi), which restricts fan-in of the bottom level gates. The gates above the bottom level (or the "internal" gates) are allowed to have any fan-in. At the end, we will relax these conditions and prove the theorem for any d-depth circuit (this part is easy).

Assume, without loss of generality that, the gates at the bottom level are OR gates (if not consider $\neg C$). Each gate at one level above ($(d-1)^{th}$ level) is an AND gate which gets its input from the OR gates at level d. Think of each such AND gates and along with the OR gates as a small circuit. Any such small circuit sc is computing a t-AND-OR formula, because of the bottom fan in condition. Choose a random p-restriction ρ and consider the circuit $C|_\rho$. By the switching lemma, with probability $\geq 1-(5\gamma_0)^t$, the formula computed by the small circuit sc (in $C|_\rho$) has DC $\leq t$. As we discussed, this formula is (also) a t-OR-AND formula. Thus, we can *replace* the AND-OR circuit sc by an OR-AND circuit, where the AND gates have fan-in $\leq t$. Suppose there are s_{d-1} AND gates at level $d-1$. Assume that we were lucky and our random restriction ρ is good so that we are able to replace all these s_{d-1} AND-OR circuits by s_{d-1} OR-AND circuits with bottom fan-in $\leq t$. The resultant

circuit is made of OR gates in level $d-1$, OR gates is level $d-2$ and AND gates in level d. We can now *merge* the levels $d-1$ and $d-2$ in $C|_\rho$ to get a circuit that has only $d-1$ levels. There are a few things to note. The new circuit may have more gates at its bottom level than the original circuit. But, number of internal gates in the new circuits is $s - s_{d-1} \leq s$. Thus, the number of internal gates didn't increase. Next, bottom fan-in of the new circuit is $\leq t$. The new circuit has only $d-1$ levels. To summarize, the new circuit is of type $C^{d-1}(s,t)$ and is equivalent to $C|_\rho$. Of course, the new circuit is not computing the same function as the original one. But, this is not an issue when it comes to the parity function. We will elaborate this shortly.

Now the idea is to apply the above process of switching $d-2$ times: we pick a random p-restriction ρ_1 and apply it to C, then pick a random p-restriction ρ_2 and apply it to $C|_{\rho_1}$ and so on. Suppose we were lucky in picking all these $d-2$ random restrictions. Then, we will be left with a circuit C' of type $C^2(1,t)$.

Suppose the original circuit C computes parity on n bits. What does the new circuit C' compute? After applying all the $d-2$ random restrictions, some of the n variables would have been assigned 1 or 0 and the rest would remain as variables (i.e assigned *). Let the number of variables remaining be N (which is a random variable). Observe that C' computes the parity on these N variables.

Suppose all the $d-2$ random restrictions were good and suppose $N > t$. Then, C' is a circuit of type $C^2(1,t)$ that computes parity on $N > t$ variables. That is impossible. (C' computes a formula $G_1 \wedge G_2 \wedge \ldots \wedge G_w$, where each G_i is an OR of $\leq t$ literals. In particular, G_1 has some $a \leq t < N$ literals. Set all these literals to 0. Then output of C' is 0. But, since $N > a$, G_1 does not include some variable x. Set all the variables except those in G_1 and x to be 0. Now, set x appropriately, so that the parity is 1. Thus, C' does not compute parity of N variables).

The rest of proof is to show that with non-zero probability two properties are satisfied: i) the $d-2$ random restrictions are good (i.e. they allow us to "switch" t-AND-OR circuits to t-OR-AND circuits in all instances) and ii) $N > t$. We first note that instead of picking $d-2$ random restrictions, we could equivalently pick just one random restriction. Suppose we have a formula F we apply a random p_1-restriction followed by a random p_2-restriction. Observe that, equivalently, we can apply a random $(p_1 \cdot p_2)$-restriction. (Distribution of the boolean functions obtained in the two cases will be the same). In our scenario, instead of applying $d-2$ random p-restriction one by one, we can equivalently apply a single random p^{d-2}-restriction.

We have a circuit C of type $C^d(s,t)$ and a random p^{d-2}-restriction ρ. We need an estimate

on the probability that $C|_\rho$ can be transformed (by switching) into a $C^2(1,t)$ circuit. As C has s internal gates, we will need do s many "switches". The probability of failing in any one of these instances is bounded $\leq (5pt)^\Delta = (5\gamma_0)^t$. Thus, probability that we fail to convert $C|_\rho$ into an equivalent $C^2(1,t)$ circuit is $\leq s \cdot (5\gamma_0)^t$. Formally,

$$\Pr[C|_\rho \text{ is not equivalent to a } C^2(1,t) \text{ circuit}] \leq s \cdot (5\gamma_0)^t \tag{11.2}$$

Now we estimate the random variable N, the number of input variables of $C|_\rho$. $E[N] = n \cdot p^{d-2} = n \cdot (\gamma_0/t)^{d-2}$.

We will fix γ_0 and t to obtain a bound on $E[N]$ and the RHS of (11.2). Set $\gamma_0 = 1/10$ and $t = \gamma_0 n^{1/(d-1)}$ Then,

$$\Pr[C|_\rho \text{ is not equivalent to a } C^2(1,t) \text{ circuit}] \leq s \cdot (5\gamma_0)^t = s \cdot 2^{-(0.1)n^{\frac{1}{(d-1)}}}.$$

We have $E[N] = n^{1/(d-1)}$. Then, using Chernoff bound, we get

$$\Pr[N < t] = \Pr[N < \gamma_0 \cdot E[N]] < e^{-\frac{(1-\gamma_0)^2}{2} \cdot n^{\frac{1}{d-1}}} < e^{-(0.4)n^{\frac{1}{d-1}}}$$

Let $c < 0.1$ be a constant. For sufficiently large n, if $s \leq 2^{-c \cdot n^{1/(d-1)}}$, then

$$s \cdot 2^{-(0.1)n^{\frac{1}{(d-1)}}} + e^{-(0.4)n^{\frac{1}{d-1}}} < 1.$$

Let us summarize. Let $s < 2^{-c \cdot n^{1/(d-1)}}$ and C be a circuit of type $C^d(s,t)$ that computes parity of n bits. Then, with non-zero probability, $C|_\rho$ can be transoformed into a $C^2(1,t)$ circuit that computes parity on $N > t$ bits. In particular, there exists a random restriction ρ_0 that satisfies both these properties. But, a circuit of type $C^2(1,t)$ cannot compute parity on $> t$ bits. A contradiction. We have proved the following theorem.

THEOREM 11.12 *For $s \leq 2^{-c \cdot n^{1/(d-1)}}$, circuits of type $C^d(s,t)$ cannot compute parity on n bits. Here, c can be any constant < 0.1.*

It is now easy to prove Theorem 11.10. Observe that a circuit of size s and depth d can be viewed as a circuit of type $C^{d+1}(s,1)$. Then use Theorem 11.12. Later, we will prove a better version of the switching lemma, do a careful analysis and improve the contant c from 0.1 to 0.143781.

11.3.4 Switching Lemma: Proof

In this lecture, we prove the switching lemma.

LEMMA 11.13 *Let G be a t-And-Or formula $G_1 \wedge G_2 \wedge \ldots \wedge G_w$. Let ρ be a random p-restriction. Then, for all $\Delta \geq 0$,*

$$\Pr[\ \mathrm{DC}(G|_\rho) \geq \Delta\ ] \ \leq\ (5pt)^\Delta. \tag{11.3}$$

LEMMA 11.14 *Let G be a t-And-Or formula $G_1 \wedge G_2 \wedge \ldots \wedge G_w$. For any β, $0 < \beta < t$, let ρ be a random p-restriction, where $p = \frac{\beta}{t-\beta}$, and let $\alpha = \beta/ln\left[\frac{1+\sqrt{1+4e^{\beta}}}{2}\right]$. Then for all $\Delta \geq 0$, we have*

$$\Pr[DC(G|\rho) \geq \Delta] \leq \alpha^{\Delta}.$$

Proof. We prove these two lemmas together. We will prove the following stronger claim:

For *any* boolean function F,

$$\Pr[\ \mathrm{DC}(G|_\rho) \geq \Delta \mid F|_\rho \equiv 1\ ] \ \leq\ \alpha^{\Delta}, \tag{11.4}$$

where α will be set to $5pt$. (If the condition is not satisfied, the conditional probability is defined to be 0.) Lemma 11.13 follows by taking F to be the constant function 1.

The intuition is as follows. We will assign some random restriction ρ with parameter p. Note that p is $\ll t$, the bfi. Thus, one expect for a conjunct, say G_1, the number of $*$ left in G_1 after this ρ is 0, i.e., all the variables are assigned one way or another. Since we assign it with $\pm$ with equal probability, and since G_1 is an OR, we expect one of the variables is assigned in the right way so that $G_1 \equiv 1$. Thus, $G_1 \equiv 1$ is a low information event. We will "carry" this information along and proceed to G_2. It is the "rare" event that some x_i in G_1 which gets a $*$ that we want to charge a price (in probability) of p.

As we move along in this process, we will be carrying more and more events of the form: over a collection subsets of literals, each subset has at least one literal which gets assigned in a particular way (0 or 1). The general form of such a condition is no less generic than saying a certain AND of OR's which is evaluated to true. But that is nothing but the condition that an arbitrary boolean function being true under the restriction. This is the "information" accumulated so far in the process of dealing with G_i one by one.

Note that, at least intuitively, given some arbitrary boolean function F being true under the restriction ρ, (i.e., $F|_\rho \equiv 1$), does not reduce the probability p that any variable receiving $*$. Now we prove the theorem formally.

The statement (11.4) is trivially true for $\Delta = 0$, since the RHS becomes 1 in this case. Thus, we may assume $\Delta > 0$. We prove (11.4) by induction on w, the number of clauses conjuncted to form G. The base case of $w = 0$ is trivial, since $G \equiv 1$ by definition and the statement holds since the LHS is 0. By induction, assume that (11.4) holds for all conjuncts of up to $w - 1$ clauses.

Let G be a t-And-Or formula $G_1 \wedge G_2 \wedge \ldots \wedge G_w$. Let $G' = G_2 \wedge \ldots \wedge G_w$. Let ρ be a random p-restriction. By renaming literals, we can assume WLOG that $G_1 = \bigvee_{i \in T} x_i$ for some T with $|T| \leq t$.

To prove the claim, we consider two cases $G_1|_\rho \equiv 1$ and $G_1|_\rho \not\equiv 1$. The case of $G_1|_\rho \equiv 1$ is easy. $G_1|_\rho \equiv 1$ implies that $G|_\rho \equiv G'|_\rho$. So, by induction

$$\Pr[\ \mathrm{DC}(G|_\rho) \geq \Delta \mid F|_\rho \equiv 1, G_1|_\rho \equiv 1\ ] \ =\ \Pr[\ \mathrm{DC}(G'|_\rho) \geq \Delta \mid (F \wedge G_1)|_\rho \equiv 1\ ] \ \leq\ \alpha^{\Delta}.$$

Rest of the proof deals with the case $G_1|_\rho \not\equiv 1$. That is, we want to prove the following statement as well.

$$\Pr[\ \mathrm{DC}(G|_\rho) \geq \Delta \mid F|_\rho \equiv 1, G_1|_\rho \not\equiv 1\ ] \ \leq\ \alpha^\Delta \tag{11.5}$$

We have renamed the variables so that $G_1 = \bigvee_{i\in T} x_i$. Then $G_1|_\rho \not\equiv 1$ means that for each $i \in T$, $\rho(i) = 0$ or $*$. For each ρ such that $G_1|_\rho \not\equiv 1$, consider the set of all $i \in T$ such that $\rho(i) = *$. Moreover, if $\rho(i) = 0$ for all $i \in T$, then $G_1|_\rho \equiv 0$ and hence, $G|_\rho \equiv 0$ implying $DC(G) = 0$. Thus, it is not the case that $\rho(i) = 0$ for all $i \in T$. So,

$$\begin{aligned}
&\{\rho\ :\ F|_\rho \equiv 1, G_1|_\rho \not\equiv 1, \mathrm{DC}(G|_\rho) \geq \Delta\} \\
&\quad = \bigcup_{\emptyset\neq Y\subseteq T} \{\rho\ :\ \rho(Y) = *, \rho(T-Y) = 0, F|_\rho \equiv 1, \mathrm{DC}(G|_\rho) \geq \Delta\,\}.
\end{aligned} \tag{11.6}$$

Let

$$a_Y \ \ = \ \ \Pr[\ \rho(Y) = * \wedge \rho(T-Y) = 0 \mid F|_\rho \equiv 1 \wedge G_1|_\rho \not\equiv 1\ ]. \tag{11.7}$$

So, (11.8) can be written as

$$\begin{aligned}
&\Pr[\ \mathrm{DC}(G|_\rho) \geq \Delta \mid F|_\rho \equiv 1, G_1|_\rho \not\equiv 1\ ] \\
&\quad = \sum_{\emptyset\neq Y\subseteq T} a_Y \cdot \Pr[\ \mathrm{DC}(G|_\rho) \geq \Delta \mid F|_\rho \equiv 1 \wedge G_1|_\rho \not\equiv 1 \wedge \rho(Y) = * \wedge \rho(T-Y) = 0] \\
&\quad = \sum_{\emptyset\neq Y\subseteq T} a_Y \cdot \Pr[\ \mathrm{DC}(G|_\rho) \geq \Delta \mid F|_\rho \equiv 1 \wedge \rho(Y) = * \wedge \rho(T-Y) = 0]
\end{aligned} \tag{11.8}$$

We will bound this sum from above by considering the individual terms. First consider the case of a fixed $|Y| < \Delta$.

Fix ρ such that $\mathrm{DC}(G|_\rho) \geq \Delta$ and $F|_\rho \equiv 1 \wedge \rho(Y) = * \wedge \rho(T-Y) = 0$. We claim that there exists $\sigma_Y : Y \to \{0,1\}$, such that $\mathrm{DC}(G|_\rho|_{\sigma_Y}) \geq \Delta - |Y|$.

Suppose not. Then for all $\sigma_Y : Y \to \{0,1\}$, $\mathrm{DC}(G|_\rho|_{\sigma_Y}) < \Delta - |Y|$. So we can construct a decision tree for $G|_\rho$ as follows. Start with a full binary tree of depth $|Y|$ in which each level determines the value of x_i for some $i \in Y$. Now let each leaf of this full binary tree, which represents a restriction σ_Y, be the root of a decision tree for $G|_\rho|_{\sigma_Y}$ of depth $\leq \Delta - |Y|$. The result is a decision tree for $G|_\rho$ of depth $\leq \Delta$. So $\mathrm{DC}(G|_\rho) < \Delta$, which is a contradiction.

We conclude from this contradiction that such a σ_Y exists. We also note that $\sigma_Y \neq 0^Y$. For if $\sigma_Y = 0^Y$, then $G_1|_\rho|_{0^Y} \equiv 0$, so $G|_\rho|_{0^Y} \equiv 0$, so $\mathrm{DC}(G|_\rho|_{0^Y}) = 0$.

Since $\sigma_Y \neq 0^Y$, we have $G_1|_\rho|_{\sigma_Y} \equiv 1$, so $G|_\rho|_{\sigma_Y} \equiv G'|_\rho|_{\sigma_Y}$ and $\mathrm{DC}(G'|_\rho|_{\sigma_Y}) = \mathrm{DC}(G|_\rho|_{\sigma_Y}) \geq \Delta - |Y|$.

Now, again treating ρ as a random p-restriction, we have

$$\Pr[\ \mathrm{DC}(G|_\rho) \geq \Delta \mid F|_\rho \equiv 1 \wedge \rho(Y) = * \wedge \rho(T-Y) = 0]$$

$$
\begin{aligned}
&\leq \Pr[\exists \sigma_Y : Y \to \{0,1\},\ \mathrm{DC}(G'|_\rho|_{\sigma_Y}) \geq \Delta - |Y| \mid F|_\rho \equiv 1 \wedge \rho(Y) = * \wedge \rho(T-Y) = 0] \\
&\leq \sum_{\substack{\sigma_Y : Y \to \{0,1\} \\ \sigma_Y \neq 0^Y}} \Pr[\ \mathrm{DC}(G'|_\rho|_{\sigma_Y}) \geq \Delta - |Y| \mid F|_\rho \equiv 1 \wedge \rho(Y) = * \wedge \rho(T-Y) = 0]
\end{aligned}
\tag{11.9}
$$

G' is a formula with $w-1$ clauses. We would like to invoke the induction hypothesis to bound the above sum. But, the condtion "$F|_\rho \equiv 1 \wedge \rho(Y) = * \wedge \rho(T-Y) = 0$" does not fit the induction hypothesis. We can overcome this as follows. Suppose $\rho(Y) = * \wedge \rho(T-Y) = 0$. Then, $F|_\rho \equiv 1$ iff for any (partial) truth assignment $\tau_Y : Y \to \{0,1\}$, we have $F|_\rho|\tau_Y \equiv 1$. To express this formally, set

$$
\begin{array}{lcl}
0^{T-Y} & = & \text{the all 0 assignment on } T-Y, \\
\widetilde{F} & = & \bigwedge_{\tau_Y : Y \to \{0,1\}} F|_{0^{T-Y}}|_{\tau_Y} \ \text{ and} \\
\widetilde{\rho} & = & \rho \text{ restricted to the complement of } T.
\end{array}
$$

Then whenever $\rho(Y) = * \wedge \rho(T-Y) = 0$, as in the condition on the probabilities in (11.9),

$$
\widetilde{F}|_{\widetilde{\rho}} \equiv 1 \iff F|_\rho \equiv 1
$$

Again, suppose $\rho(Y) = *$ and $\rho(T-Y) = 0$. Then, for any $\sigma_Y : Y \to \{0,1\}$, we have $G'|_\rho|\sigma_Y$ is equivalent to $(G'|_{0^{T-Y}}|_{\sigma_Y})|_{\widetilde{\rho}}$. Thus,

$$
\begin{aligned}
&\Pr[\ \mathrm{DC}(G'|_\rho|_{\sigma_Y}) \geq \Delta - |Y| \mid F|_\rho \equiv 1 \wedge \rho(Y) = * \wedge \rho(T-Y) = 0] \\
&\leq \Pr[\ \mathrm{DC}((G'|_{0^{T-Y}}|_{\sigma_Y})|_{\widetilde{\rho}}) \geq \Delta - |Y| \mid \widetilde{F}|_{\widetilde{\rho}} \equiv 1]
\end{aligned}
$$

As $G'|_{0^{T-Y}}|_{\sigma_Y}$ has (at most) $w-1$ clauses, we can apply induction hypothesis and get

$$
\Pr[\ \mathrm{DC}((G'|_{0^{T-Y}}|_{\sigma_Y})|_{\widetilde{\rho}}) \geq \Delta - |Y| \mid \widetilde{F}|_{\widetilde{\rho}} \equiv 1] \leq \alpha^{\Delta - |Y|}
$$

So (11.9) becomes

$$
\Pr[\ \mathrm{DC}(G|_\rho) \geq \Delta \mid F|_\rho \equiv 1 \wedge \rho(Y) = * \wedge \rho(T-Y) = 0] \ \leq \ (2^{|Y|} - 1)\alpha^{\Delta - |Y|} \tag{11.10}
$$

We have proved the above bound for $|Y| < \Delta$. Now consider the case $|Y| \geq \Delta$. Here (11.10) holds trivially, because $|Y| \geq \Delta > 0$ and $\alpha < 1$ imply $(2^{|Y|} - 1)\alpha^{\Delta - |Y|} \geq 1$.

So (11.8) becomes

$$
\Pr[\ \mathrm{DC}(G|_\rho) \geq \Delta \mid F|_\rho \equiv 1, G_1|_\rho \not\equiv 1\ ] \ \leq \sum_{\emptyset \neq Y \subseteq T} a_Y \cdot (2^{|Y|} - 1)\alpha^{\Delta - |Y|} \tag{11.11}
$$

Let

$$
b_Y \ = \ \Pr[\ \rho(Y) = * \mid F|_\rho \equiv 1 \wedge G_1|_\rho \not\equiv 1\ ]. \tag{11.12}
$$

Clearly $b_Y \geq a_Y$. Also, we see intuitively that $Z \subseteq T$, $b_Z = \Pr[\ \rho(Z) = * \mid F|_\rho \equiv 1 \wedge G_1|_\rho \not\equiv 1\ ] \leq q^{|Z|}$, where $q = p/(p + \frac{1-p}{2})$ is the probability of ρ assigning any variable to be $*$ given that it is assigned to be either $*$ or 0. For we already saw that $G_1|_\rho \not\equiv 1$ means that each variable in Z is assigned either 0 or $*$. The additional condition that $F|_\rho \equiv 1$ can only decrease the probability that some variable is assigned a $*$. We will give a rigorous proof that $b_Z \leq q^{|Z|}$ at the end of these notes.

It follows that

$$\begin{aligned}
\Pr[\ \mathrm{DC}(G|_\rho) \geq \Delta \mid F|_\rho \equiv 1, G_1|_\rho \not\equiv 1\ ] &\leq \sum_{\emptyset \neq Y \subseteq T} a_Y \cdot (2^{|Y|} - 1)\alpha^{\Delta - |Y|} \\
&= \sum_{Y \subseteq T} a_Y \cdot (2^{|Y|} - 1)\alpha^{\Delta - |Y|} \qquad (11.13) \\
&\leq \sum_{Y \subseteq T} b_Y \cdot (2^{|Y|} - 1)\alpha^{\Delta - |Y|} \\
&\leq \sum_{Y \subseteq T} q^{|Y|} \cdot (2^{|Y|} - 1)\alpha^{\Delta - |Y|} \\
&\leq \alpha^\Delta \left[\left(\sum_{Y \subseteq T} \left(\frac{2q}{\alpha}\right)^{|Y|} \right) - \left(\sum_{Y \subseteq T} \left(\frac{q}{\alpha}\right)^{|Y|} \right) \right] \\
&= \alpha^\Delta \left[\left(1 + \frac{2q}{\alpha}\right)^{|T|} - \left(1 + \frac{q}{\alpha}\right)^{|T|} \right] \qquad (11.14)
\end{aligned}$$

The last equality in the above derivation is obtained using the identity, $\sum_{X \subseteq A} x^{|X|} = (1 + x)^{|A|}$.

If we set $c = 1/\log_e \phi \approx 2.078$, where $\phi = \frac{1+\sqrt{5}}{2} \approx 1.618$ is the golden ratio, then we have $e^{2/c} - e^{1/c} = \phi^2 - \phi = 1$. Then, setting $\alpha = cqt < 5pt$, we get

$$\left(1 + \frac{2q}{\alpha}\right)^t - \left(1 + \frac{q}{\alpha}\right)^t = \left(1 + \frac{2}{ct}\right)^t - \left(1 + \frac{1}{ct}\right)^t < e^{2/c} - e^{1/c} = 1. \qquad (11.15)$$

since $(1 + \frac{\lambda}{t})^t < e^\lambda$ for all t (to see this, compare (term by term) the binomial expansion of LHS and Taylor series of RHS).

We have shown that

$$\Pr[\ \mathrm{DC}(G|_\rho) \geq \Delta \mid F|_\rho \equiv 1, G_1|_\rho \not\equiv 1\ ] \ < \ \alpha^\Delta.$$

This completes the proof of

$$\Pr[\ \mathrm{DC}(G|_\rho) \geq \Delta \mid F|_\rho \equiv 1\ ] \ < \ (5pt)^\Delta.$$

♣

Now we prove the tighter bound for Lemma 11.14. Note that

$$b_Y = \sum_{Y \subseteq Z \subseteq T} a_Z,$$

and by the Möbius Inversion Formula,

$$a_Y = \sum_{Y \subseteq Z \subseteq T} (-1)^{|Z-Y|} b_Z$$

Substituting $\sum_{Y \subseteq Z \subseteq T} (-1)^{|Z-Y|} b_Z$ for a_Y in (11.13), we have

$$\begin{aligned}
&\Pr[\ \mathrm{DC}(G|_\rho) \geq \Delta \mid F|_\rho \equiv 1, G_1|_\rho \not\equiv 1\ ] \\
&\leq \sum_{Y \subseteq T} \sum_{Y \subseteq Z \subseteq T} (-1)^{|Z-Y|} b_Z \cdot (2^{|Y|} - 1) \alpha^{\Delta - |Y|} \\
&= \sum_{Z \subseteq T} b_Z (-1)^{|Z|} \alpha^\Delta \sum_{Y \subseteq Z} \left[\left(\frac{-2}{\alpha} \right)^{|Y|} - \left(\frac{-1}{\alpha} \right)^{|Y|} \right]
\end{aligned}$$

Therefore

$$\begin{aligned}
&\Pr[\ \mathrm{DC}(G|_\rho) \geq \Delta \mid F|_\rho \equiv 1, G_1|_\rho \not\equiv 1\ ] \\
&\leq \alpha^\Delta \sum_{Z \subseteq T} b_Z (-1)^{|Z|} \left[\left(1 - \frac{2}{\alpha} \right)^{|Z|} - \left(1 - \frac{1}{\alpha} \right)^{|Z|} \right] \\
&= \alpha^\Delta \sum_{Z \subseteq T} b_Z \left[\left(\frac{2}{\alpha} - 1 \right)^{|Z|} - \left(\frac{1}{\alpha} - 1 \right)^{|Z|} \right] \\
&\leq \alpha^\Delta \sum_{Z \subseteq T} q^{|Z|} \left[\left(\frac{2}{\alpha} - 1 \right)^{|Z|} - \left(\frac{1}{\alpha} - 1 \right)^{|Z|} \right] \\
&= \alpha^\Delta \left\{ \left[1 + q \left(\frac{2}{\alpha} - 1 \right) \right]^{|T|} - \left[1 + q \left(\frac{1}{\alpha} - 1 \right) \right]^{|T|} \right\} \\
&\leq \alpha^\Delta \left\{ \left[1 + q \left(\frac{2}{\alpha} - 1 \right) \right]^{t} - \left[1 + q \left(\frac{1}{\alpha} - 1 \right) \right]^{t} \right\}
\end{aligned}$$

Now, we want to choose an appropriate α so that the quantity in curly braces above is ≤ 1. Set $q = \beta/t$. Then,

$$\left[1 + \left(\frac{2}{\alpha} - 1 \right) \frac{\beta}{t} \right]^t - \left[1 + \left(\frac{1}{\alpha} - 1 \right) \frac{\beta}{t} \right]^t < e^{\left(\frac{2}{\alpha} - 1 \right) \beta} - e^{\left(\frac{1}{\alpha} - 1 \right) \beta}$$

So, we want to maintain $e^{(2/\alpha - 1)\beta} - e^{(1/\alpha - 1)\beta} < 1$. Solving this equation, we get

$$\alpha = \frac{\beta}{ln \left[\frac{1 + \sqrt{1 + 4e^\beta}}{2} \right]}. \tag{11.16}$$

This completes proof of Lemma 11.14. ♣

Now we will show that for any $Z \subseteq T$, $b_Z = \Pr[\ \rho(Z) = * \mid F|_\rho \equiv 1 \wedge G_1|_\rho \not\equiv 1\ ] \leq q^{|Z|}$, where $q = p/(p + \frac{1-p}{2})$. Before we proceed, note that for $Z \subseteq T$, we have

$$\Pr[\ \rho(Z) = * \mid G_1|_\rho \not\equiv 1\ ] \ = \ q^{|Z|},$$

since $G_1|_\rho \not\equiv 1$ means that ρ assigns only $*$ or 0 on T.

We now show that

$$b_Z \leq \Pr[\ \rho(Z) = * \mid G_1|_\rho \not\equiv 1\ ]$$

This is trivial if $Z = \emptyset$. Suppose $Z \neq \emptyset$.

Note that $b_Z \leq \max_{\rho'} \Pr[\ \rho(Z) = * \mid F|_\rho \equiv 1, G_1|_\rho \not\equiv 1, \rho|_{Z^c} = \rho'\ ]$.

Consider any fixed restriction ρ' on the complement of Z, $\rho' : Z^c \to \{0, 1, *\}$. Then, there is a unique extension of ρ' over Z, call it ρ^*, that satisfies $\rho^*(Z) = *$.

We claim that

$$\Pr[\ \rho(Z) = * \mid F|_\rho \equiv 1, G_1|_\rho \not\equiv 1, \rho|_{Z^c} = \rho'\ ] \ \leq \ q^{|Z|}.$$

The event $\rho(Z) = *$ refers to the unique ρ^*, under the condition $\rho|_{Z^c} = \rho'$. If $F|_{\rho^*} \equiv 1$ then $F|_\rho \equiv 1$ for all extensions ρ of ρ' to Z. Hence $F|_\rho \equiv 1, G_1|_\rho \not\equiv 1, \rho|_{Z^c} = \rho'$ refers to the $2^{|Z|}$ assignments ρ, such that $\rho(i) \in \{0, *\}$ for all $i \in Z$. Out of these $2^{|Z|}$ assignments, $\rho(Z) = *$ occurs with probability $q^{|Z|}$. On the other hand, if $F|_{\rho^*} \not\equiv 1$, then the above conditional probability is 0 and the claim trivially holds. Hence, the claim is true and $b_Z \leq q^{|Z|}$. ♣

11.3.5 Switching Lemma: Improved Lower Bounds

We now improve the bounds in switching lemma. Using the lemma, we establish lower bounds on size of circuits computing or approximating parity.

In the last lecture we proved the following lemma.

LEMMA 11.15 *Let G be a t-And-Or formula $G_1 \wedge G_2 \wedge \ldots \wedge G_w$. For any β, $0 < \beta < t$, let ρ be a random p-restriction, where $p = \frac{\beta}{t-\beta}$, and let $\alpha = \beta/ln\left[\frac{1+\sqrt{1+4e^\beta}}{2}\right]$. Then for all $\Delta \geq 0$, we have*

$$\Pr[DC(G|\rho) \geq \Delta] \leq \alpha^\Delta.$$

In the above lemma, α is minimized when $\beta = \beta_0 \approx 0.227537$. In which case, $\alpha = \alpha_0 \approx 0.4164447$. Let $\gamma_0 = \beta_0/2 \approx 0.1137685$.

Using Lemma 1, we will prove the Lemma 2, a stronger version of switching lemma. The key is the the following composite property of random restrictions. Observe that a p_1-restriction followed by a p_2-restriction has the same effect with a single p_1p_2-restriction. This property holds because the boolean variables are independently assigned at each step.

LEMMA 11.16 *Let G be a t-And-Or formula $G_1 \wedge G_2 \wedge \ldots \wedge G_w$, and let ρ be a random γ_0/t-restriction. Then for all $\Delta \geq 0$, we claim*

$$\Pr[DC(G|_\rho) \geq \Delta] \leq {\alpha_0}^\Delta$$

Proof. Let $q = \beta_0/t$ and $p = \frac{q}{2-q}$. Then $q = \frac{2p}{1+p} = \frac{p}{p+\frac{1-p}{2}}$ is the probability a variable is assigned a * in a random p-selection under the condition that it is assigned * or 0.

We have shown that

$$\Pr[DC(G|_{\rho'}) \geq \Delta] \leq {\alpha_0}^\Delta,$$

where ρ' is a random p-restriction.

Since $p = \frac{q}{2-q} > \frac{q}{2} = \frac{\gamma_0}{t}$, we know that $\gamma_0/(pt)$ is still a number less than 1. Because of the composite property of random restriction, a random γ_0/t-restriction ρ can be realized by first applying a random p-restriction ρ', followed by a $\frac{\gamma_0}{pt}$-restriction. Note that $DC(G|\rho') < \Delta$ means there exists a decision tree with depth less than Δ, which can compute G. Therefore we would also be able to compute G within less than Δ depth with the more stringent restriction ρ. That is to say,

$$\Pr[DC(G|_\rho) \geq \Delta] \leq \Pr[DC(G|_{\rho'}) \geq \Delta] \leq {\alpha_0}^\Delta.$$

11.3.6 Circuit Lower Bounds

Consider general constant depth circuits. Denote by $C^d(s,t)$ the class of depth d circuits with bfi (the abbreviation of bottom fanin) $\leq t$, and the number of gates above the first level $\leq s$. Denote by $C^d(s)$ the class of depth d circuits without a bfi condition but with total size $\leq s$. It is clear that a circuit in $C^d(s)$ can be considered as a circuit in $C^{d+1}(s,1)$, by adding an extra layer of gates with fan-in 1.

The following lemma is proved using the switching lemma. In Lecture 16, we discussed on how to use the switching lemma to prove circuit lower bounds. We use the same ideas here and hence, we provide only a sketch of the proof.

LEMMA 11.17 *For all $C \in C^d(s, \gamma_0 n^{1/d})$, we have*

$$\Pr[DC(C|_\rho) \geq \gamma_0 n^{1/d}] \;\leq\; s \cdot \alpha_0^{\gamma_0 n^{1/d}} \;\approx\; s \cdot 2^{-0.143781 \cdot n^{1/d}},$$

where ρ is a random $1/n^{\frac{d-1}{d}}$-restriction.

Proof. Let $t = \gamma_0 n^{1/d}$ and $p = 1/n^{\frac{1}{d}}$. Let $C \in C^d(s,t)$. Denote the number of gates on each level as $s_1, s_2, \ldots, s_d$ from the bottom to the top (output level). Clearly, $s_d = 1$ and $\sum_{i=1}^{d-1} s_i = s$. Apply Lemma 2 repeatedly $d-1$ times, each time with a random p-restriction.

After applying the first random restriction, suppose all the s_1 many t-AND-OR circuits at level 1 have DC $\leq t$. Then, we can switch these into t-OR-AND circuits and merge first and second levels eliminating a level. This process also eliminates s_1 gates from the circuit. Nonetheless, for each gate at the bottom level, it is possible that we cannot switch. By Lemma 2, for any one of the s_1 circuits, probability that we fail to to switch is $\leq \alpha_0^t$. So the probability of failure at this level is at most $s_1 \cdot \alpha_0^t$. Accumulating the probability of the failure on each level, and combining with the Lemma 2, we have

$$\Pr[DC(C|_\rho) \geq \gamma_0 t] \;\leq\; \sum_i s_i \cdot \alpha_0^t = s \cdot \alpha_0^t = s \cdot \alpha_0^{\gamma_0 n^{1/d}} \;\approx\; s \cdot 2^{-0.143781 \cdot n^{1/d}}$$

Finally, by the composite property of random restrictions, applying $d-1$ random p-restrictions has the same effect as one random p^{d-1}-restriction. The proof is complete.

We can apply Lemma 3 to $C \in C^d(s)$ by first transforming them into $C \in C^{d+1}(s,1)$. But we can actually do slightly better by a more delicate technique. Here we omit the proof of the following better bound.

LEMMA 11.18 *For all $C \in C^d(s)$, we have*

$$\Pr[DC(C|_\rho) \geq \gamma_0 n^{1/d}] \;<\; s \cdot \alpha_0^{\gamma_0 n^{1/d}} \;\approx\; s \cdot 2^{-0.143781 \cdot n^{1/d}},$$

where ρ is a random $\alpha_0/(2n^{\frac{d-1}{d}})$-restriction.

These results can be used to prove circuit lower bounds for the parity function. Consider any circuit C in $C^d(s, \gamma_0 n^{1/(d-1)})$. Apply $d-2$ rounds of random $1/n^{1/(d-1)}$-restrictions. With probability $> 1 - s \cdot 2^{-0.143781 \cdot n^{1/(d-1)}}$, we get a circuit in $C^2(1, \gamma_0 n^{1/(d-1)})$ after switching and merging. The process is equivalent to applying a single random $n^{(d-2)/(d-1)}$-restriction. Let N be the random variable for number of variables left (i.e., variables assigned *). Then, its expectation $E[N] = n^{1/(d-1)}$. By Chernoff bound we have,

$$\Pr[N \leq \gamma_0 n^{\frac{1}{d-1}}] < e^{-\frac{(1-\gamma_0)^2}{2} \cdot n^{\frac{1}{d-1}}} < e^{-0.3927 n^{\frac{1}{d-1}}}.$$

Hence, if $s < 2^{0.143781 \cdot n^{1/(d-1)}}$, the probability is approaching 1 that both C is reduced to a circuit in $C^2(1, \gamma_0 n^{1/(d-1)})$ and $N > \gamma_0 n^{1/(d-1)}$. Suppose the circuit we started with computes parity on n variables. Then, the circuit obtained after applying the random restriction computes parity on the remaining N variables. Clearly, a $C^2(1,t)$ circuit cannot compute parity on $> t$ variables (see Lecture 16). We have proved the following lemma.

LEMMA 11.19 *For all $C \in C^d(s, \gamma_0 n^{1/(d-1)})$, if C computes the parity function, then its size s must satisfy*

$$s \geq 2^{0.143781 \cdot n^{1/(d-1)}}.$$

Lemma 11.19 can be used to obtain lower bounds for general circuits (without bfi). Again, we can simply transform a circuit in $C^d(s)$ into a circuit in $C^{d+1}(s, 1)$, then apply Lemma 11.19. Using a more direct and finer analysis, one can prove the following lemma.

LEMMA 11.20 *For all $C \in C^d(s)$, if C computes the parity function, then its size s must satisfy*

$$s \geq 2^{0.143781 \cdot n^{\frac{1}{d-1}}}$$

11.3.7 Inapproximability Type Lower Bounds

Now we consider the inapproximability type lower bound. By *inapproximability*, we mean circuits with certain restrictions (like size, depth and bfi) cannot compute parity on significantly more than half of the possible cases. Specifically, for the parity function, we can simply guess 0 and 1 as the function value. So, it is easy to get 50% success. We want to show that, one cannot do significantly better. The decision tree depth lower bound is ideally suited for deriving the inapproximability type lower bound, and the decision tree perspective was introduced precisely for this reason. Our goal is to show that, when the sizes of the circuits are below some lower bound, the circuits will make asymptotically 50% error on all possible inputs.

Let C be a depth d circuit. Note that after some restriction ρ, if C is reduced to a decision tree of depth smaller than the number of variables left, then for exactly half of the 0-1 extensions of ρ, C agrees on the parity. This is because at every leaf of the decision tree, the circuit C is completely determined.

Consider $\Pr[\ C(x_1, \ldots, x_n) = \oplus(x_1, \ldots, x_n)\ ]$, where $\oplus(x_1, \ldots, x_n)$ denotes the parity function, and the probability is over all 2^n assignments. This random restriction technique can be realized by first assigning any random restriction, followed by an unbiased 0-1 assignments for all the remaining variables. Let E_1 denote the event that after the random restriction, we end up with a decision tree of depth not more than t, and let E_2 denote the event that the number of variables N assigned to * is more than t. Then let $E = E_1 \wedge E_2$, and let $[\, C = \oplus\,]$ denote $[\, C(x_1, \ldots, x_n) = \oplus(x_1, \ldots, x_n)\,]$ for convenience. As we already pointed out, $\Pr[\, C = \oplus \,|\, E\,] = 1/2$ due to a property of the parity function.

Expending in terms of conditional probabilities, we have

$$\begin{aligned}
\Pr[C = \oplus] &= \Pr[E] \cdot \Pr[C = \oplus | E] + \Pr[\neg E] \cdot \Pr[C = \oplus | \neg E] \\
&= (1 - \Pr[\neg E]) \cdot \Pr[C = \oplus | E] + \Pr[\neg E] \cdot \Pr[C = \oplus | \neg E] \\
&= \Pr[C = \oplus | E] + \Pr[\neg E](Pr[C = \oplus | \neg E] - \Pr[C = \oplus | E]).
\end{aligned}$$

As we noted, $\Pr[\, C = \oplus \,|\, E\,] = 1/2$, and $\Pr[C = \oplus | \neg E] \leq 1$. Then substitute these 2 observations into the above equation,

$$\left| \Pr[C = \oplus] - \frac{1}{2} \right| \;\leq\; \frac{1}{2} \Pr[\neg E].$$

Since $\Pr[C = \oplus] + \Pr[C \neq \oplus] = 1$, we have

$$\Pr[\, C = \oplus\,] - \Pr[\, C \neq \oplus\,] = 2 \left(\Pr[\, C = \oplus\,] - \frac{1}{2} \right),$$

and hence

$$|\Pr[\, C = \oplus\,] - \Pr[\, C \neq \oplus\,]| \;\leq\; \Pr[\neg E].$$

Now we specify the parameters of the random restrictions. Let $m = \gamma_0 n^{1/d}$. First consider any $C \in C^d(s, \gamma_0 m)$. Let $t = \gamma_0 m$ and apply Lemma 11.17. With a random $1/n^{(d-1)/d}$-restriction, we have

$$\Pr[\neg E_1] \leq s\alpha_0^t \approx s\dot{2}^{0.143781 \cdot m}.$$

Again by using the Chernoff bound, we estimate $\Pr[\neg E_2] = \Pr[N \leq \gamma_0 m]$ as follows.

$$\Pr[\neg E_2] \leq e^{-\frac{(1-\gamma_0)^2}{2} m} < e^{0.3927m}.$$

Thus $\Pr[\neg E_2]$ is dominated by $\Pr[\neg E_1]$. This analysis gives the following bound.

LEMMA 11.21 *For all $C \in C^d(2^{0.07189 n^{1/d}}, \gamma_0 n^{1/d})$, we have*

$$|\Pr[\, C = \oplus\,] - \Pr[\, C \neq \oplus\,]| \;\leq\; 2^{-0.07189 n^{1/d}}.$$

Again straightforward application of the above lemma gives inapproximability results for general circuits (without bfi). A more careful analysis leads to the following lemma.

LEMMA 11.22 *For all circuits $C \in C^d(2^{0.07189 n^{1/d}})$, we have*

$$|\, \Pr[C = \oplus] - \Pr[C \neq \oplus]| \leq 2^{0.07189 n^{1/d}}.$$