CS 830: RANDOMNESS AND COMPLEXITY 04/14/05

Lecture 24: Circuit lower bounds (continued)

instructor: Jin-Yi Cai Scribe: Scott Diehl, Jeff Kinne

In this lecture, we (roughly) follow [CW04] pages 18-23. We continue our discussion of lower bounds for constant depth circuits. We begin by finishing the proof a lemma from the previous lecture. We also give a preview of how to prove circuit lower bounds for parity.

1 Finish Lemma

Recall the setup from the last lecture. G is a t-And-Or formula, which can be written $G_1 \wedge G_2 \wedge \ldots \wedge G_w$ for each G_i an or of t terms. Letting $G' = G_2 \wedge \ldots \wedge G_w$, we can rewrite this as $G = G_1 \wedge G'$. We will relabel the variables if necessary so that the variables occuring in G_1, which we will denote by the set T, all appear positively in G_1 and occur first in the variable ordering, so that $G_1 = \bigvee_{i \in T} x_i$. Further, we denote by Y the set of variables in T that are set to * by a random restriction ρ, and Z will be some superset of Y in T, $Y \subseteq Z \subseteq T$.

We were considering the case where $G_1 \not\equiv 1$ under a random p-restriction ρ. This occurs if and only if $\rho|_T$ consists entirely of * and 0's.

LEMMA 1.1. *Let G be a t-And-Or formula $G_1 \wedge G_2 \wedge \ldots \wedge G_w$ and F be any Boolean function on the same variables as G. Let ρ be a random p-restriction. Then for all $\Delta \geq 0$,*

$$\Pr[DC(G|_\rho) \geq \Delta \mid F|_\rho \equiv 1] \leq \alpha^\Delta$$

where $\alpha = 5pt$.

Proof. In a previous lecture, we completed the proof assuming the claim that the probability that ρ restricted to an arbitrary Z is all * (under certain conditions) is at most $q^{|Z|}$. All that remains is to prove the claim, which we will do now.

CLAIM 1.2.

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

where $q = \Pr[\rho(i) = * | \rho(i) = 0, *] = \frac{p}{p+(1-p)/2} = \frac{2p}{1+p} < 2p$.

Proof of claim: We will consider all partial restrictions ρ' to all of the varaibles outside of Z, and then consider the probability that each ρ' is extended to a ρ which assigns $*$ to Z. Namely, let $\rho' : \{Z^c\} \to \{0, 1, *\}$ and break up the probability into a sum:

$$\begin{aligned} &\Pr[\rho(Z) = * \mid F|_\rho \equiv 1, G_1|_\rho \not\equiv 1] \quad = \\ \sum_{\rho' : Z^c \to \{0,1*\}} &\Pr[\rho|_{Z^c} = \rho' \mid F_\rho \equiv 1, G_1|_\rho \not\equiv 1] \quad \cdot \quad \Pr[\rho(Z) = * \mid F|_\rho \equiv 1, G_1|_\rho \not\equiv 1, \rho|_{Z^c} = \rho'] \end{aligned} \quad (1)$$

Let us fix a particular ρ' and consider the term in the sum. Let ρ^* be the unique random-restriction of ρ' that we consider a "success", extending ρ' to $*$'s on Z: $\rho^*|_{Z^c} = \rho'$ and $\rho^*|_Z = *$.

We evaluate the factor

$$\Pr[\rho(Z) = * \mid F|_\rho \equiv 1, G_1|_\rho \not\equiv 1, \rho|_{Z^c} = \rho'] \tag{2}$$

of the sum (1) in two cases, based on whether or not F restricted by ρ^* is identically 1. If $F|_{\rho^*} \equiv 1$, then it must be the case that $F|_\rho \equiv 1$ for all restrictions ρ that are extensions of ρ'. This is because if $F|_{\rho^*} \equiv 1$, then F evaluates to 1 no matter what the values of the variables in Z are, so that the condition $F|_\rho \equiv 1$ holds for all $2^{|Z|}$ possible extensions ρ of ρ'. Note also that $G_1|_\rho \not\equiv 1$ when $\rho|_Z = *$. Therefore, in this case (2) evaluates to $q^{|Z|}$, the probability that any extension of ρ' is assigned all $*$'s.

On the other hand, if $F|_{\rho^*} \not\equiv 1$, then the condition that $F|_\rho \equiv 1$ for ρ extending ρ' implies that any such ρ must assign a definite value to some variable in Z. Therefore, the conditional probability (2) that $\rho(Z) = *$ in this case is 0.

We have shown that in both cases, the term (2) is at most $q^{|Z|}$. Factoring this term out of the sum (1), we can write

$$\begin{aligned}\Pr[\rho(Z) = * \mid F|_\rho \equiv 1, G_1|_\rho \not\equiv 1] &\leq q^{|Z|} \cdot \sum_{\rho': Z^c \to \{0,1*\}} \Pr[\rho|_{Z^c} = \rho' \mid F_\rho \equiv 1, G_1|_\rho \not\equiv 1] \\ &= q^{|Z|},\end{aligned}$$

where the last equality holds because the sum is now over the probabilities of all possible outcomes of a random process, so it must evaluate to 1. □

The proof of the claim completes the proof of the lemma. □

Note that when we want to use this lemma to derive circuit lower bounds, we will set the value p appropriately. Setting $p = \frac{1}{10t}$ will suffice so that pt, the expected number of $*$'s assigned to each clause is significantly less than 1. In this case, a random restriction is likely to eliminate many clauses of G.

2 Lower bounds for parity preview

Our ultimate goal in considering the decision tree complexity of functions is to derive circuit lower bounds for parity. The following lemma will allow us to iteratively reduce the depth of a constant depth circuit by converting the small decision tree produced by a random restriction of an And-Or (described in the last section) into an Or-And of small bottom fan-in size.

LEMMA 2.1. *Given a boolean function F, if $DC(F) \leq t$, then F can be expressed as both a t-And-Or and as a t-Or-And.*

Proof. To obtain a t-Or-And, consider all the paths of the shortest decision tree for F that end in a "1" node. For each of these paths, we create a conjunct of t variables which is true when each of the t variables on the path take the values indicated by the path. F can be expressed as the Or of all these terms.

To obtain a t-And-Or, we can follow the above process to obtain a conjunct for each 0-path. $\overline{F}$ is then the Or of all of these t-Ands, so by DeMorgan's Law, we have an expression of F as a t-And-Or. □

Exercise 2.2. *If F is both a t_1-Or-And and a t_1-And-Or, show that $DC(F) \leq t_1t_2$.*

Suppose we have a depth 3 circuit which is an OR of AND's of OR's, where the bottom fan-in is bounded by t. Consider a subcircuit which is an input to the final OR. This subcircuit will be a t-AND-OR, and Lemma 1.1 tells us that if we take a random p-restriction, we will with high probability be left with a function that has low decision tree complexity. We can then use lemma 2.1 to switch this AND of OR into an OR of AND with bounded bottom fan-in. If we are able to do this flip-flop for each subcircuit fanning into the final OR of the circuit, we will be left with a circuit that is an OR of OR's of AND's. Since the probability of being able to accomplish this switch for each subcircuit is exponentially close to 1, we can accomodate exponentially many subcircuits fanning into the topmost OR. Thus with high probability, the process we have described reduces the depth of the circuit by 1.

Recall that if we wish to compute parity with an AND of OR's (or with an OR of AND's), then each sub-clause will have to contain every variable. Otherwise, we would be able to set the variables such that the circuit computes the wrong value for parity. We now apply the above switching idea when we have a depth d circuit which we wish to show does not compute parity. We will iteratively take random p-restrictions and do the AND-OR flip-flop whenever we can. If we finish the process with a depth 2 circuit (by taking $d-2$ iterations plus one iteration to initially reduce the bottom fan-in) and are left with a circuit that has too few variables in each branch, the circuit could not possibly compute parity on this restriction.

It remains to work out the exact parameters of each restriction described in this step so that the desired results hold with nonzero probability. The exact details are described in [CW04], but we will give a sketch to derive an approximation of the settings here. As described above, we will consider $d-1$ successive restrictions, each time applying Lemmas 1.1 and Lemma 2.1 to produce a circuit computing the restricted function with depth one fewer. The first restriction can be thought of as reducing the bottom fan-in (by thinking of the bottom-most gates as 1-AND-OR's or 1-OR-AND's), and in the remaining steps we would like to keep the bottom fan-in the same. If at each step we consider a p_1-restriction, the restriction resulting in compounding each of these is a p_1^{d-1}-restriction, since each variable has $d-1$ chances to be set away from $*$. Thus setting $p_1 = 1/n^{1/d}$ results in a $1/n^{(d-1)/d}$ restriction, and at each step we can reliably switch a $O(n^{1/d})$-AND-OR to a $O(n^{1/d})$-OR-AND or vice-versa.

APPENDIX

A Improvements of Lemma 1.1

Here we state without proof improvements of Lemma 1.1 that are achieved by tweaking parameters. See [CW04] for further details.

Lemma A.1. *Let G be a t-And-Or. Then $\forall \beta$ such that $0 < \beta < t$, let ρ be a random p-restriction, where $p = \frac{\beta}{t-\beta}$. Then $\forall \Delta \geq 0$,*

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

where $\alpha = \beta / \ln(\frac{1+\sqrt{4+e^\beta}}{2})$.

If we set $\beta \approx .2275$, this will minimize α, leading to the following.

Corollary A.2. *Let G be a t-And-Or, ρ a γ_0/t-restriction. Then* $\forall\Delta \geq 0$,

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

with $\beta_0 \approx .2275, \gamma_0 = \beta_0/2 \approx .1137\alpha_0 \approx .416$.

References

[CW04] Jin-Yi Cai, Osamu Watanabe, "On Proving Circuit Lower Bounds Against the Polynomial-time Hierarchy", submitted to *SIAM Journal of Computation*, revised 2/10/04.