Recent advances in Complexity CIS 6930/CIS 4930 September 5, 2002

Lecture 4

Lecturer: Dr. Meera Sitharam Scribe: Andrew Lomonosov

Main result Parity has no small ($\leq 2^{n^{1/d}/10}$ size) depth d circuits of unbounded fan-in. Hastad (1987). Previous results of FSS - Furst, Saxe, Sipser, and also Ajtai has showed it for small polysize ($\leq n^k$ for some k) depth circuits of bound fan-in.

Exercise 1 *recall that all symmetric functions have size* $\leq n$, *depth* $\leq \log n$ *circuits. Now show* $\exists 2^{n^{1/d}}$ *- sized , depth* $< d$ *(unbound fan-in) circuits for parity.*

Hint: partition the variables. $Parity_{S_1}, Parity_{S_2}, \ldots; \cup_i S_i = \{1, \ldots n\}$. *See Figure 1.*

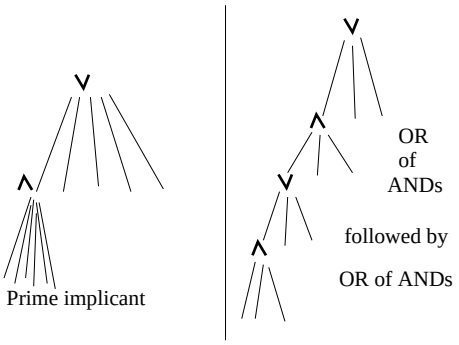

Figure 1: Exercise hint

Intuitive structure of proof of main result.

1. (Known fact). There are no small depth 2 circuits for parity. Moreover, any OR of ANDs circuit for parity has (bottom) AND-fan-in at least n.
2. Depth d circuits with small bottom fan-in can be converted to depth $d-1$ circuits with small bottom fan-in.

If at last level we could write AND-of-ORs as OR-of-ANDs, then we can combine top OR with one directly above, reducing depth by 1.

See Figures 2 and 3 for an example of how to make conversion (without bottom fan-in restriction).

Question: how to do this (conversion above) while keeping small bottom fan-in?

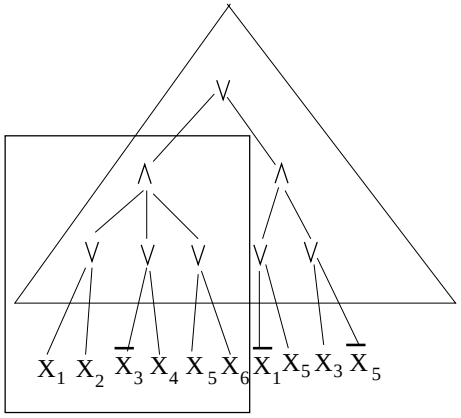

Figure 2: Original circuit

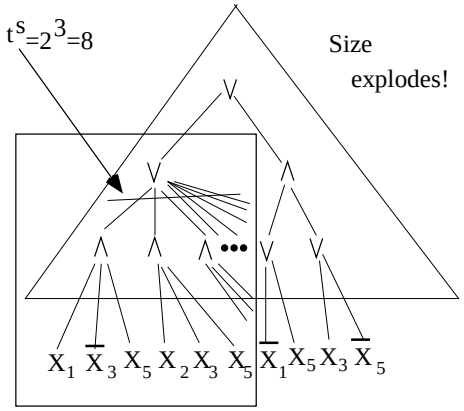

Figure 3: Decreasing depth/ increasing size of the original circuit

Let $X = \{x_1, \ldots, x_n\}$ be the input variables to a circuit C computing a function f. A *restriction* ρ is a mapping from X to $\{0, 1, *\}$.

We interpret ρ as presetting the variables assigned 0 or 1 and leaving variable those assigned later. Under ρ we may simplify C by eliminating gates whose values become determined. Call this the *induced circuit* $C|_\rho$ computing the *induced function* $f|_\rho$.

In the probabilistic arguments to follows we will be selecting restrictions from certain probability distributions. Fix $0 < p < 1$. Let R_p be the probability distribution on restrictions over X where each $x_i \in X$ is independently assigned a value in $\{0, 1, *\}$ so that $Prob[\rho(x_i) = *] = p$ and $Prob[\rho(x_i) = 0] = Prob[\rho(x_i) = 1] = (1 - p)/2$.

The following series of results lead to the parity lower bound, starting from Hastad's switching lemma. The proof of these results were verbally described in class. Here are they formally.

Lemma 1 Hastad's switching lemma. *Let f be a function $\{0, 1\}^n \to \{0, 1\}$ computed by an AND-of-ORs circuit (ORs have fan-in t). Let ρ be a random restriction from R_p. Then probability that $f|_\rho$ has a minterm of size greater*

than s is $\leq \alpha^s$, where $\alpha = \gamma pt$ and $\gamma = 2/\ln\phi \approx 4.16$ for $\phi = (1+\sqrt{5})/2$, the golden ratio.

Lemma 2 Stronger lemma. *Let f be a function $\{0,1\}^n \to \{0,1\}$ computed by an AND-of-ORs circuit (ORs have fan-in t). Let ρ be a random restriction from R_p. Let F be an arbitrary function. Then probability that ($f|_\rho$ has a minterm of size greater than s provided that $F|_\rho \equiv 1$) is $\leq \alpha^s$, where $\alpha = \gamma pt$ and $\gamma = 2/\ln\phi \approx 4.16$ for $\phi = (1+\sqrt{5})/2$, the golden ratio.*

Definition 3 *In the results below, fan-in is only restricted for gates at the input level. Also S denotes number of gates of unbounded fan-in, i.e number of gates that are not at the bottom level.*

Theorem 4 *For all $p, d, 0 \leq k \leq d-1$ if f is a function $\{0,1\}^n \to \{0,1\}$, computable by a depth d circuit of size S with OR on top and of fan-in t, then for a random ρ from R_{p^k} probability that $f|_\rho$ cannot have a depth $(d-k)$ circuit of size S with OR on top and of fan-in t, this probability is less than $S(\gamma pt)^t$, where $\gamma \approx 4.16$.*

Note: book's version of this theorem is incorrect (they use different S).
Proof: Consider the random restriction ρ as being composed from k restrictions $\rho = \rho_1\rho_2\ldots\rho_k$ drawn from R_p. Obtain the sequence of functions $f_1, \ldots, f_{k+1}$ where $f_{i+1} = f_i|_{\rho_i}$. At each step of this sequence there is a collection of OR-on-top of fan-in t (or AND-on-top of fan-in t if $d-i$ is odd) bottom-level subcircuits in the circuit for f_i which may become AND-on-top of fan-in t (or OR-on-top of fan-in t) under ρ_i and then merge with the gates above them. If this successfully occurs for each subcircuit in every f_i then f_{k+1} has depth $(d-k)$ circuit of size S with OR on top and of fan-in t. The probability that it fails at any particular subcircuit is at most $(\gamma pt)^t$ by the Hastad Switching Lemma. Hence the probability that it fails at any of the at most S subcircuits encountered is bounded above by $S(\gamma pt)^t$. ■

The following corollary is independently interesting as a type of Ramsey Theorem.

Corollary 5 *If f is a function $\{0,1\}^n \to \{0,1\}$, computable by a depth d circuit of size S with OR on top and of fan-in t, where $t \geq \log S$, then there is a restriction ρ assigning at least $n/3(10t)^{d-1} - t$ stars such that $f|_\rho$ is a constant function.*

Proof: By the theorem above, if $\rho = 1/10t$ and ρ is drawn from a $R_{p^{d-1}}$, then the probability that $f|_\rho$ is not computable by a depth 1 circuit of size S with OR on top and of fan-in t is at most $S(\gamma\rho t)^t = S\beta^t \leq (2\beta)^t$ where $\beta = \gamma/10 < 0.42$. Hence Prob[$f|_\rho$ is not computable by a depth 1 circuit of size S with OR on top and of fan-in t is < 0.84. Furthermore ρ is expected to have np^{d-1} stars. An easy calculation shows that Prob[ρ has fewer than $np^{d-1}/3$ stars] < 0.15. Since the sum of these probabilities is less than 1, there is a restriction ρ for which neither event occurs. Finally, since any nonconstant function computable by a depth 1 circuit of size S with OR on top and of fan-in t may be forced to 1 by setting at most t inputs we may extend ρ by including these t additional settings and guarantee that $f|_\rho$ is constant. ■

Using the preceding corollary we can now obtain the desired lower bounds for the parity function PARITY$(x_1, \ldots, x_n) = (\Sigma x_i) mod 2$.

Theorem 6 *For all $n, d > 0$, PARITY is not computable by a depth d circuit of size S with OR on top and of fan-in* $\log S$ *, where $S < 2^{(1/10)n^{1/d}}$.*

Proof: If PARITY were computable by a depth d circuit of size S with OR on top and of fan-in $\log S$ for $S < 2^{(1/10)n^{1/d}}$, then by the above corollary there would be a restriction ρ assigning at least one star such that $\text{PARITY}|_\rho$ is constant. This contradiction proves the theorem. ■

Corollary 7 *Polynomial-size parity circuits must have depth at least* $\log n/(c + \log\log n)$ *for some constant c.*

The bound in the above theorem cannot be significantly improved as it is quite close to the easily obtained upper bound.

Theorem 8 *For all n and d, PARITY is computable by a depth d circuit of size S with OR on top and of fan-in* $\log S$ *where $S = n2^{n^{1/d}}$.*