

# Lecture No. 7

Date:02-12-95

Scribe: Ramkrishna Chatterjee

**Theorem 1** *Let  $C$  be a  $n$ -input probabilistic circuit accepting  $L$  with error probability  $\leq e(n)$ . There exists a deterministic circuit of same size and depth as  $C$ , which computes  $\chi_L$  (characteristic function of  $L$ ) correctly on  $\geq 2^n - (2^n e(n))$  inputs.*

*Proof:* Suppose  $C$  uses  $r$  probabilistic bits. Consider the  $2^r \times 2^n$  boolean matrix  $M$  whose rows are indexed by  $r$ -bit probabilistic sequences (assuming lexicographic ordering) and columns are indexed by  $n$ -bit input sequences (again assuming lexicographic ordering). Let  $X_j$  be the  $j^{\text{th}}$  input string and  $\alpha^i$  be the  $i^{\text{th}}$  string of probabilistic bits.  $M[i, j]$  is 1 if  $C(\alpha^i, X_j) = \chi_L(X_j)$ . Otherwise  $M[i, j] = 0$ . By definition of  $C$

$$\forall j (1 \leq j \leq 2^n) \frac{\# \text{ of } 0\text{'s in the } j^{\text{th}} \text{ column}}{2^r} \leq e(n)$$

Let  $B$  = smallest number of 0's in any row of  $M$  and  $Z$  = total number of 0's in  $M$ . So we have

$$2^r B \leq Z \leq 2^n 2^r e(n)$$

Hence  $B \leq 2^n e(n)$ . Let  $k$  be one of the rows in which number of 0's is  $B$ . We can get the required deterministic circuit by hardwiring the values of the probabilistic bits used by  $C$  to  $\alpha^k$ .

**Corollary 1** *Suppose  $L \in AC^0(p)$ , where  $p$  is a prime number.  $\forall k$  there is a polynomial  $q$  (of  $n$  variables) over  $GF(p)$  of degree  $(\log n)^{o(1)}$  such that for all but at most  $\frac{2^n}{n^k}$  strings  $X \in \{0, 1\}^n$   $\chi_L(X) = q(X)$ .*

*Proof:* Let  $C_n$  be the depth 2 deterministic circuit constructed in the above proof. It has a  $Mod_p$  gate at the second level and  $\wedge$  gates at the first

level. Let  $g$  be one such  $\wedge$  gate. Let

$$\begin{aligned} t_{gi} &= 1 \text{ if neither } X_i \text{ nor } \bar{X}_i \text{ is input to } g \\ t_{gi} &= 0 \text{ if } X_i \text{ and } \bar{X}_i \text{ are both inputs to } g \\ t_{gi} &= X_i \text{ if } X_i \text{ is an input to } g \text{ but } \bar{X}_i \text{ is not} \\ t_{gi} &= 1 - X_i \text{ if } \bar{X}_i \text{ is an input to } g \text{ but } X_i \text{ is not} \end{aligned}$$

$$t_g(X) = \prod_{i=1}^n t_{gi}$$

It is easy to see that  $g(X) = 1$  if and only if  $t_g(X) = 1$ . Now let

$$r(X) = \sum_{\wedge \text{ gates } g} t_g(X)$$

Consider  $q(X) = 1 - (r(X))^{(p-1)}$ . Suppose  $C_n(X) = 1$ . This means  $r(X) = 0 \pmod p$  and hence  $q(X) = 1$  (interpreting  $q(X)$  as a polynomial over  $GF(p)$ ). Now suppose  $C_n(X) = 0$  (i.e., the number of  $\wedge$  gates outputting 1's is not a multiple of  $p$ ). Little Fermat's implies that  $(r(X))^{(p-1)} = 1 \pmod p$  and hence  $q(X) = 0$ . But  $C_n$  correctly computes  $\chi_L$  on all but  $\frac{2^n}{n^k}$  inputs and hence  $q$  also does the same.

Fan-in of each  $\wedge$  gate is at most  $(\log n)^{O(1)}$ . This means degree of  $q(X)$  is at most  $(p-1)(\log n)^{O(1)} = (\log n)^{O(1)}$  (as  $p$  is constant).

**Corollary 2**  $GF(p) \subseteq GF(p^k)$ . So we can consider  $q(X)$  to be a polynomial over  $GF(p^k)$ .

**Theorem 2** If  $L \in AC^0(p)$  then it is accepted by a family  $\{C_n\}$  of depth 4 circuits of size  $2^{(\log n)^{O(1)}}$ , where each circuit is made up of  $\wedge$ ,  $\vee$ ,  $Mod_p$ , and  $\neg$  gates ( $\neg$  gates appear only at the leaves).

*Proof:* Suppose  $L \in AC^0(p)$ . We know that  $\forall k$   $L$  is accepted by a family  $B_n$  of depth 2 probabilistic circuits (of the same form as indicated in the

statement of the theorem) of size  $2^{(\log n)^{O(1)}}$  using a polynomial number of probabilistic bits, which accepts  $L$  with error probability  $e(n) \leq \frac{1}{n^k}$ . We construct the family  $\{C_n\}$  from  $\{B_n\}$  as follows. First we choose  $k$  such that  $\frac{1}{n^k} < \frac{1}{2n^2}$ . Now let  $D_n$  be a circuit formed by taking  $\wedge$  of  $n^2$  independent copies of  $C_n$ . Let us compute the probability of error for  $D_n$ . Let  $X \in L$  and length of  $X$  is  $n$ . So  $Prob(error) = Prob(\text{at least one } C_n \text{ outputs } 0) < \frac{n^2}{2n^2} = \frac{1}{2}$ . Now suppose  $X$  does not belong to  $L$ . In this case  $Prob(error) = Prob(\text{all of the } C'_n \text{ output } 1) < (\frac{1}{2})^{n^2} < \frac{1}{2n^2}$ .

Now construct a circuit  $F_n$  by taking  $\vee$  of  $n$  independent copies of  $D_n$ . Suppose  $X \in L$ .  $Prob(F_n(X) = 0) = Prob(\text{all } D'_n \text{ output zero}) < \frac{1}{2^n}$ . Next consider  $X$  not in  $L$ .  $Prob(F_n(X) = 1) = Prob(\text{at least one } D_n \text{ outputs } 1) < \frac{n}{2n^2} < \frac{1}{2^n}$  for large enough  $n$ . So error probability  $e(n)$  for  $F_n$  is  $< \frac{1}{2^n}$ .

Now from the proof of the previous theorem we know that there exists an assignment to the probabilistic bits used by  $F_n$ , such that the number of 0's in that row  $< 2^n \frac{1}{2^n} = 1$ . So if we hardwire this assignment to the probabilistic bits, we will get the required depth 4 deterministic circuit.

**Remark:** The theorem we just proves shows that any constant depth of *polynomial*-size circuits (of AND, OR, and MOD $p$  gates, for  $p$  prime) is equivalent to a depth 4 family of size  $2^{\log^{O(1)} n}$ , thus showing that, in this setting, depth reduction can be achieved with a slight penalty in terms of size. The same proof shows that any constant-depth family of circuits (of the same type of gates) of size  $2^{(\log n)^{O(1)}}$  can be reduced to a depth 4 family of circuits also of size  $2^{(\log n)^{O(1)}}$ .