Lecture No. 10

Date:02-20-95
Scribe: Ramkrishna Chatterjee

We start by showing how to compute $Mod_{p^a}(a > 0)$ using Mod_p gates. For this we need the following fact from number theory.

Fact 1 *$Y = 0 \bmod p^a$ if and only if*

$$Y = 0 \bmod p$$

$$\binom{Y}{p} = 0 \bmod p$$

$$\binom{Y}{p^2} = 0 \bmod p$$

$$\cdots$$

$$\binom{Y}{p^{a-1}} = 0 \bmod p$$

Let X be the given input bit string and $\bar{X} = \sum X_i$. It is easy to see that $\binom{\bar{X}}{p^j} \bmod p = \left(\sum_{S \subseteq \{1,2,\ldots,n\}\ and\ |S|=p^j} \wedge_{k \in S} X_k\right) \bmod p$. Let C_j be the circuit which computes $\binom{\bar{X}}{p^j} \bmod p$ using the above formula. So $\wedge_{0 \le j \le a-1} C_j$ computes $\bar{X} \bmod p^a$.

Let $m = \prod_{j=1}^{r} p_j^{a_j}$, where p_j is prime. It is easy to see that $X = 0 \bmod m$ if and only if $\forall 1 \le j \le r\ X = 0 \bmod p_j^{a_j}$. Let B_j be the circuit which computes $Mod_{p_j^{a_j}}$. Then $\wedge_j B_j$ computes Mod_m. Since we can compute $Mod_{p_j^{a_j}}$ using mod_{p_j} and $\wedge$ gates, we can compute mod_m using $mod_{p_1}, \cdots, mod_{p_r}$ and $\wedge$ gates.

Next we want to prove the following theorem.

Definition 1 $ACC = \bigcup_m AC^0(m)$.

Theorem 1 *If $L \in ACC$ then $\exists$ primes $p_1, \cdots, p_r$ such that L is accepted by a constant depth family of probabilistic circuits of size $2^{\log^{o(1)} n}$ having $mod_{p_1}, \cdots, mod_{p_r}$ gates at the top levels and $\wedge$ gates of fan-in $\log^{o(1)} n$ at level 1.*

Proof: Suppose, $L \in ACC$ then $\exists m$ such that $L \in ACC^0(m)$.This means L is accepted by a family of constant depth circuits of polynomial size and which are made up of $\wedge, \vee, \neg$ (only at the leaves) and mod_p gates. We start with such a circuit C and transform it into the required circuit using the following steps.

Step 1: Replace all $\wedge$ gates with $\vee$ and mod_p gates (as explained in Lecture 6). Replace each $\vee$ gate with depth 5 subcircuits for parity and $\wedge$'s of fan-in $\log^{o(1)} n$ with probabilistic input bits (as explained in Lecture 6).

Step 2: Level the circuit. As a result on each level we have only one kind of mod_p gate. This increases the depth of the circuit at most by constant multiplicative factor. This makes the next step possible.

Step 3: Use distributive law to change $\wedge$ of mod_p's to mod_p of $\wedge$'s.

We can simplify the circuit further by using the following lemma to be proved later.

Lemma 1 *Let f be any symmetric function. Let C be any depth-2 circuit of size $2^{\log^{o(1)} n}$ with an " f gate " at the root and mod_p gates at level one. Then C can be simulated by a depth two circuit of size $2^{\log^{o(1)} n}$ with $\wedge$ gates of fan-in $\log^{o(1)} n$ on level 1 and a symmetric gate at the root.*

By successive application of the above lemma we can reduce the circuit obtained after step 3 to an equivalent depth-2 circuit. Hence we have the following theorem.

Theorem 2 *If $L \in ACC$ then L is accepted by a probabilistic depth-2 family of circuits of size $2^{\log^{o(1)} n}$ with $\wedge$ gates of fan-in $\log^{o(1)} n$ on level 1 and a symmetric gate at the root.*

Now we continue with the proof of Lemma 1. For this we need to define Toda Polynomials.

Definition 2

$$P_2(Y) = 3Y^2 - 2Y^3$$

$$P_{2^i}(Y) = P_2\left(P_{2^{i-1}}(Y)\right) \; for \; i > 1$$

$$P_k(Y) = P_{k+1}(Y) \; if \; k \; is \; not \; a \; power \; of \; 2$$

Claim 1 $\forall m \geq 1 \; and \; \forall y \geq 0$

$$Y = 0 \bmod m \Rightarrow P_k(Y) = 0 \bmod m^k$$

$$Y = 1 \bmod m \Rightarrow P_k(Y) = 1 \bmod m^k$$

Proof: First we prove it when k is a power of 2. Let $k = 2^i$. We proceed by induction on i.

Base Case: $i = 1$

Case 1: Suppose $Y = 0 \bmod m$. This means $Y = cm$ for some constant c. So $P_2(Y) = 3c^2m^2 - 2c^3m^3 = 0 \bmod m^2$.

Case 2: Suppose $Y = cm + 1$. $\Rightarrow P_2(Y) = 3(cm+1)^2 - 2(cm+1)^3 = 3c^2m^2 + 3 + 6cm - 2c^3m^3 - 2 - 6c^2m^2 - 6cm = -3c^2m^2 - 2c^3m^3 + 1 = 1 \bmod m^2$.

Induction: Suppose the claim holds for $\forall i < t$. Let $k = 2^t$. Now $P_{2^t}(Y) = P_2\left(P_{2^{t-1}}(Y)\right)$.

Case 1: $Y = cm$. But by the inductive hypothesis $P_{2^{t-1}}(Y) = c_1 m^{2^{t-1}}$. $\Rightarrow P_2^t(Y) = 3c_1^2 m^{2^t} - 2c_1^3 m^{2^t + 2^{t-1}} = 0 \bmod m^{2^t}$.

Case 2: $Y = cm + 1$. So by inductive hypothesis $P_{2^{t-1}}(Y) = c_2 m^{2^{t-1}} + 1$. $\Rightarrow P_{2^t}(Y) = 3c_2^2 m^{2^t} + 3 + 6c_2 m^{2^{t-1}} - 2c_2^3 m^{2^t + 2^{t-1}} - 2 - 6c_2 m^{2^{t-1}} - 6c_2^2 m^{2^t} = 1 \bmod m^{2^t}$.

Now suppose k is not a power of 2. Let 2^i be the smallest power of $2 \geq k$. By definition $P_k(Y) = P_{2^i}(Y)$. The claim holds for 2^i and m^k divides m^{2^i}. Hence, the claim holds for k.