# LECTURE NOTES

#11, Feb, 1995

Jing Wu

---

In the previous lecture, we presented Toda polynomials $P_k$ having the property that

$$\begin{aligned} x \equiv 0 \pmod{m} &\implies P_k(x) \equiv 0 \pmod{m^k} \\ x \equiv 1 \pmod{m} &\implies P_k(x) \equiv 1 \pmod{m^k} \end{aligned}$$

$P_k$ has degree $2k-1$.

Let $p$ be prime, let

$$Q_k(x) = 1 - P_k(x^{p-1})$$

$Q_k$ has degree $(p-1)(2k-1) = O(k)$

$$\begin{aligned} x \equiv 0 \pmod{p} &\implies Q_k(x) \equiv 1 \pmod{p^k} \\ x \equiv 1 \pmod{p} &\implies Q_k(x) \equiv 0 \pmod{p^k} \end{aligned}$$

Thus,

$$Q_k(\sum_{i=1}^{n} x_i) \equiv Mod_p(x_1, x_2, \cdots, x_k) \pmod{p^k}$$

Now consider a circuit:

$$\begin{array}{ccccccl} & & & f & & & \leftarrow f \text{ symmetric} \\ & & \nearrow & \cdots & \nwarrow & & \\ \boxed{Mod_p} & & & & & \boxed{Mod_p} & \leftarrow r = 2^{\log^{O(1)} n}\ Mod_p \text{ gates} \\ \nearrow\nwarrow & & & \cdots & & \nearrow\nwarrow & \\ x_{11} \cdots x_{1m} & & & & & x_{r1} \cdots x_{rm} & \end{array}$$

Define $g(l) = f([l \bmod p^k])$ (where we have chosen $k$ such that $p^k > l$, and $k > \log r = \log^{O(1)} n$)

Note this circuit computes

$$
\begin{aligned}
& f(\sum_{j=1}^{r} Mod_p(x_{j1}, x_{j2}, \cdots, x_{jm})) \\
= \quad & f(\sum_{j=1}^{r} [Q_k(x_{j1} + x_{j2} + \cdots + x_{jm}) \bmod p^k]) \\
= \quad & f(\sum_{j=1}^{r} [Q_k(x_{j1} + x_{j2} + \cdots + x_{jm})] \bmod p^k) \\
= \quad & g(\sum_{j=1}^{r} [Q_k(x_{j1} + x_{j2} + \cdots + x_{jm}))
\end{aligned}
$$

This completes the proof of Lemma 1 from the preceding lecture, which thus also completes the proof of Theorem 2 from that lecture, which states that any set in ACC is accepted by a probabilistic depth-2 family of circuits of size $2^{\log^{O(1)} n}$ with small fan-in AND gates at level 1 and a symmetric gate at level 2. However, a stronger version of this theorem also holds, showing that sets in ACC have *deterministic* circuits of this type.

In the proof of Theorem 2 in the previous lecture, we replaced the circuit

$$
\begin{array}{ccccc}
 & & \wedge & & \\
 & \nearrow & \uparrow & \nwarrow & \\
x_1 \quad \cdots & & \cdots & & \cdots \quad x_n
\end{array}
$$

with a $O(1)$ depth circuit with $\oplus$ and $\wedge$ of small fan-in with $O(n)$ probilistic bits. Now we do it with $\log^{O(1)} n$ probabilistic bits with error probability $1/n^k << 1/(\text{size of circuit})$.

First, let's see that this does give us a deterministic version of Theorem 2.

Assume that $ACC \mapsto O(1)$ depth circuits with $Mod_p$'s and $\wedge$'s of $\log^{O(1)} n$ fan-in, with $\log^{O(1)} n$ probability bits(Note, this means *all* of the subcircuits that are used to replace the $\vee$ gates use the *same* probabilistic bits). $\longmapsto$

Consider a circuit $C$ where $n^l$ $\vee$ gates have been replaced by probablistic circuits having error probability $\leq 1/n^k << 1/n^l$.

$$
\begin{aligned}
& Prob[C \text{ gives the wrong answer}] \\
\leq \quad & Prob[\text{some gate gives the wrong answer}]
\end{aligned}
$$

$$\begin{aligned} &\leq \sum_i Prob[\text{Gate } \#i \text{ gives the wrong answer}] \\ &\leq n^l/n^k < 1/n^a < 1/2 \end{aligned}$$

Thus if we make a copy of the circuit for each sequence of probabilistic bits, we get a deterministic circuit accepting our original language.

$$\begin{array}{c} \boxed{\text{MAJ}} \\ \nearrow \qquad \uparrow \qquad \nwarrow \\ \underbrace{\boxed{\phantom{xx}} \ \cdots \quad \cdots \quad \cdots \ \boxed{\phantom{xx}}}_{2^{\log^{O(1)} n} \cdot 2^{\log^{O(1)} n} = 2^{\log^{O(1)} n}} \end{array}$$

Now the proof of Theorem 2 from the previous lecture can be applied to this circuit, yielding a deterministic depth 2 circuit for our ACC language.

**Conclusion** Every set $L \in ACC$ can be recognized by a depth-two (deterministic) circuit with a symmetric gate at the root, and $2^{\log^{O(1)} n}$ AND gates (with fan-in $\log^{O(1)} n$) on level 1.

The proof of the so-called "Valiant-Vazirani" lemma that is used to reduce the number of probabilistic bits is deferred to the next lecture.

There was also a discussion of some other issues in circuit complexity.

$TC^0 = \{L|L$ is accepted by constant depth $n^{O(1)}$ polynomial size majority circuits$\}$

$$NC^1 = \{L|L \text{ is accepted by } O(1) \text{ depth } n^{O(1)} \text{ size circuit of } \wedge, \vee, Mod_{m_1}, \\ \cdots, Mod_{m_j} \text{ gates, where } m_i = n^{O(1)} \text{ or } O(\log n)\ \}$$

$$ACC \subseteq TC^0 \subseteq NC^1$$

If a class similar to $ACC$ were defined, allowing $\mathrm{Mod}_m$ gates for $m$ that is allowed to depend on the input length $n$, then in fact one obtains an alternative characterization of $TC^0$. This follows from the Chinese Remainder Theorem:

**Fact** if $r \leq n^k$ and

$$\begin{aligned} r &\equiv 0 \pmod{2} \\ r &\equiv 0 \pmod{3} \\ r &\equiv 0 \pmod{5} \\ &\dots \\ r &\equiv 0 \pmod{p_j} \end{aligned}$$

such that

$$\prod_{i=1}^{j} p_j \geq n_k$$

if and only if

$$r \equiv \prod_{i=1}^{j} p_i$$

This shows how one can use $\text{Mod}_m$ gates to compute if there are exactly $r$ bits of input that are on. Using this idea, it is then simple to simulate majority gates in constant depth, using AND, OR, and $\text{MOD}_m$ gates (where $m$ is allowed to vary).

There was also a discussion of "uniform" circuit complexity. (A circuit family $\{C_n\}$ is uniform if $C_n$ can be built "easily" from $n$ in some sense. Note that of $\{C_n\}$ is any "uniform" family of circuits of polynomial size, then the family defines a set in P. The results about ACC that were presented above allow one to prove exponential lower bounds for uniform ACC circuits.