**Notes for Lectures 5 and 6**
**Shiyu Zhou**

# 1 Feburary 1, 1995

This section is related to the previous lecture.

**Lemma 1.1** *Let $C$ be a circuit such that $C = \vee_{i=1}^{r} g_i$, where the $g_i$'s are $\wedge$ gates querying disjoint sets of input variables. Suppose $C$ takes $n$ input variables. Then*

$$|Pr_{x\in\{0,1\}^n}[C(x) = \oplus(x)] - \frac{1}{2}| \leq 1/2^n.$$

**Proof:** If some input variable is not queried at all, then it is easily seen $Pr_{x\in\{0,1\}^n}[C(x) = \oplus(x)] = \frac{1}{2}$. So we may assume that the $\wedge$ gates partition the input variables.

We proceed by induction on $r$. The case where $r = 1$ is easy to verify. Assume it holds for $r-1$ and we show for $r$.

We assume $g_r$ has fan-in $m$ $(1 \leq m \leq n)$. Let $y_0 \in \{0,1\}^m$ be the string such that $g_r(y_0) = 1$. Let $\{y_0, y_1, \ldots, y_{2^m-1}\}$ be an enumeration of $\{0,1\}^m$ such that for $0 \leq i \leq 2^{m-1} - 1$, $\oplus(y_{2i}) \neq \oplus(y_{2i+1})$. We observe the following facts.

**Fact 1:**

$$Pr_{z\in\{0,1\}^{n-m}, y\in\{0,1\}^m}[C(z,y) = \oplus(zy) \mid y \notin \{y_0, y_1\}] = \frac{1}{2},$$

since $C(z, y_{2i}) = C(z, y_{2i+1}) = \vee_{l=1}^{r-1} g_l(z)$ for all $1 \leq i \leq 2^{m-1} - 1$.

**Fact 2:** $Pr_{z\in\{0,1\}^{n-m}, y\in\{0,1\}^m}[C(z,y) = \oplus(zy) \mid y = y_0] = \frac{1}{2}$.

**Fact 3:**

$$\begin{aligned} & |Pr_{z\in\{0,1\}^{n-m}, y\in\{0,1\}^m}[C(z,y) = \oplus(zy) \mid y = y_1] - \frac{1}{2}| \\ = \; & |Pr_{z\in\{0,1\}^{n-m}}[C'(z) = \oplus(z)] - \frac{1}{2}| \\ \leq \; & 1/2^{n-m}, \end{aligned}$$

where $C' = \vee_{i=1}^{r-1} g_i$, and the equality follows from the induction hypothesis.

It is then not difficult to verify that these facts complete the proof of the lemma. □

**Theorem 1.1** *If $C$ is a depth-2 circuit with bottom fan-in $t = t(n) < n/64$, where $t(n) \to \infty$ as $n \to \infty$, then*

$$Pr_{x\in\{0,1\}^n}[C(x) = \oplus(x)] \leq 1/2 + 1/2^{n/16t}.$$

**Proof:** Let $s = \lfloor n/32t \rfloor, l = \lfloor n/64t \rfloor + s$. Then

$$\frac{n-l+s}{8tl} = \frac{n - \lfloor n/64t \rfloor}{8(\lfloor n/32t \rfloor + \lfloor n/64t \rfloor)t} > \frac{n - n/64t}{8(n/32 + n/64)} = \frac{8}{3}(1 - \frac{1}{64t}),$$

which is bigger than 2.5 for sufficiently large $n$. Therefore for any constant $c$, $(\frac{n-l+s}{8tl})^s > 2^c 2^s$ for sufficiently large $n$. It is then easy to verify that

$$\log\binom{n}{l} + n - l - s \geq \log\binom{n}{l-s} + n - l + s\log 8t + c. \tag{1}$$

Observing the fact that for any set $R$ and any positive integer $a$, the number of $x \in R$ such that $K(x|y) \geq \log|R| - a$ ($K$-random) is at least $(1 - 1/2^a)|R|$, we can see that with probability at least $1 - 1/2^s$ a randomly chosen restriction $\rho \in R^l$ is $K$-random and thus satsfies the hypothesis of the Switching Lemma by (1). By exercise Problem 1, the corrsponding $C|_\rho$ can be computed by an $\vee$ of disjoint $\wedge$'s each of fan-in at most $s$. Applying Lemma 1.1, we then have

$$Pr_{x\in\{0,1\}^n,\rho\in R^l}[C|_\rho(x|_\rho) = \oplus(x|_\rho) \mid \rho \text{ is } K\text{-random}] \leq (1/2 + 1/2^l). \tag{2}$$

Now we can see that

$$\begin{aligned} Pr_{x\in\{0,1\}^n}[C(x) = \oplus(x)] &= Pr_{x\in\{0,1\}^n,\rho\in R^l}[C(x) = \oplus(x)] \\ &\leq Pr_{x\in\{0,1\}^n,\rho\in R^l}[C|_\rho(x|_\rho) = \oplus(x|_\rho) \mid \rho \text{ is } K\text{-random}] + \\ &\quad Pr_{\rho\in R^l}[\rho \text{ is not } K\text{-random}] \\ &\leq (1/2 + 1/2^l) + 1/2^s \\ &\leq 1/2 + 1/2^{n/16t}, \end{aligned}$$

where the second inequlity follows from (2). □

# 2 Feburary 6, 1995

For the following discussion, a *circuit on $n$ input variables* has boolean inputs $x_1, x_2, \ldots, x_n$, $\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n$ at the bottom level and has $\wedge, \vee$ as the only internal gates. A *family* of circuits is sequence $C_1, C_2, \ldots$ of circuits where each $C_i$ is a circuit on $i$ input variables.

For any fixed positive integer $k$, we define $AC^0_k$ to be the set of languages that are accepted by families of circuits of polynomial size and depth $k$; and we define

$$AC^0 = \bigcup_k AC^0_k.$$

For any positive integer $p$, $AC^0(p)$ is defined in the same way as that of $AC^0$ except that we allow the presence of the $mod_p$ gates in the circuits, where $mod_p$ is defined to be

$$mod_p(x_1, x_2, \ldots, x_n) = \begin{cases} 1 & \text{if } p|\sum_{i=1}^n x_i, \text{ i.e. } \sum_{i=1}^n x_i \equiv 0 \ (mod\ p) \\ 0 & \text{otherwise.} \end{cases}$$

A *probabilistic circuit* on $n$ input variables is a circuit that has additional $r(n)$ auxiliary boolean input variables (random input bits) $\vec{y} = y_1, y_2, \ldots, y_{r(n)}$ at the bottom level besides the original $n$ input variables together with their negations. $r(\cdot)$ usually depends on the function that the circuit computes. In the following discussion, $r(n)$ will be $n^{O(1)}$.

We say that a language $L$ is *accepted by a family $\mathcal{C}$ of probabilistic circuits* if for some fixed $k$, any sufficiently large $n$ and any $x \in \{0,1\}^n$, $C_n \in \mathcal{C}$ satisfies the property that

$$Pr_{\vec{y} \in \{0,1\}^{r(n)}}[C_n(x, \vec{y}) \neq \chi_L(x)] \leq n^{-k}, \tag{3}$$

where $\chi_L(x)$ is the characteristic function of $L$.

Our goal is to prove the following theorem.

**Theorem 2.1** *Suppose $p$ is a prime and $L \in AC^0(p)$. Then $L$ is accepted by a depth-2 family of probabilistic circuits with one $mod_p$ gate at the root and $2^{\log^{O(1)} n}$ $\wedge$ gates each of fan-in $\log^{O(1)} n$.*

**Proof:** Fix $n$. Let $C$ be the circuit on $n$ input variables that belongs to the family of circuits that accepts $L$. We want to construct a probabilistic circuit $C'$ on $n$ input variables out of $C$ such that it satisfies both property (3) and the requirement of the theorem.

First we apply the following two-step procedure to the circuit $C$.

**Step 1:** Replace each $\wedge$ gate with $\vee$ and $\neg$ gates using De Morgan's Laws. Then replace all the $\neg$ gates with $mod_p$ gates, observing that for any $x \in \{0,1\}$, $mod_p(x) = \bar{x}$.

**Step 2:** Replace (bottom-up) each $\vee(z_1, z_2, \ldots, z_m)$ with the following subcircuit:

For $1 \leq i \leq m$, let $B_i = z_i \wedge b_i$ where $b_i$ is an auxiliary input variable. For $1 \leq k \leq m^{p-1}$, $A_k$ is the $\wedge$ of a distinct $(p-1)$-tuple $(B_{i_1}, B_{i_2}, \ldots, B_{i_{p-1}})$ where $1 \leq i_1, i_2, \ldots, i_{p-1} \leq m$. Let $D = mod_p(A_1, A_2, \ldots, A_{m^{p-1}})$. The desired subcircuit is then defined to be the $mod_p$ of the $\wedge$ of $l \log n$ independent copies of $D$.

By examining Step 2, we observe that if there are $d$ $B_i$'s that evaluate to 1 then there are $d^{p-1}$ $A_k$'s that evaluate to 1. By Fermat's little theorem, $d^{p-1} \equiv 1 \pmod{p}$ for all $d$ that is not a multiple of $p$. Then it is not difficult to see the fact that if $\vee(z_1, z_2, \ldots, z_m) = 1$, then gate $D$ outputs 0 with probability at least $1/2$, and in the case that $\vee(z_1, z_2, \ldots, z_m) = 0$, $D$ always outputs 1. Therefore, in the former case, the final subcircuit outputs 1 with probability at least $1 - 1/n^l$ while in the latter case it outputs 0.

Note that if in Step 2 we replace $n^a$ $\vee$ gates by the corresponding subcircuits, then by choosing $l \geq k + a$, the resulting circuit gives the same answer as the original circuit with probability at least $1 - 1/n^k$.

To prove the theorem, now it suffices to show that any constant depth and polynomial size circuit $C''$ on $n$ input variables with $\wedge$ gates of fan-in $O(\log n)$ and $mod_p$ gates is equivalent to a depth-2 circuit $C'$ on $n$ input variables with one $mod_p$ gate at the root and all $\wedge$ gates of fan-in $O(\log^{O(1)} n)$. To show this equivalence, we will apply two operations Swap and Change to the circuit $C''$.

**Swap:** The Swap operation transforms the gates $G$ of the form $\wedge$ of $O(\log n)$ $mod_p$ gates to gates of the form $mod_p$ of $n^{O(\log n)}$ $\wedge$ gates each of fan-in $O(\log n)$.

Suppose for $1 \leq i \leq q = O(\log n)$ $G_i = mod_p(z_{i,1}, z_{i,2}, \ldots, z_{i,n_i})$, where each $n_i = n^{O(1)}$, and $G = \wedge_{i=1}^{q}(G_i)$. Noticing that for any nonnegative integer $a$, $1 - a^{p-1} \equiv 1 \ (mod\ p)$

iff $a \equiv 0 \ (mod\ p)$, we have

$$G = 1 \iff \wedge_{i=1}^{q}[\sum_{k=1}^{n_i} z_{i,k} \equiv 0 \ (mod\ p)] = 1$$

$$\iff 1 - \Pi_{i=1}^{q}(1 - (\sum_{k=1}^{n_i} z_{i,k})^{p-1}) \equiv 0 \ (mod\ p)$$

Note that this polynomial on Boolean inputs can be written as a sum of terms, in the form $\sum_j c_j \prod_l^{q(p-1)} z_{l,j}$, where each $c_j$ is in $\{0, \ldots, p-1\}$, since we're only interested in the value mod $p$. Since multiplication on Boolean inputs is computed by AND gates, this can thus be computed by a $mod_p$ of $n^{O(\log n)}$ $\wedge$'s each of fan-in $O(\log n)$. This provides us with the transformed gate $G$.

**Change:** The Change operation transforms the gates $G$ of the form $mod_p$ of $mod_p$'s to gates of the form $mod_p$ of $\wedge$'s.

Suppose for $1 \leq i \leq q$, $G_i = mod_p(z_{i,1}, z_{i,2}, \ldots, z_{i,n_i})$ and $G = mod_p(G_1, G_2, \ldots, G_q)$. Then $G = 1$ iff $\sum_{i=1}^{r}(\sum_{j=1}^{n_i} z_{i,j})^{p-1} \equiv 0 \ (mod\ p)$. The expansion of the sum corresponds to the transformed gate $G$ which we describe below in words:

for each $1 \leq i \leq q$, and for $1 \leq k \leq n_i^{p-1}$, let $G'_{i,k}$ be the $\wedge$ of a distinct $(p-1)$-tuple $(z_{i,j_1}, z_{i,j_2}, \ldots, z_{i,j_{p-1}})$ where $1 \leq j_1, j_2, \ldots, j_{p-1} \leq n_i$. The transformed gate is then defined to be the $mod_p$ of all the $G'_{i,k}$.

It is not difficult to verify the fact that by repeatedly applying these two operations to $C''$, we can obtain the final circuit $C'$ of the desired form. This completes the proof of the theorem. □