Computational Complexity Theory, Fall 2010 October 29

Lecture 15: Circuits

Lecturer: Kristoffer Arnsfelt Hansen Scribe: Martin Sergio Hedevang Faester

We have seen the complexity classes

$$AC^0 \subsetneq AC[m] \subseteq TC^0 \subseteq NC^1 \subseteq \cdots$$

Recall that $TC^0 = \left\{ \begin{matrix} \text{the set of languages computable by a depth } O(1) \\ \text{circuit of MAJ-gates with size } n^{O(1)} \end{matrix} \right\}$.

In the following, we will look at a more specialized definition, in terms of the precise depth.

Definition 1. $TC^0_d = \left\{ \begin{matrix} \text{the set of languages computable by a depth } d \\ \text{circuit of MAJ-gates with size } n^{O(1)} \end{matrix} \right\}$

For example as seen in Lecture 14, we found that $MOD_m \in TC^0$. By being a little careful one can now make that more precise, namely $MOD_m \in TC^0_2$.

Our next goal will be to give circuit lower bounds for TC^0_2. An important tool for this is the following "ϵ-discriminator lemma" that allows one to "remove the output gate" of the circuit, in the sense that one of the input gates to the output must have a significant correlation with the function being computed.

Lemma 2 (Discriminator lemma)**.** *Let $f, g_1, g_2, \ldots, g_m : \{0,1\}^n \to \{0,1\}$ so $f(x) = MAJ(g_1(x), g_2(x), \ldots, g_m(x))$. Lad μ be a distribution on $\{0,1\}^n$. Then there exists some $i \in \{1, 2, \ldots, m\}$ such that $\Pr[g_i(x) = 1 | f(x) = 1] - \Pr[g_i(x) = 1 | f(x) = 0] \geq \frac{1}{m}$.*

Proof.

$$\begin{cases} \sum_{i=1}^m g_i(x) \geq \frac{m}{2} & \text{if } f(x) = 1 \\ \sum_{i=1}^m g_i(x) \leq \frac{m}{2} - 1 & \text{if } f(x) = 0 \end{cases} \Rightarrow \begin{cases} E[\sum_{i=1}^m g_i(x) | f(x) = 1] \geq \frac{m}{2} \\ E[\sum_{i=1}^m g_i(x) | f(x) = 1] \leq \frac{m}{2} - 1 \end{cases}$$

So

$$\begin{aligned} 1 &\leq E[\sum_{i=1}^m g_i(x) | f(x) = 1] - E[\sum_{i=1}^m g_i(x) | f(x) = 0] \\ &= \sum_{i=1}^m (E[g_i(x) | f(x) = 1] - E[g_i(x) | f(x) = 0]) \qquad \text{(Follows by linearity of expectation)} \\ &= \sum_{i=1}^m (\Pr[g_i(x) = 1 | f(x) = 1] - \Pr[g_i(x) = 1 | f(x) = 0]) \\ &\leq m \cdot \max_{i=1}^m (\Pr[g_i(x) = 1 | f(x) = 1] - \Pr[g_i(x) = 1 | f(x) = 0]) \end{aligned}$$

Discrepancy

The technique we will look at now is called *discrepancy*: Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. Define a $2^n \times 2^n$-matrix $M(f)$ as $M(f)_{x,y} = (-1)^{f(x,y)}$.

Let $A, B \subseteq \{0,1\}^n$ describe a combinatorial rectangle $A \times B$ in $M(f)$. Also let

$$\text{disc}_{A\times B}(f) = \frac{1}{2^{2n}} \left| \sum_{\substack{x\in A \\ y\in B}} M(f)_{x,y} \right|$$

and

$$\text{disc}(f) = \max_{(A,B)} \{\text{disc}_{A\times B}(f)\}$$

Now, let $IP_2(x,y) = x \cdot y \pmod 2$ and $M = M(IP_2)$ is given by $M_{x,y} = (-1)^{IP_2(x,y)}$. So

$$\begin{aligned}
(M^T M)_{x,y} &= \sum_{z\in\{0,1\}^n} (M^T_{x,z} M_{z,y}) \\
&= \sum_{z\in\{0,1\}^n} (-1)^{x\cdot z}(-1)^{z\cdot y} \\
&= \sum_{z\in\{0,1\}^n} (-1)^{z\cdot(x+y)} \\
&= \begin{cases} 2^n, & x = y \\ 0, & x \neq y \end{cases}
\end{aligned}$$

Hence, $M^T M = 2^n I$. Thus, for all vectors v we have $\| Mv \|^2 = (Mv)^T Mv = 2^n v^T v = 2^n \| v \|^2$. □

Lemma 3.

$$disc_{A\times B}(IP_2) \leq \frac{\sqrt{|A||B|2^n}}{2^{2n}} = 2^{-\frac{3}{2}} \sqrt{|A||B|}$$

Proof. For $S \subseteq \{0,1\}^n$, let $(1_S)_x = \begin{cases} 1 & x \in S \\ 0 & x \notin S \end{cases}$.

$$|\sum_{\substack{x\in A \\ y\in B}} M(IP_2)_{x,y}| = |1_A^T M 1_B| \overset{\text{Cauchy-Schwarz}}{\leq} \| 1_A \| \| M 1_B \| \overset{\text{Previous Obervation}}{=} \| 1_A \| \, 2^{\frac{n}{2}} \, \| 1_B \| = \sqrt{|A|} 2^{\frac{n}{2}} \sqrt{|B|}$$

Dividing by 2^{2n} gives the result. □

Theorem 4. *If C is a circuit of depth 2 consisting of MAJ-gates that computes IP_2 then the size is $\Omega(2^{\frac{n}{4}})$.*

Proof. Let $C = \text{MAJ}(C_1, C_2, \ldots, C_m)$ where each $C_i(x) = 1 \Leftrightarrow \sum_{j=1}^n a_{ij}x_j + \sum_{j=1}^n b_{ij}y_j + c_i \geq l_i/2$ and $l_i = |a_{i1}| + |a_{i2}| + \cdots + |a_{in}| + |b_{i1}| + |b_{i2}| + \cdots + |b_{in}| + |c_i|$.

Thus the size (number of wires) of C is $S = m + \sum_{i=1}^m l_i$. Consider now a specific gate C_i.

For given U, define $A_U = \{x : \sum_{j=1}^n a_{ij}x_j = U\}$ and $B_U = \{y : \sum_{j=1}^n b_{ij}y_j + c_i + U \geq l/2\}$.

We now have that

$$\{(x,y) : C_i(x,y) = 1\} = \bigcup_{U=-k_i}^{k_i} A_U \times B_U$$

where $k_i = |a_{i1}| + \cdots + |a_{in}|$.

From Lindsey's lemma, it now follows

$$\begin{aligned}
&|\{(x,y) : C_i(x,y) = 1 \wedge x \cdot y = 1\}| - |\{(x,y) : C_i(x,y) = 1 \wedge x \cdot y = 0\}| \\
&\leq \sum_{U=-k_i}^{k} ||\{(x,y) : (x,y) \in A_U \times B_U \wedge x \cdot y = 1\}| - |\{(x,y) : (x,y) \in A_U \times B_U \wedge x \cdot y = 0\}|| \\
&\leq \sum_{U=-k_i}^{k} \sqrt{|A_U||B_U|2^n} \leq (2k+1)\sqrt{2^n 2^n 2^n} \\
&\leq 2(k_i+1)2^{\frac{3}{2}n}
\end{aligned}$$

Hence,

$$\begin{aligned}
\Pr[C_i(x,y) = 1 \wedge x \cdot y = 1] - \Pr[C_i(x,y) = 1 \wedge x \cdot y = 0] &\leq \frac{2(k_i+1)2^{\frac{3}{2}n}}{2^{2n}} \\
&= 2(k_i+1)2^{-\frac{n}{2}}
\end{aligned}$$

Recall the *Discriminator lemma*: $\exists i : \Pr[C_i(x,y) = 1 | x \cdot y = 1] - \Pr[C_i(x,y) = 1 | x \cdot y = 0] \geq \frac{1}{m}$.

We will now combine these two inequalties to get the conclusion.

First note that

$$\begin{aligned}
\Pr_{x,y}[x \cdot y = 0] &= \frac{2^n + (2^n - 1)2^{n-1}}{2^{2n}} \\
&= \frac{2^{n-1} + 2^{n-1}}{2^{2n}} \\
&= \frac{1}{2} + \frac{1}{2^{n+1}}
\end{aligned}$$

so also,

$$\Pr_{x,y}[x \cdot y = 1] = \frac{1}{2} - \frac{1}{2^{n+1}}$$

Before going on, let us recall the definition for conditional probability for two events E_1 and E_2:

$$\Pr[E_1 | E_2] = \frac{\Pr[E_1 \cap E_2]}{\Pr[E_2]}$$

We now get

$$\Pr[C_i(x,y) = 1 \wedge x \cdot y = 1] = \Pr[C_i(x,y) = 1 | x \cdot y = 1] \Pr_{x,y}[x \cdot y = 1] =$$

$$\Pr[C_i(x,y) = 1 | x \cdot y = 1](\frac{1}{2} - \frac{1}{2^{n+1}}) \geq \frac{1}{2} \Pr[C_i(x,y) = 1 | x \cdot y = 1] - \frac{1}{2^{n+1}}$$

and similarly

$$\Pr[C_i(x,y) = 1 \wedge x \cdot y = 0] \leq \frac{1}{2}\Pr[C_i(x,y) = 1 | x \cdot y = 0] + \frac{1}{2^{n+1}}$$

Now we combine the inequalities:

$$\begin{aligned} 2(k_i+1)2^{-\frac{n}{2}} &\geq \Pr[C_i(x,y) = 1 \wedge x \cdot y = 1] - \Pr[C_i(x,y) = 1 \wedge x \cdot y = 0] \\ &\geq (\frac{1}{2}\Pr[C_i(x,y) = 1 | x \cdot y = 1] - \frac{1}{2^{n+1}}) - (\frac{1}{2}\Pr[C_i(x,y) = 1 | x \cdot y = 0] + \frac{1}{2^{n+1}}) \\ &= \frac{1}{2}\Big(\Pr[C_i(x,y) = 1 | x \cdot y = 1] - \Pr[C_i(x,y) = 1 | x \cdot y = 0]\Big) - 2^{-n} \\ &\geq \frac{1}{2m} - 2^{-n} \end{aligned}$$

Rearranging we have

$$2(k_i+2)2^{-\frac{n}{2}} \geq 2(k_i+1+2^{-\frac{n}{2}})2^{-\frac{n}{2}} \geq \frac{1}{2m}$$

and futher

$$4(k_i+2)m \geq 2^{\frac{n}{2}}$$

Now, $S \geq m$ and $S \geq k_i$, hence

$$S^2 \geq \Omega(2^{\frac{n}{2}})$$

from which the result follows. □

Open problem 5. $NP \subseteq TC^0_3$?. In fact, even, is $NEXP \subseteq TC^0_3$?