ITCS:CCT09 : Computational Complexity Theory	Apr 27, 2009
Lecture 14	
Lecturer: Jayalal Sarma M.N.	*Scribe: Jing He*

In previous lectures we saw different approaches for proving **PARITY** $\notin$ $\mathbf{AC^0}$. Today we will introduce another type of circuit lower bounds, namely, lower bound for monotone circuits. In 1985, Razborov proved that the **CLIQUE** problem does not have polynomial-sized monotone circuits. Before this, we familiarize ourselves with some ideas related to montonicity itself. We need some definitions and notations first.

1 Monotone Circuits

Definition 1 (Monotone circuits) *A Boolean circuit (over $\{\wedge, \vee, \neg\}$) is called* monotone *if it does not contain any **NOT** gates.*

Definition 2 (Monotone Functions) *A function $f : \{0,1\}^n \to \{0,1\}$ is monotone if and only if $(\forall x \leq y) f(x) \leq f(y)$, where the "$\leq$" is performed bitwisely.*

Proposition 3 *A function $f : \{0,1\}^n \to \{0,1\}$ is* monotone *if and only if it can be computed by a monotone circuit.*

Proof Monotone functions are closed under composition. That is if for f and g are monotone, then $f(g(u_1), g(u_2), \ldots g(u_k)$ is montone too. Since $\wedge$ and $\vee$ are montone it follows that monotone circuits can compute only monotone functions.

To see the other direction : first we define a (partially) monotone circuit for the comparator function. That is given, $x, \alpha \in \{0,1\}^n$, the circuit checks if $x \geq \alpha$. If we fix α, this function is monotone in x. It is easy to construct a monotone circuit for it too.

Now let f be a montone function. Consider the Boolean Lattice with 1^n as the maximum element and 0^n as the minimum. Any path from 0^n to 1^n has a point where the function f turns from 0 to 1. There are only $p = 2^n$ vertex disjoint paths, and this defines a boundary $\alpha_1 \ldots \alpha_p$ between 1-region and 0-region. To decide the function, the circuit has to essentially check if the given input x is greater than any of these α_i's. Now the montone circuit will have an $\vee$ gate on top with exponential fan-in, followed by comparator circuits. This gives the proof. A point to note is that the size of the circuit that we described is not polynomial in the input. ■

Now we formalize the problem we will address in this lecture. Remember that an undirected graph G with n vertices can be encoded with a binary string of length $\binom{n}{2}$, each bit of which indicates whether the corresponding edge exists. We use this encoding to define the problem $\mathbf{CLIQUE_{k,n}}$. Let $G(V, E)$ be a graph on n vertices. Clearly, G can be represented by a bit string $x_1, x_2, \ldots, x_{\binom{n}{2}}$ where x_i is 1 if the i^{th} (of the $\binom{n}{2}$ possible edges).

Definition 4

$$\mathbf{CLIQUE_{k,n}} = \left\{ x = (x_1, x_2, \ldots, x_{\binom{n}{2}}) \mid \exists \textit{ a clique of size } k \textit{ in the graph defined by } x \right\}$$

A first observation is that this function is monotone. Indeed, if we add an additional edge to a graph which already has a clique of size k, that clique does not disappear !. Now, by the above argument about monotone circuits for monotone functions, there is monotone circuit of size $2^{\binom{n}{2}}$ computing this function. Indeed, a very similar arguement gives slightly better upper bound.

Proposition 5 $\mathbf{CLIQUE_{k,n}}$ *can be computed by a monotone circuit of size* $O(n^k)$.

Proof Trivial, for all subsets of size k (there are $\binom{n}{k} = O(n^k)$ of them), and for each subset cheque whether the edge is present or not. This can be done by a monotone circuit. The size of the entire circuit is still $O(n^k)$. Notice that when $k = O(n)$ this gives an n^n bound which is not polynomial sized. ■

Now we will consider lower bounds for the problem $\mathbf{CLIQUE_{k,n}}$. We will see that the above bound is tight upto a $\sqrt{k}$ factor in the exponent.

2 Lower Bounds for CLIQUE

We will show the following theorem due to Razborov (1985).

Theorem 6 *Any monotone circuit computing* $\mathbf{CLIQUE_{k,n}}$ *must have size* $n^{\Omega(\sqrt{k})}$.

Before proving the above theorem we first give an outline. First, we want to transform any circuit C computing $\mathbf{CLIQUE_{k,n}}$ into C' which makes a lot of errors when computing the same problem. Then we prove that the error made by any single gate of C' is kind of "small". So by a union bound, we can get a lower bound for the size of C', which also gives a lower bound for the size of C if they differ not too much.

To put our idea explicitly we need some notations.

Definition 7 *An encoded graph is called a* positive input *of* $\mathbf{CLIQUE_{k,n}}$ *if it is a minimal graph containing a clique of size* k*. Let* $\mathbf{PI_{n,k}}$ *denote the collection of all such graphs.*

Definition 8 *An encoded graph is called a* negative input *of* $\mathbf{CLIQUE_{k,n}}$ *if it is a maximal graph which does not contain a clique of size* k*. Let* $\mathbf{NI_{n,k}}$ *denote the collection of all such graphs.*

It is clear that $|\mathbf{PI_{n,k}}| = \binom{n}{k}$ and $|\mathbf{NI_{n,k}}| = (k-1)^n$.

Definition 9 *A* clique indicator I_X *is a boolean function on graphs of* n *vertices which outputs 1 if and only if the induced subgraph of the input graph on vertex set* X *is a clique. A* (m,l)-approximator *is a boolean function of form* $\bigvee_{i=1}^{r} I_{x_i}$ *where* $|X_i| \leq l$ *and* $r \leq m$*.*

Suppose we have a monotone circuit C computing $\mathbf{CLIQUE_{k,n}}$. We want to transform it into a (m,l)-approximator C' for some fixed m and l. We do the transformation inductively. For a single variable $x_{i,j}$, we change it into a clique indicator $I_{\{i,j\}}$. For a formula $F_1 \vee F_2$, suppose $A = \bigvee_{i=1}^{r} I_{X_i}$ and $B = \bigvee_{j=1}^{s} I_{y_j}$ are the corresponding (m,l)-approximators of F_1 and F_2, respectively. We know that $T = A \vee B = (\bigvee_{i=1}^{r} I_{X_i}) \vee (\bigvee_{j=1}^{s} I_{y_j})$, but this is a $(2m,l)$-approximator. To compress it we need the following lemma from Erdos and Rado:

First, some terminology. A *sunflower* is a collection of p sets $\{Z_1, \ldots, Z_p\}$ such that $\forall 1 \leq i \leq j \leq p, Z_i \cap Z_j = Z$, where Z is called the *center* of the sunflower. We also call it a p-petal sunflower. The choice of these names are more-or-less self explanatory.

Lemma 10 (Sunflower Lemma) *Suppose* $S = \{S_1, \ldots, S_k\}$ *is a collection of sets for which* $(\forall 1 \leq i \leq k)|S_i| \leq l$ *and* $k \geq (p-1)^l \cdot l!$*, then there exists a* p*-petal sunflower in* S*.*

We will include a proof of the Lemma later in this draft. First we see the application. Now we choose $m = (p-1)^l \cdot l!$, where the values of p and l will be decided later. If $r + s < m$, T is already a (m,l)-approximator. If $r + s \geq m$, from the sunflower lemma we know that among $S = \{X_1, \ldots, X_r\} \cup \{Y_1, \ldots, Y_s\}$ there exists a p-petal sunflower $\{Z_1, \ldots, Z_p\}$ with center Z. We use I_Z to replace $\bigvee_{i=1}^{p} I_{Z_p}$, and repeat the above process until T becomes a (m,l)-approximator T'. Notice that T' may disagree with $T = A \vee B$ on some negative inputs since we "reduce" the size of some clique indicators. But on all positive inputs they agree with each other.

We are left with the case where $T = A \wedge B$. We have

$$\begin{aligned}
A \wedge B &= (\bigvee_{i=1}^{r} I_{X_i}) \wedge (\bigvee_{j=1}^{s} I_{Y_j}) \\
&= \bigvee_{i=1}^{r} \bigvee_{j=1}^{s} (I_{X_i} \wedge I_{Y_j}) \\
&\approx \bigvee_{i=1}^{r} \bigvee_{j=1}^{s} I_{X_i \cup Y_j} \\
&\approx \bigvee_{1 \le i \le r, 1 \le j \le s, |X_i \cup Y_j| \le l} I_{X_i \cup Y_j} \\
&= T'
\end{aligned}$$

Due to the two "$\approx$", T' may disagree with T on some negative inputs. Now T' is a (m^2, l)-approximator and we can apply the sunflower lemma again to transform it into a (m, l)-approximator, while losing some positive inputs.

By induction, we can finally get a (m, l)-approximator C' from the original circuit C. We use $size(C)$ to denote the size of a circuit C.

Claim 11 *For the C' described above, either C' outputs 0 on all positive inputs, or C' outputs 1 on $(1 - \binom{l}{2}/(k-1))(k-1)^n$ negative inputs.*

Claim 12 *C' disagree with C on at most $size(C) \cdot m^2 \binom{n-l-1}{k-l-1}$ positive inputs.*

Claim 13 *C' disagree with C on at most $size(C) \cdot m^2 \left(\binom{l}{2}/(k-1)\right)^p (k-1)^n$ negative inputs.*

If they are all correct, we have

$$size(C) \ge \frac{\binom{n}{k}}{m^2 \binom{n-l-1}{k-l-1}}$$

or

$$size(C) \ge \frac{\left(1 - \frac{\binom{l}{2}}{k-1}\right)(k-1)^n}{m^2 \left(\frac{\binom{l}{2}}{k-1}\right)^p (k-1)^n}$$

Choose $l = \lfloor \sqrt{k} \rfloor$, $p = \lceil \sqrt{k} \log n \rceil$ and $m = (p-1)^l \cdot l!$, then after some calculations we get $size(C) \ge n^{\Omega(\sqrt{k})}$.

Now we prove the three claims.

Proof of Claim 10 If C' is identical to 0 then it outputs 0 on all positive inputs. If not, C' must contain at least one clique indicator, say, I_{X_1}. Then we have

$$\begin{aligned}
& \mathbf{Prob}_{x\in\mathbf{NI_{n,k}}}[C'(x)=1] \\
\geq\ & \mathbf{Prob}_{x\in\mathbf{NI_{n,k}}}[I_{X_1}(x)=1] \\
=\ & 1-\mathbf{Prob}_{x\in\mathbf{NI_{n,k}}}[I_{X_1}(x)=0] \\
\geq\ & 1-\frac{\binom{l}{2}}{k-1}
\end{aligned}$$

So the claim follows. ■

Proof of Claim 11 Remember that C' disagrees with C on negative inputs only because of the transformation for the form $A \wedge B$, where $I_{X_i} \wedge I_{Y_j}$ is replaced with $I_{X_i \cup Y_j}$. In one transformation there are at most m^2 such terms, each of which makes at most $\binom{n-l-1}{k-l-1}$ errors on negative inputs. So the total error is upper-bounded by $size(C) \cdot m^2\binom{n-l-1}{k-l-1}$. ■

Proof of Claim 12 When we deal with the form $A \vee B$, we replace $\bigvee_{i=1}^{p} I_{Z_i}$ by their center Z. So the probability of one such replacement making errors on negative inputs is

$$\begin{aligned}
& \mathbf{Prob}_{x\in\mathbf{NI_{n,k}}}[I_Z(x)=1 \wedge (\forall 1\leq i\leq p) I_{Z_i}(x)=0] \\
\leq\ & \mathbf{Prob}_{x\in\mathbf{NI_{n,k}}}[\bigwedge_{i=1}^{p} I_{Z_i}(x)=0 \mid I_Z(x)=1] \\
=\ & \prod_{i=1}^{p} \mathbf{Prob}_{x\in\mathbf{NI_{n,k}}}[I_{Z_i}(x)=0 \mid I_Z(x)=1] \\
\leq\ & \prod_{i=1}^{p} \mathbf{Prob}_{x\in\mathbf{NI_{n,k}}}[I_{Z_i}(x)=0] \\
\leq\ & \left(\frac{\binom{l}{2}}{k-1}\right)^p
\end{aligned}$$

and at most m^2 such replacements suffices. So at each $\vee$-gate at most $m^2\left(\frac{\binom{l}{2}}{k-1}\right)^p (k-1)^n$ errors are made by C'.

When dealing with the form $A \wedge B$, we can apply a similar argument which also yields an upper-bound of $m^2\left(\frac{\binom{l}{2}}{k-1}\right)^p (k-1)^n$ for errors on negative inputs. So the total errors on negative inputs made by C' is at most $size(C) \cdot m^2 \left(\frac{\binom{l}{2}}{k-1}\right)^p (k-1)^n$. ■

Proof of Sunflower Lemma

For completeness we include the proof of Sunflower Lemma which is crucial in the above construction. We restate the lemma first.

Lemma 14 (Sunflower Lemma) *Suppose $\mathcal{S} = \{S_1, \ldots, S_k\}$ is a collection of subsets of $[n]$ such that $(\forall 1 \leq i \leq k)|S_i| \leq \ell$ and $k \geq (p-1)^\ell \cdot \ell!$, then there exists a p-petal sunflower in S. That is there exists $Z_1, \ldots Z_p \subseteq \mathcal{S}$ such that $Z_i \cap Z_j = Z$ for all i and j.*

Proof The proof is by induction on ℓ. The base case $\ell = 1$ is trivial since we can define $Z = \phi$, and have disjoint p-petals. As for the induction, pick the maximum number of disjoint subsets from S, say $Z_1, Z_2, \ldots Z_r$. If $r \geq p$ then we are done, since in this case Z could just be chosen to be the empty set. If $r < p$, define, $U = \bigcup_{i=1}^r Z_i$. By maximality, every set that was not chosen from S must intersect Z and the size of Z is at most $r\ell \leq (p-1)\ell$. Hence, by an averaging argument, there exists a $x \in Z$ such that it is contained in at least $(p-1)^\ell.(\ell-1)!$ sets of $\mathcal{S}$. Consider this collection of sets and remove x from them. The size of each set is now at most $(\ell-1)$. By induction, there is a p-petal sunflower in this set system. Adding the element x back to each of these sets (that is to their intersection Z) gives you a p-petal sunflower for the original system S. This completes the proof. ■