18.405J/6.841J Advanced Complexity Theory	March 30, 2000
Lecture 15	
Lecturer: Dan Spielman	*Scribe: Dan Adkins*

1 Proof of Razoborov's Theorem (cont.)

We continue to prove Razborov's Theorem, which was stated in the last lecture:

Theorem 1 (Razborov's Theorem) *Any monotone circuit that computes $CLIQUE_{\log n}$ must have $n^{\Omega(\log n)}$ gates.*

In the last lecture we found that every monotone circuit has a set of *minterms* and *maxterms*. We want to accept all minterms and rejects all maxterms so we define

$$\begin{aligned} C &= \{k\text{-cliques}\} = \textit{minterms} \\ D &= \{(k-1)\text{-colored graphs with edges between different colors.}\} \\ \vee\vee \end{aligned}$$

Then for a function f, define

$$\#_C f = |f^{-1}(1) \cap C| \qquad \text{and} \qquad \#_D f = |f^{-1}(1) \cap D|.$$

We proceed to prove that clean functions don't approximate $CLIQUE_k$, where k can be as low as $\operatorname{lglg} n$. This is a stronger result than we need, but that's ok.

Recall that a clean function is an OR of at most n clique indicators of size less than k. Note that in the trivial case, a clique indicator of size 0 always accepts.

Lemma 2 *For a clean function f, either*

$$\#_D f = |D| \text{ or } \#_C f \leq \frac{|C|}{2}.$$

Proof If there is an indicator of size 0, then f=1, in which case $\#_D(f) = |D|$. Otherwise, all clique indicators must have size at least 2. How many k-cliques can a clique indicator accept? At least 2 points belong to the indicator, so any k-clique consists of $k-2$ additional points from the remaining $n-2$ points. Thus, a clique indicator can accept at most at most $\binom{n-2}{k-2}$ cliques. There are only n clique indicators, therefore a clean function accepts at most $\binom{n-2}{k-2} n$ k-cliques.

$$\frac{\binom{n-2}{k-2} n}{\binom{n}{k}} \approx \frac{k^2 n}{n^2} < \frac{1}{2} \text{ for } k = \operatorname{lglg} n.$$

■

1.1 Gardening Operations

Now we show that approximate-OR ($\sqcup$) and approximate-AND ($\sqcap$) don't lose too many minterms or maxterms as measured by $\#_C$ and $\#_D$. Recall that $\sqcup$ and $\sqcap$ were defined in terms of the operations: Cover, Trim, and Weed. We will bound the effects of each of these on $\#_C$ and $\#_D$.

Cover: Given clean functions

$$f = \mathrm{OR}_i\, ind(S_i) \qquad \text{and} \qquad g = \mathrm{OR}_j\, ind(T_j)$$

$$\begin{aligned} f \wedge g &= \mathrm{OR}_{i,j}\, ind(S_i) \wedge ind(T_j) \\ cover(f \wedge g) &= \mathrm{OR}_{i,j}\, ind(S_i \cup T_j). \end{aligned}$$

Claim 3

$$\begin{aligned} \#_C cover(f \wedge g) &= \#_C(f \wedge g) \\ \#_D cover(f \wedge g) &\leq \#_D(f \wedge g). \end{aligned}$$

Proof

C: If a clique contains vertices in S_i and T_j, then it contains all edges between them.

D: Making an AND more restrictive won't cause it to accept more.

■

Trim: Given f, an OR of m clique indicators, Trim(f) is an OR of those clique indicators of size less than k (i.e. remove those of size at least k).

Claim 4

$$\begin{aligned} \#_C trim(f) &\geq \#_C(f) - m \\ \#_D trim(f) &= \#_D(f). \end{aligned}$$

Proof

C: Each clique indicator of size at least k can accept only 1 element of C, so we lost at most m k-cliques.

D: Cliques indicators of size k or more don't accept elements of D.

■

Weed: Recall that Weed consists of plucking many times. To pluck, we take petals $ind(S_1), \ldots, ind(S_p)$ such that

$$\forall i, j \qquad S_i \cap S_j = \bigcap_k S_k = Z \text{ (the core).}$$

Then, we replace $ind(S_1), \ldots, ind(S_p)$ with $ind(Z)$. This is so called because we "pluck" the petals and replace them with the core. It should be apparent that we don't remove any minterms by this process. So,

$$\#_C(weed(f)) \geq \#_C(f).$$

For f and g clean functions,

$$\begin{aligned} f \sqcup g &= weed(f \vee g) \\ f \sqcap g &= weed(trim(cover(f \wedge g))). \end{aligned}$$

Now we combine all of the individual bounds. First we look at $\#_C(f \sqcup g)$. Approximate-OR is defined directly in terms of Weed, so we immediately get that

$$\#_C(f \sqcup g) = \#_C(weed(f \vee g) \geq \#_C(f \vee g).$$

Next we look at $\#_C(f \sqcap g)$.

$$\begin{aligned} \#_C(f \sqcap g) &= weed(trim(cover(f \wedge g))) \\ &\geq trim(cover(f \wedge g)) \end{aligned}$$

The Cover operation doesn't affect the number of minterms of $f \wedge g$. The Trim operation decreases the number of minterms by m, where m is the number of clique indicators OR'ed together. If we recall that

$$cover(f \wedge g) = \mathrm{OR}_{i,j}\, ind(S_i \cup T_j),$$

then we can see that Trim gets an OR over at most n^2 clique indicators. Therefore,

$$\#_C(f \sqcap g) \geq \#_C(f \wedge g) - m \geq \#_C(f \wedge g) - n^2.$$

To summarize our knowledge so far,

$$\begin{aligned} \#_C(f \sqcup g) &\geq \#_C(f \vee g) \\ \#_C(f \sqcap g) &\geq \#_C(f \wedge g) - n^2 \\ \#_D(trim(cover(f \wedge g))) &\leq \#_D(f \wedge g). \end{aligned}$$

Lemma 5 *For f, an* OR *of clique indicators of size less than k,*

$$(*) \qquad \Pr_{G \in D}[(pluck(f)(g) = 1) \wedge (f(g) = 0)] < n^{-\lg n}.$$

Proof

$$
\begin{aligned}
(*) &= \Pr_{G\in D}[(ind(z)(G)=1) \wedge (\forall j ind(S_j)(g)=0)] \\
&= \Pr_{G\in D}[(\text{all nodes in } Z \text{ get different colors}) \wedge (\forall j \exists \text{ nodes in } S_j \text{ with the same color})] \\
&\le \prod_{G\in D} \Pr[\forall j \exists \text{ nodes in } S_j \text{ with the same color} | (\text{all nodes in } Z \text{ have different colors})] \\
&= \prod_{j} \Pr[\exists \text{ nodes in } S_J \text{ of the same color} | Z \text{ gets different colors}] \\
&\le \prod_{j=1}^{p} \Pr[\exists \text{ nodes in } S_j \text{ of the same color}] \qquad (**)
\end{aligned}
$$

$$
\begin{aligned}
&\Pr[\text{There exist 2 nodes in } S_j \text{ of the same color}] \\
&\quad = 1 - \Pr[\text{All nodes in } S_j \text{ get different colors}] \\
&\quad = 1 - \frac{\binom{k-1}{|S_j|}|S_j|!}{(k-1)^{|S_j|}} \\
&\quad \le 1 - \frac{(k-1)!}{(k-1)^{k-1}} \\
&\quad \le 1 - \frac{1}{e^{k-1}}
\end{aligned}
$$

We take the product of this polynomial over p sets S_j, showing finally that

$$(**) \le \left(1 - \frac{1}{e^{k-1}}\right)^p \le e^{-\lg^2 n} \le n^{-\lg n}.$$

■

So far, we've proven the following equalities and inequalities.

$$
\begin{aligned}
f \sqcap g &= weed(trim(cover(f \wedge g))) \\
\#_D(f \sqcup g) &\le \#_D(f \vee g) + n|D|n^{-\lg n} \\
\#_D(f \sqcap g) &\le \#_D(f \wedge g) + n^2|D|n^{-\lg n}
\end{aligned}
$$

Theorem 6 *Let H be a monotone circuit with g gates. Let H' be derived by replacing OR ($\vee$) with approximate-OR ($\sqcup$) and AND ($\wedge$) with approximate-AND ($\sqcap$). Then,*

$$
\begin{aligned}
\#_C(H') &\ge \#_C(H) - gn^2, \\
\#_D(H') &\le \#_D(H) + gn^2|D|n^{-\lg n},
\end{aligned}
$$

and H' is clean.

Proof We know either $\#_C(H') \le |C|/2$ or $\#_D(H') = |D|$. Note that we need to assume that

$$g \ge \frac{\binom{n}{\lg\lg n}}{2n^2}.$$

Then we know that either

$$\begin{aligned}\#_C(H) &\le \frac{|C|}{2} + gn^2 \qquad \text{or}\\ \#_D(H) &\ge |D| - gn^2|D|n^{-\lg n}\\ &= |D|(1 - gn^{-\lg n + 2}).\end{aligned}$$

For $CLIQUE_k$, $\#C = |C| = \binom{n}{k} \approx n^{\lg\lg n}$ and $\#D = 0$. ■