18.405J/6.841J Advanced Complexity Theory	April 2, 1998
Lecture 14	
Lecturer: Daniel A. Spielman	*Scribe: Yu Sui*

Circuit Lower Bounds

Quick review on last lecture

Definition 1 *Let $CLIQUE_k$ be the function on n-nodes graphs that outputs 1 if and only if the input graph has a k-clique.*

CLIQUE_k funtions are monotone functions.

Definition 2 *A* **Clean function** *is an OR of at most n clique indicators of size $< k$.*

Definition 3 *A* **sunflower** *is a collection of sets $S_1, S_2, ..., S_m$ such that*

$$\forall i \neq j, S_i \cap S_j = \bigcap_i S_i$$

We call $\bigcap_i S_i$ the "core" of the sunflower, and each S_j is called a "petal".

Theorem 4 (Sunflower theorem) *Let C be a collection of sets of size $\leq l$, and $|C| > (p-1)^l l!$, then C contains at least one sunflower with p petals.*

Theorem 5 (Razborov) *Any monotone circuit that computes $CLIQUE_{\log n}$ has at least n^{logn} gates.*

Theorem 6 (Alon-Boppana) $Size(CLIQUE_{n^{\frac{2}{3}}}) > 2^{\frac{n^{\frac{1}{3}}}{\log n}}$

Razborov's Theorem roughly states that no family of small monotone circuits exists for an NP-complete problem. The approach to prove is the following: Let's say that the problem is the $k-clique$ problem for a graph on n nodes. The method is to approximate with a *clean* function a circuit that is said to decide instances of the *clique* of particular size.

The inputs to the circuit are certainly clean functions (trivially, they are $\vee$ of one clique indicator of size 2). We proceed to approximate the whole circuit with a clean function by replacing every $\vee/\wedge$ gate in the circuit with an Approx-OR/Approx-AND gate, which is defined as following:

Definition 7 *For clean functions f and g:*

$$Approx-OR(f,g) = Weed(f \vee g)$$
$$Approx-AND(f,g) = Weed(Trim(Cover(f \wedge g)))$$

Where Weed = Repeated application of Pluck
Pluck = Find a sunflower among the sets/clique indicators, delete petals of the sunflower and replace with the clique indicator corresponding to the core.
Cover = Replace each minterm with the clique indicator for the nodes touching edges in the minterm.
Trim = Discard all clique indicators of size $\geq k$.

Proof continued

Define:
C = minterms = graphs with exactly one k-clique
D= complete colored graphs with $\leq k-1$ colors(i.e., each node gets a color and there are altogether $\leq k-1$ colors, and there is edge between all pairs of nodes of different colors.)

For a function a:

$$\#_C(a) = |a^{-1}(1) \cap C|$$
$$\#_D(a) = |a^{-1}(1) \cap D|$$

Where $\#_C(a)$ is the number of members of C that are accepted by a
$\#_D(a)$ is the number of members of D that are accepted by a

Let a be a monotone function, we have:

Lemma 8
a) $\#_D(Cover(a)) \leq \#_D(a)$
b) $\#_C(Cover(a)) = \#_C(a)$

Proof :
a) In Cover operation, we make the AND more restrictive–it can not accept a graph that was not accepted previously.
b) Let T be the set of edges examined by the clique indicator, and let S be the set of nodes touching these edges.
Cover(AND) accepts if every edge between nodes in S is there. Thus if AND accepts a clique, all the edges are there, and Cover(AND) accepts
■

Let a be an OR of i clique detectors, we have:

Lemma 9
a) $\#_D(Trim(a)) \leq \#_D(a)$
b) $\#_C(Trim(a)) \geq \#_C(a) - i$

Proof :
a) The Trim operation removes inputs to the OR, and so cannot make more graphs accepted
b) Each removal of a clique detector of size $\geq k$ can only cause one element of C to be rejected.
■

Lemma 10
a) $\#_C(Pluck(a)) \geq \#_C(a)$
b) $\#_D(Pluck(a)) \leq \#_D(a) + |D| * n^{-logn}$

Proof :
(a) If a graph G in C is accepted by a petal, then it is also accepted by the core. The pluck operation removes the clique indicators corresponding to the petals of the sunflower, and adds the

indicator corresponding to the core. Thus it doesn't decrease the number of graphs accepted.

(b) Let's say that the sunflower being plucked has petals $Z_1 ..., Z_i, .. Z_p$, and core Z. We consider the probability that a graph in D is accepted by $pluck(a)$ but not by a. The only way a does not accept a graph with a clique on the vertices in the core of the sunflower is if in each petal of the sunflower there are at least 2 nodes of the same color. For $pluck(a)$ to accept the graph, the core must have all different colors. The probability that both of there events happens is:

$$\begin{aligned} & \Pr[pluck(a)(G) = 1, \text{ while } a(G) = 0] && (1) \\ = \; & \Pr[(\text{all nodes in } Z \text{ have different colors}) \wedge \\ & \forall_j, (\exists \text{ two nodes of same color in } Z_j)] && (2) \\ \leq \; & \Pr[\forall_j, (\exists \text{two nodes of same color in } Z_j) | \text{all nodes in } Z \text{ have different colors}] && (3) \\ = \; & \prod_{i=1}^{p} \Pr[\exists \text{two nodes at same color in } Z_j | \text{all nodes in } Z \text{ have different colors}] && (4) \\ \leq \; & \prod_{i=1}^{p} \Pr[\exists \text{two nodes at same color in } Z_j]. && (5) \end{aligned}$$

Since

$$\Pr[\exists \text{ two nodes at same color in } Z_j] = 1 - \Pr[\text{all nodes are colored differently in } Z_j],$$

$$\Pr[\text{all nodes in } Z_j \text{ are colored differently }] > \frac{(k-1)!}{(k-1)^{k-1}} > \frac{1}{e^{k-1}},$$

Thus

$$\Pr[\exists \text{two nodes at same color in } Z_j] < 1 - \frac{1}{e^{k-1}}$$

$$\Rightarrow \quad \prod_{i=1}^{p} \Pr[\exists \text{two nodes at same color in } Z_j] < (1 - \frac{1}{e^{k-1}})^p$$

In our setting, $p = ln^3 n$, $k = lnlnn$,

$$\prod_{i=1}^{p} \Pr[\exists \text{ two nodes at same color in } Z_j] < e^{-ln^2 n} = n^{-lnn}$$

(2) $\leq$ (3) follows from the definition of conditional probability. (4) = (3) holds by the virtue of the fact that all petals are independent, since if the 2 nodes have the same color (if there are such nodes at all), then they must lie outside the core (or all the petals will have them). The $\leq$ relation of (4) to (5) holds since the events (Z_i has 2 nodes of same color) and (Z has all distinct colors) are negatively correlated (i.e., the more likely one event, the less likely the other). ■