Last Class

- Monotone Circuits
- Lower Bound for Clique

$CLIQUE_{n,k} = \{G \mid G$ has n vertices & includes a k-clique$\}$

Positive case:

Graph with only a k-clique. $\# = \binom{n}{k}$

Negative case:

$(k-1)$-colorable graphs with all edges between different colors

- Approximation method

Find an (m, l)-approximator of the output of each gate inductively.

Building process:

For OR gate $\vee$ (A, B)

$A = \vee I_{X_i}$ $B = \vee I_{Y_j}$ (m,l)-approximator

① $A \vee B = (\vee I_{X_i}) \vee (\cancel{I_{Y_j}} \vee I_{X_j})$ $(2m, l)$-approximator

② Use Sunflower lemma to pluck the petals

$I_{Z_1} \vee \cdots \vee I_{Z_p} \to I_Z$ (Z is the kernel of sunflower)

For AND gate $\wedge$ (A, B)

① $A \wedge B = \bigvee_{i,j} (I_{X_i} \wedge I_{Y_j})$

② Replace $I_{X_i} \wedge I_{Y_j}$ by $I_{X_i \cup Y_j}$,

② drop it if $|X_i \cup Y_j| > l$, get (m^2, l)-approximator

③ Pluck the petals.

Lemma: Either the final approximator C' is wrong on all positive cases, or it is wrong on at least $\left(1 - \frac{1}{k-1}\binom{l}{2}\right)$ frac of neg cases.

(Pick $l = \sqrt{k}$, wrong probability $\gtrsim \frac{1}{2}$)

Now need to show C' is close to C.

Let C' be the final (m, ℓ)- approximator produced by these operations

Each gate makes few errors on positive tests.

Lemma: # of positive cases on which C' is wrong is at most
$\text{size}(C)\, m^2 \binom{n-\ell-1}{k-\ell-1}$

Pf: Let's focus on errors introduced by approximating an OR gate.

Case 1: $\vee$ with children A, B. $A = \bigvee I_{X_i}$ $B = \bigvee I_{Y_j}$

① If we don't do plucking, everything is fine.

② Plucking also doesn't hurt positive case since we replace some I_{X_i}. I_{Y_j} by the core I_Z which will only accept more graphs.

Case 2: $\wedge$ with children A, B. $A = \bigvee I_{X_i}$ $B = \bigvee I_{Y_j}$

First step: $\bigvee (I_{X_i} \wedge I_{Y_j}) \Rightarrow \bigvee I_{X_i \cup Y_j}$

This is exact on our specific positive case (graph with only a dig

Second step: drop $I_{X_i \cup Y_j}$ where $|X_i \cup Y_j| > \ell$

The number of positive cases we drop is at most $\binom{n-(\ell+1)}{k-(\ell+1)}$

Third step: plucking.

So we only miss on Case 2, Second step. Each dropping will miss at most $\binom{n-(\ell+1)}{k-(\ell+1)}$ positive cases, we'll drop at most m^2 terms in one gate. and there are $\text{size}(C)$ gates.

Lemma: The fraction of negative test cases C' fails on is at most $\text{size}(C)\, m^2 \left(\frac{\binom{\ell}{2}}{k-1}\right)^p$.

Pf: Case 1: $\begin{array}{c} \vee \\ A \quad B \end{array}$ $\quad A = \vee I_{X_i} \quad B = \vee I_{Y_j}$

① No plucking. we are exact

② Plucking: $I_{Z_1}, \ldots, I_{Z_p} \Rightarrow I_Z$ (Z is the core of $Z_1, \ldots, Z_p$)

$$\Pr_{G \text{ neg case}}\left[I_Z(G) = 1 \wedge I_{Z_i}(G) = 0 \;\; \forall i = 1, 2, \ldots, p \right]$$

$$\leq \Pr_G\left[\bigwedge_{i=1}^{p} (I_{Z_i}(G) = 0) \;\middle|\; I_Z(G) = 1 \right]$$

$$= \prod_{i=1}^{p} \Pr_G\left[I_{Z_i}(G) = 0 \mid I_Z(G) = 1 \right] \quad (Z_1/Z,\ Z_2/Z,\ \ldots,\ Z_p/Z \text{ are disjoint})$$

$$\leq \prod_{i=1}^{p} \Pr_G\left[I_{Z_i}(G) = 0 \right] \leq \left(\frac{\binom{\ell}{2}}{k-1}\right)^p$$

Case 2 $\begin{array}{c} \wedge \\ A \quad B \end{array}$

Step 1: ~~exact~~

Step 2: doesn't hurt for negative cases

Step 3: Similar to Case 1 ②.

So the fraction is $\left(\frac{\binom{\ell}{2}}{k-1}\right)^p$, we'll do at ~~least~~ most m^2 plucking in each gate. and there are size(C) gates.

Choosing parameters: $\ell = \sqrt{k}$, $\frac{\binom{\ell}{2}}{k-1} = \frac{1}{2}$.

$p = \sqrt{k} \log n$. $\ell = \sqrt{k}$ $\quad m \leq p^\ell \ell! \leq (k \log n)^\ell$

We have $\text{size}(C) \geq \frac{2^{p-1}}{m^2}$ or $\text{size}(C) \geq \frac{\binom{n}{k}}{\binom{n-\ell+1}{k-\ell-1}} \cdot \frac{1}{m^2}$

Both gives $\text{size}(C) \geq n^{\Omega(\sqrt{k})}$

Natural proofs (Razborov – Rudich '93)

$\{f_n\}$ be family of functions

Example: $f_n = Maj_n$ or $\oplus_n$, How can we prove $f_n \notin AC^0$?

C_n = some property of $(\{0,1\}^n \to \{0,1\})$

Def: $F_n = \{f : \{0,1\}^n \to \{0,1\}\}$ $C_n \subseteq F_n$ is a natural property

if $\exists\, C_n^* \subseteq C_n$, s.t.

(constructivity) $f_n \in C_n^*$? can be solved in $2^{O(n)}$ time. (f_n is expressed as truth table)

(largeness) $|C_n^*| \geq \frac{|F_n|}{2^{O(n)}}$

A property C_n is useful against a circuit class $\mathcal{C}$ if

for ~~any~~ every sequence of functions $\{g_1, \cdots, g_n$ computed by circuits in class $\mathcal{C}$

$g_n \notin C_n$ infinitely often

A lower bound against some circuit class, say NC^1 (→ or $SIZE(n^2)$, $P/poly$) is a natural proof

if it contains, more or less explicitly, a property $\{C_n\}$ that is natural

and useful against NC^1.

~~Two~~ Examples (against $P/poly$)

① $C_n = \{f \mid C(f) \geq n^{\omega(1)}\}$

- Useful against $P/poly$, large
- But not known to be constructive

② $C_n = \{f \mid f = 3SAT\}$

- Constructive (Brute force check if $\varphi \in 3SAT$ for all φ)
- Not large (only 1 function)
- Useful if $3SAT \notin P/poly$

③ $\oplus \notin AC^0$ (switching Lemma)

$C_n = \{f \mid f$ is not constant after restriction any sets of $n - n^{\varepsilon}$ inputs$\}$

- Large (easy counting)
- Constructive (in depth-3 AC^0)
- Useful (by Switching Lemma)

④ $\oplus \notin AC^0$ (Smolensky's Proof)

Also <u>natural</u> (It is constructive for some $C_n^* \subseteq C_n\}$ and large)

Lower bound via formal complexity measures

e.g. Formula lower bound

$\mu(f)$ = some nature numbers

$\mu : F_n \to \mathbb{N}$ $\quad \mu(f \wedge g) \leq \mu(f) + \mu(g)$

$\mu(x_i) = 1$ $\quad \mu(f \vee g) \leq \mu(f) + \mu(g)$

$\mu(\overline{x_i}) = 1$

$C_n = \{f \mid \mu^*(f) \geq n^{\omega(1)}\}$

- Useful against NC^1
- Always large

Lemma: If $\exists f \in F_n$ s.t. $\mu^*(f) \geq S$, then $\mu^*(f \oplus g) \geq \frac{S}{4}$ for at least $\frac{|F_n|}{4}$ functions