

Last Class

- Monotone Circuits
- Lower bound for Clique

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

Positive case:

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

Negative case:

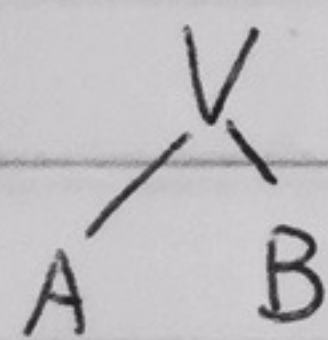
$(k-1)$ -colorable graphs with ^{all} edges between different colors

- Approximation method

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

Building process:

For OR gate



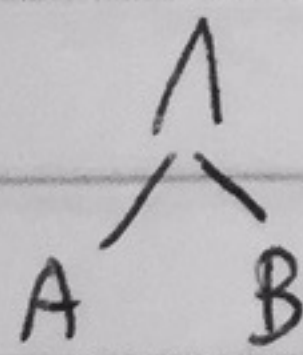
$A = V I_{x_i}$ $B = V I_{x_j}$ (m, ℓ) -approximator

① $A \vee B = (V I_{x_i}) \vee (V I_{x_j})$ $(2m, \ell)$ -approximator

② Use Sunflower lemma to pluck the petals

$I_{x_1} \vee \dots \vee I_{x_p} \rightarrow I_Z$ (Z is the kernel of sunflower)

For AND gate



① $A \wedge B = V (I_{x_i} \wedge I_{x_j})$

② Replace $I_{x_i} \wedge I_{x_j}$ by $I_{x_i} \wedge I_{x_j}$

③ drop it if $|x_i \wedge x_j| > \ell$, get (m^2, ℓ) -approximator

④ Pluck the petals.

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

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

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: $A = \vee I_{x_i}$ $B = \vee I_{y_j}$

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: $A = \wedge I_{x_i}$ $B = \wedge I_{y_j}$

First step: $\vee(I_{x_i} \wedge I_{y_j}) \Rightarrow \vee I_{x_i \cup y_j}$

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

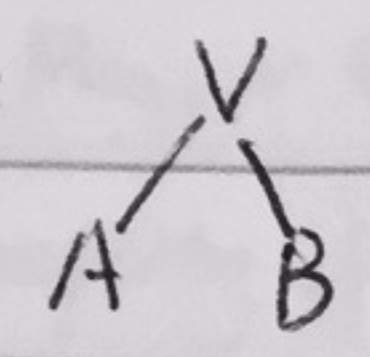
Second step: drop $I_{x_i \cup y_j}$ where $|x_i \cup y_j| > \ell$

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

Pf: Case 1:  $A = \bigvee I_{x_i}$ $B = \bigvee I_{y_j}$

① No plucking. we are exact

② Plucking: $I_{z_1}, \dots, I_{z_p} \Rightarrow I_Z$ (Z is the core of $z_1, \dots, z_p$)

$$\Pr [I_Z(G) = 1 \wedge I_{z_i}(G) = 0 \forall i=1, 2, \dots, p]$$

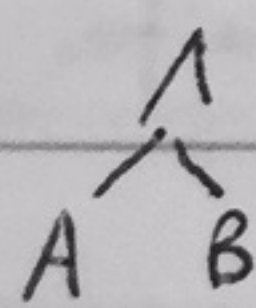
G neg case

$$\leq \Pr_G \left[\bigwedge_{i=1}^p (I_{z_i}(G) = 0) \mid I_Z(G) = 1 \right]$$

$$= \prod_{i=1}^p \Pr_G [I_{z_i}(G) = 0 \mid I_Z(G) = 1] \quad (z_1/Z, z_2/Z, \dots, z_p/Z \text{ are disjoint})$$

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

Case 2



Step 1: ~~exact~~

Step 2: doesn't hurt for negative cases

Step 3: Similar to Case 1 ②.

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

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

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

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

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

Natural proofs (Razborov - Rudich '93)

$\{f_n\}$ be family of functions

Example: $f_n = \text{Maj}_n$ or $\oplus_n$, How can we prove $f_n \notin AC^0$?

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

Def: $F_n = \{f: \{0,1\}^n \rightarrow \{0,1\}\}$ $C_n \subseteq F_n$ 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 every sequence of functions $f_1, \dots, f_n$ computed by circuits in class $\mathcal{C}$,
 $f_n \notin C_n$ infinitely often

A lower bound against some circuit class, say NC^1 is a natural proof
if it contains, more or less explicitly, a property $\{C_n\}$ that is natural
and useful against NC^1 .
→ or $\text{SIZE}(n^2)$, P/poly

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

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

– Useful against P/poly, large

– But not known to be constructive

② $C_n = \{f \mid f = \exists \text{SAT}\}$

– Constructive (Brute force check if $\varphi \in \exists \text{SAT}$ for all φ)

– Not large (only 1 function)

– Useful if $\exists \text{SAT} \notin \text{P/poly}$

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

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

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

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

Also natural (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 natural numbers

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

$$\mu(x_i) = 1$$

$$\mu(f \vee g) \leq \mu(f) + \mu(g)$$

$$\mu(\bar{x}_i) = 1$$

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

- Useful against NC^1
- Always large

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