Recap from last lecture.

We want to prove an exponential lower bound for clique-coloring.

th 1: CP proof Π $\Rightarrow$ monotone real circuit of size $\leq |\Pi| \cdot n$

proof: last lecture.

th 2: Every monotone real circuit for clique-coloring has size $2^{n^{\Omega(1)}}$.

proof sketch: approximate function computed by each gate.

assume: have a class of functions $\mathcal{C}$ s.t.

- → inputs are in the class ($x_i \in \mathcal{C}$)
- → if a gate has inputs f, g with error $e(f)$, $e(g)$, then error of gate is $e(f) + e(g) + \varepsilon$.
- → output far from $\mathcal{C}$ (any $f \in \mathcal{C}$ has large error Δ with respect to fn that circuit computes).

then need $\geqslant \Delta / \varepsilon$ gates.

Recall how to measure error of $\tilde{F}$ wrt F:

x is 0-error if ~~[illegible]~~ circuit$(x) = 0$ ~~[illegible]~~ and $\tilde{F}(x) > F(x)$.

1-error if circuit$(x) = 1$ and $\tilde{F}(x) < F(x)$.

Not a problem if circuit$(x) = 0$ and $\tilde{F}(x) < F(x)$: it only helps.

We are even more lenient and only count "extreme" inputs.

x is 0-error if x is complete $m-1$-partite graph and $\tilde{F}(x) > F(x)$.

x is 1-error if x is m-clique and $\tilde{F}(x) < F(x)$.

Observe if we change an edge then answer changes; intuitively these are inputs that are hard to compute.

Today: define class $\mathcal{C}$

prove lemmas.

We begin by defining auxilliary tool: "closed" functions.

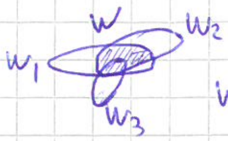
These are <u>not</u> functions in our circuit.

Fix $m = \frac{1}{8}(n/\log n)^{2/3}$, $\ell = m^{1/2}$, $r = 4m^{1/2} \cdot \log n$

def (implied set). $W_1, \ldots, W_r, W$ subsets of V, of size $\leq \ell$.

$W_1 \ldots W_r \vdash W$ if $W_i \cap W_j \subseteq W$.

Note W_i's may repeat,



$W_1, W_2, W_3 \vdash W$

def (closed functions). $\mathcal{F}_{\ell,r}$

$f: \{\text{subsets of } V \text{ of size} \leq \ell\} \to \mathbb{R}$ closed if f monotone and

$W_1 \ldots W_r \vdash W \Rightarrow f(W) \geq \min_i f(W_i)$.

What are some closed functions?

→ $|\cdot|$ is not closed: $f(\{1,2\}) = 2$; $f(\{1,3\}) = 2$.

$\{1,2\} \cap \{1,3\} \subseteq \{1\}$. but $f(\{1\}) = 1$.

→ $\mathbb{I}_U := \begin{cases} 1 & \text{if } W = U \\ 0 & \text{o/w} \end{cases}$ (indicator function) is not closed: not monotone.

→ $\mathbb{J}_U := \begin{cases} 1 & \text{if } W \supseteq U \\ 0 & \text{o/w} \end{cases}$ is closed. monotone OK.

Assume $W_1 \ldots W_r \vdash W$. if $W_i \not\supseteq U$ for some i, ~~$f(W) \geq 0$ ok~~.

$f(W) \geq 0 = f(W_i)$ OK. if $W_i \supseteq U$ for all i,

then $W \supseteq U$: $f(W) = 1 = f(W_i)$.

def. For any f, the closure of f is f^*, the minimal closed function st $f \leq f^*$.

def. W is f-minimal if $f(U) < f(W)$ $\forall U \subsetneq W$.

We will need the following lemma:

lem 3. f closed. #minimal sets of size $\leq k$ is $\leq (k+1)(r-1)^k$.

Proof. Induction on r.

$\underline{r=2}$ | suppose $> k+1$ minimal sets of size $\leq k$. then at least 2 sets are incomparable (neither contained in the other). why? longest inclusion chain has size $k+1$.

for the sake of contradiction

consider $U = W_1 \cap W_2$. $W_1, W_2 \vdash U$, so by def $f(U) \geq f(W_1)$ or $f(U) \geq f(W_2)$.

but this contradicts W_1 and W_2 minimal.

$\underline{r>2}$ | let D be f-minimal s.t. $f(D)$ is maximum.

define $f_C : \{\text{subsets of } V \setminus D \text{ of size } \leq \ell - |C|\} \to \mathbb{R}$

$$W \mapsto f(W \cup C).$$

claim: f_C closed.

claim: W minimal for f, then $W \setminus D$ minimal for f_C, $C = W \cap D$.

thus $\#f\text{-minimal sets} \leq \sum_{C \subset D} f_C\text{-minimal sets} \underset{IH}{\leq}$

$$\leq \sum_{i=0}^{k} \binom{k}{i} (k-i+1)(r-2)^{k-i} \leq (k+1) \sum \sim \underset{(1+x)^n}{=} (k+1)(r-1)^k$$

//.

Now we can finally define our class of approximating functions $\mathcal{C}$.

def Let $f : \{\text{subsets of } V \text{ of size } \leq \ell\} \to \mathbb{R}$. Then

$$\langle f \rangle : \{0,1\}^{\binom{V}{2}} \longrightarrow \mathbb{R}$$

$$G \longmapsto \max\left(f(W) : W \text{ clique of } G \text{ of size } \leq \ell\right).$$

* abusing notation to identify G with set of edges (V is fixed).

$\mathcal{C} := \{\langle f \rangle : f \text{ closed}\}$

Back to examples.

$\langle 1\!\!1 \rangle$ = size of max clique of G (capped at ℓ).

$\langle \delta 1_U \rangle$ = 1 if U is a clique of G; 0 o/w.

In fact, if U is an edge, then $\langle \delta 1_U \rangle$ just says whether G contains the edge. This proves our first point: the functions "input variable" are in $\mathcal{C}$.

But wait, is $\langle f \rangle$ even well-defined? What if G has no clique?
Then G is the empty graph. Just define $\langle f \rangle (G) = f(\emptyset)$.

We can now define what does it mean to approximate a circuit.
Formally, we build a new circuit by induction on gates.
Inputs are fine, as we just argued.
Assume we want to approximate a gate g, with inputs F_1, F_2, and $\tilde{F}_1 = \langle f_1 \rangle$, $\tilde{F}_2 = \langle f_2 \rangle$ are approximations of F_1, F_2.
Then $\tilde{F} = \langle g(f_1, f_2)^* \rangle$ is the approximation of $F = g(F_1, F_2)$.
$*$ if g is unary, then $g(f_1)$ is already closed so in fact no error comes from unary gates.

The next step is to compute the error introduced by binary gates.
First we estimate the 0-error; then the 1-error. But before that, let us see how to build a closure (i.e. f^*).

Assume f is not closed. Then there are $W_1 \ldots W_r \vdash W$ s.t.
$f(W) < \min f(W_i)$. Pick $W_1 \ldots W_r$ such that $\min f(W_i)$ is maximal.
For each $U \supseteq W$, replace $f(U)$ by $\max(f(U), \min f(W_i))$.
claim: each W updated at most once. in fact, each $U \supseteq W$ updated at most once.

$* \binom{n}{\leq \ell} = \sum_{i=0}^{\ell} \binom{n}{i}$

obs at most $\binom{n}{\leq \ell} \leq n^\ell$ updates.

We will use this to prove the following lemma:

lem 4 The 0-error of $\langle f^* \rangle$ wrt $\langle f \rangle$ is at most a $n^\ell \cdot \left(\frac{\ell^2}{2(m-1)} \right)^r$ - fraction of all complete $m-1$-partite graphs.

proof. More convenient to write as probability. i.e.

$$\Pr_{\substack{B \text{ uniform} \\ \text{compl. } m\text{-}1\text{-partite}}} \left[\langle f^* \rangle (B) > \langle f \rangle (B) \right] \leq n^{\ell} \left(\frac{\ell^2}{2(m-1)} \right)^r$$

Enough to show that $\Pr\left[\langle f \rangle \text{ increases on a replacement step}\right] \leq \left(\frac{\ell^2}{2(m-1)}\right)^r$.

then do union bound: $\Pr[E_1 \vee E_2 \vee \dots E_{n^\ell}] \leq \sum \Pr[E_i]$.

When does $\langle f \rangle (B)$ increase? $(W_1 \dots W_r \vdash W)$.

→ $\langle f \rangle (B)$ depends on W $\Rightarrow$ W is a clique in B

→ $\langle f \rangle (B)$ does not depend on W_i (otherwise increase would not affect it)

$\Rightarrow$ W_i is not a clique in B.

We can apply the following lemma:

lem 5. Let $W_1 \dots W_r \vdash W$. then

$$\Pr_{\substack{B \text{ uniform} \\ \text{compl. } m\text{-}1\text{-partite}}} \left[W_1 \text{ not a clique and } \dots \text{ and } W_r \text{ not a clique and } W \text{ clique} \right] \leq \left(\frac{\ell^2}{2(m-1)} \right)^r$$

//.

proof of Lemma 5: probability exercise.

We finished estimating the 0-error. Now let us estimate the 1-error.

Lem 6 Let $\langle f_1\rangle, \langle f_2\rangle \in \mathcal{C}$, g monotone.
The 1-error of $\langle g(f_1,f_2)^*\rangle$ wrt $\langle g(f_1,f_2)\rangle$ is at most a $4(\ell+1)\cdot 2^{-\ell}$-fraction of all m-cliques.

proof Let Z be a clique s.t. $\langle g(f_1,f_2)^*\rangle(Z) < \langle g(f_1,f_2)\rangle(Z)$.
By def of $\langle f_1\rangle$, $\langle f_1\rangle(Z) = f_1(W_1)$ for some clique $\underset{\text{of size } \le \ell}{W_1}$ of Z.
Pick W_1 minimal. Same for f_2 and W_2.

Fix a clique W of Z of size $\le \ell$.

$$g(f_1(W), f_2(W)) \underset{\substack{f \le f^* \\ g \text{ monotone}}}{\le} \big(g(f_1(W), f_2(W))\big)^* \underset{\text{def. } \langle\rangle}{\le} \langle g(f_1,f_2)^*\rangle(Z) \underset{\text{hypothesis}}{<}$$

$$< \langle g(f_1,f_2)\rangle(Z) \underset{\text{def. } W_1, W_2.}{=} g(f_1(W_1), f_2(W_2))$$

What if we take $W = W_1 \cup W_2$? get $g(f_1(W_1\cup W_2), f_2(W_1\cup W_2)) < g(f_1(W_1), f_2(W_2))$
but f_1, f_2, g monotone. is this a contradiction?
only if $f_1(W_1\cup W_2)$, $f_2(W_1\cup W_2)$ are defined. We need $|W_1 \cup W_2| > \ell$.
So either $|W_1| > \ell/2$ or $|W_2| > \ell/2$.

We proved Z 1-error clique $\Rightarrow$ Z contains a f_1-minimal set of size $> \ell/2$ or a f_2-minimal set of size $> \ell/2$. By Lemma 3, only $2(k+1)(r-1)^k$ such minimal sets of size k. Every set can be completed to $\binom{n-k}{m-k}$ cliques. Total is at most

$$\sum_{\ell/2 < k \le \ell} 2(k+1)(r-1)^k \binom{n-k}{m-k} \le 2(\ell+1) \sum (r-1)^k \left(\frac{m}{n}\right)^k \binom{n}{m} \underset{(r\frac{m}{n}) \le 1/4}{\le}$$

$$\le 4(\ell+1)\, 4^{-\ell/2} \cdot \binom{n}{m}$$

//

This finished estimating the error. We know that every gate introduced a small error. It only remains to prove that our new circuit makes a large error. How? Our circuit computes a closed function, enough to show that all closed functions make a large error.

lemma 7. Let $\langle f\rangle \in \mathcal{C}$. Either $\langle f\rangle(G) \geq 1$ $\forall G$ or

$\langle f\rangle(Z) < 1$ in a $\geq \frac{2}{9}$ - fraction of cliques.

proof. Assume $\langle f\rangle(G) < 1$ for some G. then $f(\emptyset) < 1$.

Let Z be a clique st $\langle f\rangle(Z) \geq 1$. since $f(\emptyset) < 1$,

Z contains an f-minimal set.

Argue as in lemma 6 (few minimal sets by Lemma 1 + complete).

Total is at most

$$\sum_{1\leq k\leq \ell} (k+1)(r-1)^k \binom{n-k}{m-k} \leq \binom{n}{m} \sum_{1\leq k\leq \ell} \frac{k+1}{4^k} \leq \binom{n}{m} \sum_{1\leq k} \frac{k+1}{4^k} = \binom{n}{m} \cdot \frac{7}{9}.$$

//

We have all the ingredients to prove th 2. Just put pieces together.

proof (of th 2).

Let F be the function computed by the approximated circuit.

By construction $F \in \mathcal{C}$.

Large 0-error (in 1-fraction of m-l-bipartite inputs)

Case 1: $F \geq 1$. Use lemma 4 to show many gates.

Case 2: by lemma 7, large 1-error (in 2/9 - fraction of m-clique inputs)

Use lemma 6 to show many gates.

See calculations in previous lecture. //.