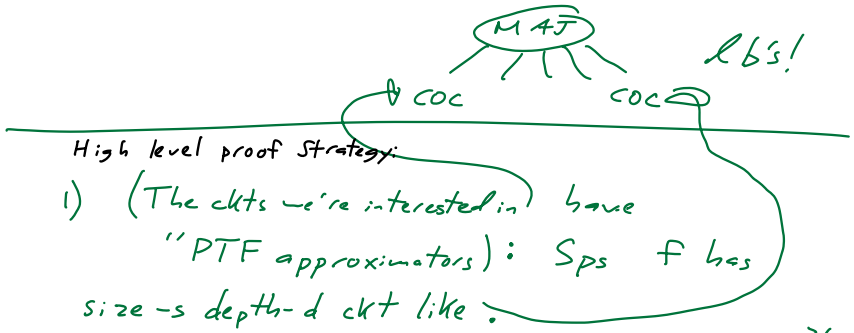
Last time: work on 2✓ + 3 (mostly done) of our proof plan to learn MAJ-of CDC:



Today: • finish 1), put together pieces to prove:

> Thm [ABFR94]: Let C be any size-s depth-d ckt for PAR of form:
>
> MAJ
> COC ... COC of ∧/∨,¬.
>
> Then $s \geq 2^{\Omega(n^{\frac{1}{4d}})}$.

- your choice! — formula l.b.
  - tiny snippet on interactive proofs
  - end early

Reminder: final is out, due Fri

Questions?

Recall we just proved:

> **Key Lemma:** Fix some $\varepsilon > 0$.
> Let $x_1, \dots, x_t$ be 0/1 variables.
> Let $\mathcal{D}$ be any dist. over $\{0,1\}^t$.
> There is a poly $a(x_1, \dots, x_t)$, of degree $O((\log \frac{1}{\varepsilon}) \cdot \log t)$ (+ with integer coeffs)
> s.t.
> $$\Pr_{x \sim \mathcal{D}}\left[a(x) = \overbrace{(x_1 \vee \dots \vee x_t)}^{0/1}\right] \geq 1 - \varepsilon$$

Most of the work was in showing: 0/1 value!

$$\circledast \quad \forall x \in \{0,1\}^t, \quad \Pr_a\left[a(x) = (x_1 \vee \dots \vee x_t)\right] \geq 1 - \varepsilon$$

This implies:

$$\forall \mathcal{D} \ \exists a \quad \Pr_{x \sim \mathcal{D}}\left[a(x) = (x_1 \vee \dots \vee x_t)\right] \geq 1 - \varepsilon. \qquad (**)$$

($\mathcal{D}$: over $x \in \{0,1\}^t$)

Analogy for why (*) → (**):

$x \leftrightarrow$ student

$a \leftrightarrow$ question on exam

"$a(x) = (x_1 \vee \dots \vee x_t)$" $\leftrightarrow$ x gets a right on exam

$1-\varepsilon \leftrightarrow 90\%$

(*): every student gets $\geq 90\%$ on exam.

(**): for every dist. over students, there's some exam question s.t. Pr[student drawn from the dist. gets that question right] $\geq 90\%$

Why? If (**) false: for some dist $\mathcal{D}^*$ over students, for every exam q_1, $< 90\%$ under $\mathcal{D}^*$ students were right.

This means overall class avg $< 90\%$ on whole exam.

But every student got $\geq 90\%$.

Corollary: Let $\varepsilon > 0$. Let $f: \{0,1\}^n \to \{0,1\}$ be computed by $\wedge/\vee/\neg$ ckt of size s, depth d.

Then there is a poly $b(x_1, \dots, x_n)$ of degree $O((\log(1/\varepsilon) \cdot \log s))^d$ (+ with integer coeffs) s.t. $b(x) = f(x)$ for $\geq (1-\varepsilon)2^n$ inputs in $\{0,1\}^n$.

$b(x) \neq f(x)$ for $\leq \varepsilon \cdot 2^n$ inputs

Pf: [First, note prev. lemma true for AND (+ NOT); sim. pf, or $(x \wedge y \wedge z) = \neg(\bar{x} \vee \bar{y} \vee \bar{z})$ $\neg x \equiv 1 - x$]

some nonunif dist. over $\{0,1\}^4$ induced by

Imagine unif dist on $(x_1, \ldots, x_n) \in \{0,1\}^n$;

consider, for each fanin-t gate, resulting dist over $\{0,1\}^t$

Each gate's fanin t is $\leq s$; so by prev lemma, for ℓ there is some deg-$O((\log(s/\varepsilon) \cdot \log s)$ poly for the gate which computes the 0/1 value of the gate correctly w.p. $\geq 1 - \varepsilon/s$ (when $x \sim \{0,1\}^n$ uniform random).

Replace each gate by its polynomial: composition is a poly $b(x)$ of degree $O((\log(s/\varepsilon) \cdot \log s))^d$ (w/ integer coeff) s.t. $b(x) = f(x)$ w.p. $\geq 1 - \varepsilon$ for $x \sim \{0,1\}^n$. ∎

Easy to add MAJ gate at root, + get Part 1 from above:

Cor (Part 1): Let $\varepsilon > 0$. Let f ($\{-1,1\}$ valued) be computed by $\wedge/\vee/\neg$ ckt of size s & depth d with MAJ on top.
There is a poly p, of deg $O\left(\log\left(\frac{s^2}{\varepsilon}\right)\cdot\log s\right)^d$ which i) never outputs 0 on $\{0,1\}^n$, &
ii) is s.t. $\operatorname{sign}(p(x)) \neq f(x)$ for $\leq \varepsilon \cdot 2^n$ pts in $\{0,1\}^n$.

Pf: Sps MAJ has r inputs. ($r \leq s$.) (assume r odd w.l.o.g.)
For subckt C_i, use prev cor. to get poly p_i of deg $O\left(\log\left(\frac{sr}{\varepsilon}\right)\cdot\log s\right)^d \leq O\left(\log\left(\frac{s^2}{\varepsilon}\right)\cdot\log s\right)^d$ that's right on C_i (right 0/1 value) on all but $\leq \left(\frac{\varepsilon}{r}\right)\cdot 2^n$ inputs.
Then

$$\operatorname{sign}\left(\sum_{i=1}^{r} p_i - \frac{r}{2}\right)$$

does the job. ∎

Put pieces together:

Let $f = PAR$.

Sps f is computed by a size-s, depth-d ckt w/ MAJ on top.

Let $\varepsilon = \frac{1}{10}$.

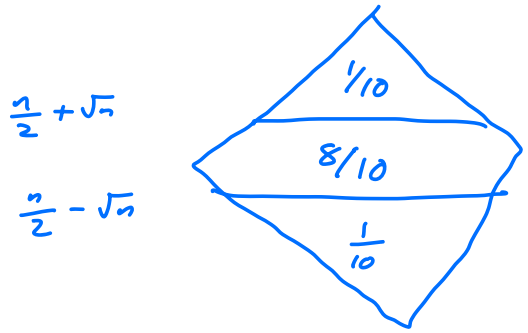
Let p = poly from last corollary (Part 1).

Know $\deg(p) \le O(\log(10s^2) \cdot \log s)^d$

$= O(\log s)^{2d} := \ell$, &

$\text{sign}(p) \neq f$ on $\le \frac{1}{10} \cdot 2^n$ inputs.

Fact: $\frac{1}{10} \cdot 2^n < \sum_{i=0}^{k} \binom{n}{i}$ for $k = \frac{n}{2} - \sqrt{n}$.



$\ell + 2k$ lemma, applied to p:

f has a weak PTF of deg $\le \ell + 2k$

$= O(\log s)^{2d} + 2(\frac{n}{2} - \sqrt{n})$.

(PAR!)

By part 3, know $n \le$. I.e.

$n \le O(\log s)^{2d} + n - 2\sqrt{n}$

$\sqrt{n} \le O(\log s)^{2d}$

$n^{\frac{1}{4d}} \leq O(\log s)$ so

$$2^{\Omega(n^{\frac{1}{4d}})} \leq s .$$

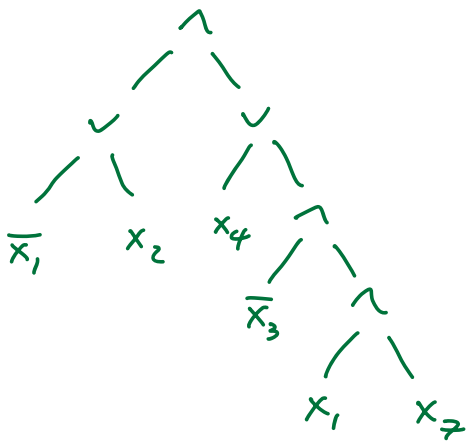
"Fun" fact: $MAJ = \text{sign}(x_1 + \ldots + x_n)$

Weighted MAJ: $\text{sign}(a_1 x_1 + \ldots + a_n x_n)$

$a_i \in \mathbb{Z}$

Q: Is all of NEXP computable by

poly size, depth 2 ?



(size 6 formula ↓ # input literals)

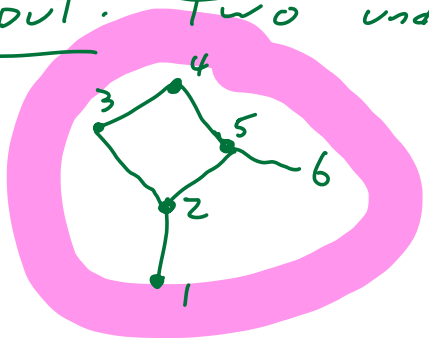
IP ....

— traditional proofs: • static object.
• verification algorithm

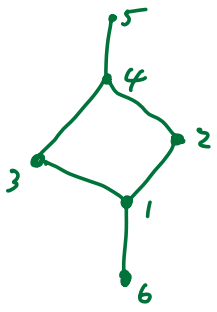
— NP: proofs, proofs, proofs.

Graph Isomorphism

Input: two undir. labeled graphs



G_1



G_2

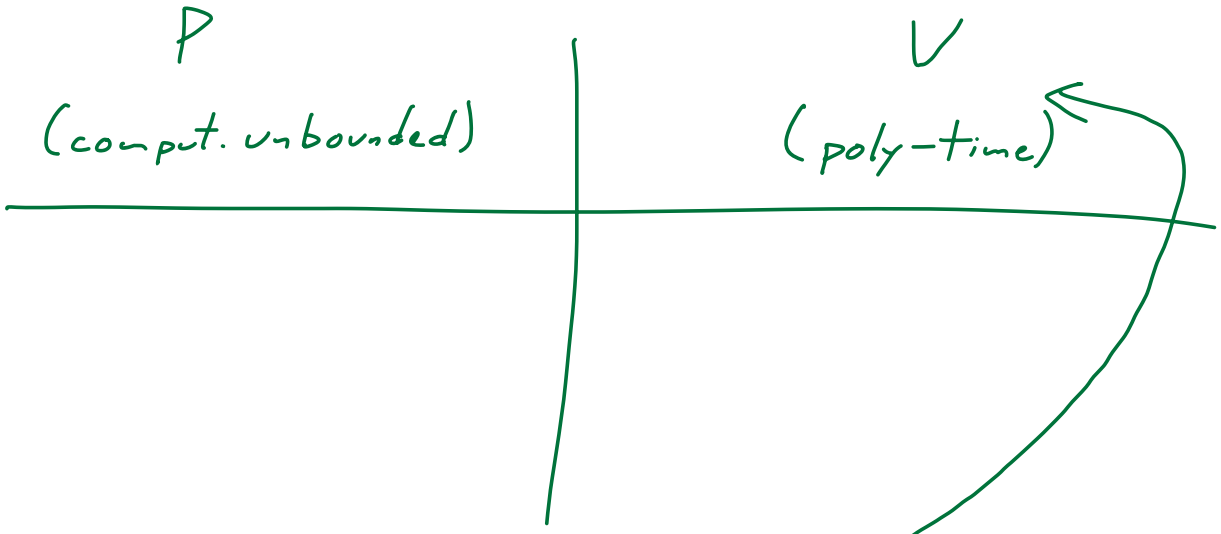
Q: Isomorphic? ($\exists$ bij. from $V_1 \to V_2$ perfectly preserving edges?)

GISO is in NP. ✓ ∃ cert.

G NONISOMORPHISM:
Y iff G_1, G_2 <u>not</u> isomorphic.

GNISO in NP? Not at all clear...
don't know how to give eff <u>static</u> cert.

But... easy to interactively prove $G_1 \not\cong G_2$ are nonisomorphic.



For P to convince that G_1 <u>not</u> iso. to G_2, they can repeat following:

- $ picks G_1 or G_2 (unseen by P). Randomly permute labels, get G; give G to prover.
- P: tells us whether G came from G_1 or G_2.

If $G_1 \not\cong G_2$ not isom: P can be right every time.

If $G_1 \cong G_2$ are isom: P passes each round w.p. $\frac{1}{2}$, hence passes all 1000 rounds only w.p. 2^{-1000}.

In fact, $IP = PSPACE$.
