Last time: • apply HSL to get $2^{n^{\frac{1}{d-1}}}$ l.b. for PAR

• start proof that  ckts

need size $2^{\Omega(n^{\frac{1}{4d}})}$ for PAR:

- PTFs, weak PTFs
- WeakPTFdeg(PAR) = n
- 3-step plan:  lb's!

High level proof strategy:

1) (The ckts we're interested in) have "PTF approximators": Sps f has size-s depth-d ckt like . Then there's a "low-deg" poly p ($\deg \approx (\log s)^{2d}$) that's "almost" a PTF for f:

$\text{sign}(p(x)) \neq f(x)$ only for a few x's.

2) (PTF approx. $\Rightarrow$ weak PTF) If f is a Bool fn + p is an "almost PTF" for f, we can modify p to get new poly $q(x)$ which is a weak PTF for f, where $\deg(q)$ only a bit larger than $\deg(p)$.

3) PAR has weak deg n. ☺ Did this!

Today: work on 2), then 1).

Questions?

First lemma for (2):

<u>Lemma:</u> Let $S \subset \{0,1\}^n$ satisfy $|S| < \sum_{i=0}^{k} \binom{n}{i}$.
Then there is a (multilin) poly $c(x_1,\dots,x_n)$ of deg $\leq 2k$ s.t.
$c(x) \not\equiv 0$; $c(x) \geq 0$; $c(x) = 0$ for every $x \in S$.

<u>Pf:</u> Every deg-k multilin. poly. over $x_1,\dots,x_n$ has $\leq \sum_{i=0}^{k} \binom{n}{i}$ coeffs.

On any given input, value of the poly = some lin comb. of its coeffs.

$$\left(\begin{array}{ll} p(x) = & c_\emptyset + c_1 x_1 + c_2 x_2 + c_{1,2} x_1 x_2 + \cdots \\ x_1 = 3,\ x_2 = 7: & c_\emptyset + 3c_1 + 7c_2 + 21 c_{1,2} + \cdots \end{array} \right)$$

Let $r(x_1,\dots,x_n)$ be deg-k poly.
The constraints "$r(x) = 0 \ \forall x \in S$" is a coll. of $|S|$ many homog. lin. eq.'s in $\sum_{i=0}^{k} \binom{n}{i}$ "variables" (coeffs of r).

Know $|S| < \sum_{i=0}^{k} \binom{n}{i}$, so # vars > # eq, + hence there's a nontrivial solution (not all-0) to this linear system. Sol gives coeffs of a poly $r(x)$ s.t. $r(x) \not\equiv 0$ + $r(x) = 0 \ \forall x \in S$.

Take $c(x) = r(x)^2$. ∎

Part (2) from above:

Lemma ("$\ell + 2k$ lemma"):

Let $f : \{0,1\}^n \to \{-1,1\}$.

Let $p(x_1, \dots, x_n)$ be a degree-ℓ poly s.t. $p(x) \neq 0 \ \forall x \in \{0,1\}^n$.

Let $S \subset \{0,1\}^n$, $S = \{\text{inputs } x \text{ s.t. } \mathrm{sign}(p(x)) \neq f(x)\}$.

If $|S| < \sum_{i=0}^{k} \binom{n}{i}$, then $\mathrm{WeakPTFdeg}(f) \leq \ell + 2k$.

Pf: Consider poly $p(x) \cdot c(x)$ where $c =$ poly from prev. lemma.

$$\left(\begin{array}{l} c(x) = 0 \ \forall x \in S \\ c(x) \geq 0 \\ c(x) \not\equiv 0 \end{array} \right) \qquad \deg(c) \leq 2k$$

$\deg(p \cdot c) \leq \ell + 2k$. It's a weak PTF for f:

- $c(x) \neq 0$ some $x \in \{0,1\}^n$, so for that x, $p(x)c(x) \neq 0$ $\quad (p(x) \neq 0 \ \forall x \in \{0,1\}^n)$ ✓
- $\forall x$: either $p(x)c(x) = 0$ (b/c $c(x) = 0$) or $p(x)c(x) \neq 0$. If $p(x)c(x) \neq 0$, means $c(x) \neq 0$, so $c(x) > 0$, so $x \notin S$, so $\mathrm{sign}(p(x)c(x)) = \mathrm{sign}(p(x)) = f(x)$

∎

Key to part 3: handling (in suitable sense) just one gate:

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.

$$\Pr_{x \sim \mathcal{D}} \left[a(x) = \overbrace{\underline{(x_1 \vee \dots \vee x_t)}}^{0/1} \right] \geq 1 - \varepsilon$$

Pf: Let $V_0 = \{x_1, \dots, x_t\}$ be init. set of vars.
For $i = 1, \dots, 1 + \log_2(t)$, let $V_i \subseteq V_{i-1}$ be obt. by removing each elt w.p. $\frac{1}{2}$. (random sets)
Let $p_0, p_1, \dots, p_{1+\log t}$ be

$$p_i(x) = \sum_{x_j \in V_i} x_j .$$

Each p_i is a deg-1 (random) poly.

Fix any input asst $z \in \{0,1\}^t$ s.t. some $z_j = 1$

(i.e. $OR(z_1, \dots, z_t) = 1$, i.e. $p_0(z) \geq 1$.)

Claim: $\Pr[$at least one of $p_0(z), p_1(z), \dots, p_{1+\log t}(z) = 1$ $] \geq \frac{1}{3}$.

Pf: One of foll. 3 cases must hold:

both other cases: $p_0(z) > 1$.

1) $p_0(z)$ is 1. ☺

2) $p_0(z), \dots, p_{1+\log t}(z)$ all > 1.

For this to happen, need some j s.t. $z_j = 1$ to $\underbrace{\text{survive all } 1+\log_2 t \text{ halvings}}$.

For any fixed j, $\Pr[\ \ ] = \frac{1}{2^{1+\log t}} = \frac{1}{2 \cdot t}$

So prob. any j survives $\leq t \cdot \frac{1}{2 \cdot t} = \frac{1}{2}$.

I.e. $\Pr[$this case (2)$] \leq \frac{1}{2}$.

3) There's some i s.t. $p_i(z) > 1$ but $p_{i+1}(z) \leq 1$.

Given value of $p_i(z)$, know

$$\Pr[p_{i+1}(z) = 0] = 2^{-p_i(z)}$$

$$+ \Pr[p_{i+1}(z) = 1] = p_i(z) \cdot 2^{-p_i(z)}$$

So
$$\Pr[p_{i+1}(z) = 1 \mid p_{i+1} \leq 1] = \frac{p_i(z) \cdot 2^{-p_i(z)}}{(p_i(z) + 1) \cdot 2^{-p_i(z)}}$$

$$= \frac{p_i(z)}{(p_i(z) + 1)}.$$

So if i is s.t. $p_i(z) > 1$

$\qquad + \; p_{i+1}(z) \le 1$,

$\Pr[p_{i+1}(z) = 1] \ge \frac{2}{3}$.

(prob. 1 ☺)

Since we have $\ge \frac{1}{2}$ chance of case 1 or case 3 (prob. $\ge \frac{2}{3}$ ☺),

we have $\ge \frac{1}{2} \cdot \frac{2}{3} = \frac{1}{3}$ chance of ☺

$\blacksquare$

Let's define poly.

rand. poly

deg $\le O(\log t)$

$$p(x) := \prod_{i=0}^{1+\log t} (1 - p_i(x)).$$

If $x_1 = \ldots = x_n = 0$: $\quad p(x) = 1$ for sure

If some x_i is 1: $\quad$ some i has $p_i(x) = 1$ $\quad$ w.p. $\ge \frac{1}{3}$.

so $\quad$ w.p. $\ge \frac{1}{3}$, $\quad p(x) = 0$.

Let $p'(x)$ be product of $O(\log \frac{1}{\varepsilon})$ many p's as above (independent).

$$\mathrm{Deg}(p') = O(\log \tfrac{1}{\varepsilon} \cdot \log t).$$

If $x_1 = \ldots = x_n = 0$: $\quad p'(x) = 1$ for sure.

If some x_i is 1: $\quad \Pr[p'(x) \neq 0] \leq \left(\frac{2}{3}\right)^{O(\log \frac{1}{\varepsilon})} < \varepsilon$, i.e.

$$\Pr[p'(x) = 0] \geq 1 - \varepsilon.$$

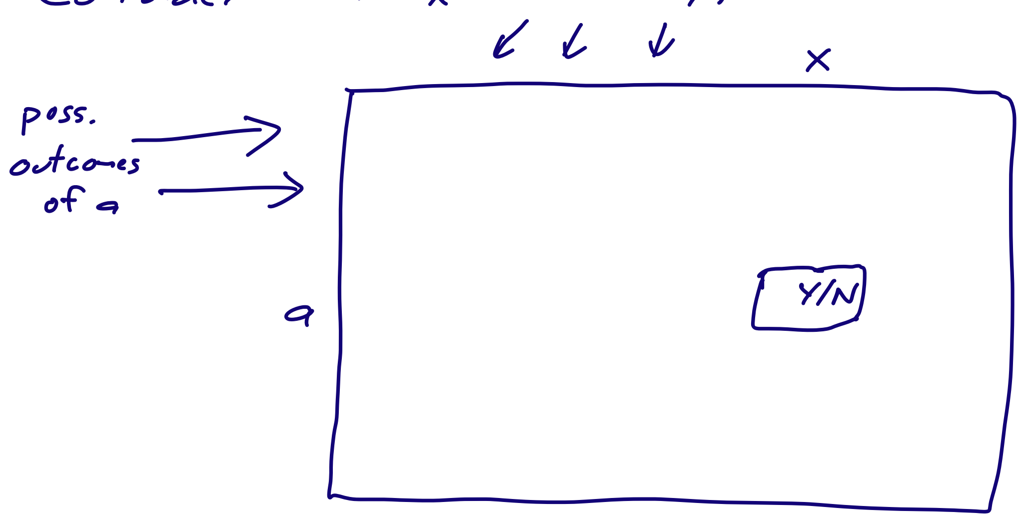
Define $a(x) = 1 - p'(x)$. We've shown:

$$\circledast \quad \forall x \in \{0,1\}^t, \quad \Pr_a\Big[a(x) = \overbrace{(x_1 \vee \ldots \vee x_t)}^{0/1 \text{ value!}}\Big] \geq 1 - \varepsilon.$$

This implies:

$$\forall \underbrace{\vartheta}_{\text{over } x \in \{0,1\}^t} \; \exists a \quad \Pr_{x \sim \vartheta}[a(x) = (x_1 \vee \ldots \vee x_t)] \geq 1 - \varepsilon. \quad (**)$$

Consider matrix: $\quad x \in \{0,1\}^t$



Y: $a(x) = x_1 \vee \ldots \vee x_t$ $\qquad$ N: $a(x) \neq x_1 \vee \ldots \vee x_t$.

(*): every col. is $1-\varepsilon$ frac Y's

acc. to dist over a's.

So for any dist over columns (any ϑ), prob. $[Y] \geq 1-\varepsilon$.

So given ϑ, there must be some row s.t. picking a ϑ-rand. elt of that row gives Y w.p. $\geq 1-\varepsilon$. This is (**)

some outcome of a

a