Last time: • using HSL to get $2^{\Omega(n^{\frac{1}{d-1}})}$ size l.b. for depth-d ckts for PAR
• Proof of "weak SL"
• Proof of HSL (given "Key Fact")

Today: • finish) ! (by proving ! !

→ • average-case l.b. for AC^0 ckts for PAR (small extension of worst-case l.b. we did)

→ • Depth-2 avg-case lb (O'Donnell & Wimmer):
Any CNF that agrees with (some explicit f) on 90% of all inputs must have $2^{\Omega(\frac{n}{\log n})}$ clauses

• Start $\mathbb{F}_2$-polynomials: an avg-case l.b. for them.

Scribe: Mark Questions?

Recall Key Fact we need to prove, to finish pf of HSL:

Key Fact: Any restriction σ is Angel(ρ) for $\leq (4w)^t$ many bad ρ's.

Pf: Let σ = Angel(ρ) for some bad ρ.
We'll describe how to recover ("decode") ρ from

(σ + a little extra info)

F is "up in the sky"; known.

↓ bd # poss. for this: gives a bd on # poss ρ s.t. σ = Angel(ρ).

Aux info: 2 rows of t #s in each row, + little extra

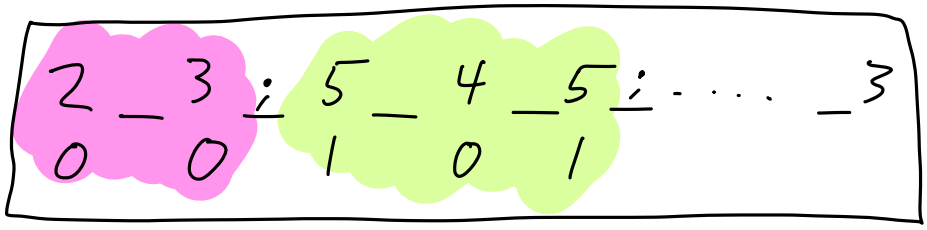
First row: elt of $[w]^t$. — w^t

2^{nd} row: elt of $\{0,1\}^t$ — 2^t

$\leq (4w)^t$ poss. lst

extra info: in each of $t-1$ pos. between 2 elts of row, put [;] or put nothing. 2^{t-1}

Ex:



Since $\leq (4w)^t$ poss. for aux info: once show can decode ρ from (σ + aux info), gives Key Lemma.

Q: How to decode ρ from (σ + aux info)?

Issue: don't know which t fixed bits of σ are from Angel(ρ) (vs fixed already in ρ).

If knew: replace them by * in σ, & get ρ.

We'll identify those vars by first finding v_1, then v_2, ...

Here's how: Recall COT(F,ρ) has V_1 = surviving vars in lst of F that's not killed to 0 by ρ.

Imagine restricting F by σ.

σ: ext. of ρ, so any term killed to 0 by ρ is killed to 0 by σ.

But lst term in F not killed by ρ is sat. by

$\sigma = \text{Angel}(\rho)$! So 1st term in F that's sat. by σ is where V_1 came from.

Ex:

$$F = (x_1 \wedge \bar{x}_2) \vee \boxed{(\bar{x}_1 \wedge \bar{x}_2 \wedge x_8)} \vee (\bar{x}_2 \vee x_4 \vee x_5 \vee \bar{x}_6) \vee \dots$$

Killed by σ, so not where V_1 came from

satisfied by σ: this is where V_1 came from!

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
$\sigma =$	0	0	1	1	1	0	1	1

Q: which vars in term we just found are V_1 ones?

A: use aux info: term is width w, read elts of 1st row to get info abt which of the w vars in term are $*$ in ρ.  means "that's it for this term."

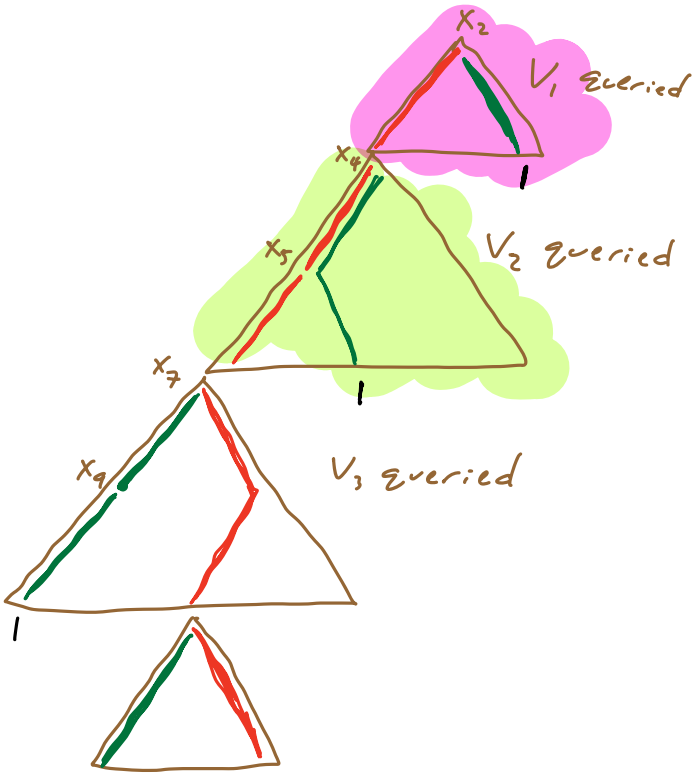
We found V_1 ! 

How to move on to find V_2? Use 2nd row to learn how to traverse V_1-block of COT to follow Devil(ρ) path; i.e., 2nd row tells us how Devil(ρ) (i.e. P) fixes the V_1 vars.

Morph σ by replacing V_1 vars w/ those bits. $\sigma \rightsquigarrow \sigma'$

Continue.

→ Now 1st term in F sat by σ' must be what V_2 came from.



Can continue, & end up recovering ρ: obt. by replacing all $V_1, V_2, \ldots$ vars in σ with *'s.

End of HSL

Proj. topic: Variants/extensions of HSL.

- pf cxity
- derand. versions
- ⋮

Let's give avg-case LB for AC^0!

↳ Reuse earlier work:

can go over prev. args, & all our "w.p. $\geq \frac{1}{2}$" are actually very strong:

$M \geq 2^{cn^{1/d}}$ $\left(c = c_d = \frac{1}{100^d}\right)$

for ↓, can verify each fail. prob. $\leq \frac{1}{M^5}$.

$O(d)$ many: overall,

w.p. $1 - \frac{O(d)}{M^5}$, the ckt C_{d-2} is

a depth-2 ckt w/ bottom fanin $\leq 10 \log M$,

over $n_{d-2} \geq \frac{n}{200(200 \log M)^{d-2}}$ vars.

Now do 1 more rand restr., with $p = \frac{1}{100 \log M}$. $t = 10 \log M$

$$\Pr[\, C_{d-2} \text{ doesn't collapse to depth-}(10 \log M) \text{ OT} \,] \leq \frac{1}{M^5}.$$

$$CB \Rightarrow \Pr[\text{fewer than } \frac{n_{d-2}}{200 \log M} \text{ vars survive}]$$

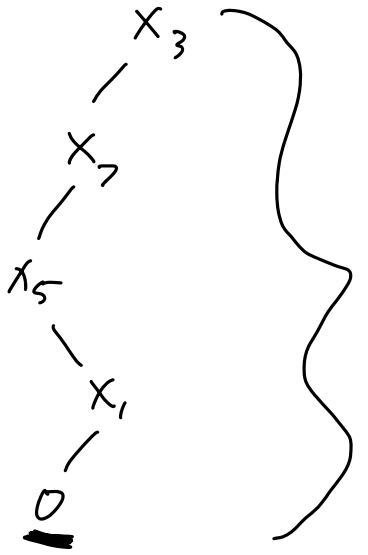
$$\leq \exp\left(-\frac{n}{c \cdot (\log M)^{d-1}}\right) \leq \frac{1}{M^5}.$$

So overall, w.p. $\geq 1 - \frac{O(d)}{M^5}$, get

(10 log M) depth OT, $\geq \frac{n}{c \cdot (\log M)^{d-1}}$ vars

survive.

Key fact: any OT of depth d has corr. 0, under $\mathcal{U}$, with any PAR on $> d$ vars



$PAR(x_1, x_3, x_5, x_7, x_8)$

right + wrong $=_y$ likely.

So OT only right w.p. $\frac{O(d)}{M^5} \leq \varepsilon$.

Reinterpreting:

Thm: Let C be a ckt of size $M = 2^{cn^{\frac{1}{d}}}$, depth d.

Then PAR_n is ε-hard for C, where

$\varepsilon \geq 2^{-cn^{1/4}}$

↳ avg-case LB for PAR!

Project topic: refinements of avg-case LB's for AC^0.

Would be awesome to show, for some explicit f, that can make bigger smaller.

Don't know how. ☹

Now: O'Donnell + Wimmer:

bigger, + bigger. } not for PAR_n, only for $d=2$.

$d=2$ above: $= 2^{n^{1/d}} = 2^{\sqrt{n}}$

$= \frac{1}{2^{\sqrt{n}}}$.

$F^* =$

→ Consider ONFTRIBES fn on $n = w2^w$ vars:

$$F^*(x_1, \ldots, x_n) = \underbrace{(x_1 \wedge \ldots \wedge x_w) \vee (x_{w+1} \wedge \ldots \wedge x_{2w}) \vee \ldots}_{\frac{n}{\log n} = \frac{n}{w} = 2^w \text{ terms, } w \text{ vars/term.}}$$

$(w \approx \log n - \log\log n, \quad n = w2^w)$

Thm (O'D/w): Any CNF g that agrees w/ F^* on 90% of all 2^n inputs must have $2^{\Omega\left(\frac{n}{\log n}\right)}$ clauses.

→ (we'll extend to get avg case l.b. for all depth-2 ckts...)

1st step:

Fact: if g is s-clause CNF, there's a CNF g' which is ε-close to g, i.e. $\Pr_{x \sim \mathcal{U}}[g(x) = g'(x)] \geq 1-\varepsilon$, s.t. g' has width of every clause $\leq \log(s/\varepsilon)$.

Pf: Any clause of length t falsif. w.p. $\frac{1}{2^t}$.

So

Removing a clause of width $> \log(s/\varepsilon)$ changes g on $\leq \frac{1}{2^{\log(s/\varepsilon)}} = \frac{\varepsilon}{s}$ frac. of inputs.

UB over all ($\leq s$) such clauses removed. ∎

So to give O'D/W thm, enough to argue

> ✡ Any CNF g' that 0.2-approx. F^* must have width $\geq \frac{1}{4} \cdot 2^w = \Omega\left(\frac{n}{\log n}\right)$.

Pf ($✡ \Rightarrow$ O/W): Sps g 0.1-appx F^* + has s clauses.

Fact $\Rightarrow$ there's a width $-\log(10s)$ CNF g' s.t. it 0.1-appx g.

So g' 0.2-appx F^*, so ✡ say $\log(10s) \geq \Omega\left(\frac{n}{\log n}\right)$. ∎

Goal:

> ✡ Any CNF g' that 0.2-approx. F^* must have width $\geq \frac{1}{4} \cdot 2^w = \Omega\left(\frac{n}{\log n}\right)$.

width-w DNF

width $\frac{1}{4}2^w$ CNF!

Obs: Rand restr / SL won't suffice:

F^*, like g', is depth-2 ckt, so rand. restr. will simplify F^* like g'.

width-w DNF

Need a way to "keep F^* complex" while "making g' simple" ... do it via

random projections.

Def: A projection ρ is a mapping

$$\{x_1, \ldots, x_n\} \longrightarrow \{0, 1, y_1, \ldots, y_t\}.$$

---

fixes vars, + identifies groups of vars.

Ex:

$\rho(x_1) = 1$
$\rho(x_2) = 0$
$\rho(x_3) = \rho(x_4) = y_1$
$\rho(x_5) = \rho(x_6) = y_2$
$\vdots$

$f|_\rho$

[They let us "carefully preserve structure" in target fn (F^*) so it "survives".]

Key to arg: O'D-W "trick": clever

way to draw unif n-bit string, using rand proj.

$\rho = 1yy111yy1$

Lemma ✩: Let $\rho \sim \{y_{\frac{1}{2}}, 1_{\frac{1}{2}}\}^w \setminus \{1^w\}$ ("projection")

$$y \sim \{0_{1-\frac{1}{2^w}}, 1_{\frac{1}{2^w}}\}.$$

Doing ρ then y gives unif string in $\{0,1\}^w$.

Pf: $z = 1^w$: $\Pr[\text{get } z] = \frac{1}{2^w}$:)

For $z \neq 1^w$: $\Pr[\text{get } z] = \underbrace{\frac{1}{2^w - 1}}_{\text{get } \rho \text{ compat. w/ } z} \cdot \underbrace{\left(1 - \frac{1}{2^w}\right)}_{\text{get } 0} = \frac{1}{2^w}$. ∎

Let's prove ✩:

> ✩ Any CNF g' that 0.2-approx. F^* must have width $\geq \frac{1}{4} \cdot 2^w = \Omega\left(\frac{n}{\log n}\right)$.

Pf: Do a global version of trick: indep. copy of (!) ρ for each of 2^w terms of F^*.

(recall $F^*(x_1, \dots, x_n) = (x_1 \wedge \dots \wedge x_w) \vee (x_{w+1} \wedge \dots \wedge x_{2w}) \vee \dots$)

$\quad\quad\quad\quad\quad\quad\quad\quad 11y_1 1y_1 \dots \quad\quad y_2 y_2 111 y_2 \dots$

In draw of $\rho_1, \rho_2, \dots \rho_{2^w}$, for each $i \in [2^w]$, all surviving vars under $\rho_i \rightsquigarrow y_i$

- F^* "stays ~~complex~~ balanced under ρ":

w.p. 1 over $\rho = (\rho_1, \rho_2, \ldots, \rho_{2^w})$,

$$F^* \wedge \rho = Y_1 \vee Y_2 \vee \ldots \vee Y_{2^w} .$$

$Y_i \sim \{0_{1-\frac{1}{2^w}}, 1_{\frac{1}{2^w}}\}$ ↙ , so

$$\mathbb{E}_{Y_1,\ldots,Y_{2^w}} \left[F^* \wedge \rho(Y) \right] = 1 - (1 - \tfrac{1}{2^w})^{2^w} \approx 1 - \frac{1}{e} \approx 0.63.$$

- Any non-super-wide CNF is very biased (either towards 0 or towards 1) after ρ:

Fix any CNF g' of width $\leq \frac{1}{4} \cdot 2^w$, consider any fixed outcome ρ of proj.

Consider $g' \wedge \rho$, a CNF over $Y_1, \ldots, Y_{2^w}$.

2 poss:

1) Every clause of $g' \wedge \rho$ has ≥ 1 neg var

$$g' \wedge \rho = (\bar{Y}_1 \vee \ldots) \wedge (\bar{Y}_7 \vee \ldots) \wedge \ldots .$$

Means

$$g' \wedge \rho(0^{2^w}) = 1.$$ Each y_i is 0 w.p. $1 - \frac{1}{2^w}$,

But $F^* \wedge \rho(0^{2^w}) = 0.$

so $\Pr[x = 0^{2^w}] = (1 - \frac{1}{2^w})^{2^w} \approx 0.37.$

So in this case $g' \wedge \rho \neq F^* \wedge \rho$ disagree on 37% of y-outcomes.

$\geq .2$

2) Not every clause of $g' \wedge \rho$ has ≥ 1 neg var.

i.e. $g' \wedge \rho$ contains a clause

$$C = y_1 \vee y_2 \vee \dots \vee y_k \qquad k \leq \frac{1}{4} \cdot 2^w \text{ vars}$$

$$\Pr_y[g' \wedge \rho(y) = 1] \leq \Pr_y[C(y) = 1] \overset{\text{U.B.}}{\leq} \frac{1}{4} \cdot 2^w \cdot \frac{1}{2^w} \leq \frac{1}{4}.$$

But $\Pr_y[F^* \wedge \rho(y) = 1] = \Pr_y[y_1 \vee \dots \vee y_{2^w} = 1]$

$$\approx 0.63.$$

So in this case $g' \wedge \rho \neq F^* \wedge \rho$ disagree on $(.63 - \frac{1}{4}) \geq .2$ of y-outcomes.

So overall, have

$$\Pr_{x \sim \{0,1\}^n \text{ unif}}[F^*(x) \neq g'(x)]$$

$$\overset{\text{trick}}{=} \mathop{\mathbb{E}}_{\rho \sim ?}\left[\Pr_y[F^* \wedge \rho(y) \neq g' \wedge \rho(y)]\right]$$

$$\overset{\text{for every } \rho}{\geq} 0.2$$

$\therefore$ this is ✡.

To defeat all depth-2 ckts:

switch $\wedge/\vee$ & get

Cor: Any DNF g' that 0.1-appx CNF$_{\text{TRIBES}}^{n\text{-var}}$

must have $\geq 2^{\Omega(n/\log n)}$

Consider

$$f: \{0,1\}^{2n=2w2^w} \to \{0,1\}$$

$$f(a,b) = \text{DNF TRIBES}(a) \vee \text{CNF TRIBES}(b).$$

OFFICIAL HW PROBLEM: any depth-2 ckt that 0.01-approx. $f(a,b)$ must have size $\geq 2^{\Omega(\frac{n}{\log n})}$

Proj topic: Other applic. of random projections.

New unit: Lower Bds for $\mathbb{F}_2$-polynomials

$\{0,1\} \equiv \mathbb{F}_2 \pmod 2$.

monomial over $\mathbb{F}_2$: $x_{i_1} x_{i_2} \cdots x_{i_k}$ deg-k, $i_1, \ldots$ distinct

$\hookrightarrow$ AND$(x_{i_1}, \ldots, x_{i_k})$ (no neg.)

Never need to consider x_1^2 x_2^3 $0^2 = 0$

all multilinear.

$1^2 = 1$ etc.

$\mathbb{F}_2$-polynomial : sum of monomial

$a + b \equiv a \oplus b = PAR(a,b)$.

$x_1 x_2 + x_1 x_3 x_4 + x_2 x_3 x_4 + \cdots$

highest

deg = deg of any monom.

2^n multilin. monom.

2^{2^n} " polys.

2^{2^n} f: $\{0,1\}^n \to \{0,1\}$

Easy fact: Every $f: \{0,1\}^n \to \{0,1\}$ has a unique expression as an $\mathbb{F}_2$-poly. ($\mathbb{F}_2^n \to \mathbb{F}_2$)

(induc. on n).

Our goal: degree lower bounds.

Worst-case bds: easy! :)

$AND(x_1, \ldots, x_n) = x_1 \cdots x_n$: degree n.

Notation: $DEG_d = \{$all fns $f: \{0,1\}^n \to \{0,1\}$ that have deg-d $\mathbb{F}_2$-polys$\}$.

Correlation bds: hard!

Open q: Prove some $f: \{0,1\}^n \to \{0,1\}$, $f \in NP$, is $\frac{1}{n}$-hard for $OEG_{\log n}$ for some distr. $\mathcal{D}$ over $\{0,1\}^n$.

We'll do 2 corr bds:

1) degree $\Theta(\sqrt{n})$, but corr $= \Theta(1)$

2) degree $\ll \log n$, but tiny correl.