Last time:

- a little more on formulas (KRW conj.; depth $=\Theta(\log \text{size})$; full-basis formulas) $\tilde{\Omega}(n^2)$
- start constant-depth ckts
  - $2^{\Omega(n^{1/(d-1)})}$ size u.b. for depth-d ckts for PAR
  - intuition for, statement of, the Switching Lemma:

> **Håstad's Switching Lemma:**
>
> Let $f(x_1,\dots,x_n)$ be computed by a width-w DNF. CNF
> For $t \geq 1$, $0<p<1$,
>
> $$\Pr_{\rho\sim R_p}\left[\text{DT-depth}(f|_\rho) \geq t\right] \leq (7\cdot p\cdot w)^t$$

Today:

- 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
- average-case l.b. for AC^0 ckts for PAR

Yuhao!

Scribe: Ryan

Questions?

Using HSL to get strong l.b. for depth-d ckt computing PAR_n:

> **Håstad's Switching Lemma:**
>
> Let $f(x_1,\dots,x_n)$ be computed by a width-w DNF. CNF
> For $t \geq 1$, $0<p<1$,

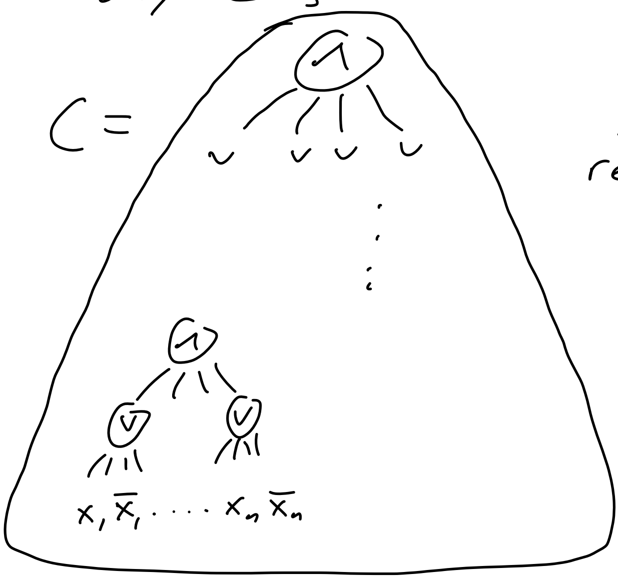
$$\Pr_{\rho \sim R_p}\left[\text{DT-depth}(f\restriction_\rho) \geq t\right] \leq (7 \cdot p \cdot w)^t$$

Let C be depth-d, size-M ckt for PAR.
(We'll argue $M \geq 2^{\Omega(n^{\frac{1}{d-1}})}$.)

$n^{\frac{1}{\log n}} = 2$

Say C is AND–OR ... –AND–OR

$C =$



Stage 0: initial "trim" to reduce bott. fan-in.

Hit C with $\rho \sim R_{\frac{1}{100}}$:

$*$-prob. $= \frac{1}{100}$

1 " $= \frac{49.5}{100}$

0 " $= \frac{49.5}{100}$.

If some bott. level gate ($\vee$) has fanin $> 10 \log M$:
prob. fixed to 1 + vanishes $\geq 1 - (.505)^{10 \log M}$
$\gg 1 - \frac{1}{M^5}$

- UB over all ($\leq M$) bott level gates:

(1) w.p. $> \frac{1}{2}$ this ρ kills all gates of fan-in $> 10 \log M$

(2)
- Also w.p. $> \frac{1}{2}$, at least $\frac{n}{200}$ vars survive ρ (*)

→ some ρ makes both occur; fix that ρ.
Call C_0 the ckt $C\restriction_\rho$:
/

↳ • C_0 computes PAR or its neg on $\geq \frac{n}{200}$ vars
• C_0 has bott. fan-in $\leq 10 \log M$.

Stage 1: Hit C_0 w. $\rho \sim R_{\frac{1}{100 \log M}}$.

Each depth-2 ckt at bott. of C_0 is a $(10 \log M)$-width CNF: can apply HSL. Take $t = 10 \log M$:

HSL $\Rightarrow$ this depth-2 ckt collapses to a $\leq (10 \log M)$-depth DT except w/ fail. prob. $(7pw)^{t = 10 \log M} = (.7)^{10 \log M} \cong \frac{1}{M^5}$

UB over all $(\leq M)$ $\Rightarrow$ •(1) w. prob. $> \frac{1}{2}$, each subckt becomes depth-$10 \log M$ DT, hence " " " CNF

(2) • w. p. $> \frac{1}{2}$, # surviving vars

$$\geq \left(\frac{n}{200}\right) \cdot \frac{1}{200 \log M}$$

Fix a ρ sat (1) + (2). $C_1 = C_0 \upharpoonright \rho$

C_1 computes PAR or neg on vars, + is a depth-$(d-1)$ ckt w/ $\le M$ gates at dist 2 from bottom.

Repeat.

Current ckt	depth	bott. fan-in	# vars in play
C	d	n	n
C_0	d	$10 \log M$	$\frac{n}{200}$
C_1	$d-1$	$10 \log M$	$\frac{n}{200 \cdot (200 \log M)}$
C_2	$d-2$	$10 \log M$	$\frac{n}{200 \cdot (200 \log M)^2}$
$\vdots$			
C_{d-2}	2	$10 \log M$	$\frac{n}{200 \cdot (200 \log M)^{d-2}}$

C_{d-2} computes PAR or neg. on vars, & is $10 \log M$ width CNF.

So must have $\frac{n}{200^{d-1} (\log M)^{d-2}} \le 10 \log M$

So $M \geq 2^{\Omega_d\left(n^{\frac{1}{d-1}}\right)}$.

PAR$(x_1, \ldots, x_{50})$:

Let's prove a Weak Switching lemma!

Weak Switching Lemma:

Let $f(x_1,\dots,x_n)$ be computed by a width-w $\overset{\text{CNF}}{\text{DNF}}$.
For $t \geq 1$, $0 < p < 1$,

$$\Pr_{\rho \sim R_p}\left[\text{DT-depth}(f\restriction_\rho) \geq t\right] \leq \left(40\, p\, w\, 2^w\right)^t$$

- HSL pf: 1) restrict f by ρ, 2) analyze DT for $f\restriction_\rho$
- Weak SL pf: 1) construct DT, T, for f; 2) analyze $T\restriction_\rho$.

DT T, hit by ρ: easy to understand :)

$$T = \begin{array}{ccc} & x_i & \\ \swarrow & & \searrow \\ T_0 & & T_1 \end{array} \qquad \text{Hit by } \rho:$$

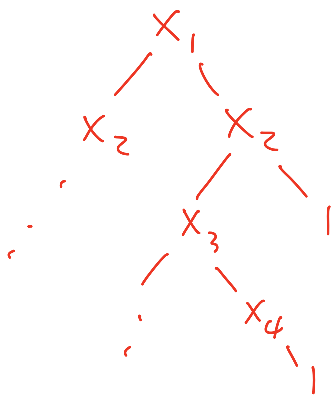
$$T\restriction_\rho \text{ is } \begin{cases} \begin{array}{ccc} & x_i & \\ \swarrow & & \searrow \\ T_0\restriction_\rho & & T_1\restriction_\rho \end{array} & \text{if } x_i \leftarrow * \\ T_0\restriction_\rho & \text{if } x_i \leftarrow 0 \\ T_1\restriction_\rho & \text{if } x_i \leftarrow 1 \end{cases}$$

Key def:

Def: A DT T is <u>w-clipped</u> if every node in T has $\geq$ one leaf at dist. $\leq w$ below it.

Lemma: Any width-w $\overset{\text{CNF}}{\text{DNF}}$ is $\equiv$ to a w-clipped DT.

$$(x_1\, x_2) \vee (\bar{x}_1\, x_3) \vee (x_3\, x_4)$$



Pf: Build T by querying vars in each succ. term.
Read/query vars in current term 1 by 1, moving on to next term when curr. term falsified.

w-clipped b/c at any internal node v, branch sat. current term ends in 1-leaf at dist. $\leq w$. ■

Get WSL from

w-clipped Switching Lemma:

Let $f(x_1,\dots,x_n)$ be computed by a w-clipped DT.
For $t \geq 1$, $0 < p < 1$,

$$\Pr_{\rho \sim R_p}\left[\text{DT-depth}(f\restriction_\rho) \geq t\right] \leq \left(40\, p\, w\, \underline{\underline{2}}^{w}\right)^t$$

Our goal.

Define $\text{Branches}(T)$ = all root-to-leaf paths/branches in T.

RW down a tree T: $\qquad T =$ a OT

<u>Def</u> (dist. $\mathcal{W}(T)$ over Branches(T)):
dist. on Branches(T) corr. to unif random walk down from root:
path $\pi \in$ Branches(T) has mass $2^{-|\pi|}$ under $\mathcal{W}(T)$ $\qquad |\pi| =$ length of π.

<u>Lemma</u>: <u>TFAE</u>: $\qquad$ Let T be a OT (proper — no var occurs twice on any branch)

- $\mathcal{V}_1(T)$: draw $\rho \sim R_p$, consider $T \upharpoonright \rho$, output $\sigma \sim \mathcal{W}(T\upharpoonright\rho)$.
- $\mathcal{V}_2(T)$: draw $\pi = (\overset{(x_3,0)}{\pi_1}, \overset{(x_1,1)}{\pi_2}, \ldots) \sim \mathcal{W}(T)$, output sub-list σ obt. by going through $\pi_1, \pi_2, \ldots$ + including it w. prob. p.
  (length of $\sigma \sim \mathrm{Bin}(|\pi|, p)$)

(OFFICIAL HW PROBLEM)

<u>Pf of w-clipped SL</u>:

Observe: for any ρ, have
$$\mathrm{depth}(T\upharpoonright\rho) \geq t \implies \Pr_{\sigma\sim\mathcal{W}(T\upharpoonright\rho)}[|\sigma| \geq t] \geq 2^{-t}.$$

So have

$$\Pr_{\rho\sim R_p}[\mathrm{depth}(T\restriction_\rho)\geq t] \leq \Pr_{\rho\sim R_p}\Big[\underbrace{\Pr_{\sigma\sim \mathcal{W}(T\restriction_\rho)}[|\sigma|\geq t]}_{=Z} \geq 2^{-t}\Big]$$

Markov: if $Z\geq 0$ is any RV, have
$\Pr[Z\geq 2^{-t}] \leq 2^t\cdot \mathbb{E}[Z]$.

$$\leq 2^t\cdot \mathbb{E}_{\rho\sim R_p}\Big[\Pr_{\sigma\sim\mathcal{W}(T\restriction_\rho)}[|\sigma|\geq t]\Big] \quad (\text{Markov})$$

$$= 2^t\, \mathbb{E}_{\pi\sim\mathcal{W}(T)}\Big[\Pr_{Y\leftarrow \mathrm{Bin}(|\pi|,p)}[Y\geq t]\Big] \quad (\equiv \text{lemma})$$

$$\leq 2^t\cdot \mathbb{E}_{\pi\sim\mathcal{W}(T)}\Big[p^t\cdot\binom{\pi}{t}\Big]$$

$$= (2p)^t\cdot \mathbb{E}_{\pi\sim\mathcal{W}(T)}\Big[\binom{|\pi|}{t}\Big] \overset{?}{\leq} (40pw2^w)^t.$$

Claim: if T w-clipped, $\mathbb{E}_{\pi\sim\mathcal{W}(T)}\Big[\binom{|\pi|}{t}\Big] \leq (20w2^w)^t$

Pf: Let $X=$ first time (# tosses) of fair coin to get w consec. H.

$X\in\{w, w+1, w+2, \dots\}$

This X stochastically dominates $|\pi|$ for $\pi\sim\mathcal{W}(T)$:

$\forall \alpha,\quad \Pr[X\geq\alpha]\geq \Pr[|\pi|\geq\alpha]$.

$\Longrightarrow$ for any mon. ↑ fn g, have

$$\mathbb{E}[g(X)] \geq \mathbb{E}[g(|\pi|)].$$

So suff to show $\mathbb{E}\left[\binom{X}{t}\right] \leq (20w \cdot 2^w)^t$.

Can show $\mathbb{E}[X^t] \leq (7wt2^w)^t$ (induc.)

OFFICIAL HW PROBLEM

So $\mathbb{E}\left[\binom{X}{t}\right] \leq \mathbb{E}\left[\left(\frac{eX}{t}\right)^t\right] \leq \left(\frac{e}{t}\right)^t \cdot (7wt \cdot 2^w)^t$

$< (20w2^w)^t$. ■

Let's prove the HSL!

> **Håstad's Switching Lemma:**
>
> Let $f(x_1, \dots, x_n)$ be computed by a width-w DNF. (CNF)
> For $t \geq 1$, $0 < p < 1$,
>
> $$\Pr_{\rho \sim R_p}[\text{DT-depth}(f|_\rho) \geq t] \leq (10 \cdot p \cdot w)^t$$

Note: think of p as small: $< \frac{1}{10w}$.

So $*$ are unlikely...

Let $F = T_1 \vee T_2 \vee \dots$ width-w DNF.

(fix order of terms).

What happens to one term under $\rho \sim R_p$?

$$T_i = \begin{array}{ccc} x_1 \wedge & \bar{x}_3 \wedge & x_4 \\ 1 & * & * \end{array} \quad ?$$

- Some lit. could get set to 0; $T_i \upharpoonright_\rho \equiv 0$.
  i.e. T_i vanishes from $F \upharpoonright_\rho$
  If <u>every</u> T_i has this happen, $\underline{F \upharpoonright_\rho \equiv 0.}$

- Could have each of T_i's w lits get 1.
  If this happens for <u>any</u> T_i, $\underline{F \upharpoonright_\rho \equiv 1.}$

- O/w, maybe some lit. in T_i get $*$,
  other " " " " 1
  Means T_i (potentially) "shrinks", but survives.

So overall, F could $\leftarrow$ 1
$\leftarrow$ 0
$\leftarrow$ some T_i vanish to 0, others may shrink.

<u>Ex:</u>

$$F = \underbrace{\cancel{(x_1 \wedge \bar{x}_2 \wedge x_4)}}_{T_1} \vee \underbrace{(\cancel{x_2} \wedge \boxed{x_5} \wedge \cancel{\bar{x}_6})}_{T_2} \vee \underbrace{(x_3 \wedge \bar{x}_5 \wedge x_7)}_{T_3}$$

$$\quad * \;\; \bar{1} \;\; 1 \qquad 1 \;\; * \;\; \bar{0} \qquad * \;\; * \;\; *$$

ρ:	x_1	x_2	x_3	x_4	x_5	x_6	x_7
	$*$	1	$*$	1	$*$	0	$*$

$\underline{T_1 \upharpoonright_\rho = 0}$, $\underline{T_2 \upharpoonright_\rho = x_5}$, $\underline{T_3 \upharpoonright_\rho = x_3 \wedge \bar{x}_5 \wedge x_7}$, so

$$\boxed{F \upharpoonright_\rho = (x_5) \vee (x_3 \wedge \bar{x}_5 \wedge x_7)}$$

Goal: whp_ρ, <u>some</u> DT for $F \upharpoonright_\rho$ is shallow.

We'll argue that whp$_\rho$, a particular way of writing a DT for $F\restriction_\rho$ is shallow.

$\text{COT}(F,\rho)$ "canonical DT for F after ρ"

Here's def of $\text{COT}(F,\rho)$ $\qquad F = T_1 \vee T_2 \vee \ldots$

1) If $F\restriction_\rho$ killed to 0 or 1, that's $\text{COT}(F,\rho)$. O/w,

2) Find first T_i not killed by ρ.
$\text{COT}(F,\rho)$ obliviously queries all surviving vars in that term "block of vars"

3) Recurse at each leaf: for each leaf, do (1), (2) under augmented restriction corresp. to leaf.

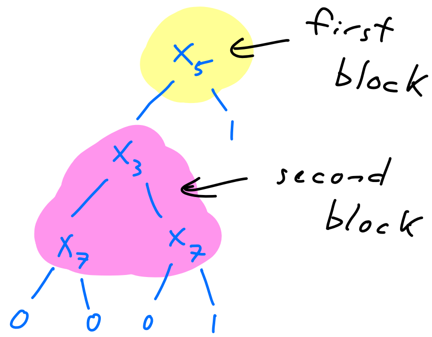
Note: when $\text{COT}(F,\rho)$ queries a block of vars, some ! asst/path sat. all lits in that restricted term, + get a 1-leaf in $\text{COT}(F,\rho)$ there.

Example above, cont:

$COT(F, \rho)$:

$$F\restriction_\rho = (x_5) \vee (x_3 \wedge \bar{x}_5 \wedge x_7)$$

$x_3 \wedge x_7$



Define BAD = set of restric. ρ s.t. $COT(F, \rho)$ has depth $\geq t$.

To show: $\Pr_{\rho \sim R_p}[\rho \in BAD] \leq (10pw)^t$.

Fix a bad ρ. $COT(F, \rho)$ has depth $\geq t$.
Let P = leftmost path of depth $\geq t$ in $COT(F, \rho)$.
We assume depth of P is $= t$.

So $\rho + P$ is a restric; call it $Devil(\rho)$.
(Fixes t more vars than ρ did.)

$Devil(\rho)$ has "segments" based on blocks of $COT(F, \rho)$ that are queried along P.

V_1 = 1st block

V_2 = 2nd " " ""

V_1 = 1st block = $\{x_2\}$,

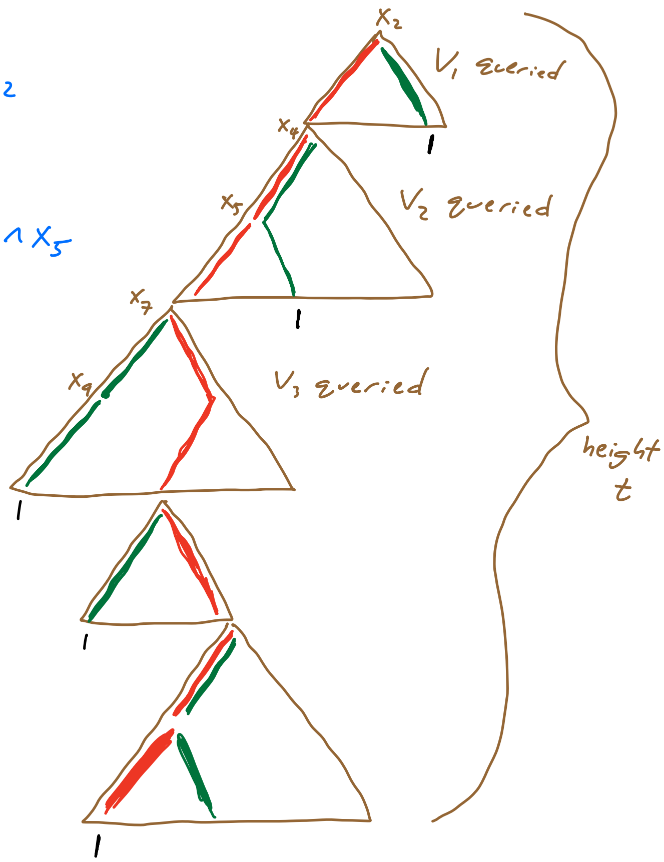
un-killed term of $F|_\rho$ is x_2

V_2 = 2nd block = $\{x_4, x_5\}$,

un-killed term of $F|_\rho$ is $\bar{x}_4 \wedge x_5$

V_3 = 3rd block = $\{x_7, x_9\}$

un-killed term of $F|_\rho$ is $\bar{x}_7 \wedge \bar{x}_9$



	x_1	x_2	x_3	x_4	x_5
ρ:	1	*	0	*	*
Devil(ρ):	1	0	0	0	0
Angel(ρ):	1	1	0	0	1

Let δ_1 = restric. fixing V_1 as in Devil(ρ)

Let δ_2 = " " V_2 " " "

So Devil(ρ) is $\rho \circ \delta_1 \circ \delta_2 \circ$

Consider another restr. based on ρ: Angel(ρ)

Angel(ρ), like Devil(ρ), fixes t addit. vars beyond ρ:

$V_1, V_2, \ldots$ (same as Devil(ρ).

Fixes vars in V_i to reach the 1-leaf of the block V_i. "Disconnected" in tree.

Angel + Devil disagree in each block.

---

given $\overset{\text{bad}}{\rho}$,

Q: is Angel(ρ) or ρ more likely under R_p?

↳, by a lot: more fixed bits, + fixed bits much more likely than $*$'s.

In more detail: fix any $\rho \in \{0,1,*\}^n$ with k many $*$'s.

$$\Pr_{R_p}[\rho] = \left(\frac{1-p}{2}\right)^{n-k} \cdot p^k$$

So for any bad ρ with k $*$'s,

$$\frac{\Pr[\rho]}{\Pr[\underbrace{\mathrm{Angel}(\rho)}_{k+t\ *'s}]} = \frac{\left(\frac{1-p}{2}\right)^{n-k} \cdot p^k}{\left(\frac{1-p}{2}\right)^{n-(k-t)} \cdot p^{k-t}}$$

$$= \left(\frac{2p}{1-p}\right)^t \underset{\text{p small, so}}{\leq} (2.5p)^t.$$

So for any bad ρ, have

$$\Pr_{R_p}[\rho] \leq (2.5p)^t \cdot \Pr_{R_p}\{\mathrm{Angel}(\rho)\}. \quad (!)$$

Key fact (next time):

Any restriction σ is $\mathrm{Angel}(\rho)$ for $\leq (4w)^t$ many bad ρ's.

Sum(!) over all bad ρ:

$$\Pr_{R_p}[\mathrm{BAD}] = \sum_{\rho \in \mathrm{BAD}} \Pr[\rho]$$

$$\overset{(!)}{\leq} \sum_{\rho \in \mathrm{BAD}} (2.5p)^t \cdot \Pr[\overbrace{\mathrm{Angel}(\rho)}^{\sigma}]$$

$$\leq (2.5p)^t \cdot (4w)^t \cdot \Big(\overbrace{\sum_{\sigma} \Pr_{R_p}[\sigma]}^{=1}\Big)$$

$$= (10pw)^t.$$

Next time:
- Key fact
- avg case AC^0 lower bds
- " " l.b. DNF/CNFs
- __________ ↳ "random projections"
- $\mathbb{F}_2$-polynomials
