Last time: • $R_\varepsilon^{pub}(EQ) = O(\log\frac{1}{\varepsilon})$ (end of comm. cxity)

• Start unit on **Circuit complexity:**

- review basics
- Shannon's nonconstructive l.b. $\frac{2^n}{2 \cdot n}$ for almost every $f: \{0,1\}^n \to \{0,1\}$
- start small-depth ckt lb's

Today: • simplifying assumptions for small-depth ckts

• PAR : $\approx 2^n$ l.b. (u.b.) for depth-2

$\approx 2^{n^{\frac{1}{d-1}}}$ u.b. for depth d

(*) $\approx 2^{n^{\frac{1}{d-1}}}$ l.b. " " " :

based on random restrictions, Håstad Switching Lemma, (won't prove)

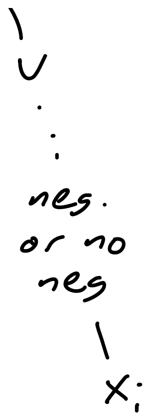
iterative depth reduction

Questions?

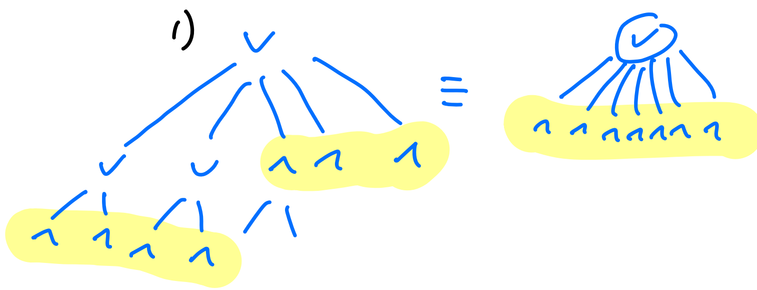
Second simplif. assumption: If have a size-s, depth-d formula F, can assume wlog that 1) gates alternate on any root-to-leaf path, & 2) push all neg. to bottom so adj. to input vars

$\wedge$
$\vee$
$\wedge$
⋮

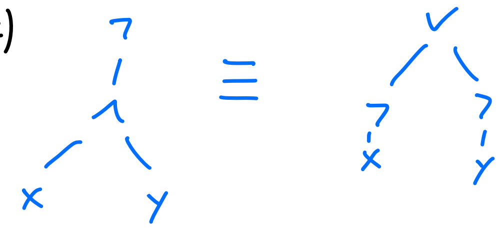
("alternating formulas")



1)

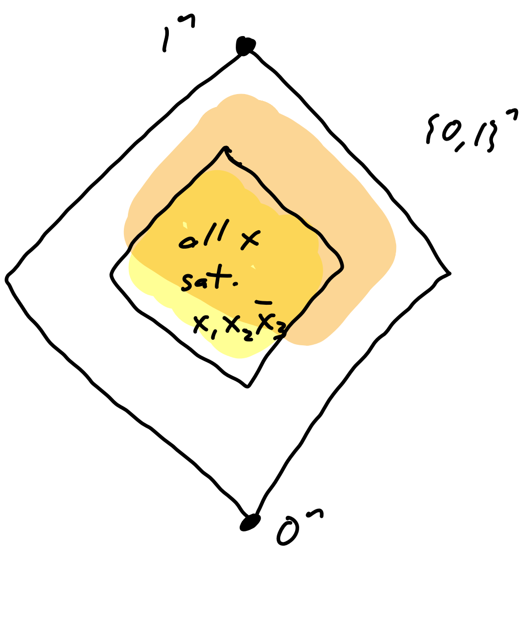


2)



So suff for us to prove lb's against depth-d, unbounded fanin alternating formulas.

? what's a hard fn for DNFs? CNFs?



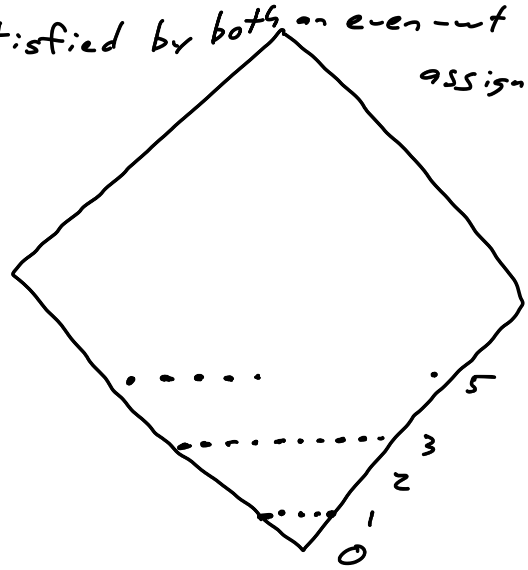
DNF: union of subcubes

$x_1 x_2 \bar{x}_3 \vee \bar{x}_2 x_6 x_7 x_8$

terms in DNF = #subcubes

$x_1 x_2 \dots x_{n-1}$: satisfied by both an even-wt & an odd-wt assignment: no good for PAR.

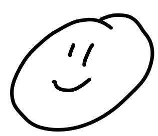
PAR: very tough to write as union of subcubes!



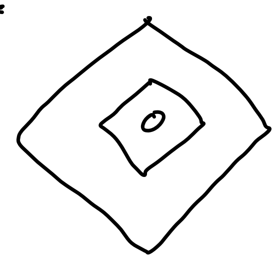
Any term in any DNF for PAR must have all n diff. vars (exactly one sat asst).

2^{n-1} s.a. for PAR : any DNF for PAR must have 2^{n-1} terms.

Same for CNFs w/ 0's, 1's reversed.

Depth 2:  $(x_1 \vee x_2 \vee x_3) \wedge$

000***

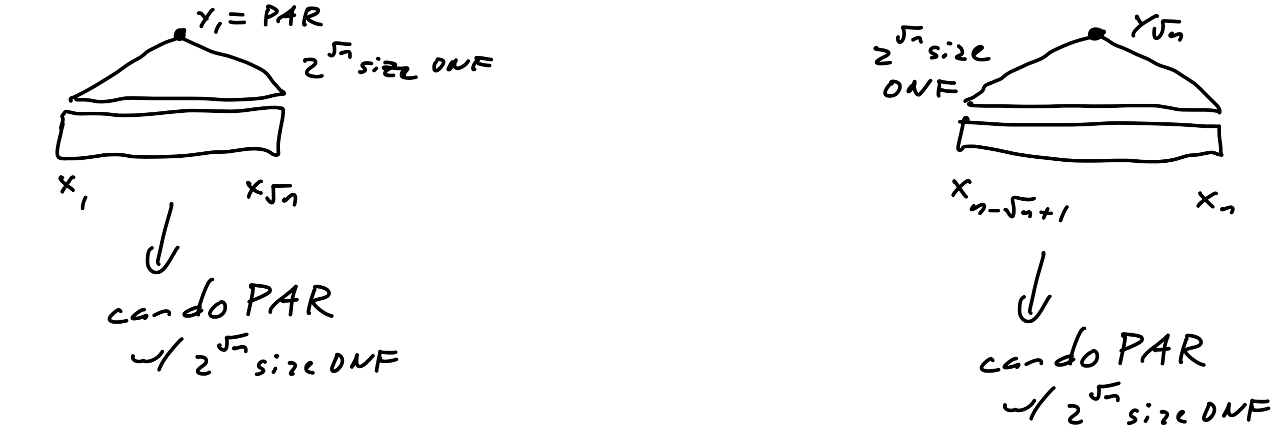


Depth 3? harder...

start w/ u.b. : what's a depth 3 ckt for PAR?

Here's a way

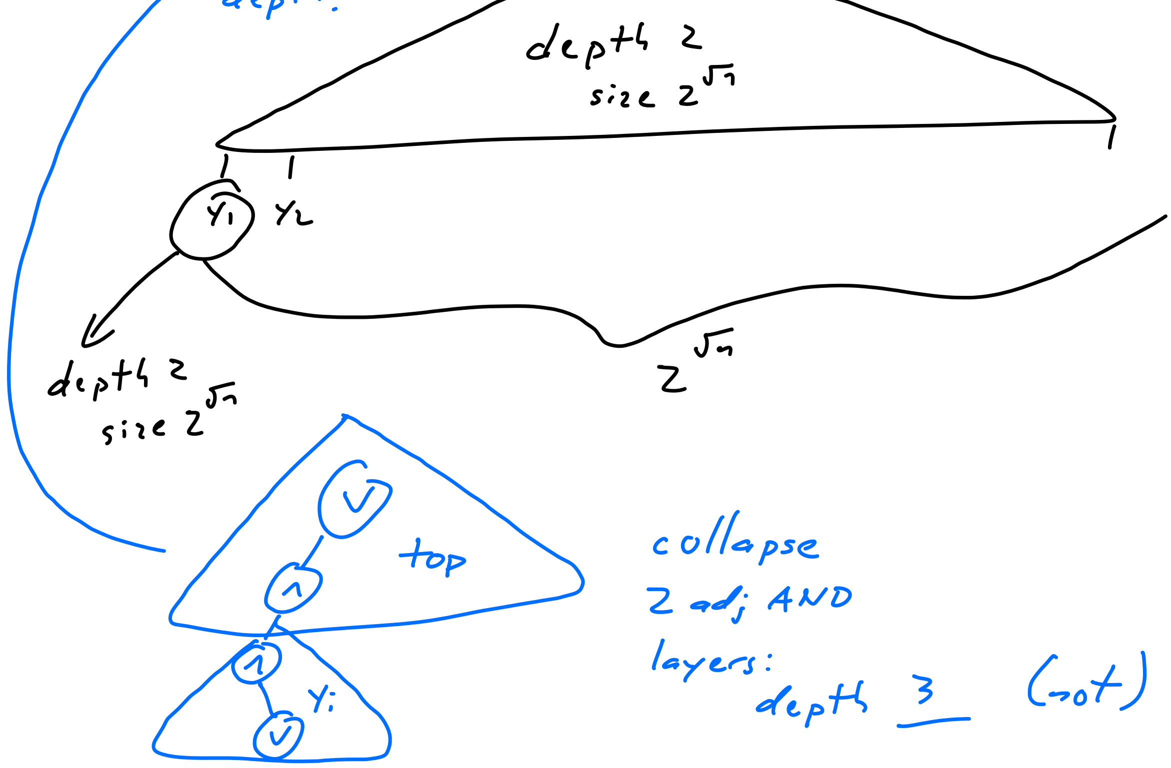
- Divide n vars into $\sqrt{n}$ blocks of $\sqrt{n}$ vars each.



- Compute $PAR(y_1, \dots, y_{\sqrt{n}})$: can do w/ DNF or CNF of size $2^{\sqrt{n}}$. Overall size:

$$2^{2\sqrt{n}} = 2^{\sqrt{n}} \cdot 2^{\sqrt{n}}$$

save 1 on depth!



collapse 2 adj AND layers: depth $\underline{3}$ (not)

So, can compute PAR_n w/ depth-3 size $2^{2\sqrt{n}}$ form. OR-AND-OR or AND-OR-AND

Can iterate: for any d, there's a formula of depth d & size $\approx 2^{d n^{\frac{1}{d-1}}}$ for PAR. $d = O(1)$: size $2^{n^{\frac{1}{d-1}}}$.

? l.b. ? Best possible construc!

<u>Thm</u> [Håstad '86] : Fix const $d \geq 2$ (indep. of n). Any family of depth-d $\wedge/\vee/\neg$ ckts for PAR_n must have size $2^{\Omega(n^{\frac{1}{d-1}})}$.

Super hi level idea of pf:

a) - Know DNFs must be huge to compute PAR

b) - if could eff convert C (depth-d ckt) to a DNF, w/o blowing up size too much, would mean C had to be huge.

Problem:

b) super-false: even converting a CNF to a DNF can blow up size enormously!

$(x_1 \vee x_2) \wedge (x_3 \vee x_4) \ldots \wedge (x_{n-1} \vee x_n)$:

$\hookrightarrow$ as DNF, need $2^{n/2}$ terms.

Fix: b) is true if we hit C with a "random restriction".

A "restriction" ρ of $x_1, \ldots, x_n$ is a fn $\rho : \{x_1, \ldots, x_n\} \to \{0, 1, *\}$

($*$ means don't change it)

$p \in (0,1)$ a prob.

Random restriction "$\rho \leftarrow R_p$":

indep. for each x_i,

$$x_i \to \begin{cases} 0 & \text{w.p. } \frac{1-p}{2} \\ 1 & \text{w.p. } \frac{1-p}{2} \\ * & \text{w.p. } p. \end{cases}$$

Ex: $n = 5$ draw $\rho \leftarrow R_{0.3}$:

$\rho(x_1) = *$
$\rho(x_2) = 0$
$\rho(x_3) = 0$
$\rho(x_4) = 1$
$\rho(x_5) = *$

write "$f\restriction_\rho$" to mean: apply ρ, then f.

$$f\restriction_\rho(x) = f(x_1, 0, 0, 1, x_5)$$

$$f = x_1 x_3 x_4 \vee \overline{x_2} x_5 \vee x_1 x_5 \vee x_2 x_3 x_4$$

$$f\restriction_\rho = 0 \vee x_5 \vee x_1 x_5 \vee 0$$

$$= x_5$$

width-w DNF: each term has $\leq w$ literals going in

$\wedge$ $\leq w$

$x_1\ x_7 \cdots$

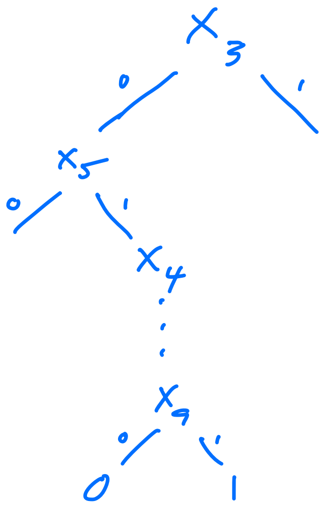
Håstad Switching Lemma: "hitting any small-width DNF or CNF w/ $\rho \in R_p$ is very likely to simplify it a lot - it will be computable by a shallow decision tree."

CNF

Let $F(x_1, \ldots, x_n)$ be a width-w DNF.
Fix any $t \geq 1$, any $p \in (0,1)$. Then

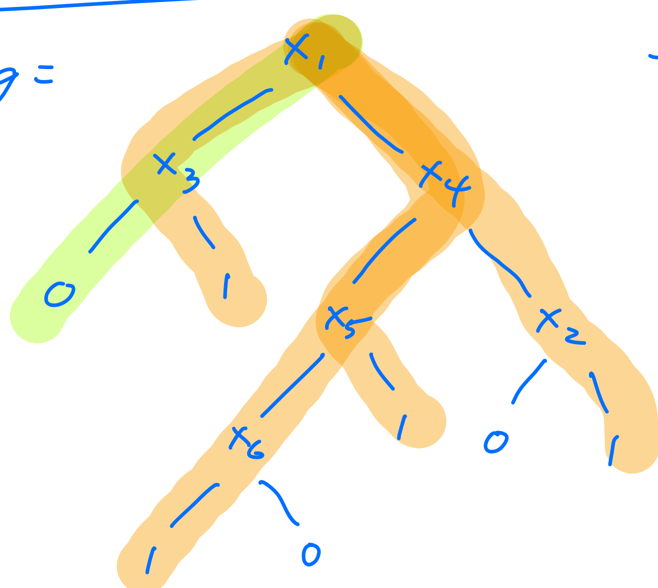
$$\Pr_{\rho \leftarrow R_p}\left[(\text{DT-depth of } f\restriction_\rho) \geq t\right] \leq (5pw)^t.$$

DT for a fn:



need $p < \frac{1}{5w}$, or useless bound

$g =$



If g has a depth-t DT, it has

- a width-t DNF

&

- a width-t CNF

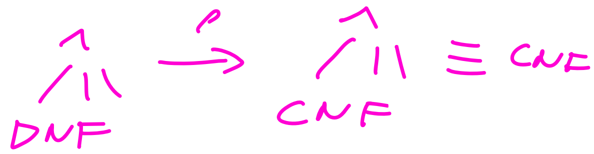
DNF: $x_1 x_3 \vee x_1 \bar{x}_4 x_5 \vee x_1 \bar{x}_4 \bar{x}_5 \bar{x}_6 \vee x_1 x_4 x_2$

CNF: $(x_1 \vee x_3) \wedge \dots$

With HSL, will repeatedly "switch" bottom 2 layers of depth-d ckt to "the other type":

$$\text{DNF} \xrightarrow{\rho} \text{CNF}$$

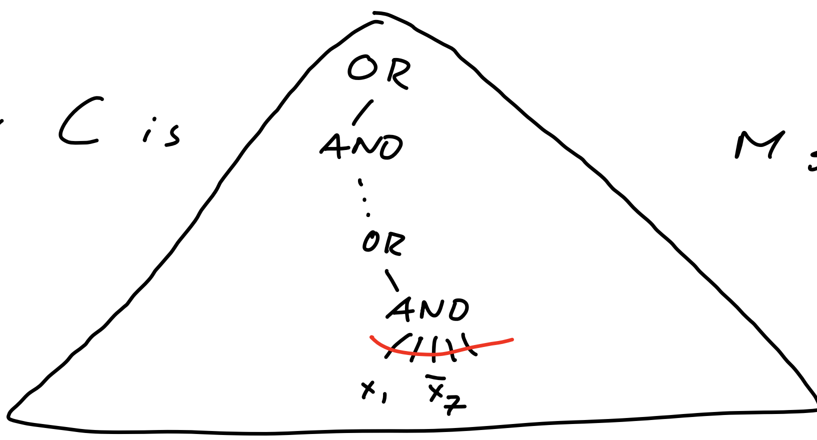
$$\text{CNF} \xrightarrow{\rho} \text{DNF}$$

then collapse: 

Reduce depth.

Meanwhile, PAR stays alive despite restrictions.

Proof that depth-d, size-M ckt C for PAR must have $M \geq 2^{\Omega(n^{\frac{1}{d-1}})}$:

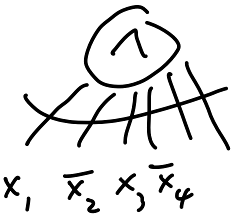
Say C is 

M gates,

Stage 0: "initial trim of fan-in"

Hit C with $\rho \leftarrow R_p$, $p = \frac{1}{100}$. What happens?

Consider any fixed bott-level AND



fanin ℓ: $\Pr[\wedge \text{ becomes } 0] \geq 1 - 2^{-\Omega(\ell)}$.

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

w.p. $> \frac{1}{2}$ (over ρ), every gate w/ fanin $> 10 \log M$ gets destroyed.

Also,

W.p. $> \frac{1}{2}$, # surv. vars. $\geq \frac{p}{2} \cdot n = \frac{n}{200}$.

So there is some ρ outcome s.t. both happen: fix it. Let C_0 = new resulting ckt.

C_0 has size $\leq M$

bott fanin $\leq 10 \log M$

C_0 computes PAR (or $\overline{\text{PAR}}$) over $\geq \frac{n}{200}$ vars.

Next time: • apply HSL + get $2^{\Omega(n^{\frac{1}{d-1}})}$ lower bd :)

- start diff pf against stronger ckt model, using polynomials.
