Last time:
- finished overview: PRG ⇒ avg-case lb
- mentioned det. approx. counting
- Boolean formulas: various worst-case lbs.
  - Shannon: non-explicit $\Omega\left(\frac{2^n}{\log n}\right)$ l.b.
  - Subbot.: $\Omega(n^{1.5})$ for PAR
  - Andr.: $\Omega(n^{2.5})$ for $A(x,y)=f_y(x)$

(dried persimmons)

rand. restr.

Today:
- a little more on formulas (KRW conj.: depth = $\Theta(\log$ size); full-basis formulas)
- start constant-depth ckts ⇝ $2^{\Omega(n^{1/d-1})}$ size l.b. for depth-d ckts

Scribe: Ekene

Questions?

Saw $\Omega(n^{2.5})$ l.b. for $A(x,y)$ form. size :)

Q: do better, by recursive constr. of hard fn... ?

KRW '95 conjecture:

Given $g: \{0,1\}^m \to \{0,1\}$

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

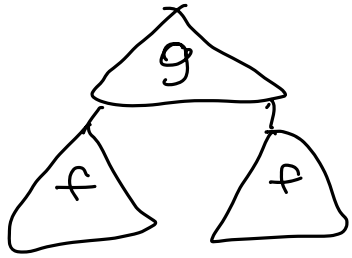
write $g \circ f: \{0,1\}^{mn} \to \{0,1\}$ for disjoint compos.

$g(f(x_1,\dots,x_n), f(x_{n+1},\dots,x_{2n}), \dots, f(x_{nm-n+1},\dots,x_{nm}))$.

Clear that depth$(g \circ f) \le$ depth(f) + depth(g):

KRW conj: in fact $\approx$ depth(f) + depth(g).

Proj. topic:



If true, we'd get strong size lb's...

Depth vs Size (of formulas)

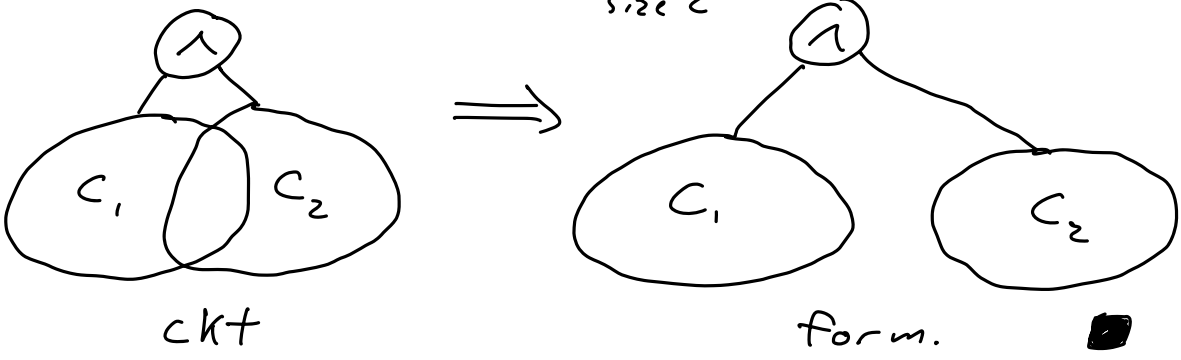
size: $A(x,y)$ — ckt: $O(n)$; form: $\Omega(n^{3-o(1)})$ } biggest known gap

depth: no gap for any f:

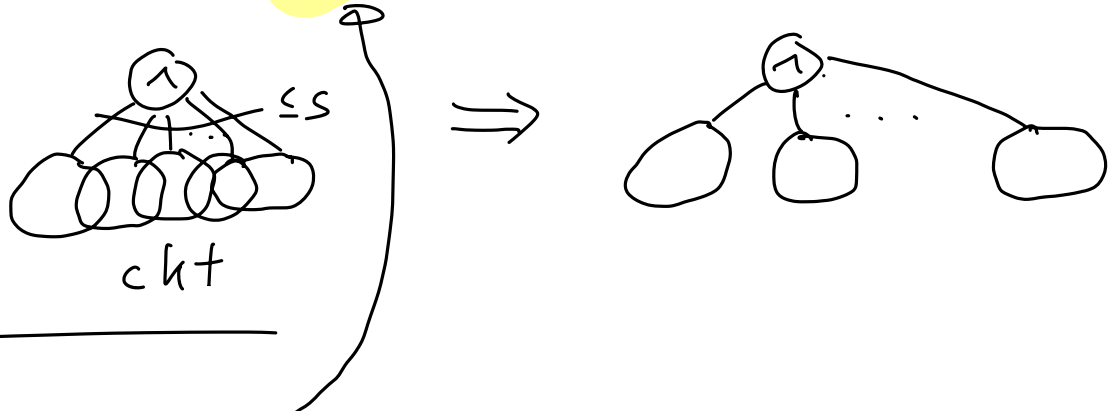
Claim: if f has a fanin-2 depth-d $\wedge/\vee/\neg$ ckt, then " " " " " " " " formula.

↳ of size 2^d

Pf:



Related claim: if f has unbounded fan-in ckt of depth d & size s, then form. of size s^d.



Q: do we need this blowup?
Rossman '14: in some settings, yes.

Project topic...

What's rel. between form. size & form. depth?

Binary $\wedge, \vee, \neg$

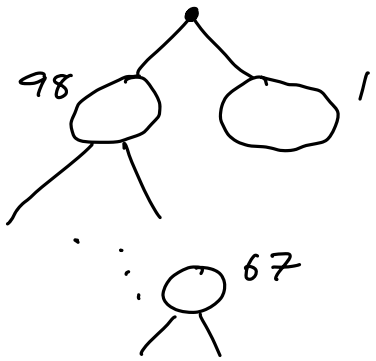
Thm: For any Bool fn f, have $\text{depth}(f) = \Theta(\log(\text{size}(f)))$.

Pf: For F a form., it's a bin. tree, so $\text{depth}(F) \geq \log \text{size}(F)$.

Other direction: to show: $\text{depth}(f) \leq O(\log(\text{size}(f)))$.

Key: Lemma: Let T be a rooted bin tree w/ s leaves. Then T has some subtree with s' leaves for some $s' \in [s/3, 2s/3]$.

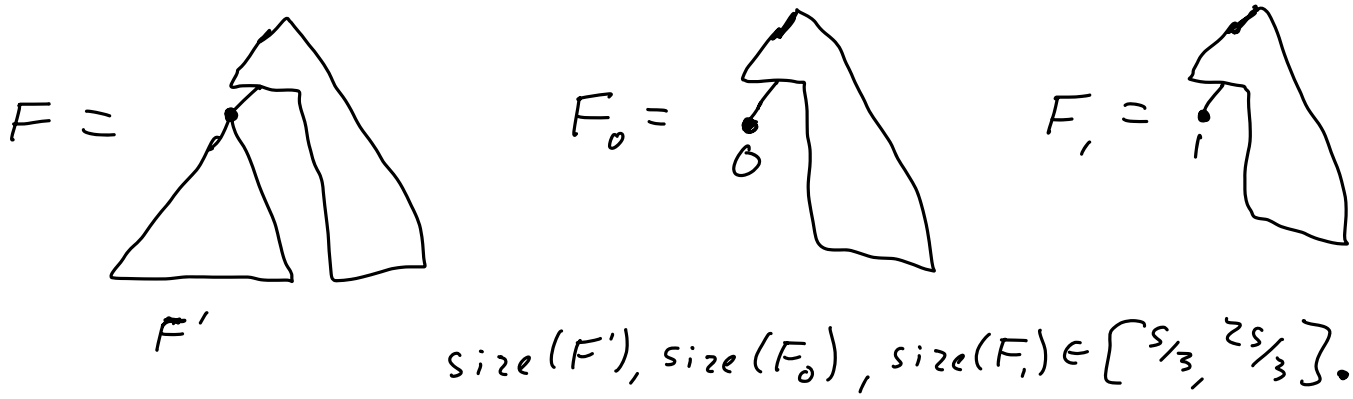
99 leaf tree



Go to larger child each time: decrease by $\geq$ half, so can't skip from $> \frac{2s}{3}$ to $< s/3$. ∎

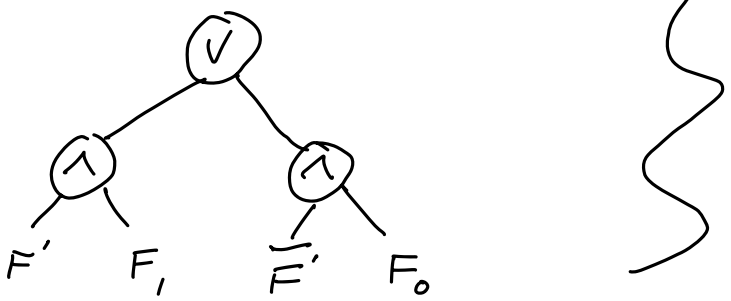
Pf of $\text{depth}(f) \leq O(\log \text{size}(f))$: Fix form. F of size s for f. Let F' be its subform. of size $s' \in [s/3, 2s/3]$.

Let $F_0 = F$ but with F' repl. by 0
$F_1 =$ " " " " " " 1.



$size(F'), size(F_0), size(F_1) \in [s/3, 2s/3]$.

Have $F = (F' \wedge F_1) \vee (\overline{F'} \wedge F_0)$.



"balancing F"

Recursively balance each of F', F_0, F_1.

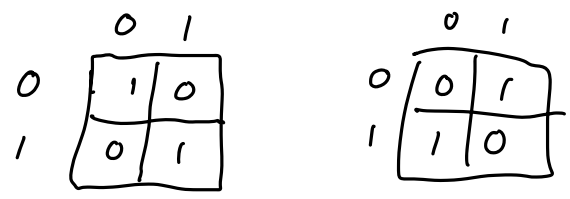
Depth? "max.

Define $D(s)$ = depth resulting from this procedure, over all size $\leq s$ formulas".

$D(s) \leq D(2s/3) + 2 \Rightarrow D(s) = O(\log s)$. ∎

Full-basis formulas: any 2-var gate is ok. Binary trees.

Same as ⊕ or ∧ or $\overline{x_i}$.



What happens?

- Shannon $\Omega\left(\frac{2^n}{\log n}\right)$ still holds
- $\oplus(x_1,\dots,x_n)$: form. size n (not $\Omega(n^{1.5})$ or n^2)

Best known l.b. for an explicit f: Neciporuk '67
$\Omega\left(\frac{n^2}{\log n}\right)$ 2 pages.

We'll do a tweak of Andre'ev fn to get $\Omega\left(\frac{n^2}{\log n \cdot \log\log n}\right)$.
(no rand restr!)

Here it is:

Let $b = \log n$, $m = \frac{n}{b} = \frac{n}{\log n}$. Define 2^n-var fn

$$A'(\underbrace{x_1,\dots,x_n}_{x},\underbrace{y_1,\dots,y_n}_{y}) = f_y(\underbrace{x_1 \wedge \dots \wedge x_m}_{\text{block 1}}, \underbrace{x_{m+1} \wedge \dots \wedge x_{2m}}_{\text{block 2}}, \dots)$$

b blocks, m vars/block.

($\wedge$ not $\oplus$ in each block)

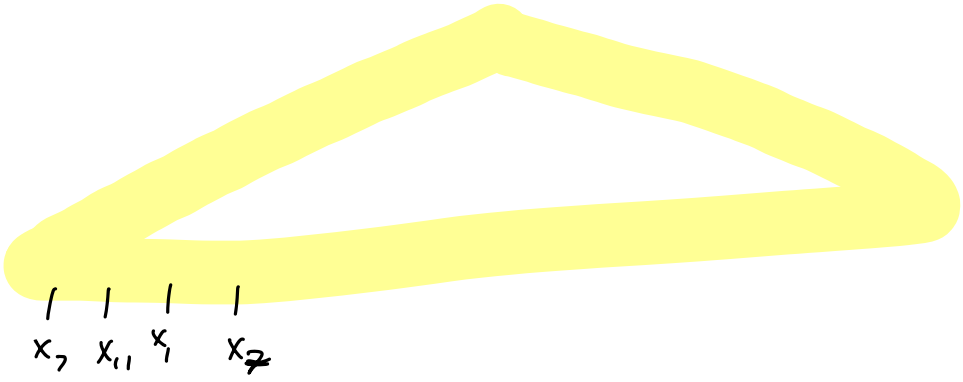
Claim: Any full-basis form. for $A(x,y)$ must have size $\geq \Omega\left(\frac{n^2}{\log n \cdot \log\log n}\right)$.

Pf Let F = min size form. for A, $\text{size}(F) = s$.

$B_1 = x_1 \dots x_m$
$\vdots$ $x_{m+1} \dots x_{2m}$ } b blocks of m vars each

$B_b = x_{n-m+1} \cdots x_n$

For each block B_i, select the var. in it w/ smallest # occurrences in F. (say $x_m, x_{2m}, \ldots$)



→ Set all others vars in each block to 1.

This causes i^{th} AND $x_{i(m-1)+1} \wedge \ldots \wedge x_{im}$ to collapse to just x_{im}.

So f_y collapsed to $f_y(x_m, x_{2m}, \ldots, x_{bm})$

For worst n-bit string y, get that form. size of $f_y \geq \Omega\left(\frac{n}{\log \log n}\right)$.

But since we picked least popular var out of the m in each block, have tot # occ. of $x_1, \ldots, x_n$ in F (i.e. s) is $\geq m \cdot \Omega\left(\frac{n}{\log \log n}\right)$, so done. ∎

$m = \frac{n}{\log n}$

Some other things that are known:

- MAJ_n requires $\Omega(n \cdot \log n)$ full-basis size.

- MCC gives $\Omega(n \cdot \log^2 n)$ for an explicit fn

"non-Neciporuk/Andre'ev" lb's.

Proj. topic

Constant-Depth-Circuits

- unbounded fan-in  $\overline{x_i}$ ckts
- depth d = small (const or slow growing fn of n)

- $AC^0_{d,s}$: size-s, depth-d ckts (s = # gates)

ONF, CNF : $d=2$ case

Motivation: • parallel time d with s processors, each proc. just does $\wedge$ or $\vee$.

• Would get results for other models from good enough lb's on AC^0. Ex:

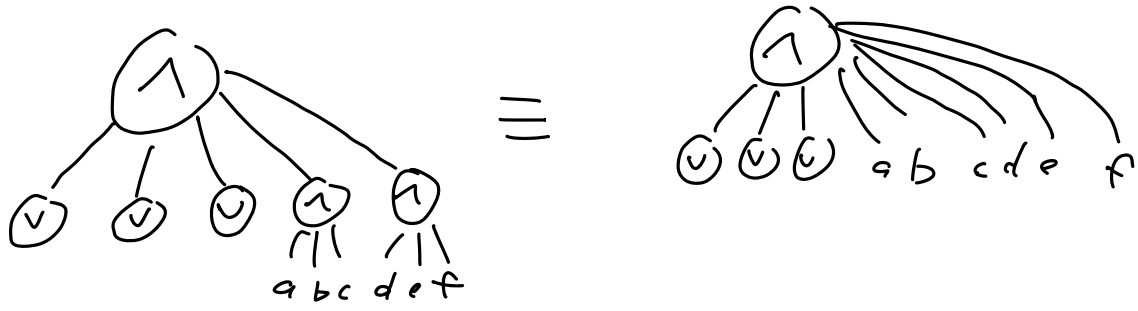
Valiant: if $f: \{0,1\}^n \to \{0,1\}$ requires any depth-3 ckt to have size $2^{\omega\left(\frac{n}{\log\log n}\right)}$, then f can't be computed by ckt that has both $O(n)$ size & $O(\log n)$ depth.

Simplifying note #1: can view our size-s

depth-d ckt as size-s^d depth-d formula.

So can consider only formulas.

Simplifying note #2: given a ↓, can assume all neg. at leaves, ∧ gates alternate:



So we can assume our ckts are in fact unbounded fan-in, alternating formulas of depth d.

Break

Intuition / u.b. / ∧ key tool for l.b.: "switching lemma".

↓

What $f: \{0,1\}^n \to \{0,1\}$ could be hard for AC^0?

↳ DNFs ($d=2$)?

Claim: Any DNF for n-var PAR

(

must have 2^{n-1} $\wedge$ gates: one for each sat. asst.

→ If ONF has a term of length $n-k$, $k \geq 1$

it can't compute PAR:

$n = 5$ ONF has $x_1 \bar{x}_2 x_3 \bar{x}_4$:

↳ as a term:

↳ accept both 10100

& 10101

but PAR shouldn't accept both

So each term in any ONF for PAR has length n, so accepts 1 sat asst, so need 2^{n-1} terms.

Likewise, any CNF for PAR must have 2^{n-1} clauses.

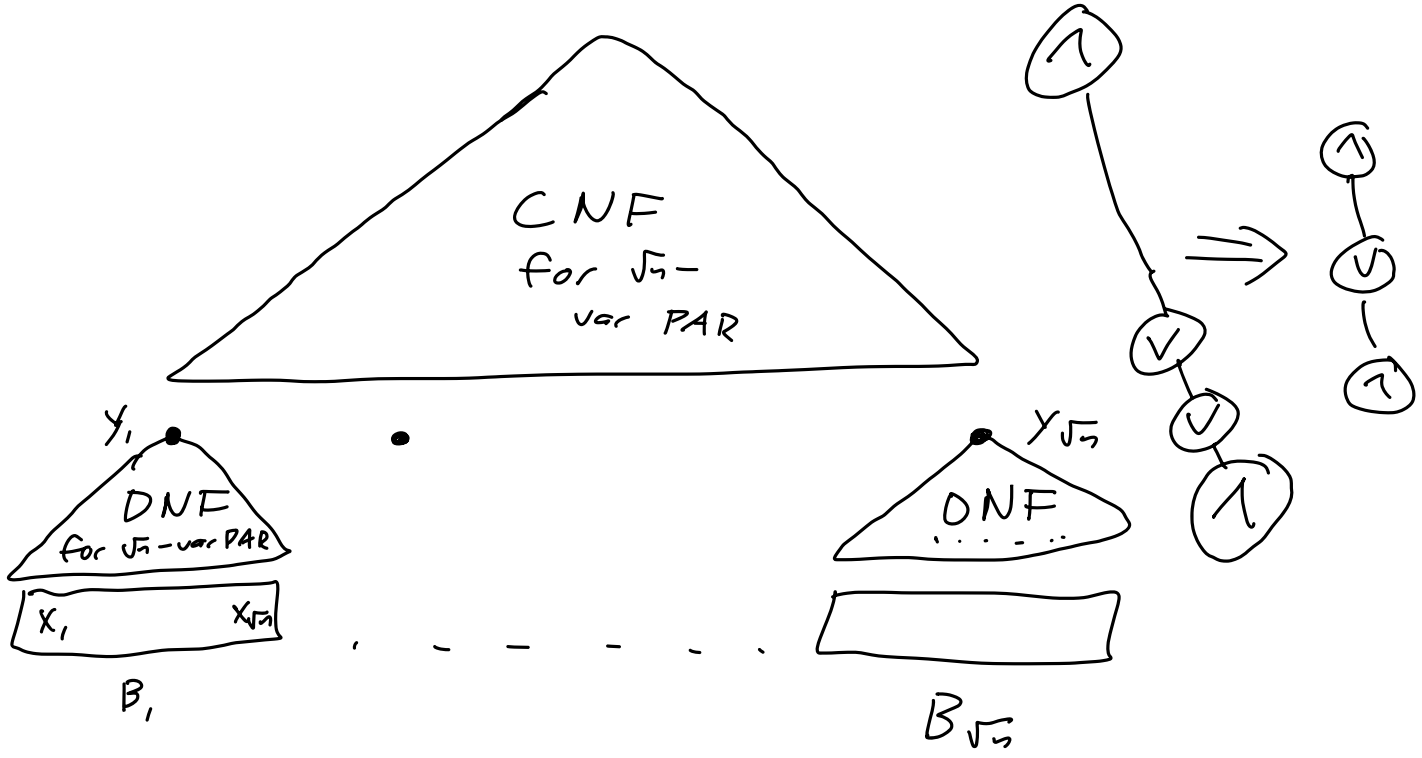
(& have ONF, CNF for PAR of size 2^{n-1}).

$d = 3$? Can compute PAR with depth-3 ckt of size $\approx 2^{\sqrt{n}}$:

- divide n inputs into $\sqrt{n}$ many $\sqrt{n}$-size blocks.
- Use ONF, of size $\approx 2^{\sqrt{n}}$, to compute PAR on each block $y_1, \ldots, y_{\sqrt{n}}$ outputs
- If use ONF for PAR$(y_1, \ldots, y_{\sqrt{n}})$: total size $\approx 2^{\sqrt{n}}$, depth 4

  Instead, use a CNF to compute PAR$(y_1, \ldots, y_{\sqrt{n}})$, &

  collapse 2 layers of $\vee$'s into one layer



Get depth 3, size $(\sqrt{n}+1)2^{\sqrt{n}}$.

Official HW problem:

$\exists$ ckt of size $\approx 2^{n^{\frac{1}{d-1}}}$, depth-$d$,

for PAR_n.

Best possible!

Thm: (Håstad '84): for $d \leq \frac{\log(n)}{\log\log n}$, depth-$d$ ckts for PAR_n must have size $2^{\Omega(n^{\frac{1}{d-1}})}$.

do have avg-case, PRGs

- FSS, Yao: earlier weaker results. } combinatorics
- Håstad: the above. Switching lemma

don't know avg case

- Razborov, Smolensky ⇝ algebraic arguments

lb's, PRGs

giving, e.g. $2^{\Omega(1/d)}$ for $\wedge/\vee/\neg/+$ ckts of depth d for mod_3, etc.

Proj topic:

Key to l.b. of Håstad: his "Switching Lemma"

Thm: (Håstad '84): for $d \leq \frac{\log(n)}{\log\log n}$, depth-$d$ ckts for PAR_n must have size $2^{\Omega(n^{\frac{1}{d-1}})}$

SL...? How does it give

Why/how is this true?

Understand $d=2$...

Dream: can we convert const-depth C for PAR to DNF or CNF for PAR, w/o increasing size too much?

If so, done, by our super-strong DNF/CNF lb's.

How to ↑? If could "flip" bottom 2 levels of C from, say, CNF to DNF, could reduce depth by 1, + repeat...?

Problem: even an $O(n)$-size CNF can require DNF size $2^{\Omega(n)}$.

$(x_1 \vee x_2) \wedge (x_3 \vee x_4) \wedge \cdots \wedge (x_{n-1} \vee x_n)$: DNF size is $2^{n/2}$.

Fix: random restrictions.

For $0 \le p \le 1$, R_p : dist. over restr. $\rho : [n] \to \{0, 1, *\}$ s.t. indep. $\rho(x_i) \to_p *$

$\to 0$ with $\frac{1-p}{2}$

$\to 1$ with $\frac{1-p}{2}$

If hit k-var AND with $\rho \sim R_p$:

$\mathbb{E}[\text{surv. vars}] = p \cdot k$ - but in fact,

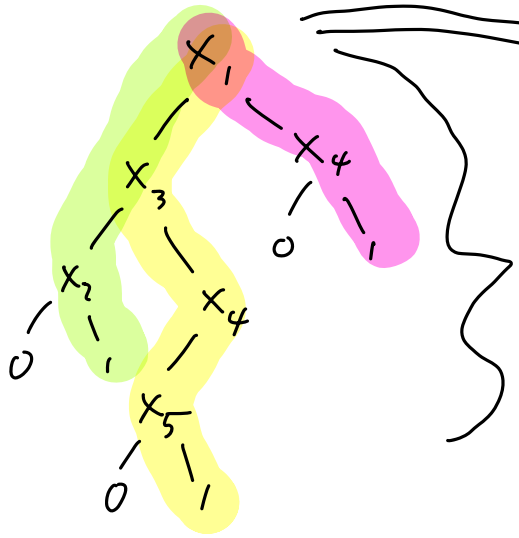
$\Pr[\text{doesn't become const-0}]$

$= \left(\frac{1+p}{2}\right)^k$.

Quick interlude on DTs vs DNFs/CNFs:

Fact: If f computed by depth-d DT T,
then " " " width-d DNF
" " " " " CNF.

Pf:



$(x_1 \wedge x_4) \vee (\bar{x}_1 \wedge \bar{x}_3 \wedge x_2) \vee$
$(\bar{x}_1 \wedge x_3 \wedge \bar{x}_4 \wedge x_5)$

depth d, so each term in DNF has width $\leq d$

Likewise for CNFs. ∎

Håstad's Switching Lemma:

CNF

Let $f(x_1, \ldots, x_n)$ be computed by a width-w DNF.
For $t \geq 1$, $0 < p < 1$,

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

- No dep. on n or size of f.
- CNF
- Only meaningful if $p < \frac{1}{7w}$, but then for $p = \frac{1}{14w}$, get 2^{-t}

Next time:
- use HSL to get $2^{\Omega(n^{\frac{1}{d-1}})}$ l.b.
- pf of weak SL
- " " actual SL.