COMS 6998

Last time:
- overview of some restricted comput. models we'll consider; worst-case, avg-case lb's; PRGs
- PRG ⇒ worst-case lb

Today:
- finish overview: PRG ⇒ avg-case lb
- det. approx. counting
- ✡ Boolean formulas: various worst-case lbs.

Scribe(s): Yiming Li

Questions?

Lemma: (PRG ⇒ average-case lb)

Let $\mathcal{C}$ be a class of n-bit fns f s.t. $\mathcal{C}$ closed under restrictions

Let $G: \{0,1\}^s \to \{0,1\}^n$ be ε-PRG for $\mathcal{C}$, where $s < n$, $\varepsilon < 1/2$. Let $r = s + \log\frac{1}{\varepsilon} \leq n$.

Define $h: \{0,1\}^r \to \{0,1\}$ as outputting 1 on x if some string in range of PRG starts with x:

$$h(x) = 1 \quad \text{iff} \quad \exists\, y \in \{0,1\}^s,\ z \in \{0,1\}^{n-s-1} \text{ s.t. } G(y) = (x, z)$$

(y: s bits; x: r bits; z: $n-r$ bits)

Let $\mathcal{C}'$ be all restric. of fns in $\mathcal{C}$ by fixing last $n-r$ bits, leaving first r alive.

Let $\mathcal{D} = \frac{1}{2}\cdot \mathcal{U}_r + \frac{1}{2} G(\mathcal{U}_s)_{1:r}$. → over $\{0,1\}^r$

Then h is ε-hard for $\mathcal{C}'$ w.r.t. $\mathcal{D}$. ← avg-case lb!

Pf: Let $\mathcal{U} \sim \mathcal{U}_r$ (unif. over $\{0,1\}^r$), $\mathcal{U}' \sim \mathcal{U}_s$ ($\{0,1\}^s$)

$r = s + \log\frac{1}{\varepsilon}$.

Fix any $f \in \mathcal{C}'$, say $f(x) = f_0(x, a)$ some fixed $a \in \{0,1\}^{n-r}$, some $f_0 \in \mathcal{C}$.

Then

$$\Pr_{X\sim\mathcal{D}}[f(X)=h(X)] = \frac{1}{2}\Pr[f(\mathcal{U})=h(\mathcal{U})] + \frac{1}{2}\Pr[f(G(\mathcal{U}')_{1:r}) = h(G(\mathcal{U}')_{1:r})]$$

($h(G(\mathcal{U}')_{1:r}) = 1$, so)

$$= \frac{1}{2}\Pr[f(\mathcal{U})=h(\mathcal{U})] + \frac{1}{2}\Pr[f(G(\mathcal{U}')_{1:r})=1]$$

$$\le \frac{1}{2}\Pr[f(\mathcal{U})=0] + \frac{1}{2}\Pr[h(\mathcal{U})=1] + \frac{1}{2}\left(\Pr[f(\mathcal{U})=1] + \varepsilon\right)$$

($f=h=0$ or $f=h=1$; $f \in \mathcal{C}' \le \mathcal{C}$ + G^{ε} fools $\mathcal{C}$)

$2^r = 2^{s+\log\frac{1}{\varepsilon}} = \frac{1}{\varepsilon}\cdot 2^s$

$$= \frac{1}{2} + \frac{\varepsilon + \mathbb{E}[h]}{2} \le \frac{1}{2} + \frac{2\varepsilon}{2} = \frac{1}{2} + \varepsilon.$$

Can similarly argue: $\Pr_{X\sim\mathcal{D}}[f(X)=h(X)] \ge \frac{1}{2} - \varepsilon$.

$\therefore$ $h=1$ on 2^s of 2^r inputs

■

So....

WC LB (s_0, s_t, q, s_ε), then Corr. bds, then PRG's.

AC LB (t, q, s_ε)

Weird uncle: Deterministic Approximate Counting algs.

PRGs nice b/c they let us derandomize obliviously ...

the 2^s n-bits outputs fool every $f \in \mathcal{C}$ w/o looking at f.

If you know what f is, could conceivably use it...

you want $\mathbb{E}[f] \pm \varepsilon$

(D) → (Deterministic Approx. Count)

Def: (DAC) Let $\mathcal{C}$ be a class of representations of fns $\{0,1\}^n \to \{0,1\}$.

An alg. is an ε-DAC for $\mathcal{C}$ if it's det. $\forall$, on input any $F \in \mathcal{C}$, outputs a value in

$$\left[\mathbb{E}[F(\mathcal{U})] - \varepsilon,\ \mathbb{E}[F(\mathcal{U})] + \varepsilon\right].$$

Can show: if have poly(n)-time $(\varepsilon = 0.1)$-DAC for $\mathcal{C} = \{\text{all poly}(n)\text{-size ckts}\}$, then $P = BPP$.

Fact: For various $\mathcal{C}$'s, can give ε-DAC's which are faster than $2^s \cdot \text{poly}(n)$, where

s = seed length of best known ε-PRG.

Conventions:

$|a-b| \le \varepsilon \iff \boxed{a \approx_\varepsilon b}$

$\mathcal{U}_s$: unif. over $\{0,1\}^s$

$\{\pm 1\}^s$

$\mathbb{E}[f]$ means $\mathbb{E}[f(\mathcal{U})]$

Scribe:

Use **bold** for random vars ☺

$\mathbb{E}[f(\mathbf{x})]$

Unit: Bool. Formulas

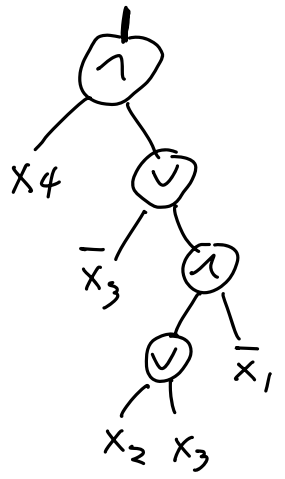
(worst-case lbs)

(readings on web).

Basics: Def: Bool. formula: rooted bin. tree with

- leaf nodes (lab. with x_i or $\bar{x}_i$)
- internal nodes (lab. $\wedge$ or $\vee$) binary

($\mathcal{U}_2$ basis, de Morgan)

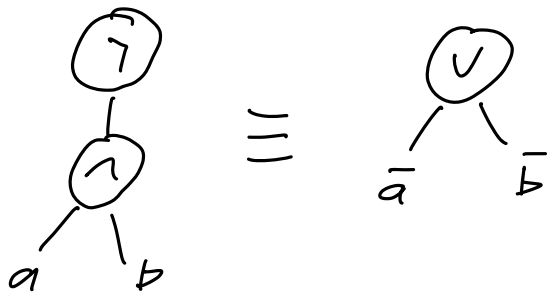


Form. on $\{0,1\}^n$ computes a fn in obvious way.

Size of formula F = # leaves
$= (\#\text{ int. } + 1)$

depth = length of longest root-to-leaf path.

WLOG all negations at leaves:



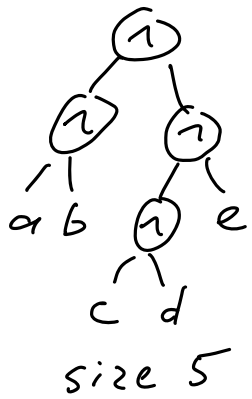
Def: Given $f: \{0,1\}^n \to \{0,1\}$,

formula size — size(f) = size of smallest F computing f

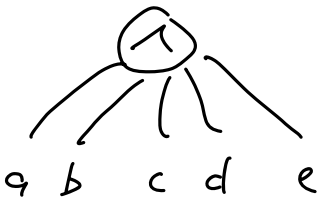
" depth — depth(f) = depth " " " " " " .

(Sometimes: unbounded fan-in allowed.

Size unchanged



size 5



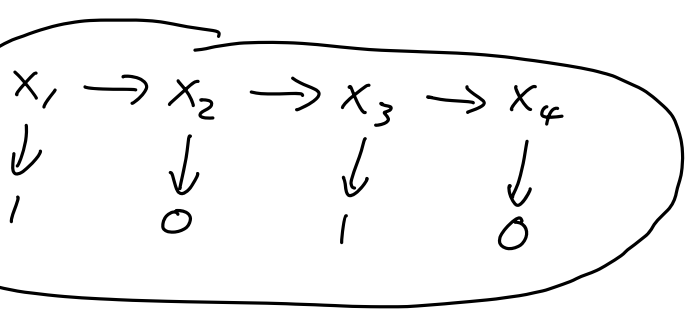
depth changes.

DNF, CNF: depth-2
unbounded fan-in.

Ex: "decision list" function:

This

if $x_1 \to 1$
else if $x_2 \to 0$
" " $x_3 \to 1$
⋮

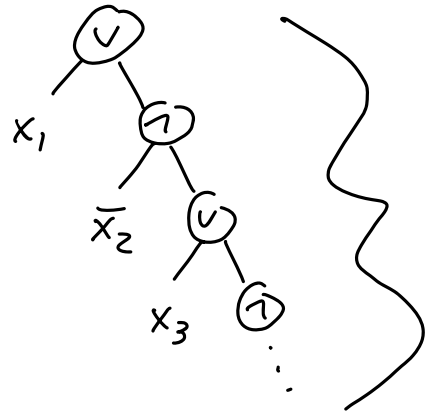


Formula:

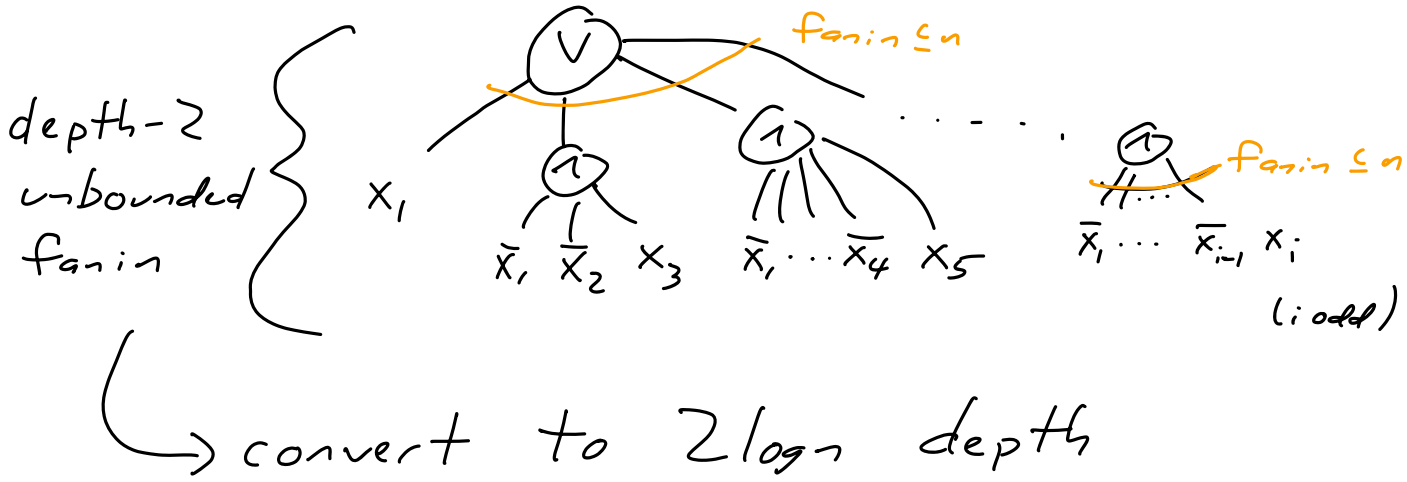
$$x_1 \vee (\bar{x}_2 \wedge (x_3 \vee (\bar{x}_4 \wedge (\dots))\dots)$$

size = n , min. possible so size(f) = n ☺

→ depth(this F) = n



$O(\log n)$ depth F for this fn: DNF.

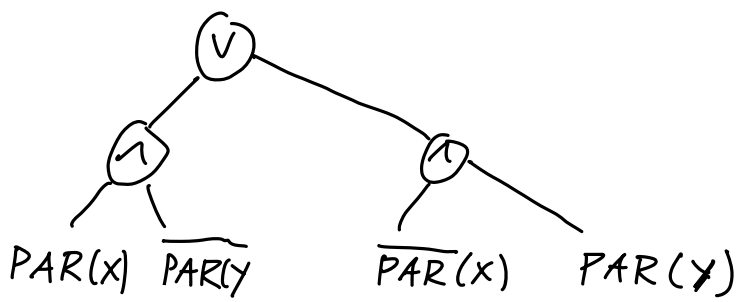


↳ convert to $2\log n$ depth $\Theta(n^2)$ size formula.

Ex 2: Parity fn $f(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i \bmod 2$

Recursive: $\frac{n}{2}$ bits each

$PAR(X, Y) =$



$s(i)$ = size for i vars

$s(1) = 1$ $\quad s(2i) = 4s(i)$

$s(n) = n^2$. Optimal!

FACT: There are $O(n)$-size ckts for PAR_n.

We'll do $\Omega(n^{1.5})$ lower bound, using PRG-relevant techniques.

Shannon's (exponential!) lower bd on formula size.

via counting arguments

Fact: There are 2^{2^n} many $f: \{0,1\}^n \to \{0,1\}$.

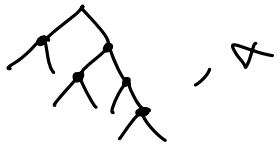
Thm (Shannon): $1 - 2^{-n}$ fraction (actually more) of all n-bit $f: \{0,1\}^n \to \{0,1\}$ have form. size$(f) \geq 2^n/(2\log n)$.

Pf: We show: for $s = \frac{2^n}{2\log n}$,

$$(\#\text{ of Bool. for}_n\text{. of size } s \text{ over } x_1, \ldots, x_n) \ll 2^{2^n} \cdot \frac{1}{2^n}.$$

Here's why:

Any formula F specified by

Ⓘ • tree struc. of binary tree 

Ⓘⓘ • labels of all nodes.

We'll bd # specifications.

Ⓘ: s-leaf form. has $s-1$ internal nodes.

Can describe any such tree as elt of

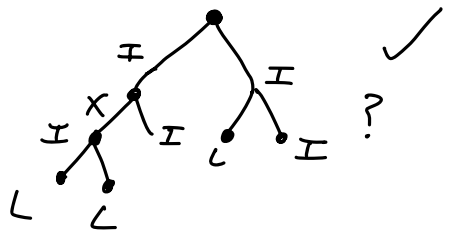
$$\{II, IL, LI, LL\}^{s-1}$$

I = internal

L = leaf (1st child, 2nd child)

✓ ✗ ?

II II ⌞I ⌞⌞ :



✓

?

Every tree has ! such a descrip., so # tree struc w/ s-1 int. nodes $\leq 4^{s-1}$. (good enough)

(II) #labelings: 2^{s-1} for s-1 int. nodes (i) (v)

$(2n)^s$ for s leaves $x_1, \ldots, \overline{x_n}$.

So # size-s form. over $\{0,1\}^n$ is $\leq$

$$\underbrace{4^{s-1}}_{\#\text{trees}} \cdot \underbrace{2^{s-1} \cdot (2n)^s}_{\#\text{labels}} \leq (16n)^s$$

For $s = \frac{2^n}{2\log n}$, this is

$$(16n)^{2^n/2\log n} = 2^{2^n \cdot \frac{(\log n)+4}{2\log(n)}} \overset{\text{for } n \text{ suff large}}{<} 2^{0.51 \cdot 2^n}$$

$$<< 2^{2^n} \cdot \frac{1}{2^n}.$$

Note: DNF or CNF for f: $\leq 2^{n-1}$ terms

n lit / term, so easy $n \cdot 2^{n-1}$ u.b.

OFFICIAL HW PROBLEM:

extend to avg-case l.b. under $\mathcal{U}$.

This l.b. not satisfying: not explicit.

Break

Subbotovskaya's lower bound via random restrictions → for an explicit fn !

Sub. '61: analyzed effect of random restrictions on Bool. formulas.

Idea: given form F computing $f(x_1, \ldots, x_n)$

- set some of inputs x_i to 0/1 values, leaving rest "free"
- Argue this shrinks F "by a lot", yet size after restric. ≥ 1.

This means size(F) must have been large!

Def A restriction ρ is a mapping $[n] \to \{0, 1, *\}$

ρ is a partial assignment to vars $x_1, \ldots, x_n$;

$i \to *$: x_i is left unassigned.

$$\rho \in \{0,1,*\}^n.$$

We write $f\restriction_\rho$ to denote restric. of f by ρ.

Ex: $\rho = (1,0,1,*,*,1)$, f is 6-var f_n,

$f\restriction_\rho(x) = f(1,0,1,x_4,x_5,1)$. ("zoom in" on subcube of f)

Let R_k denote dist. over restrictions: following
choose k vars u.a.r. for $*$,
other $n-k$ get 0/1 $\$$

Thm: (Sub.) Let $f: \{0,1\}^n \to \{0,1\}$, let $\rho \leftarrow R_k$.
w.p. $\geq 3/4$ (over ρ),

$$\text{size}(f\restriction_\rho) \leq 4 \cdot \left(\frac{k}{n}\right)^{3/2} \cdot \text{size}(f).$$

Applic: Let $k=1$, let $f = PAR_n$.

$f\restriction_\rho$ is x_i or $\overline{x_i}$ so $\text{size}(f\restriction_\rho) = 1$.

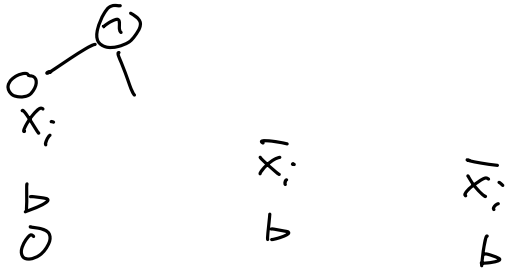
so $1 \leq 4 \cdot (1/n)^{3/2} \cdot \text{size}(f)$ $\quad \not\downarrow$

$\text{size}(f) \geq \frac{1}{4} \cdot n^{3/2}$ $\quad \cup$

Pf of ★: Let F be opt (smallest) form. for f. $size(F) = s$.

View ρ as constr. in $n-k$ stages:
each stage - pick un-fixed var at rand., pick 0/1, assign. Analyze one stage: what happens to F?

1st stage: pick x_i. $b \in \{0,1\}$

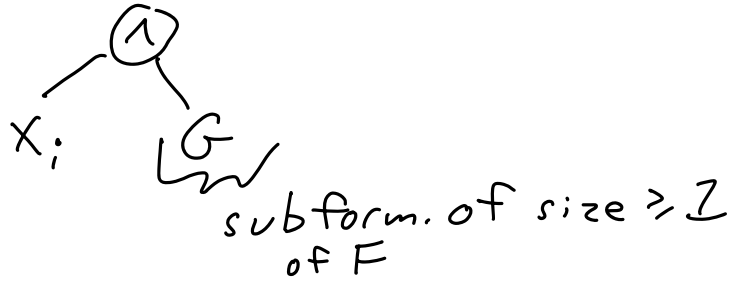


Fixing x_i to b, all inst. of x_i or $\bar{x}_i$ vanish.

$\mathbb{E}[\#\text{occ. of } x_i \text{ or } \bar{x}_i] = \frac{s}{n}$. So $\mathbb{E}[\text{size of } F]$ shrinks by s/n ☺

Key: F shrinks by *more* (in expectation).

Consider any occurrence of x_i or $\bar{x}_i$ in F, i.e.



G doesn't have any x_i or $\bar{x}_i$: G only matters if $x_i = 1$, + then by repl. any x_i ($\bar{x}_i$) in G with 0, would have smaller form (contrad.).

w.p. $\frac{1}{2}$ $x_i \leftarrow 0$, & then G vanishes, so ≥ 1 more lit. vanishes.

So $\mathbb{E}[\#$ lit. vanish b/c of this "secondary effect"$] \geq \frac{1}{2} \cdot \frac{s}{n}$.

And $\mathbb{E}[$size of $F|_\rho$ after 1st stage$] \leq s - \frac{3}{2}\frac{s}{n}$

$$= s\left(1 - \frac{3}{2n}\right)$$

$$\leq s \cdot \left(1 - \frac{1}{n}\right)^{3/2}.$$

Repeat (on opt. form. each time).

2nd step: $n-1$ vars, so $\mathbb{E}[$size after 2 stages$]$

$$\leq s \cdot \left(1 - \frac{1}{n}\right)^{3/2} \cdot \left(1 - \frac{1}{n-1}\right)^{3/2}$$

$$= s \cdot \left(\frac{n-1}{n}\right)^{3/2} \cdot \left(\frac{n-2}{n-1}\right)^{3/2}$$

So after $n-k$ stages,

$$\mathbb{E}[\text{size}] \leq s \cdot \left(\frac{n-1}{n}\right)^{\frac{3}{2}} \cdots \left(\frac{k}{k+1}\right)^{\frac{3}{2}} = s \cdot \left(\frac{k}{n}\right)^{3/2}.$$

Markov: w.p. $\geq 3/4$ size$(f|_\rho) \leq 4 \cdot s\left(\frac{k}{n}\right)^{3/2}$

History: Γ = "shrinkage exponent"
= best # in place of $3/2$ s.t. still true.

$\Gamma \leq 2$ (PAR)

Nisan-Impagliazzo '91: $\Gamma \geq 1.55$

Paterson-Zwick '91: $\Gamma \geq 1.63$

Hastad '93: $\Gamma \geq 2 - o(1)$

Tal '14: better $o(1)$.

Project topic?

Andre'ev's lower bound

↳ '87: clever way to get $n^{\Gamma+1}$ form. size l.b. for an explicit f.

We saw: there's an n-var fn with form. size $\geq \frac{2^n}{2 \log n}$.

Scale down to $b := \log_2 n$ vars:

there's some $(\log n)$-var fn requiring form. size $\gtrsim \frac{n}{\log \log n}$. Call this $\psi(x_1, \ldots, x_b)$ $_{\log n}$.

Warmup to Andre'ev fn:

Let $m = \frac{n}{b} = \frac{n}{\log n}$.

View $x_1, \dots, x_n$ as b blocks of m vars / block.
Define $f_\psi : \{0,1\}^n \to \{0,1\}$ as

$$f_\psi(x_1, \dots, x_n) = \psi(\overline{x_1 \oplus \dots \oplus x_m}, \overline{x_{m+1} \oplus \dots \oplus x_{2m}}, \dots, \overline{x_{n-m+1} \oplus \dots \oplus x_n}).$$

Apply (Sub. thm) to f_ψ, using $K = b \cdot \ln(4b)$
(so $\rho \sim R_K$ leaves $b \cdot \ln(4b)$ vars alive, $*$).

$\to$: w.p. $\geq 3/4$ over $\rho \sim R_K$, have

(*) $\text{size}(f_\psi \restriction_\rho) \leq 4 \cdot \left(\frac{K}{n}\right)^r \cdot \text{size}(f_\psi)$.

Also have:

Claim: w.p. $\geq 3/4$ over $\rho \sim R_K$, ρ assigns ≥ 1 (#)
$*$ to each block.

Pf: Calculation: Fix a block $i \in [b]$.

$$\Pr_\rho[\text{block } i \text{ gets no } * \text{ under } \rho] = \frac{\binom{n-m}{K}}{\binom{n}{K}} \leq \left(\frac{n-m}{n}\right)^K$$

$$= \left(1 - \frac{1}{b}\right)^{b \cdot 4\ln(b)} \leq \frac{1}{4b}.$$

UB over all b blocks

So w.p. $\geq \frac{1}{2}$, $\rho \sim R_K$ sat. (*) $\forall$ (#).

Fix any such ρ. For such a ρ,

$f_\psi|_\rho$ has ψ as a subfunc., so

$$\text{size}(f_\psi|_\rho) \geq \text{size}(\psi) \geq \frac{n}{\log\log n}.$$ So,

$$\frac{n}{\log\log n} \leq \text{size}(\psi) \leq \text{size}(f_\psi|_\rho)$$

$$\leq 4\left(\frac{K}{n}\right)^\Gamma \cdot \text{size}(f_\psi)$$

$$= 4 \cdot \left(\frac{(\log n)\cdot \ln(4\ln n)}{n}\right)^\Gamma \cdot \text{size}(f_\psi).$$

So $\text{size}(f_\psi) = \tilde{\Omega}(n^{\Gamma+1})$.

This f_ψ is not explicit...

Trick: give ψ as input.

View $\psi(x_1,\dots,x_b)$ as $(2^b = n)$-bit string;

for any $y \in \{0,1\}^n$ (view as b-bit fn),

have $$f_y(x_1,\dots,x_m) = y(x_1\oplus\dots\oplus x_m, \dots, x_{n-m+1}\oplus\dots\oplus x_n).$$

□

Andreev's actual fn:

$A(\overset{n \text{ bits}}{x,y}) =$ _____.

Some $y \in \{0,1\}^?$ gives $\chi_?$ so

so size $(A(x,y)) \geq$ size $(f_\chi) \geq \tilde{\Omega}(n^{\lceil +1 \rceil})$.

A is in P: in fact,

OFFICIAL HW PROBLEM:

Show $A(x,y)$ is computable by

$O(n)$-size ckt.

A has
- ckt size $O(n)$
- form. size $\tilde{\Omega}(n^3)$

} biggest gap known!

Proj topic: KRW conjecture.
