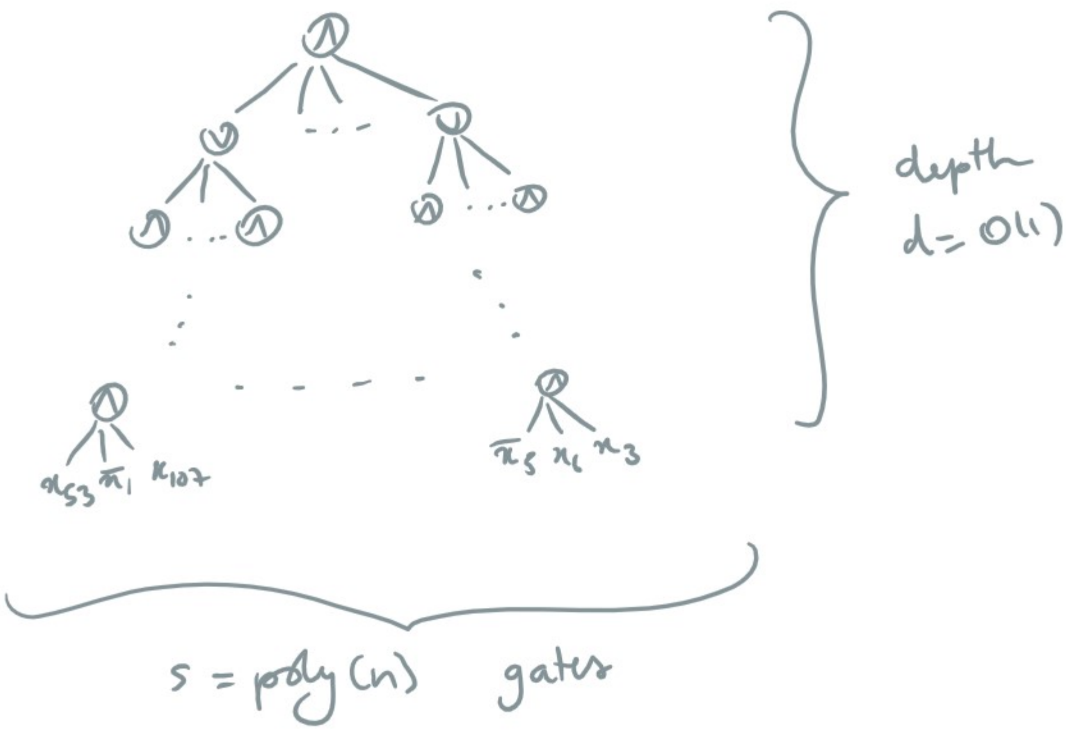
Furst-Saxe-Sipser

Friday, November 4, 2022 12:09

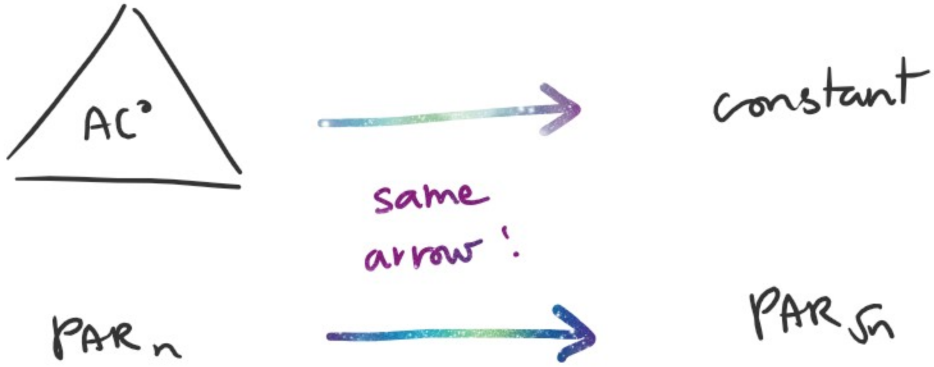
Theorem

$\mathrm{PAR} \notin AC^0$

i.e. $x_1 \oplus \cdots \oplus x_n$ cannot be computed by



Proof plan : magic



Random restrictions

For each variable:

- w.p. p, keep it alive ($*$)
- o/w, fix it ($0/1$ w.p. $\frac{1-p}{2}$ each)

e.g. $\rho = (0, 1, 1, *, 0, \dots, *, 1)$

$$\underset{\{0,1\}^n \to \{0,1\}}{f} \xrightarrow{\rho} \underset{\{0,1\}^{\text{stars}(\rho)} \to \{0,1\}}{f|_\rho}$$

Proof plan: magic

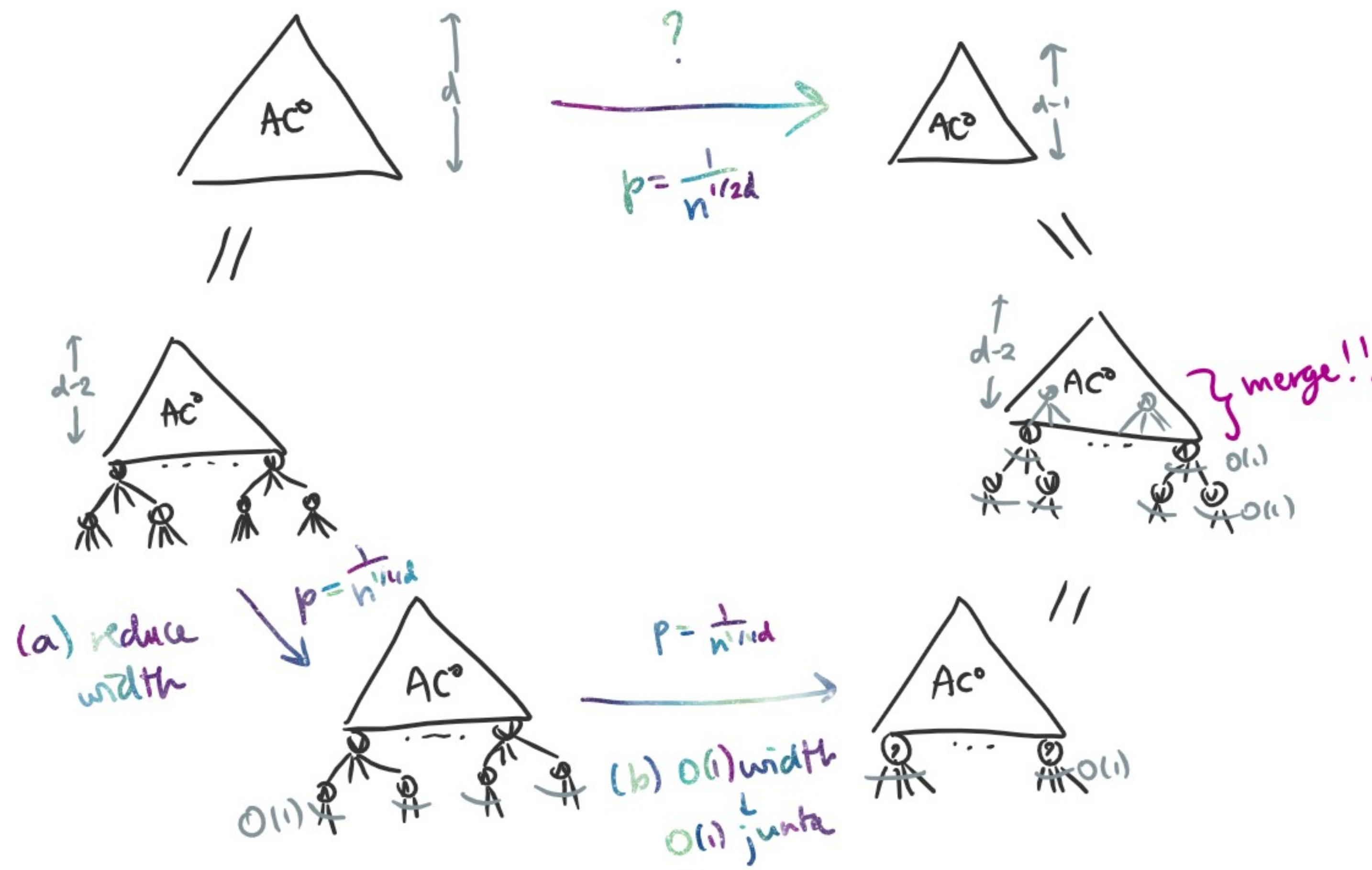
$$AC^0 \xrightarrow{\text{"hard" part}} \text{constant}$$

random restriction with $p = \frac{1}{\sqrt{n}}$

$$PAR_n \xrightarrow[\text{clear}]{} PAR_{\sqrt{n}}$$

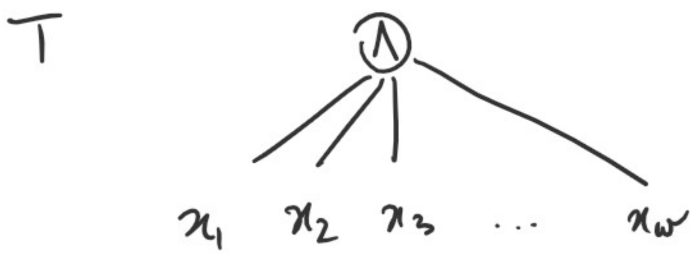
* or at least, clear that not constant whp

Intermediate goal : reduce depth



(do this on the other whiteboard)

Step (a) : reduce width



ρ : 1 0 * 1

if get any 0's, whole $\wedge$ collapses to 0

if get a 1, disappears

If get a 1, disappears

$\nearrow$ wide? likely to collapse

$\searrow$ narrow? few stars

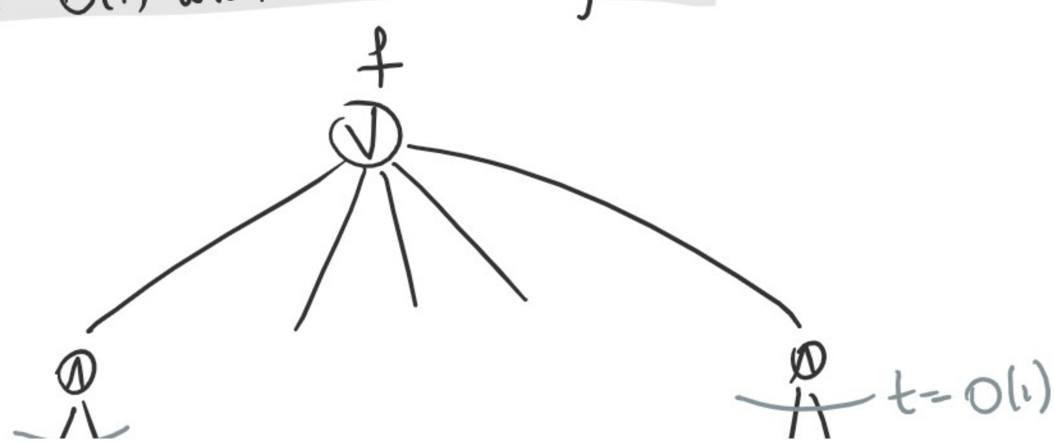
$$\to \Pr[T|_\rho \not\equiv 0] \le (\text{chance of } \rho_i \text{ not } 0)^w$$
$$\le (3/4)^w$$

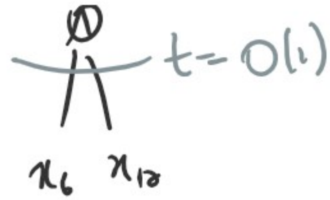
$\Rightarrow$ WLOG, $w \le 10 \log s = O(\log n)$

$$\to \Pr[\#\text{stars} \ge t] \le \binom{w}{t} p^t$$
$$= \binom{O(\log n)}{t} n^{-\Omega(t)}$$
$$= n^{-\Omega(t)}$$

$\Rightarrow$ get $O(1)$ stars wp $\ge 1 - \frac{1}{s^{10}}$

Step (b): $O(1)$ width $\to$ $O(1)$-junta





<u>Idea</u> : treat those $\wedge_{O(1)}$ as (biased) input vars and do the same thing

any of them has a $\Omega(1)$ chance to

but correlated :(

- many$^{\geq r}$ <u>disjoint</u> terms? likely to collapse
- few disjoint terms? Can reduce width !

$$\rightarrow \Pr[f|_\rho \not\equiv 1] \leq (\text{chance of } T|_\rho \not\equiv 1)^r$$
$$\leq (1 - 1/4^t)^r$$
$$\leq (1 - \Omega(1))^r$$
$$\leq 2^{-\Omega(r)}$$

$\Rightarrow$ WLOG, $r \leq O(\log s)$

→ Get $r = O(\log s)$ terms $T_1, \dots, T_r$ that intersect with every term.

And $\Pr[\# \text{stars in } T_1, \dots, T_r \geq l]$

$$\leq \binom{O(r)}{l} p^l$$

$$\leq n^{-\Omega(l)}$$

so get $l \leq O(1)$ stars whp.

$\Rightarrow$ Just query those $l = O(1)$ stars and recurse on the 2^l possible assignments to decrease width by 1.

If had width t, will get junta on $\sim (2^l)^t = O(1)$ variables.

(and then make it a CNF, getting $2^{2^{O(lt)}}$ blowup

$\Rightarrow$ need $2^{2^{O(lt)}} \leq s$ but $l, t \geq d \frac{\log s}{\log n}$

$\Rightarrow$ works as long as $\frac{\log s}{\log n} < \frac{\sqrt{\log \log s}}{d}$

$\Longleftrightarrow s < n^{\frac{\sqrt{\log \log n}}{d}}$)

Last steps

- $2d$ r.r.'s with $p = \frac{1}{n^{1/4d}}$ $\equiv$ one r.r. with $p = \sqrt{n}$
- once get to $d=2$, get

Statements of switching lemmas

$$\Pr[f|_\rho \text{ not width-}t] \leq s \cdot O(p)^{\Omega(t)}$$

$$\Pr[f|_\rho \text{ not } c\text{-junta}] \leq s \cdot O(p)^{\Omega\left(\frac{\log c}{t}\right)}$$

$$\leq s \cdot O(p)^{\Omega(\sqrt{\log c})}$$

b/c $\ell = \frac{\log c}{t}$