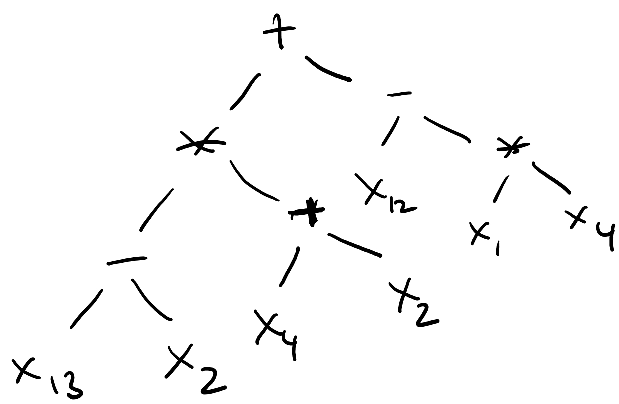
CC-Lecture-20-5-2020

20 May, 2020 10:10

- $NEXP \not\subseteq ACC^0$

Barrington, Ben-Or & Cleve

$r_1 \leftarrow x_{12} * x_2$
$r_2 \leftarrow x_4 + x_2$
$r_3 \leftarrow r_2 * r_1$
$r_4 \leftarrow x_1 * x_4$
$r_5 \leftarrow x_{12} - r_4$
$r_6 \leftarrow r_5 + r_3$



$R \quad +, -, *$

$R, +,$

register model: $r_1, r_2, r_3, \ldots r_k$ ... working registers
$x_1, x_2, \ldots \; x_n$ ... input registers

ring $(R, +, \cdot)$ R finite / infinite

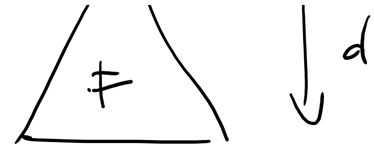
R ... $n \times n$ matrices over $GF[2]$
R ... $GF(2)$
R ... $GF[p]$

instructions

$r_i \leftarrow r_j \pm r_k$ r_j, r_k can be also input registers

$r_i \leftarrow r_j$

- length of the pgm
- # working r's uses



- # working it uses

<u>**Thm**</u> (Ben-Or, Cleve)

Any formula F of depth d can be ~~ev~~ evaluated by a register pgm of length 4^d & using 3 working registers.

Pf:

$$r_i \leftarrow r_i \pm r_j * r_k \qquad j,k \neq i$$

$$r_i \leftarrow r_i \pm x_j \qquad \text{WLOG}$$

$$\begin{pmatrix} r_i \leftarrow r_i + r_j * r_k \\ r_i \leftarrow r_i - r_j * r_k \end{pmatrix}$$

Goal: $F = f(x_1,\dots,x_n)$ $\left[r_1 \leftarrow r_1 \pm \underline{r_2} * f(x_1,\dots x_n) \right] \leftarrow P$

initially set: $r_1 \leftarrow 0$

$r_2 \leftarrow 1$

$r_1 \overset{P}{=} f(x_1 \dots x_n)$

- $\underline{F = x_i}$ $\qquad r_1 \leftarrow r_1 + r_2 * x_i \leftarrow P$
- $F = \underset{P_1}{f(x_1 \dots x_n)} + \overset{P_2}{g(x_1 \dots x_n)}$

$$\left.\begin{array}{ll} r_1 \leftarrow r_1 + r_2 * f(x_1, \dots x_n) &] \; P_1 \\ r_1 \leftarrow r_1 + r_2 * g(x_1, \dots x_n) &] \; P_2 \end{array}\right\} P$$

- $F = f(x_1, \dots x_n) * g(x_1, \dots x_n)$

1. $r_3 \leftarrow r_3 + r_2 * f(x_1 \dots x_n)$] P_1

2. $r_1 \leftarrow r_1 + r_3 * g(x_1 \dots x_n)$] P_2' $\quad r_1 + \boxed{r_3 * g(x_1 \dots x_n)} + r_2 * f * g$

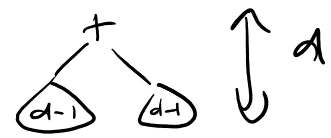
3. $r_3 \leftarrow r_3 - r_2 * f(x_1 \dots x_n)$] P_1' $\quad r_3$

4. $r_1 \leftarrow r_1 - r_3 * g(x_1 \dots x_n)$] P_2'' $\quad r_1 + r_2 * f * g$

→ 3 registers

→ length ?

$|length| \leq 4^d$

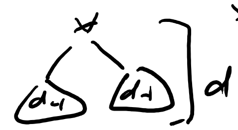


"x_i"

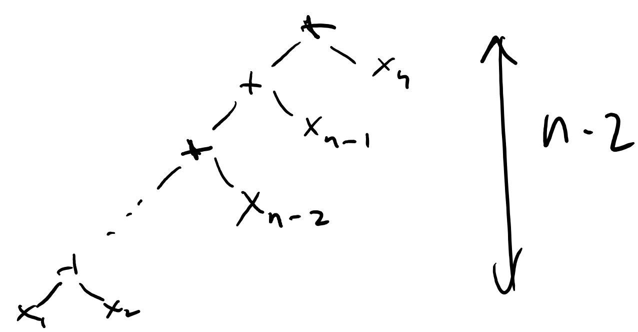
$\leq 4^{d-1} + 4^{d-1} \leq 2 \cdot 4^{d-1} \leq 4^d$ "+"

"*"

$\leq 4^{d-1} \cdot 4 = 4^d$



$\Rightarrow |length| \leq 4^d$



- formulas can be balanced to depth $O(\lg n)$. [Brent '70's]

→ polynomial length of the pgm.

8

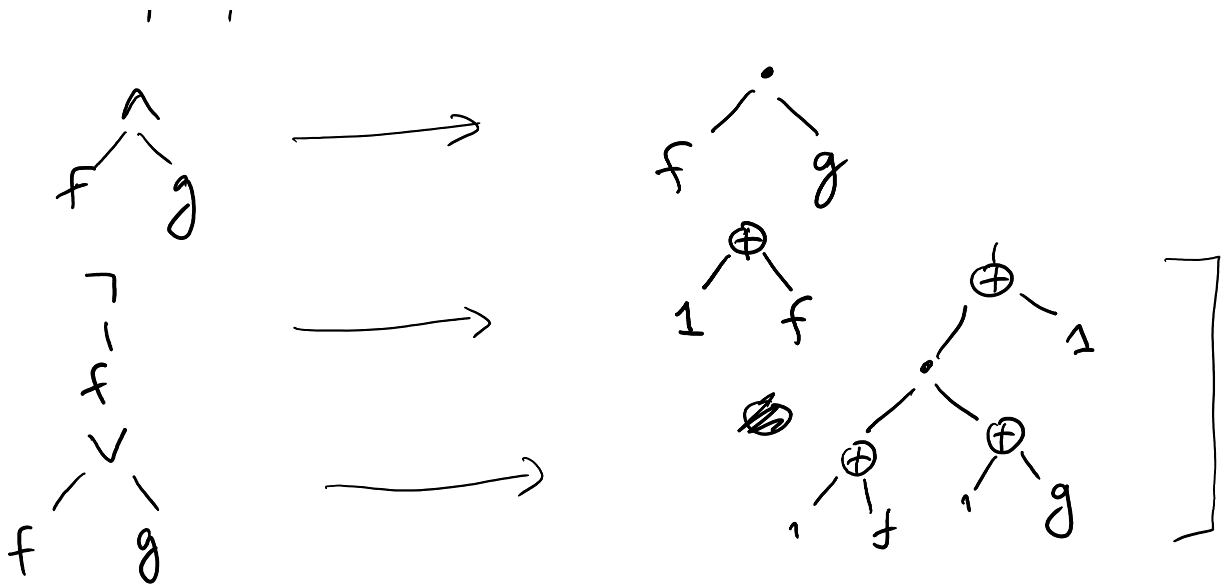
Barrington: Boolean formula of depth d ⟶ branching pgm width 5, length 4^d

$\vee, \wedge, \neg$ ⟶ $\oplus, \cdot$

$0, 1$

$(\{0,1\}, +, \cdot)$ ⟷ $(\{0,1\}, \oplus, \cdot) = GF[2]$

$\wedge$ $\qquad\qquad$ $\cdot$



$d \xrightarrow{\text{depth}} 3d$

Ben-OR & Cleve

register pgm of lgth $\leq 4^{3d}$

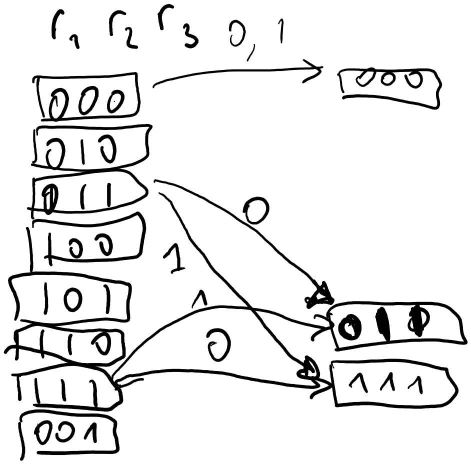
3 registers GF[2]

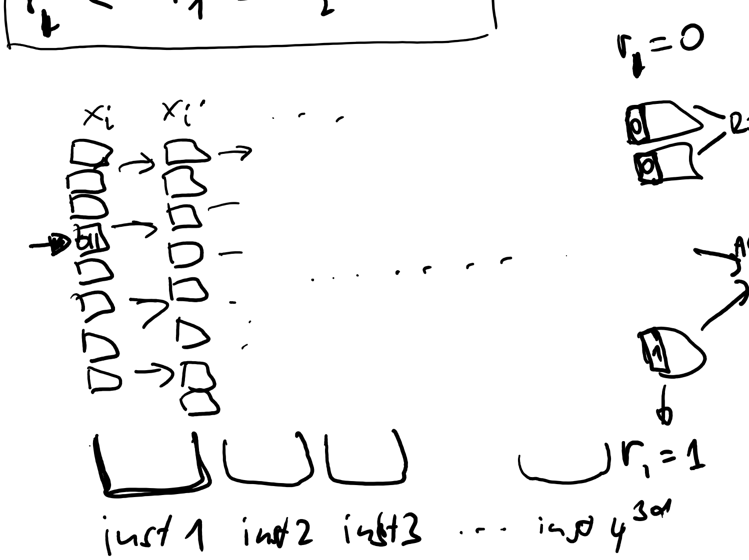
$x_1 \dots x_n$

$x_1 \dots x_n$

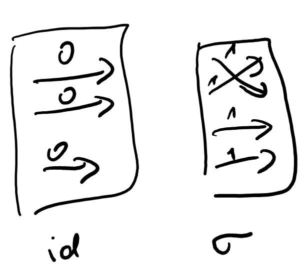
Ex: $\boxed{r_1 \leftarrow r_1 \pm r_2 * x_i}$

x_i





"permutation" b.p.



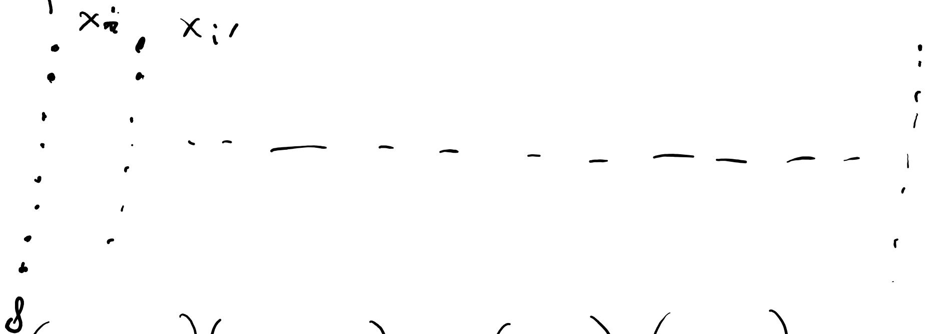
$\sigma_1^{x_i} \cdot \sigma_2^{x_{i'}} \cdots \sigma^{x_i} \cdots$

$\underbrace{r_1 \cdot r_1^{-1} \tau_2^{x_i} r_2}_{\sigma_2} \cdot r_2^{-1} \cdots$

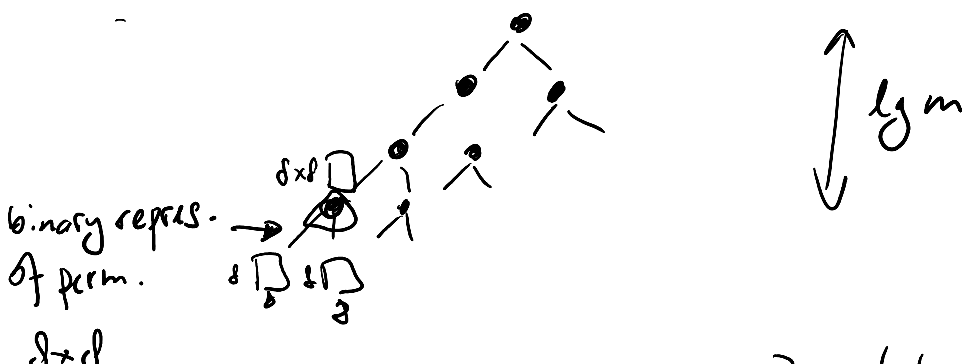
$NC^1 \longleftrightarrow F \longleftrightarrow$ b.p.

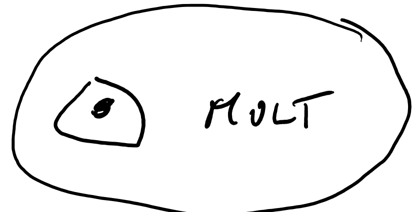
$O(\lg n)$-depth ckt's $\quad$ $O(\lg n)$-depth $\quad$ lgth $n^{O(1)}$ width 8

- b.p. $\rightarrow$ NC^1 ckt



$\sigma_1^{x_i} \cdot \sigma_2^{x_{i'}} \cdots \quad \sigma_m^{x_j} = \sigma$





$\rightarrow$ ckt $O(\lg m)$ depth

NC^1 ckt.

$O(1)$-width BP $\longrightarrow$ 8-width BP

$O(1)$

$O(1)$-width BP $\longrightarrow$ 8-width BP

length m length $m^{O(1)}$.

<u>next time</u> $NEXP \notin ACC^0$