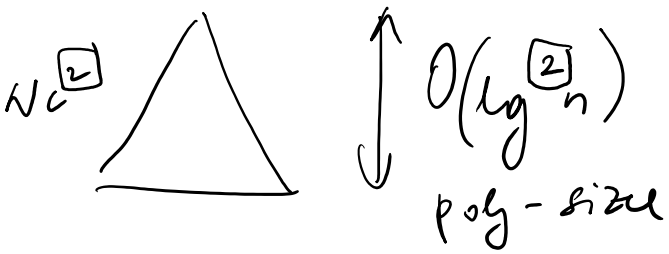
CC-Lecture-22-4-2020

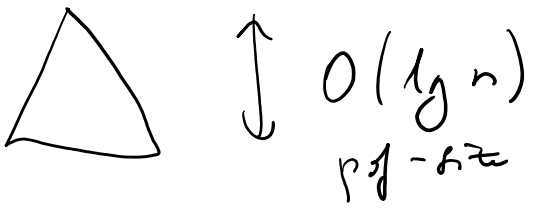
22 April, 2020 10:19

$NC^1, NC^2, \ldots$

$NL \subseteq NC^2$



Boolean formulas $\equiv$ NC^1 of poly-size



Q: $EXP \subseteq NC^1$?

$P \subseteq NC^1$?

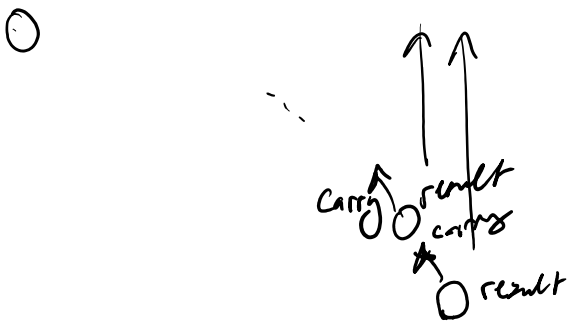
$NP \subseteq NC^1$?

$P, NP, EXP \subseteq NC^2$?

$NL \subseteq P$

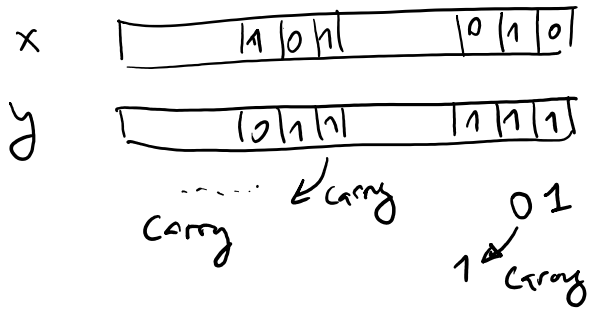
$\subseteq NC^2$

NC^1 - ADDITION, MULTIPLICATION, DIVISION



$O(n)$-size

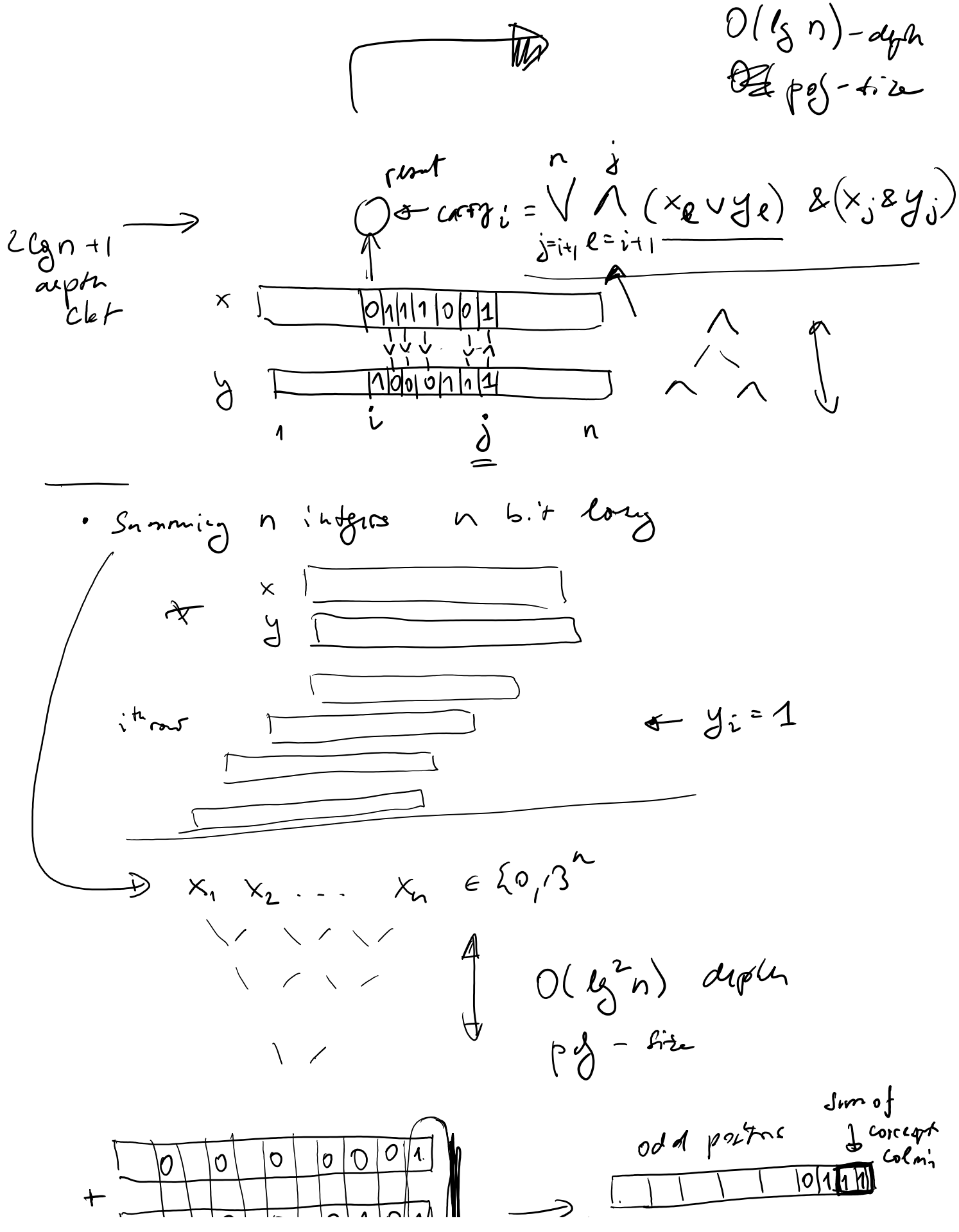
$O(n)$-depth

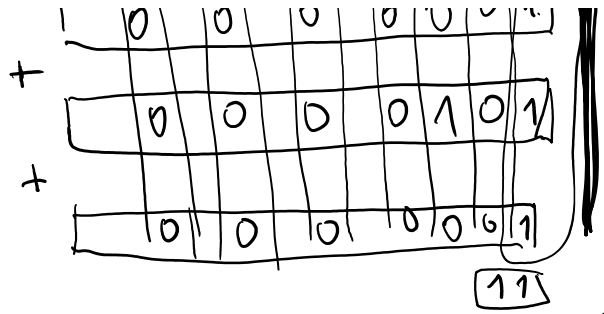


n-bit

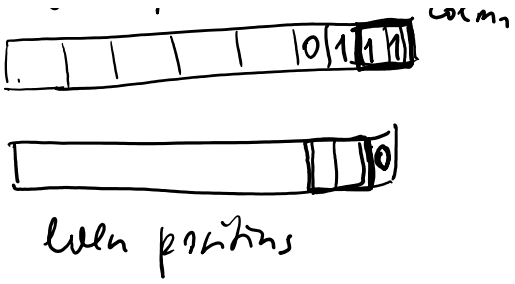
n-bit

$O(\lg n)$-depth


O(lg n) - depth
poly - size
2 lg n + 1
depth
circuit
carry_i = ⋁_{j=i+1}^{n} ⋀_{k=i+1}^{j} (x_k ∨ y_k) & (x_j & y_j)
x
y
0 1 1 1 0 0 1
1 0 0 0 1 1 1
1
i
j
n
• Summing n integers n bit long
x
y
i^th row
y_i = 1
x_1 x_2 ... x_n ∈ {0,1}^n
O(lg^2 n) depth
poly - size
+
0 0 0 0 0 0 1
odd positions
sum of corresponding column
0 1 1 1



clear the even positions



even positions

Sum 3 integers $\longrightarrow$ sum of 2 integers

n integers $\xrightarrow{O(1)\text{-depth}}$ $\frac{n}{3} \cdot 2 = \frac{2}{3}n$ integers

$\xrightarrow{O(1)\text{-depth}} \left(\frac{2}{3}\right)^2 n \to \left(\frac{2}{3}\right)^3 n \to \dots \to$ 2 int's

$\log_{\frac{3}{2}} n$ ... #levels

$O(\log n)$ - depth ckt reduces sum of n ints into sum of 2 ints.

$\Rightarrow O(\log n)$ depth circuit for addition of n ints

$\rightarrow$ MULTIPLICATION

Ex: n bits $x_1 \dots x_n$ $\longrightarrow$ $\left[\sum_{i=1}^{n} x_i \geq \frac{n}{2}\right] = MAJ(x_1 \dots x_n)$

NC^1

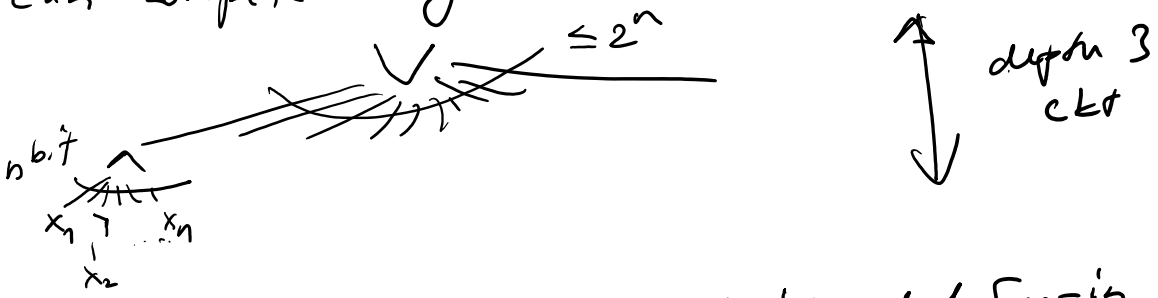
Constant - depth circuits allow gates with unbounded fan-in

$\bigvee_{i=1}^{n}$ $\bigwedge_{i=1}^{n}$

AND, OR, NOT

$2^{O(n)}$ size

Ex: can compute any fcn if size $\leq 2^n$



→ $O(1)$-depth, poly-size, unbounded fan-in AND, OR, NOT.

AC^0 ... ckts

Q: Are all fcn's in AC^0?

Observation: $AC^0 \subseteq NC^1$

- $f \in AC^0$ if $\exists C_1, C_2, \ldots C_n \ldots$ $\exists d \in \mathbb{N}, p \ldots$ poly
  C_n computes f_n
  $|C_n| \leq p(n)$ depth $C_n \leq d$

- For each polynomial ~~$p(n)$~~ for each constant ~~d~~ for large enough n, there is fcn $g_n : \{0,1\}^n \to \{0,1\}$ s.t. g_n doesn't have ckt's of size $p(n)$ & depth $d(n)$

$n^{\lg n}$

$\lg n$

ckts $\leq 2^{p^2(n)}$

fcn's $= 2^{2^n}$

$2^{p^2(n)} \ll 2^{2^n}$

$2^{(n^{\lg n})^2} \ll 2^{2^n}$

for large enough n

for every polynomial $p(n)$

$p(n) \leq n^{\lg n}$

$\Rightarrow \exists$ fcn's not computable by AC^0-circuit families.

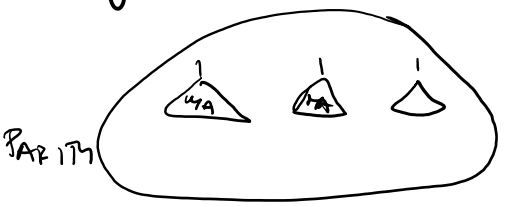
- ADDITION of 2 n-bit integers $\in AC^0$
- MULTIPLICATION of 2 n-bit integers $\notin AC^0$
- PARITY $\notin AC^0$

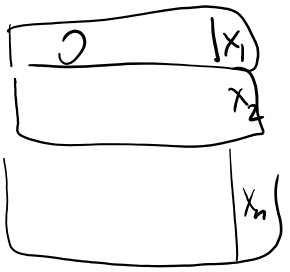
$$PARITY(x_1,\dots x_n) = \sum_{i=1}^{n} x_i \pmod 2$$

(Exc)

- ADDITION of n integers $\notin AC^0$
- MAJ $\in AC^0$

Exc





Thm: PARITY $\notin AC^0$

Furst-Saxe-Sipser '83
Ajtai '83, Håstad '85, ...
Razborov-Smolensky '87

PARITY $\in P$
$\Rightarrow P \notin AC^0$

$P \subseteq NC^1$?

PARITY $\in AC^0[q]$ — q ... prime $\neq 2$. e.g. $q=3$

↳ AC^0-like cl's

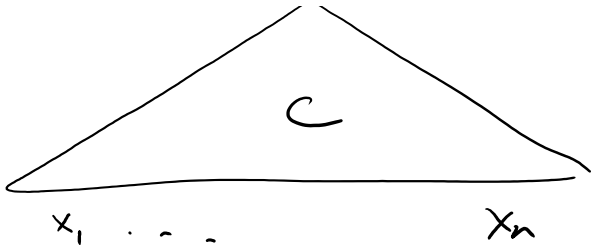
$AC^0[q]$ { gate: AND, OR, NOT, MOD-q ; depth: $O(1)$; size: poly

$$MOD\text{-}q(y_1,\dots y_m) = \left[\sum_{i=1}^{m} y_i \text{ is divisible by } q\right]$$

Ex: $MOD\text{-}2(y_1,\dots y_m) = \neg PARITY(y_1,\dots y_m)$

$AC^0[q]$

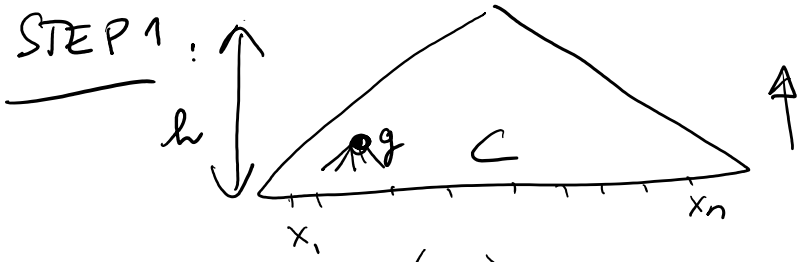
⇝ polynomial $p_C(x_1,\dots x_n)$

1) 

$\rightsquigarrow$ polynomial $p_C(x_1 \dots x_n)$
small degree $\approx n^{1/3}$
for most inputs $x \in \{0,1\}^n$
$C(x) = p_C(x_1 \dots x_n)$.

2) PARITY $(x_1 \dots x_n)$ is not computed by polynomial of degree $\leq n^{1/3}$.

MOD-ℓ ... polynomials over $GF[q] = \mathbb{Z}_q$
(q integers $+_{(\mathrm{mod}\,2)}$ $\cdot_{(\mathrm{mod}\,2)}$)
$\{0, \dots, q-1\}$

STEP 1 :


size S

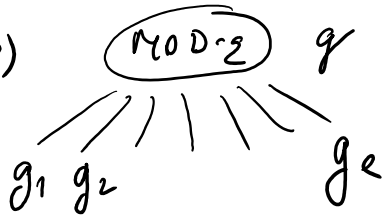
OR, MOD-2, NOT

$p_g(x_1 \dots x_n)$ ... design p_g inductively from bottom up

$h = 0$: $g = x_i$ $\quad p_g(x_1 \dots x_n) = x_i$

$h \geq 1$: 

$g = \mathrm{NOT}\, g'$ $\quad p_g(x_1 \dots x_n) = 1 - p_{g'}(x_1 \dots x_n)$

b) 

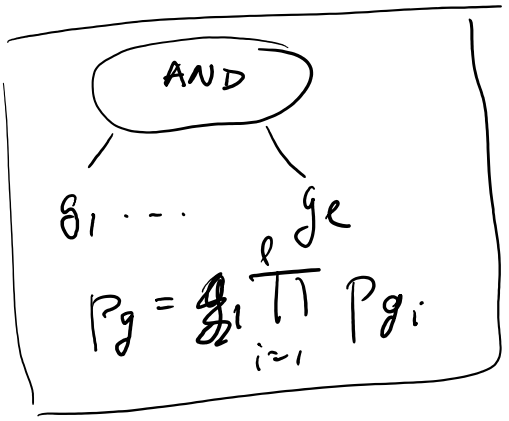
$$p_g = \left(\sum_{i=1}^{\ell} p_{g_i} \right)^{q-1}$$

reduces all values from $GF[q]$ to 0/1

~~(Euler's theorem)~~

(Fermat's Lema)

c)



try 1:

$$P_g = \left(\sum_{i=1}^{\ell} g_i \right)^{g-1}$$