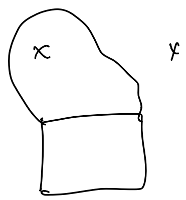
Lecturer: Ramprasad Saptharishi
Course: Complexity

Barrington's Theorem:

Ref: [Viola] Gems in TCS

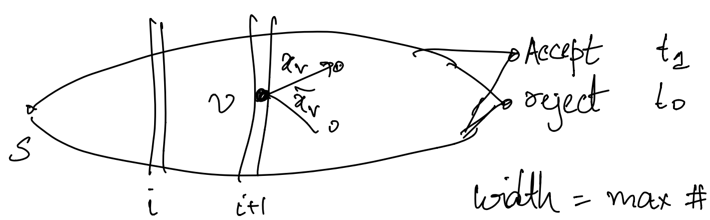
Picture Hanging Problem

- k - nails.
- Picture should not fall
- If <u>any</u> of the nails removed, then picture falls.



<u>An abstraction for space bounded computation</u>. (random access model).

Defn: (Det. Branching Program): Layered graph



Every vertex has 2 outgoing edges labelled x_v & $\bar{x}_v$ for some input bit x_v

width = max # vertices in a layer.

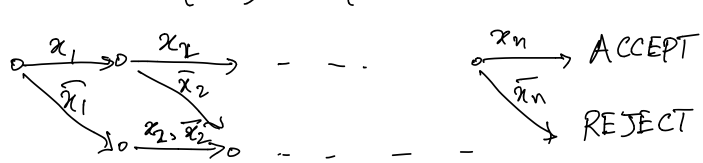
Length = time. Each layer is "possible states".

This BP computes $f:\{0,1\}^n \to \{0,1\}$ if

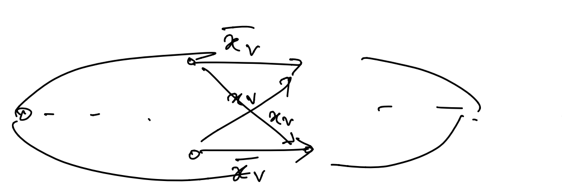
$f(x) = 1 \iff \exists$ "a path from s to accept"

Oblivious det. BP: All vertices at a given layer read the same input bit.

Eg: AND: $\{0,1\}^n \to \{0,1\}$



PARITY:



MAJ : $\{0,1\}^n \longrightarrow \{0,1\}$ 1 if $\geq n/2$ bits are 1.

Width 3, exp length.

(Try out every $\binom{n}{n/2}$ subset, and do AND on each).

Qn: Can MAJ be computed by BPs of $O(1)$ width, and length poly(n)?

[Barrington] Yes. Width 5. For <u>any</u> fn that can be computed in NC^1.

NC^1: functions $f: \{0,1\}^n \longrightarrow \{0,1\}$ that are computable by circuits of

- $\wedge, \vee, \neg$ gates
- depth = $O(\log n)$
- fan-in = 2
- size = poly(n)

Key idea: Group theory, commutators.

Group BP: Seq of instructions of the form $[i, g_{i_0}, g_{i_1}]$

$[7, \pi_1, \sigma_1]$ $[14, \pi_2, \sigma_2]$ $[7, \pi_3, \sigma_3]$ ...

"Start with id. Read input i.

If $x_i = 1$, multiply with g_{i_1}

$x_i = 0$, " " g_{i_0} "

This G. BP α-computes a fn $f: \{0,1\}^n \to \{0,1\}$

if $f(x) = 0$, then final perm = id.

$f(x) = 1$, " " " = α

$G = S_5$

Lemma 1: If we have a G-BP that α-computes f and α - any 5-cycle.
Then if β is any other 5-cycle, then we also have a G-BP that β-computes f of the same length.

Pf: If α, β are both 5-cycles, then $\exists\, \rho$ s.t.

$$\rho^{-1} \alpha . \rho = \beta$$

$(\alpha_1\ \alpha_2\ \alpha_3\ \alpha_4\ \alpha_5)$ $\qquad\qquad$ $\rho : \alpha_i \longrightarrow \beta_i$

$(\beta_1\ \beta_2\ \beta_3\ \beta_4\ \beta_5)$

Pre- & post-multiply by ρ^{-1} & ρ resp. $\square$

Lemma: If we have a G-BP that α-computes f,
then " " " " " α-computes $\bar{f}$.

Pf: Multiply by α^{-1} at the end. This gives a G-BP that α^{-1}-computes $\bar{f}$. But α^{-1} has same cycle structure as α.
Use prev lemma. $\square$

Lemma: If we have a G-BP that α-computes f
" " " β-computes g
then there is a G BP " $\alpha\beta\alpha^{-1}\beta^{-1}$-computes $f \wedge g$
of length $\leq 4.\max(\text{length}(f), \text{length}(g))$.

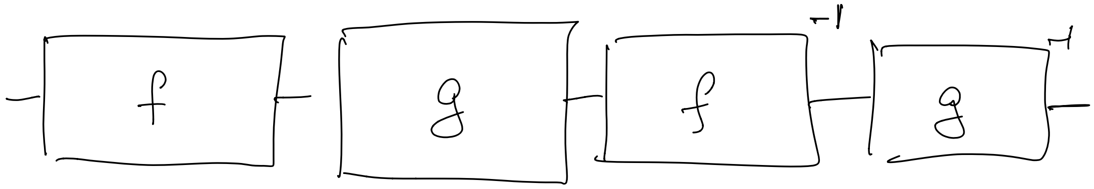
Pf:

f	g	
1	1	$\alpha\beta$
1	0	α
0	1	β
0	0	id

$\boxed{\alpha \text{ or id}}$ $\qquad\qquad$ $\boxed{\beta \text{ or id}}$

▷ If either of them = id, output = id

▷ If both are non-triv, then output to be non-triv.



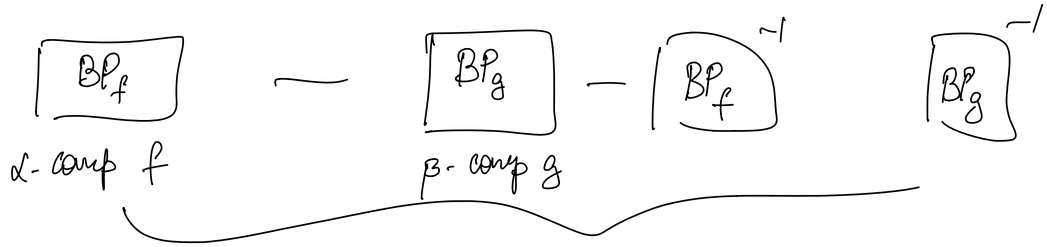
	f	g	
11	α	β	$\alpha\beta\alpha^{-1}\beta^{-1}$
10	α	id	$\alpha \, id \, \alpha^{-1} \, id = id$
01	id	β	$id \, \beta \, id \, . \, \beta^{-1} = id$
00	id	id	id.

This is a G-BP that γ-computes $f \wedge g$ where $\gamma = \alpha\beta\alpha^{-1}\beta^{-1}$

Meaningful iff $\alpha\beta\alpha^{-1}\beta^{-1} \neq id$. $(\alpha\beta \neq \beta\alpha)$

Fact: $\overset{\alpha}{(12345)}\overset{\beta}{(13542)}(12345)^{-1}(13542)^{-1}$

$= (13254)$.

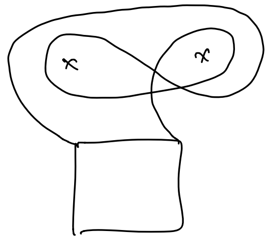


$\alpha\beta\alpha^{-1}\beta^{-1}$ comp. $f \wedge g$

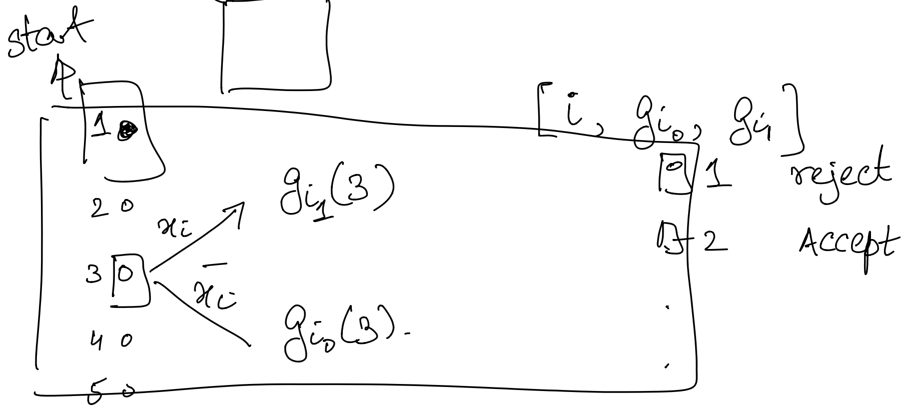
$\Downarrow$

(12345) - com $f \wedge g$

Cor: If f is computable by a circuit (fan-in 2) of depth d, then f is (12345)-comp. by a G-BP of length 4^d



$aba^{-1}b^{-1}$



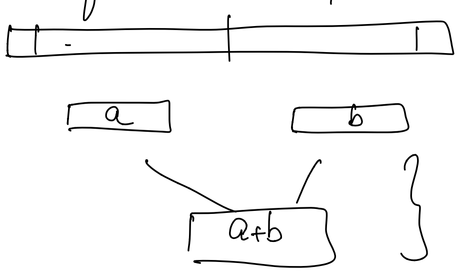
Want α, β, γ that are non-triv. and

- α, β, γ are all conjugates of each other
- $\gamma = \alpha\beta\alpha^{-1}\beta^{-1}$.

A_5 = set of even permutations of 5 elements.

NC^1

Circuit for MAJORITY:



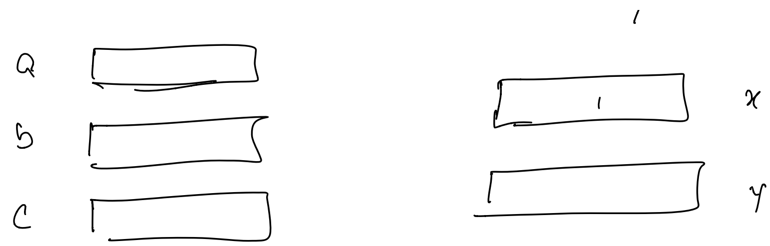
n bits $\quad n = 2^l$.

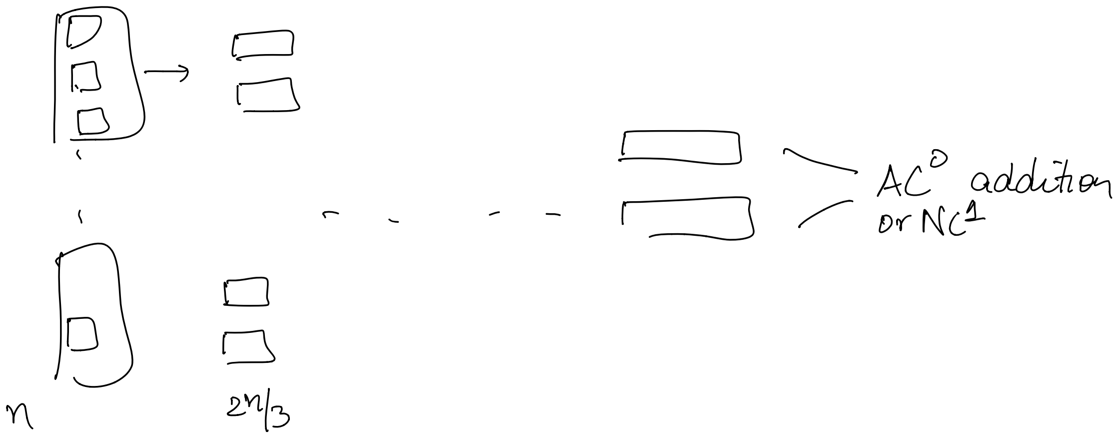
depth $O(\log\log n)$ $\quad$ $O(\log n \log\log n)$ overall.

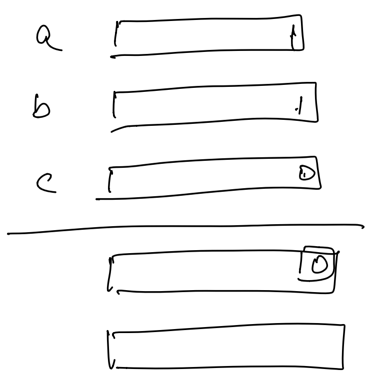
Fact: Addition of two l-bit numbers can be done in $AC^0 \subseteq NC^1$
(unbounded fan-in $\wedge, \vee$, & $\neg$ gates
$O(1)$ depth
poly size).

3-to-2 transformation:

Given 3 numbers a, b, c. of l-bits
Want to output 2 numbers x, y of $\leq l+1$ bits
such that $a+b+c = x+y$.







74
29
0 9 3 · 8
0 1 0 · 8

addition without carry

carry.