Topics course on KRW conjecture
Fall 2020, UCSD

Sajin Koroth (Simon Fraser University)

Outline

- Administrative Stuff
- Motivation : P vs NC^1 (poly-time vs efficient parallel)
- Computation Model : Circuits
- P vs NC^1 as a circuit complexity problem
- KRW Conjecture : Naive ?= Optimal
- KRW Conjecture $\implies$ P $\neq$ NC^1

Administrative Stuff

- Grading
  - 3 HW, 1 Project : TBD (Scribing?)
- Course mailing list : krw-course---fall-2020-ucsd@googlegroups.com
- Piazza : https://piazza.com/ucsd/fall2020/cse291i00/home
- Office Hours : Tentatively 11-1pm Fridays (check poll on Piazza, poll closes Wednesday)
- Lecture Hours : Monday, Wednesday 11am-12:20pm
- Upcoming update : Relevant research papers on website

Motivation : P vs NC^1 (poly-time vs efficient parallel)

Parallel vs Sequential computation

- Most of linear algebra can be done in parallel
- Gaussian elimination is an outlier
    - Intuitively its an inherently sequential procedure
    - There are theoretical reasons to believe so
    - There is an efficient sequential algorithm

P vs NC^1

Class P of poly-time solvable problems

Are there problems with efficient sequential algorithms which do not have efficient parallel algorithms ?

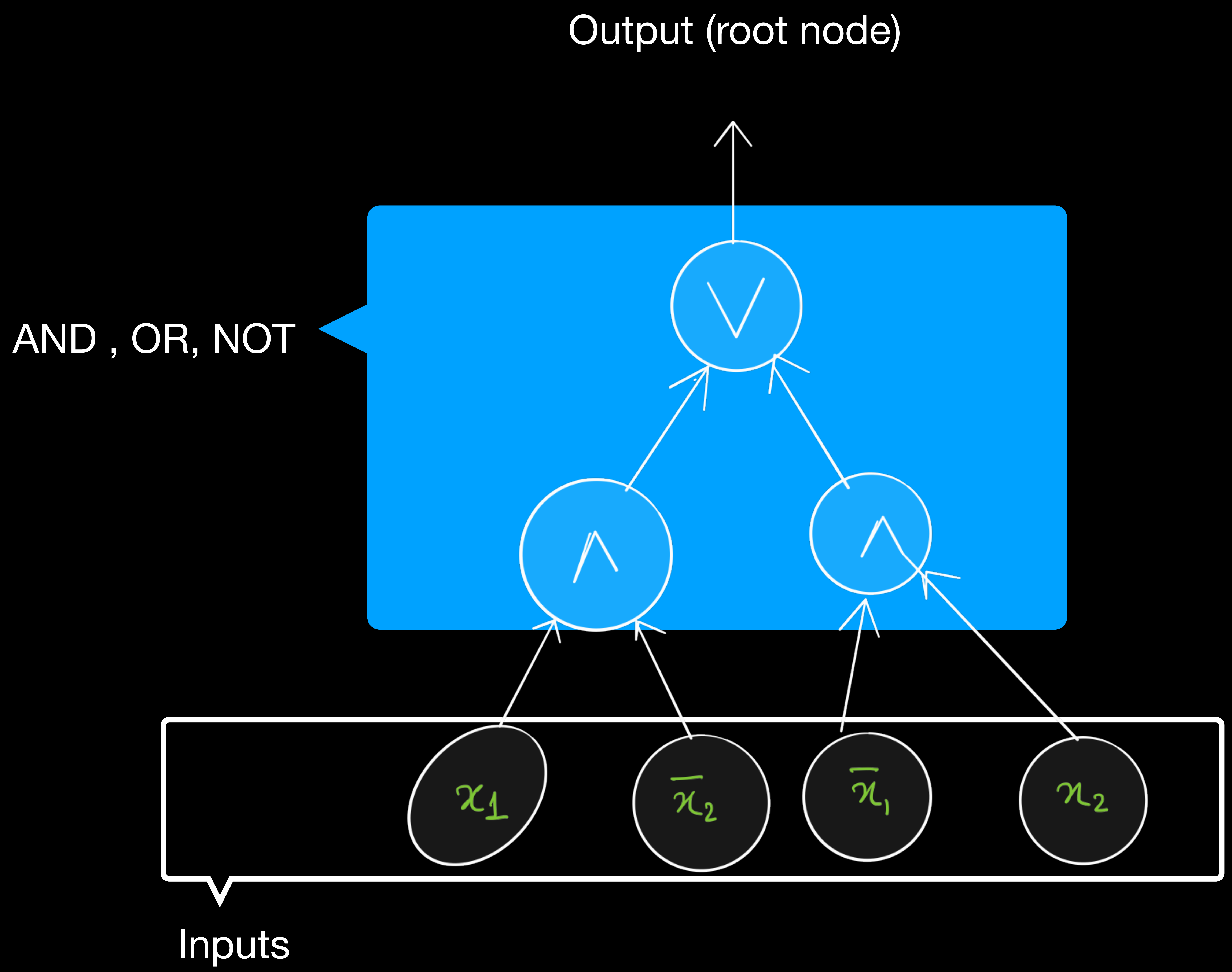
Modeled as circuits

Computation Model : Circuits

An Example

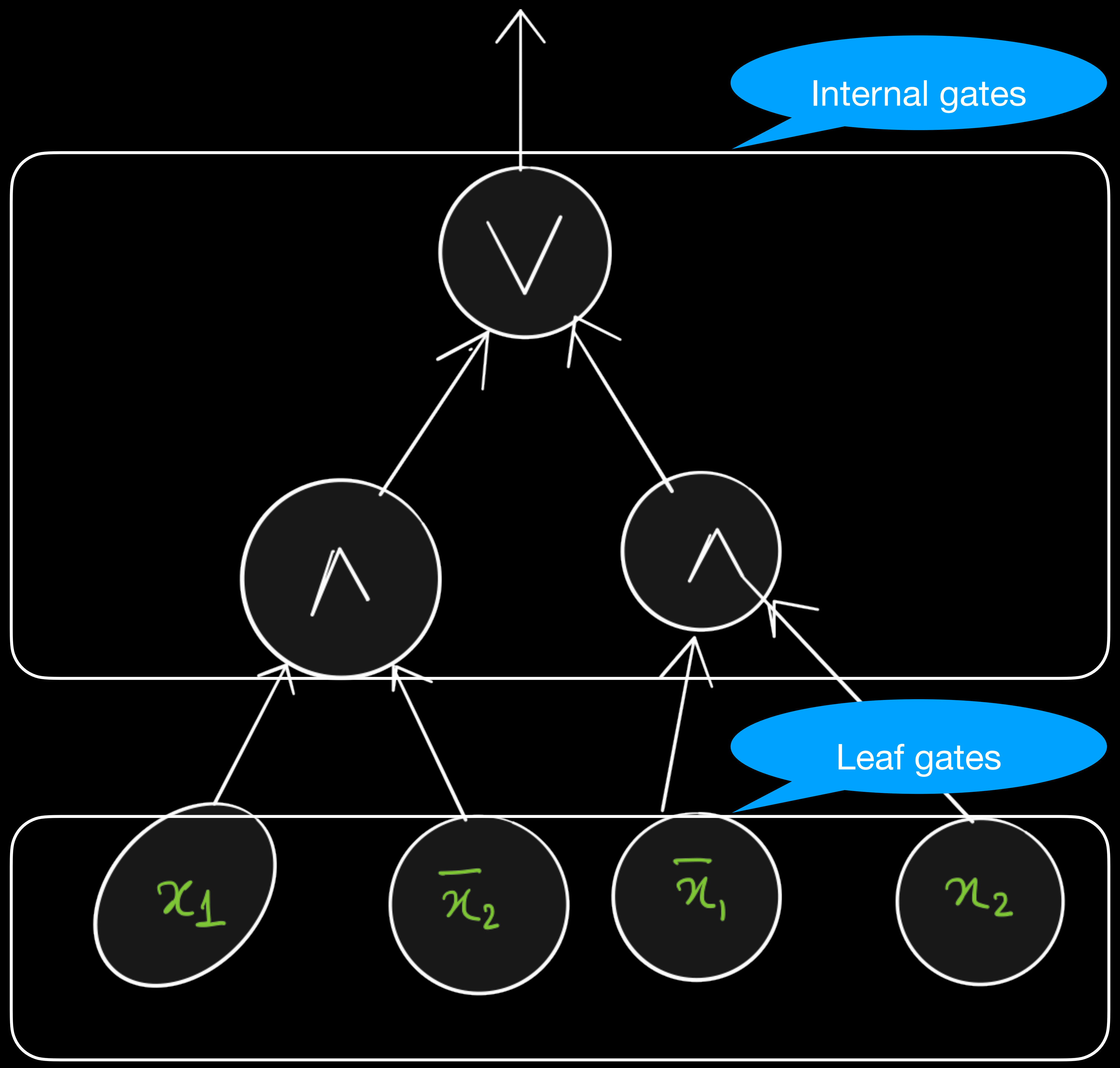
Parity Function

x_1	x_2	$x_1 \oplus x_2$
0	0	0
0	1	1
1	0	1
1	1	0



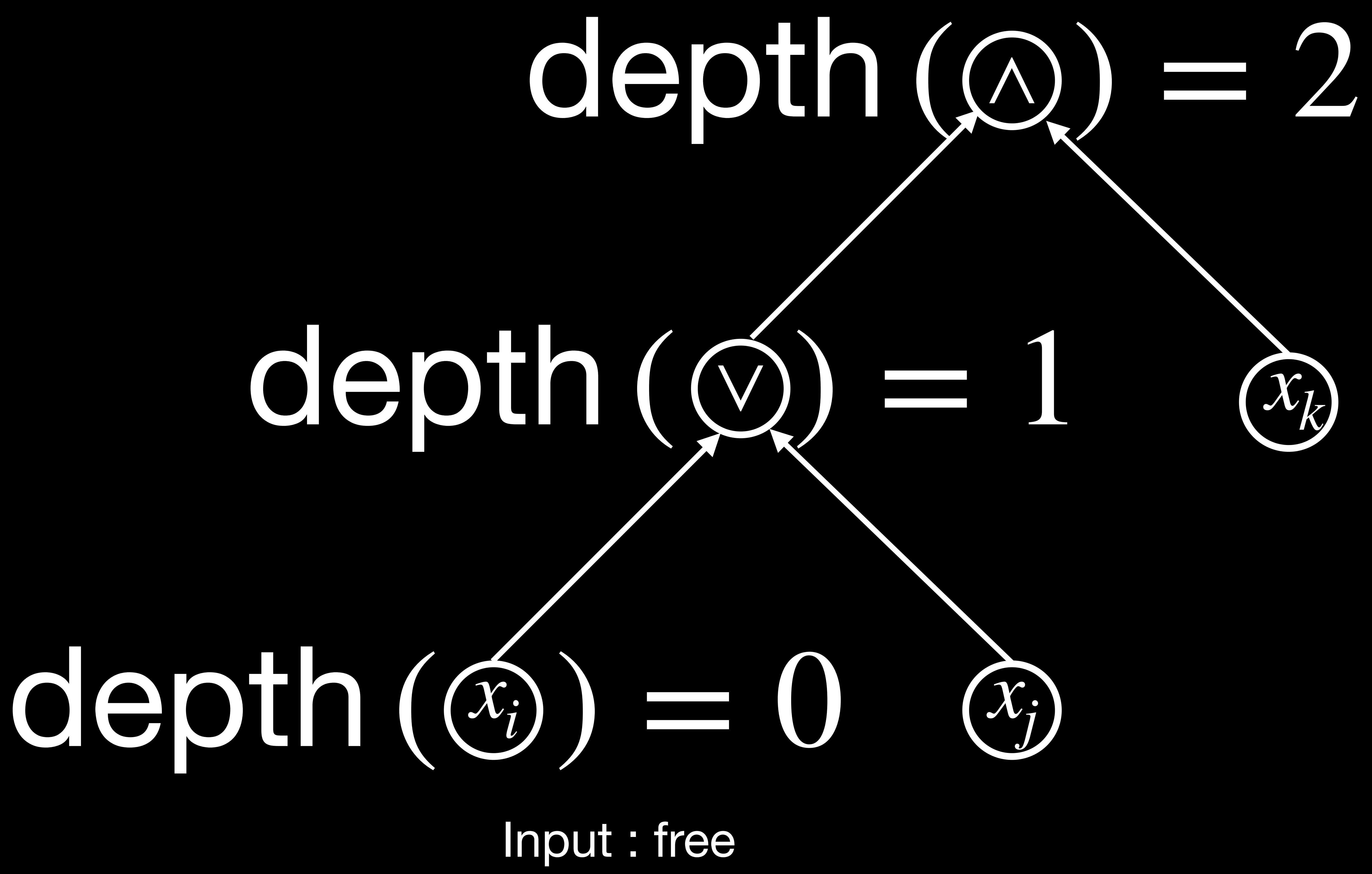
Circuit complexity

- Complexity parameters :
  - Size : # of gates
  - Depth : length of the longest path from root to leaf
  - Fan in : 2, Fan out



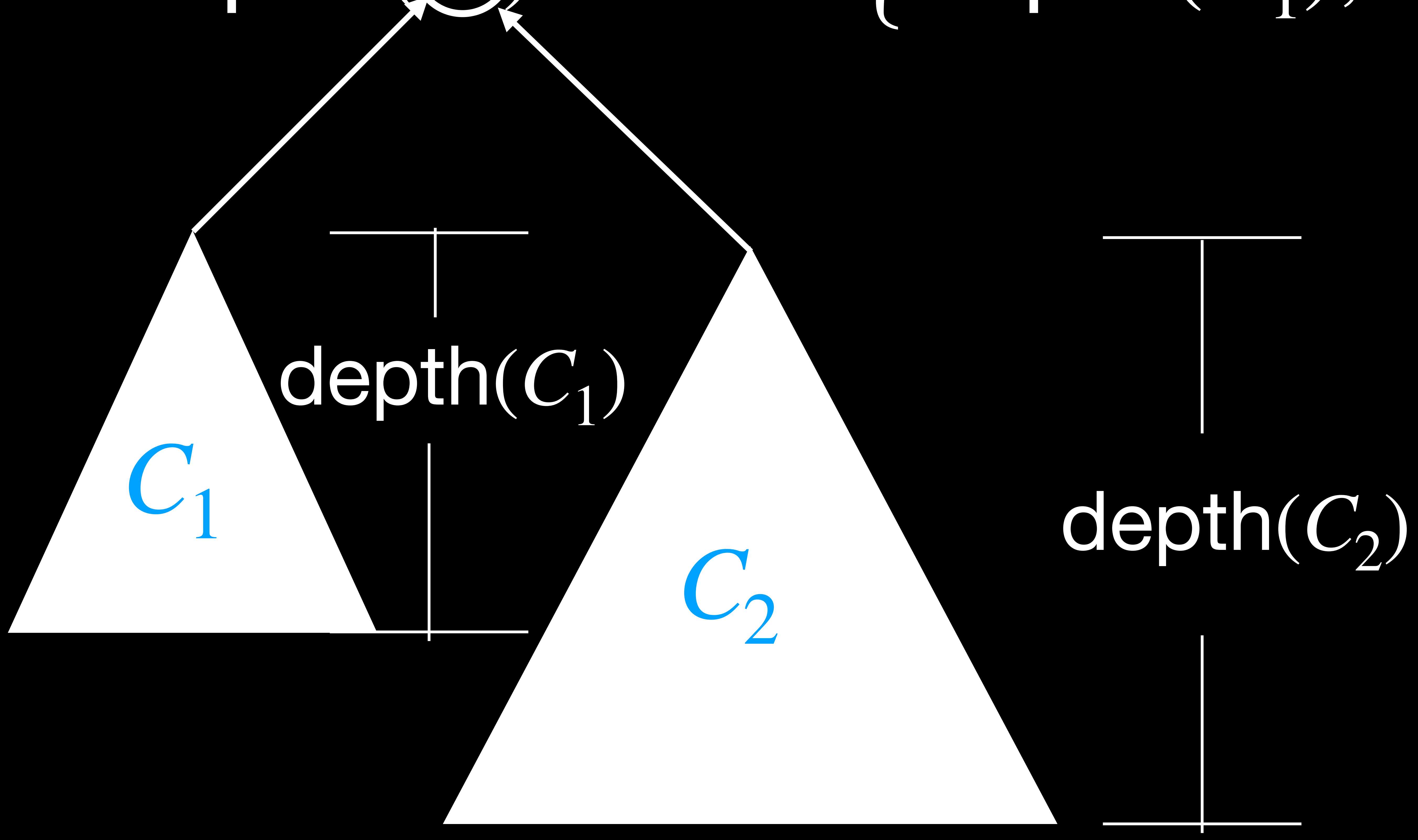
Depth $\approx$ Parallel Time

- Depth : length of the longest path from root to leaf
- Node : computation that needs unit time



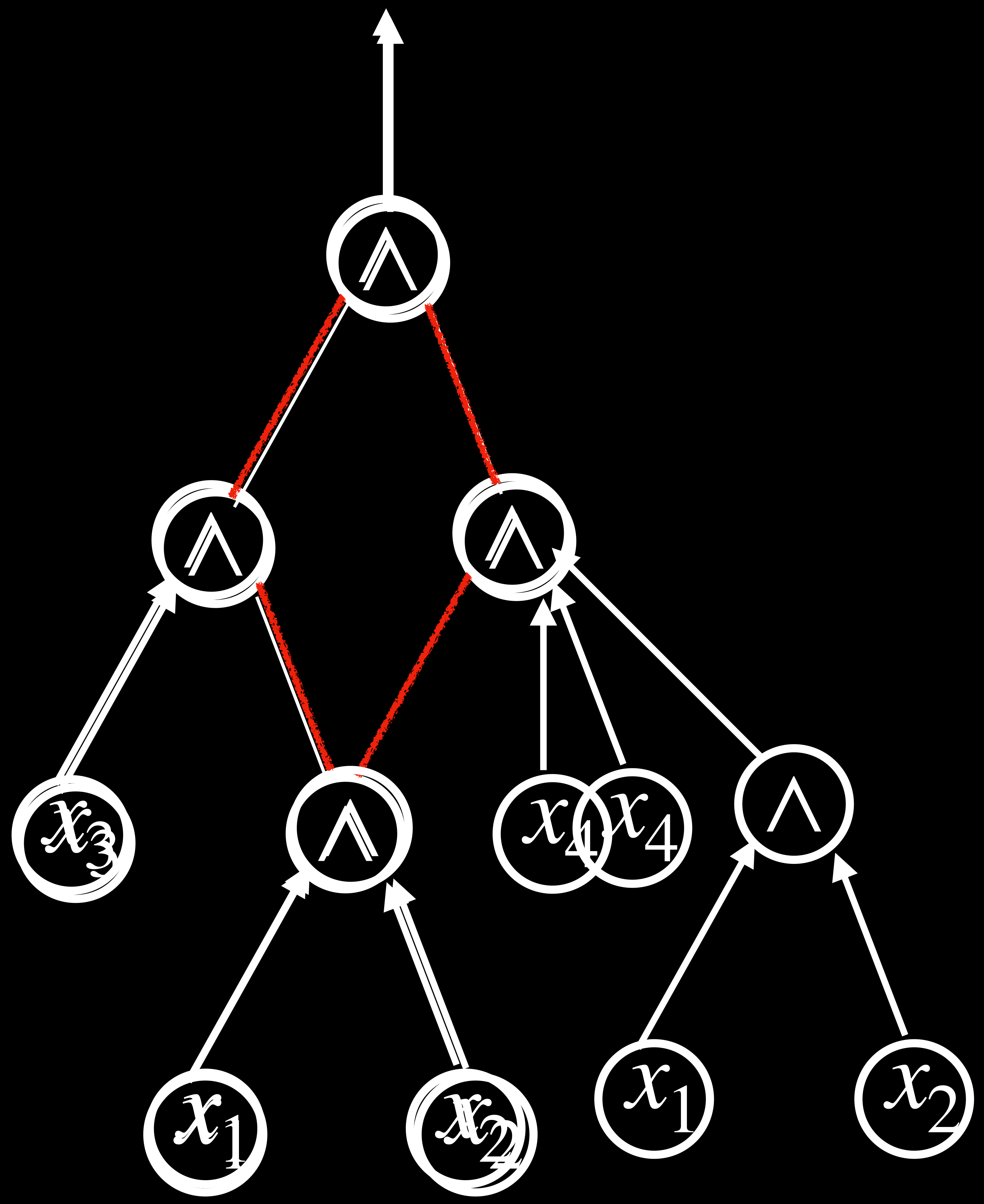
Depth ≈ Parallel Time

$$\text{depth}\left(\textcircled{$\wedge$}\right) = \max\left\{\text{depth}(C_1), \text{depth}(C_2)\right\} + 1$$



Circuit complexity

- Formulas :
  - Underlying DAG is a tree
  - No reuse of computation
  - Depth = log (Size)



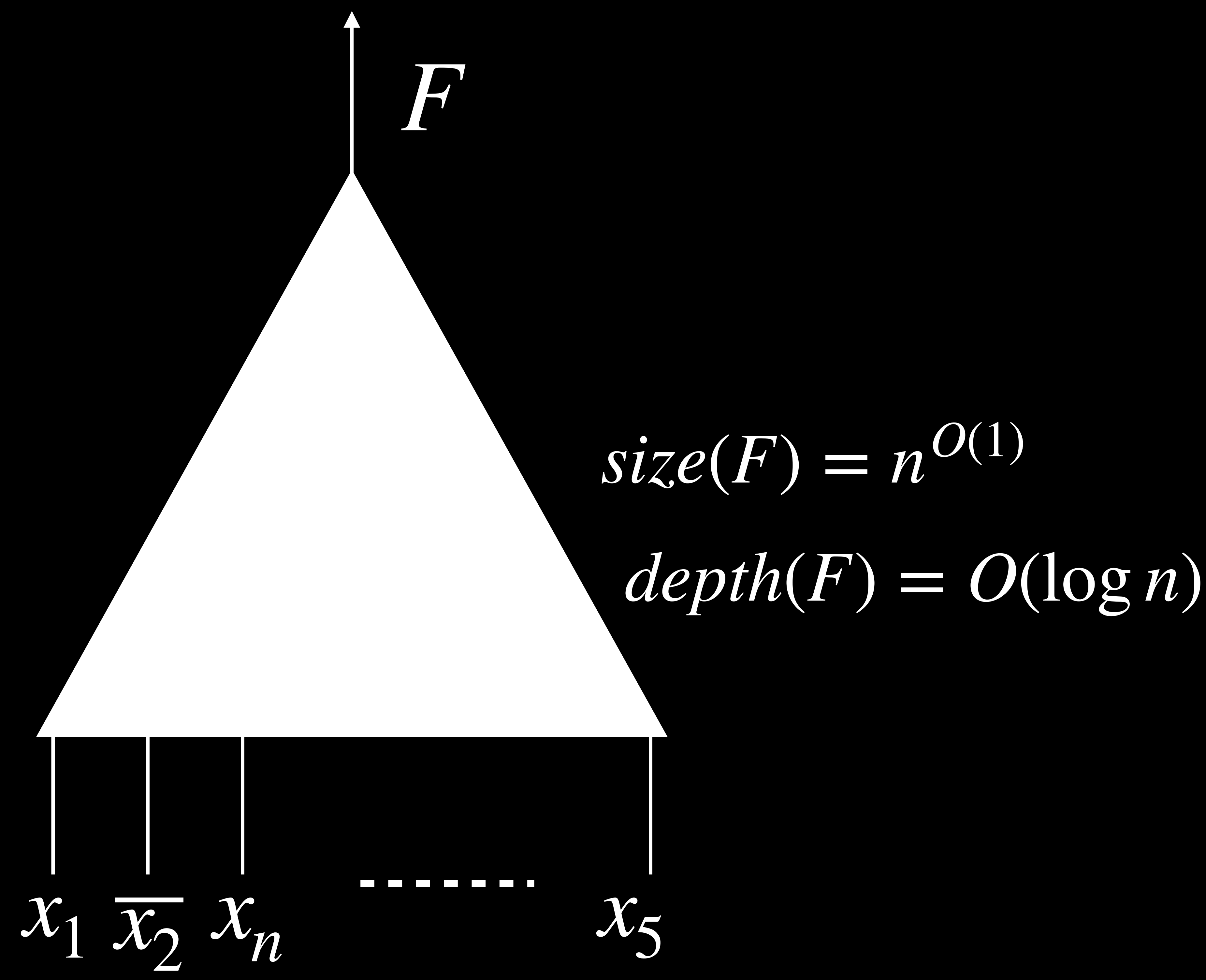
Circuit complexity

- Size s, depth d circuit $\approx$ Size $2^d \times s$ formula
- Poly size , log depth circuit $\approx$ Polynomial Size formula

Circuit complexity

Class NC^1 = Poly-Size Formulas

- Efficient parallel computation (formally CREW PRAM):
  - Polynomially many processors
  - Logarithmic computation time



In formula, $depth(F) = O(\log size(F))$

Circuit complexity

P vs NC^1 rephrased

- A Boolean function f (candidates: Perfect matching, Gaussian elimination etc)
  - That can be computed in poly-time ($f \in P$)
  - Any de-Morgan formula computing it has super-poly size ($f \notin NC^1$)

Equivalently super-logarithmic depth

Best formula lower bounds

Hastad's result

- (Tal'14) : $\Omega\left(\dfrac{n^3}{\log^2 n \log\log n}\right)$ size
- Equivalently $3\log n$ depth
- P vs NC^1 : super poly-size / super logarithmic depth
- Meta-mathematical barrier : Natural proofs

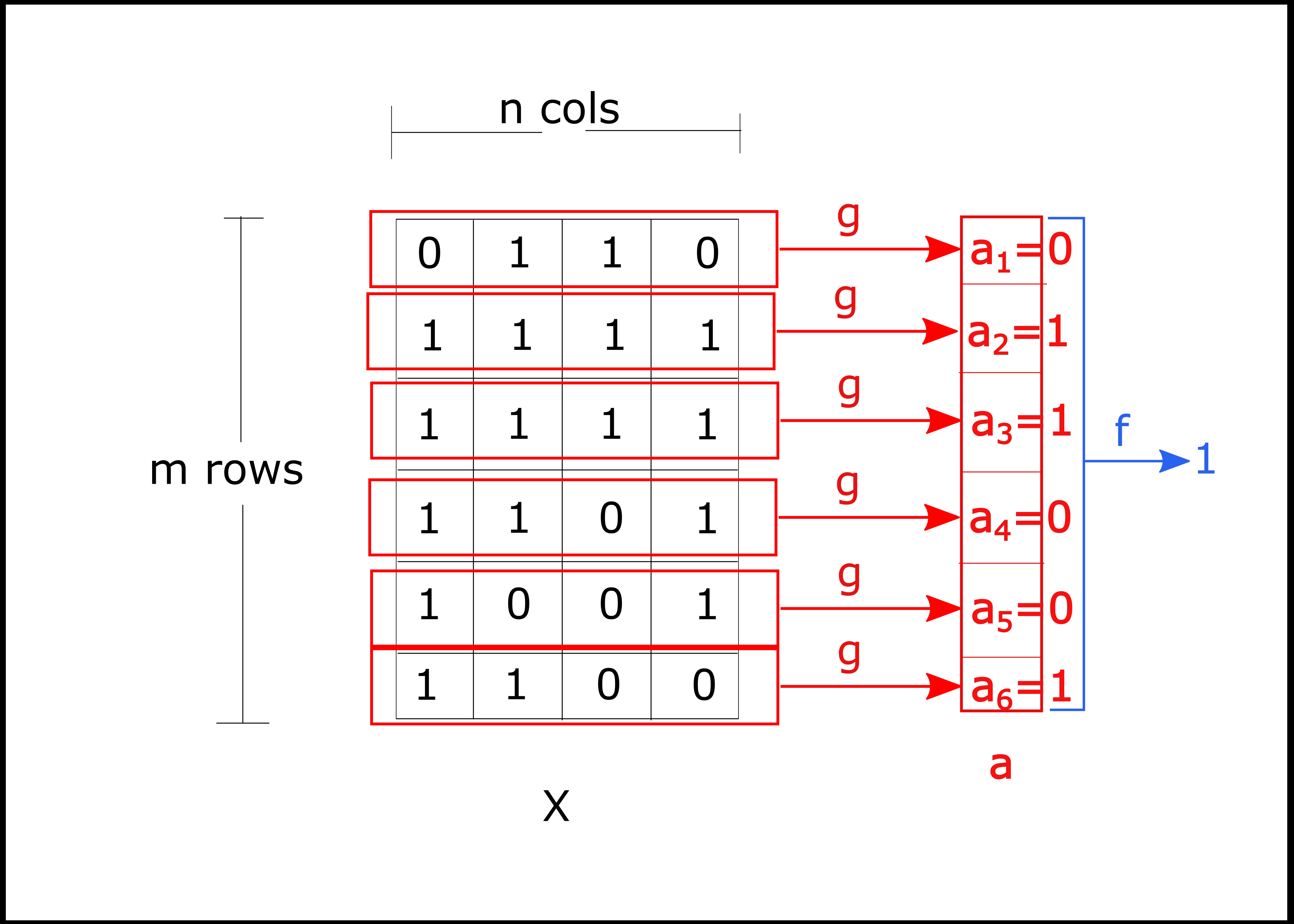
KRW Conjecture

KRW Conjecture

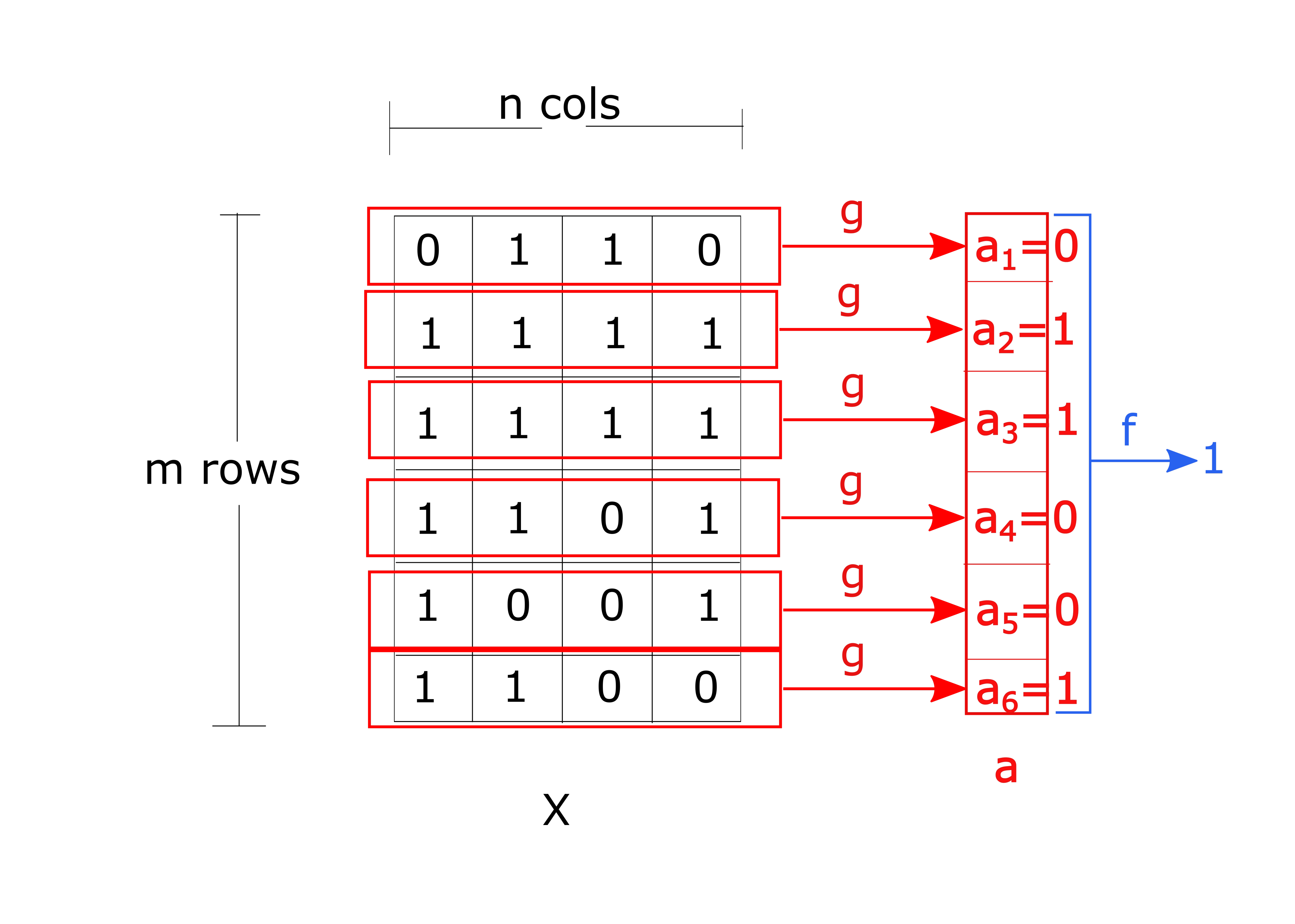
- Karchmer, Raz, Wigderson
- Study block-composition to study depth
- Block-composition : Given
  - $f : \{0,1\}^m \to \{0,1\}$ (say $f(z_1, z_2, \ldots, z_m)$)
  - $g : \{0,1\}^n \to \{0,1\}$ (say $g(y_1, y_2, \ldots, y_m)$)
  - $f \circ g : \left(\{0,1\}^n\right)^m \to \{0,1\}$
  - $f \circ g(x_{1,1}, x_{1,2}, \ldots, x_{1,n}, \ldots, x_{m,1}, \ldots, x_{m,n})$
    - $= f(z_1, \ldots, z_m)$
    - $z_i = g(x_{i,1}, \ldots, x_{i,n})$

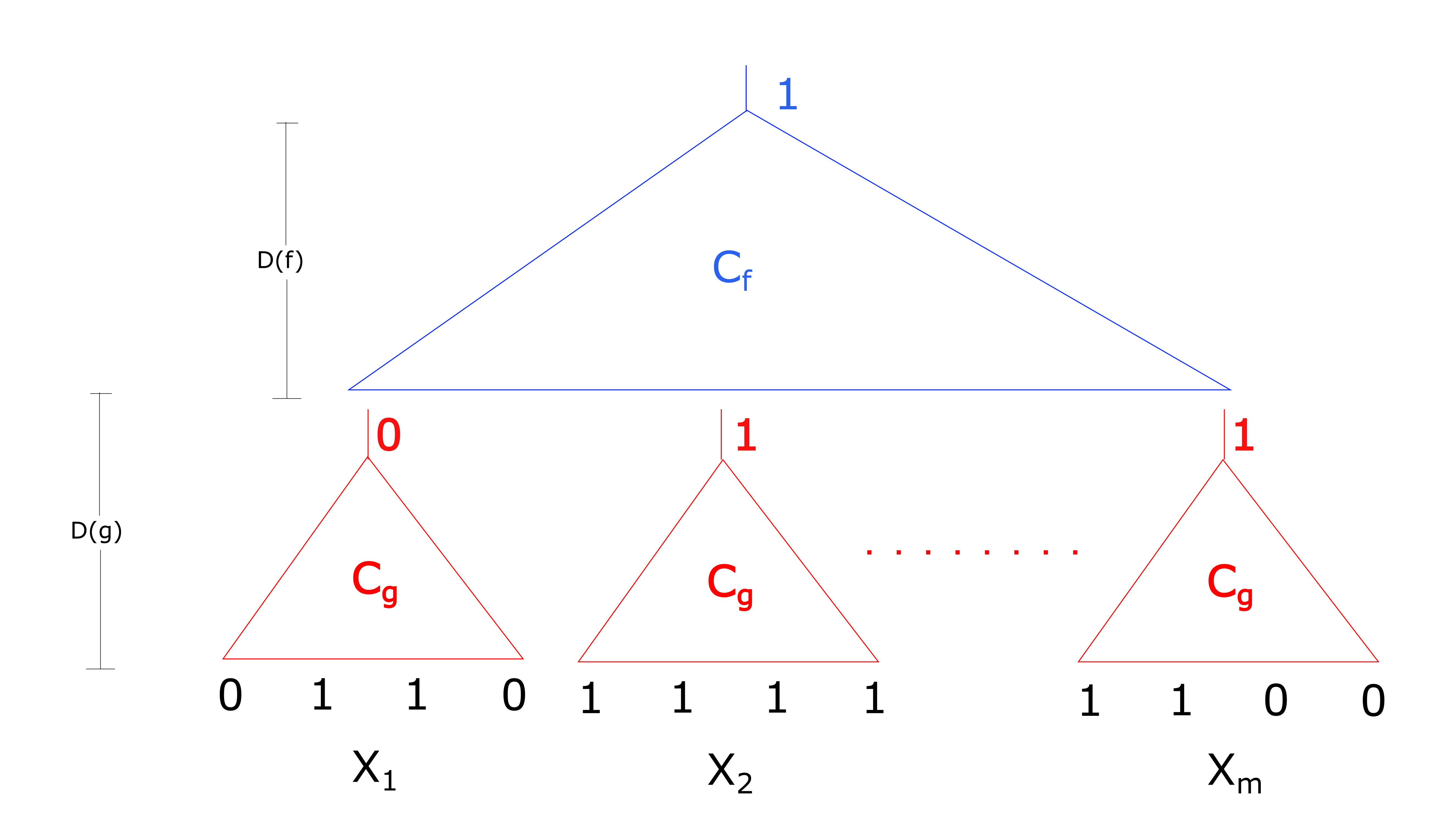
KRW Conjecture

$$f \circ g(x_{1,1}, x_{1,2}, \ldots, x_{1,n}, \ldots, x_{m,1}, \ldots, x_{m,n}) = f(g(x_{1,1}, x_{1,2}, \ldots, x_{1,n}), \ldots, g(x_{m,1}, \ldots, x_{m,n}))$$



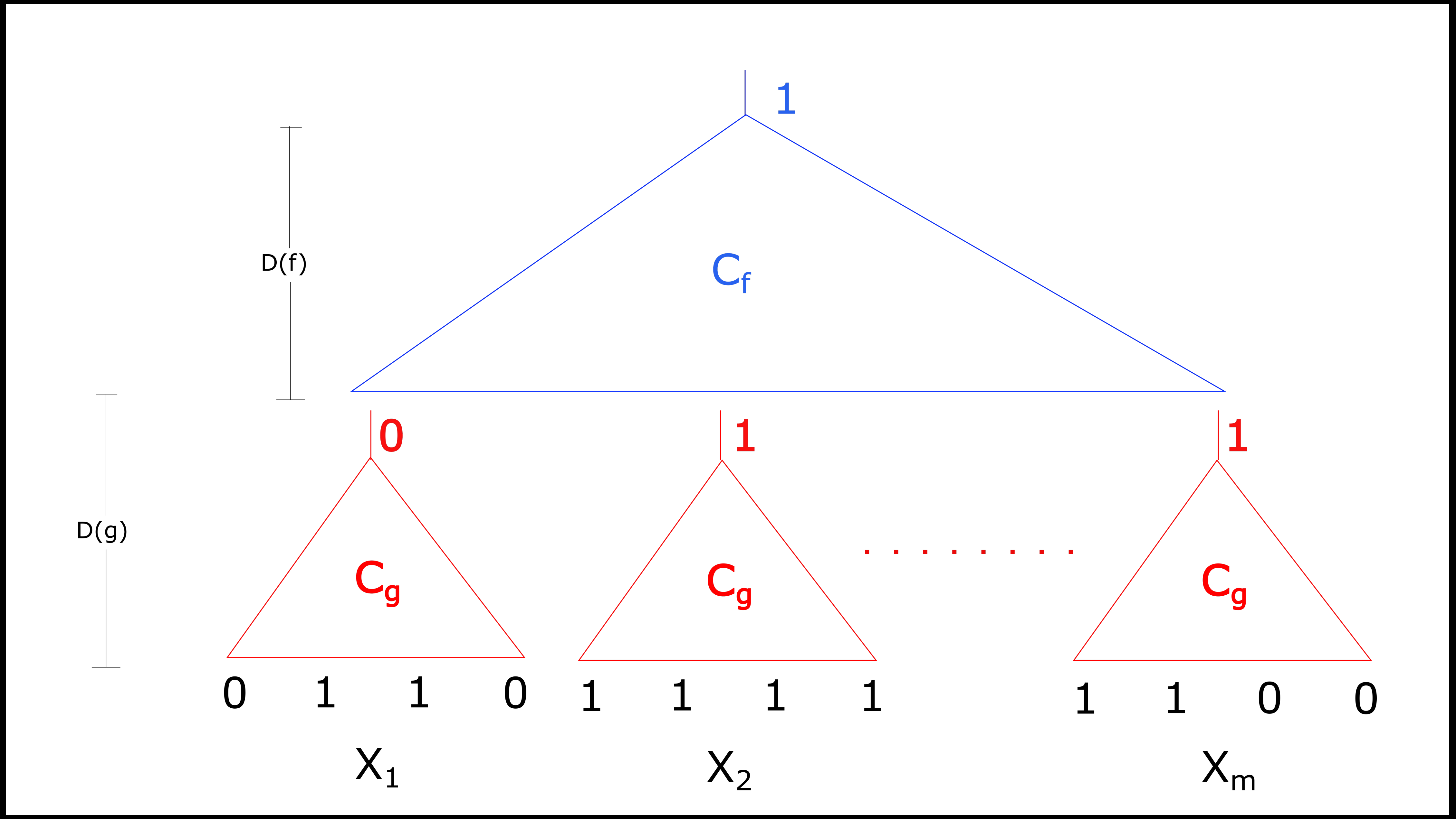
KRW Conjecture -> Naive ?= Optimal





KRW Conjecture

- Fact :
  depth$(f \circ g) \leq$ depth(f) + depth(g)
- KRW Conjecture (f,g non constant)
  depth$(f \circ g) \approx$ depth(f) + depth(g)
  - Explicit function in P which does not have log depth circuits
  - $P \neq NC^1$ (efficiently solvable problem with no efficient parallel algorithms)



KRW Conjecture

$\implies \mathbf{P} \neq \mathbf{NC}^1$

(Over to handwritten notes)

KRW Conjecture

- KRW Conjecture
  - depth$(f \circ g) \approx$ depth(f) + depth(g)
  - Many versions of $\approx$
    - Let $1 \geq \epsilon > 0$
    - a) depth$(f \circ g) \geq$ depth$(f) + \epsilon \cdot$ depth(g)
    - b) depth$(f \circ g) \geq \epsilon$depth$(f) + \cdot$depth$(g)$

Thank you