$AC^0[\oplus]$ FORMULAS VERSUS AC^0 CIRCUITS

BEN ROSSMAN
(UNIV. OF TORONTO)

SRIKANTH SRINIVASAN
(IIT BOMBAY)

Boolean functions

$f : \{0,1\}^n \to \{0,1\}$ – Computational problem

Boolean functions

$f : \{0,1\}^n \to \{0,1\}$ – Computational problem

Algorithm for f : "Expression" for f using "simple" operations.

Boolean functions

$f : \{0,1\}^n \rightarrow \{0,1\}$ – Computational problem

Algorithm for f : "Expression" for f using "simple" operations.

"Simple" operations

AND: $\wedge_m : \{0,1\}^m \rightarrow \{0,1\}$

$$\wedge_m(x_1, \ldots, x_m) = \min\{x_1, \ldots, x_m\}$$

Boolean functions

$f: \{0,1\}^n \to \{0,1\}$ – Computational problem

Algorithm for f : "Expression" for f

using "simple" operations.

"Simple" operations

AND: $\wedge_m : \{0,1\}^m \to \{0,1\}$

$\wedge_m(x_1, \ldots, x_m) = \min\{x_1, \ldots, x_m\}$

OR: $\vee_m(x_1, \ldots, x_m) = \max\{x_1, \ldots, x_m\}$

NOT: $\neg x = 1 - x$

Boolean formulas

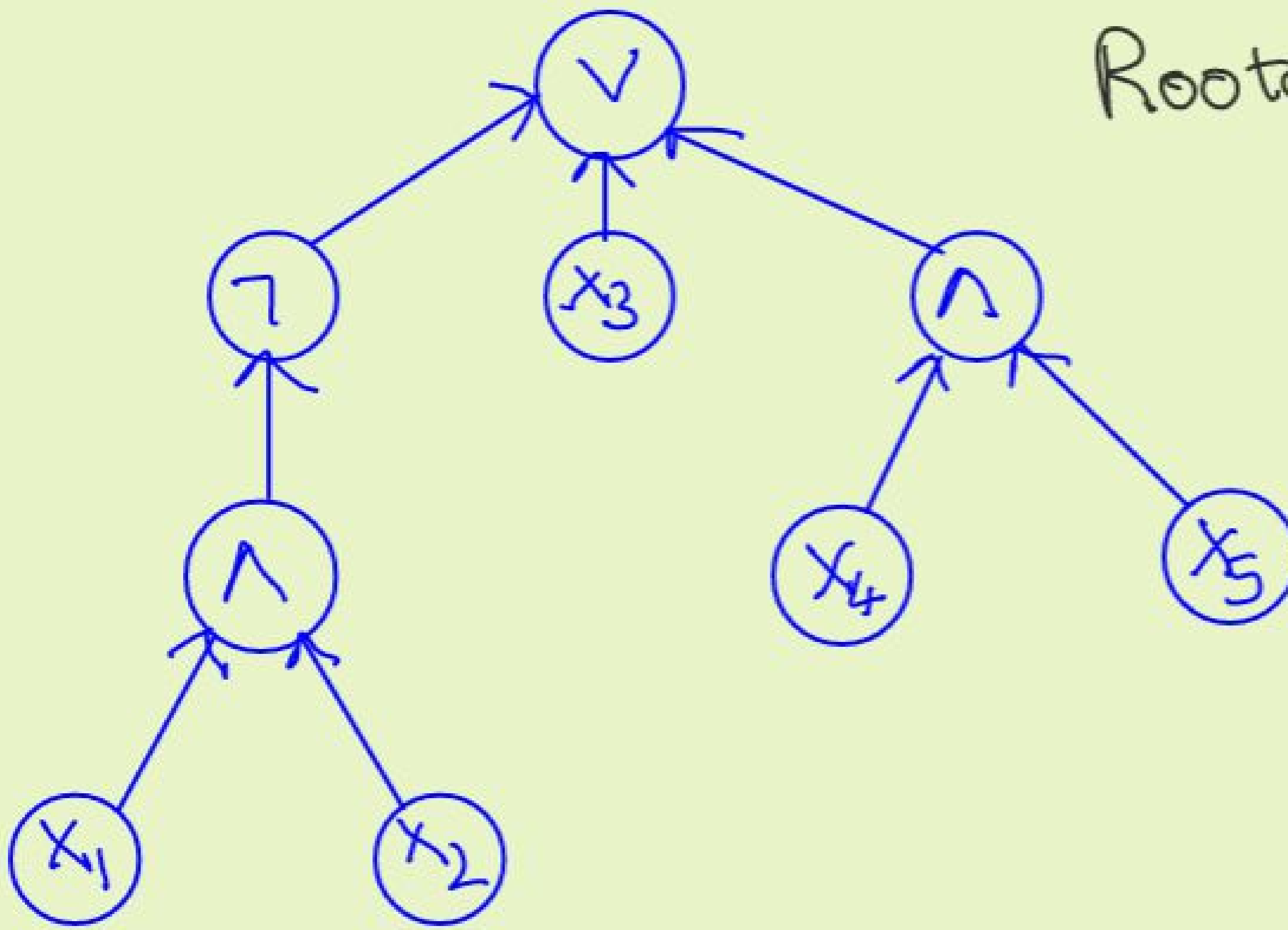
$$f(x_1, x_2, x_3, x_4, x_5) = \neg(x_1 \wedge x_2) \vee x_3 \vee (x_4 \wedge x_5)$$

Boolean formulas

$$f(x_1, x_2, x_3, x_4, x_5) = \underbrace{\neg(x_1 \wedge x_2) \vee x_3 \vee (x_4 \wedge x_5)}_{\text{Boolean formula}}$$

Boolean formulas

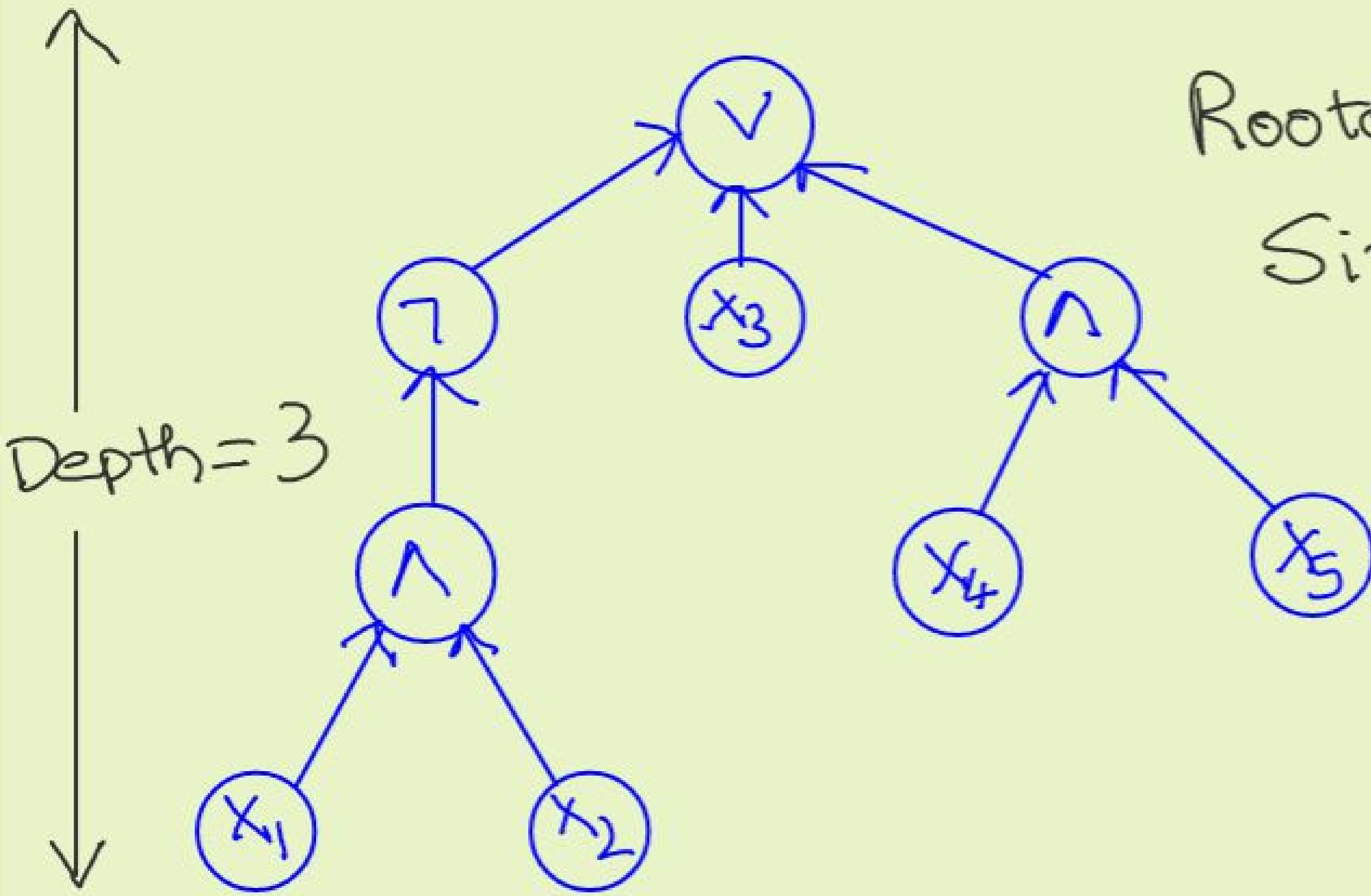
$$f(x_1, x_2, x_3, x_4, x_5) = \underbrace{\neg(x_1 \wedge x_2) \vee x_3 \vee (x_4 \wedge x_5)}_{\text{Boolean formula}}$$



Rooted directed tree

Boolean formulas

$$f(x_1, x_2, x_3, x_4, x_5) = \underbrace{\neg(x_1 \wedge x_2) \vee x_3 \vee (x_4 \wedge x_5)}_{\text{Boolean formula}}$$

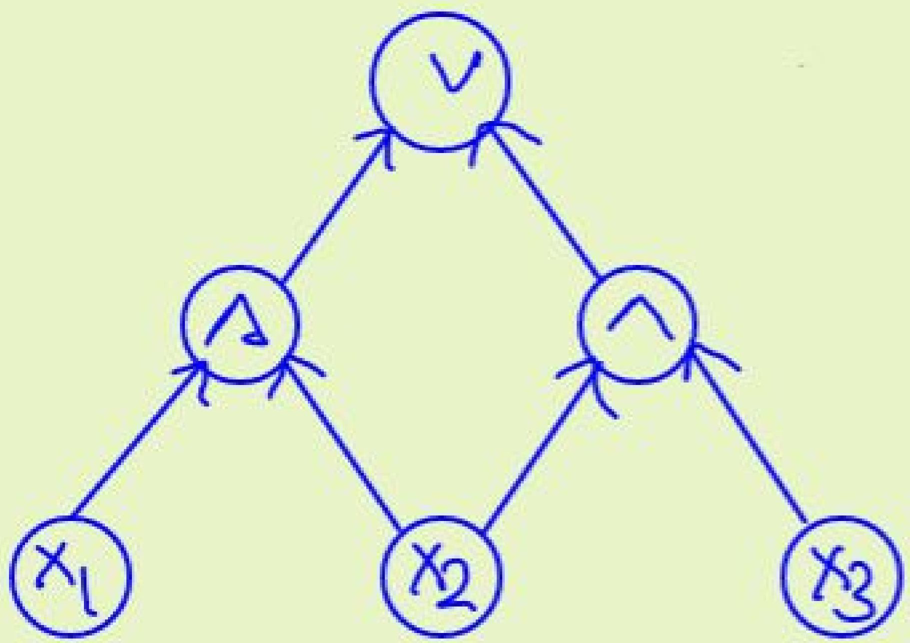


Rooted directed tree

Size = # of nodes
= 9

Boolean circuits

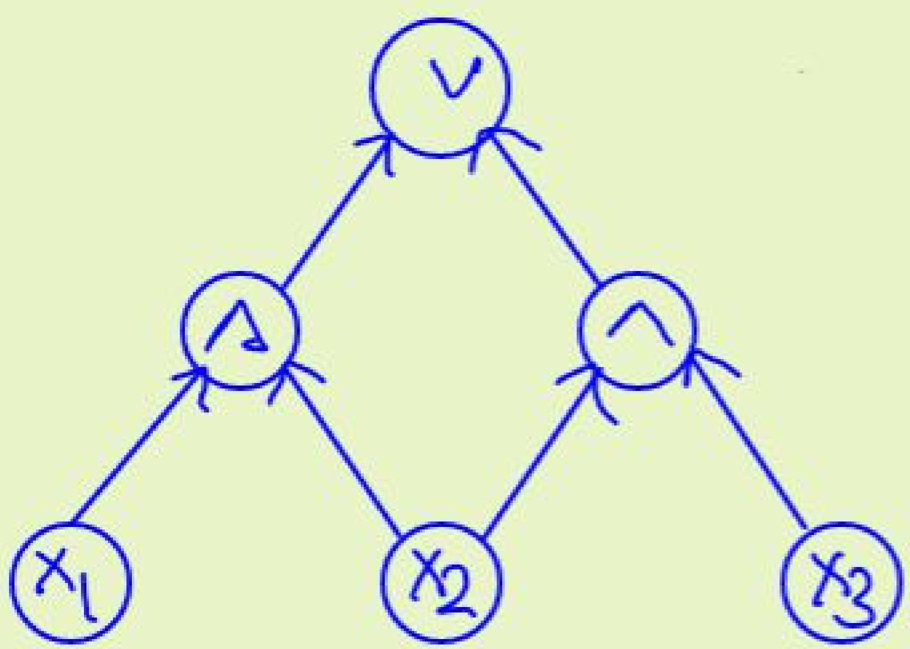
$f(x_1, x_2, x_3) =$



Boolean circuit

Boolean circuits

$f(x_1, x_2, x_3) =$



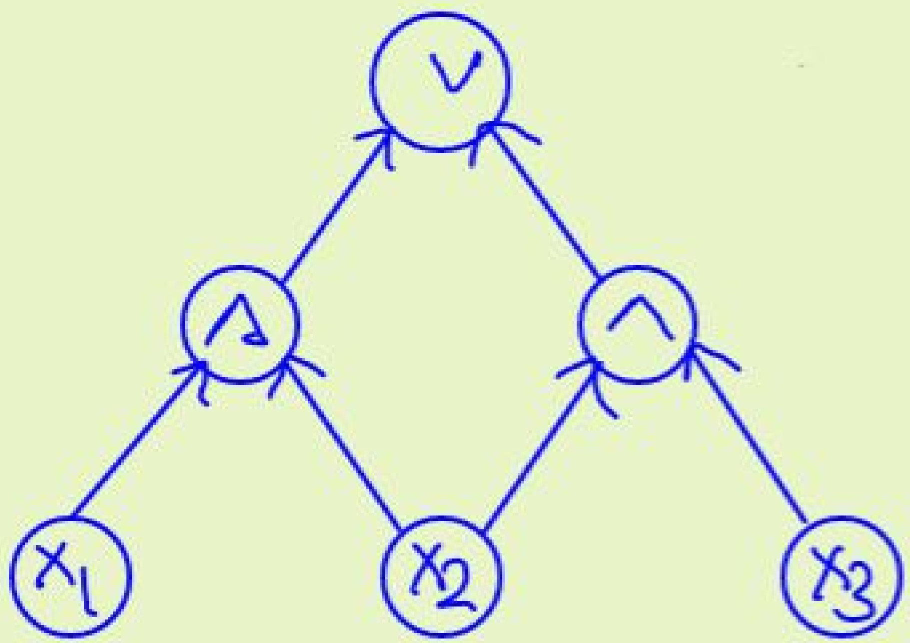
Boolean circuit

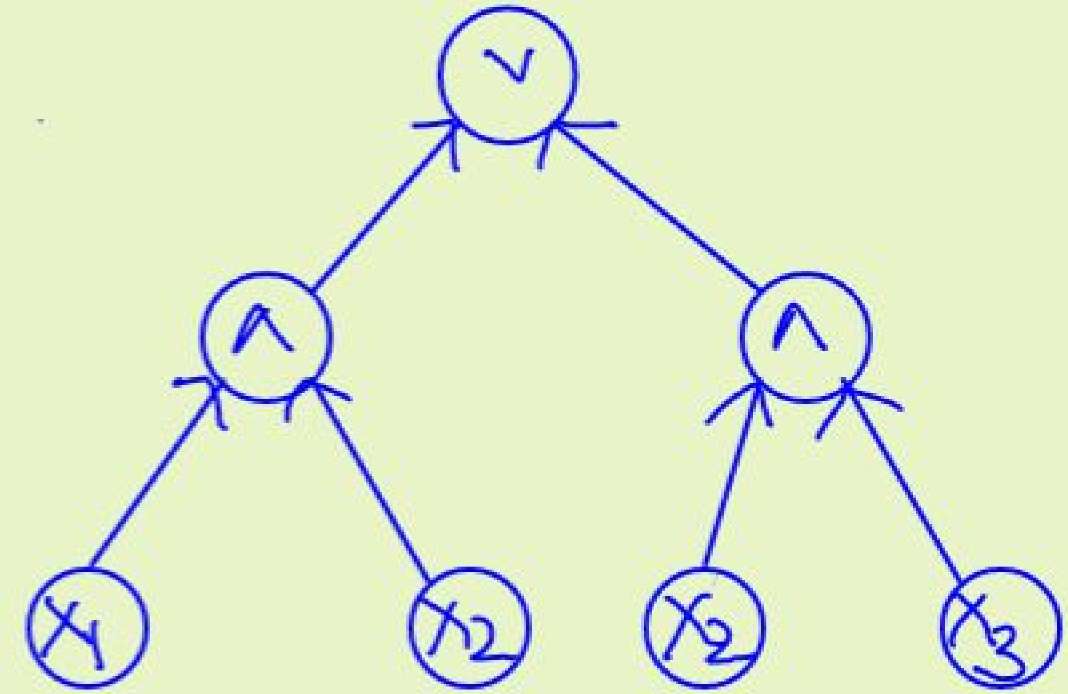
Size = # of nodes = 6

Depth = 2

Boolean circuits

$f(x_1, x_2, x_3) =$





Boolean circuit

Size = # of nodes = 6

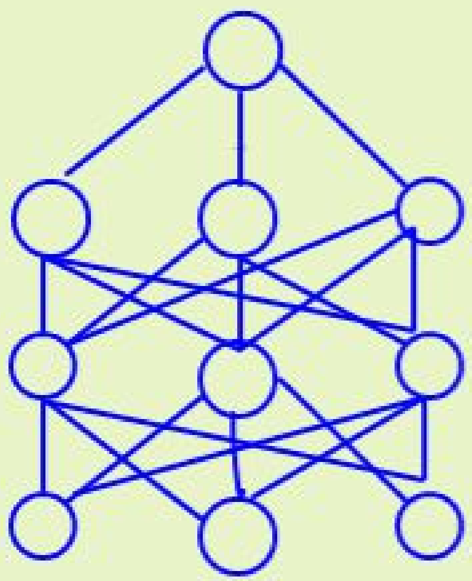
Depth = 2

Equivalent formula

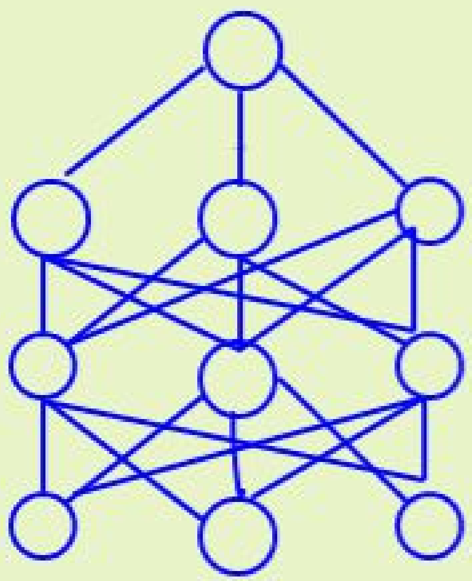
Size = 7

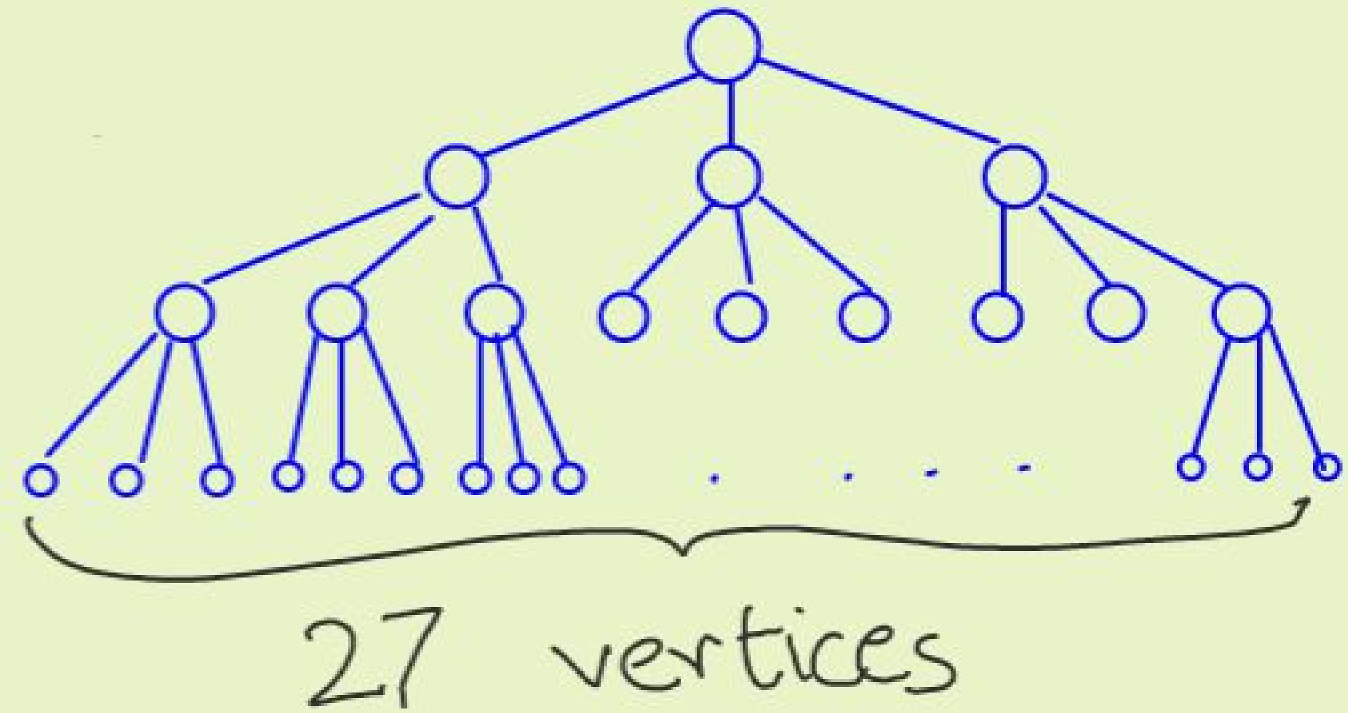
Depth = 2

Converting circuits to formulas

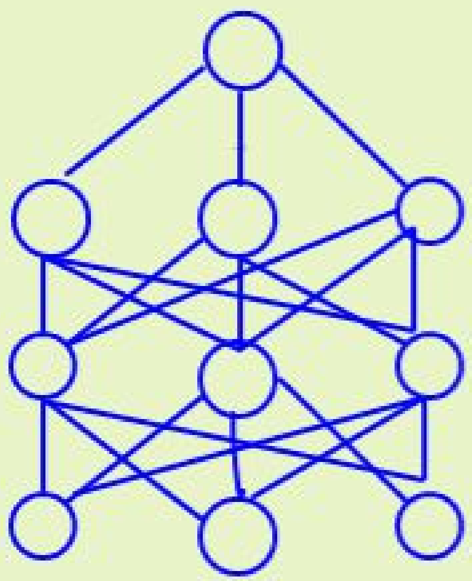


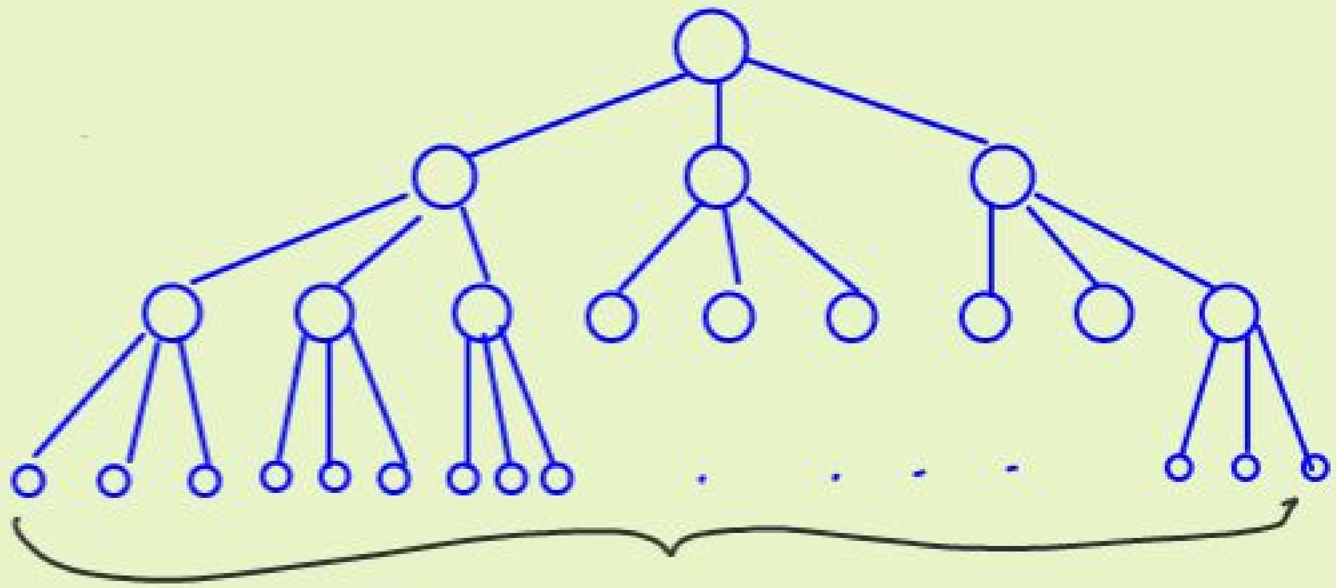
Converting circuits to formulas





Converting circuits to formulas



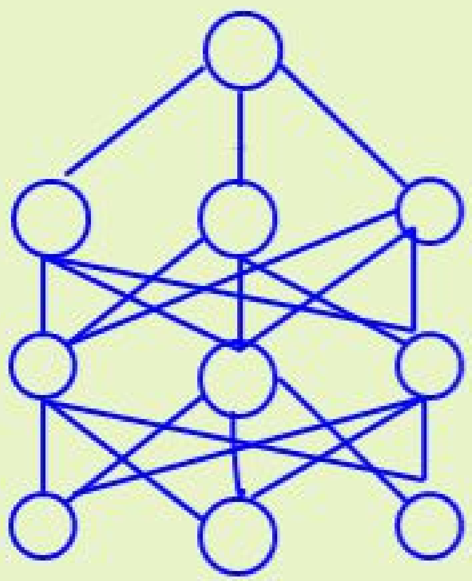


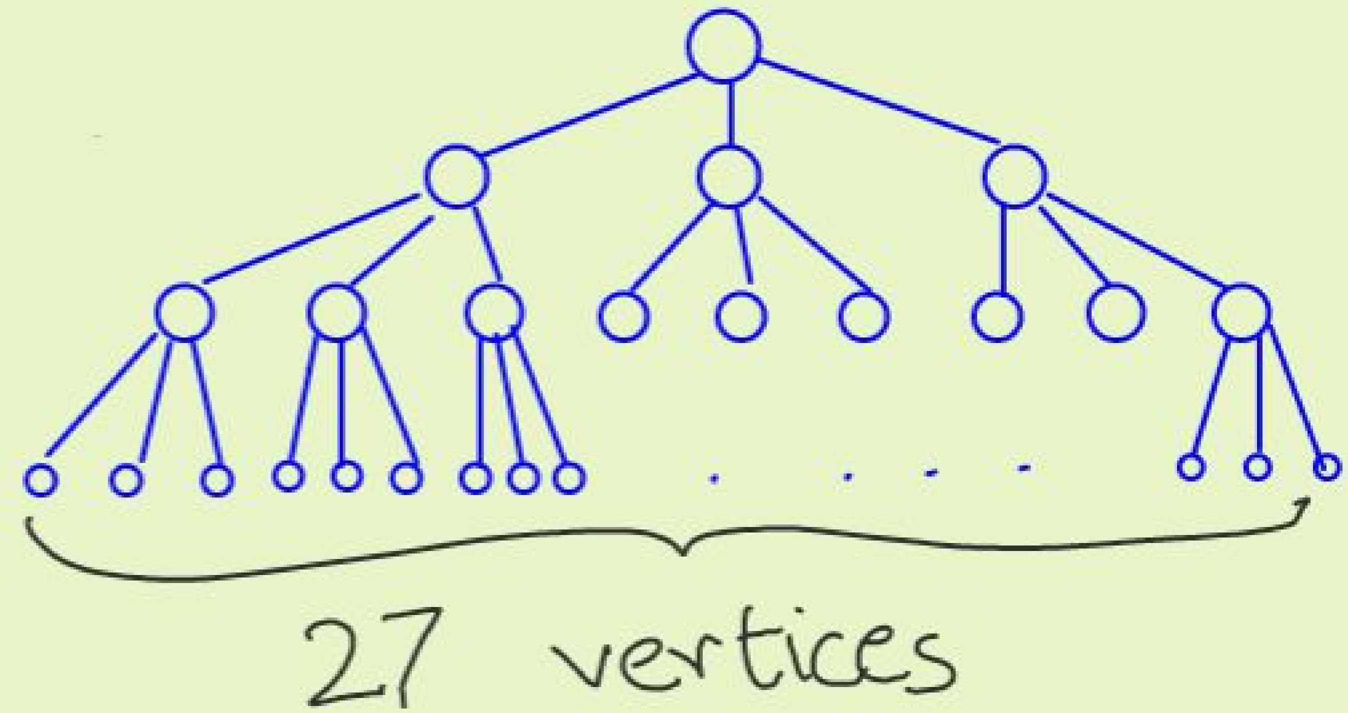
Circuit

size s $\longrightarrow$ Formula size s^d

depth d | depth d

Converting circuits to formulas





Circuit		Formula
size s	$\longrightarrow$	size s^d
depth d	Optimal?	depth d

Question

Can every circuit of size s be con-
-verted to a formula of size $\ll s^d$?

Question

Can every circuit of size s be con-
-verted to a formula of size $\ll s^d$?

Expected answer: NO

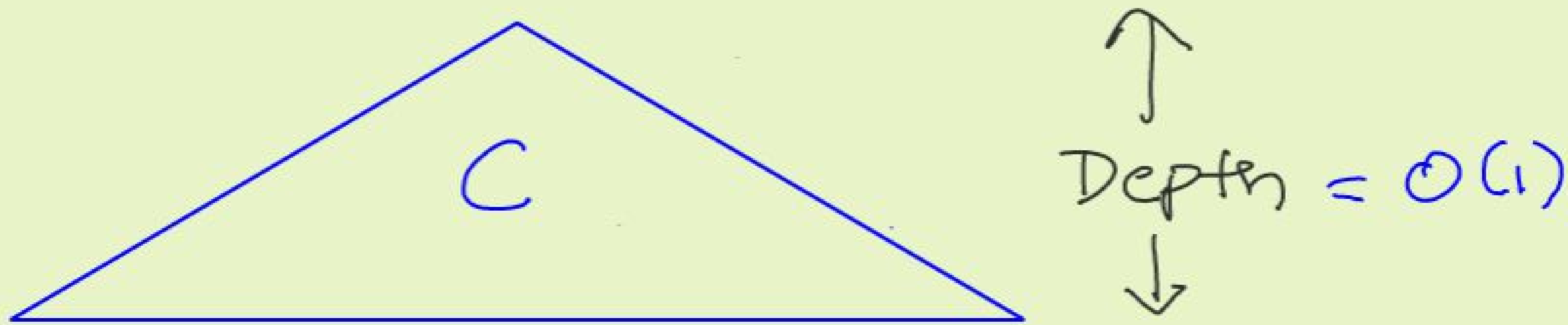
Question

Can every circuit of size s be con-
-verted to a formula of size $\ll s^d$?

Expected answer: NO

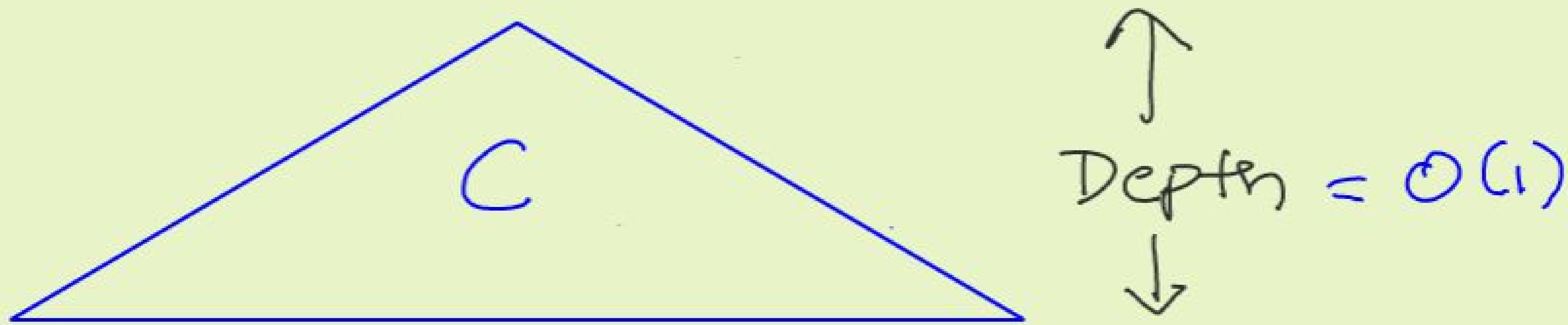
This work: $d = O(1)$

AC^0 ckts



Constant-depth $\{\wedge, \vee, \neg\}$ circuits

AC^0 ckts



Constant-depth $\{\wedge, \vee, \neg\}$ circuits

Eg: $d = 2$: DNF / CNF formulas.

Background on AC^0

Background on AC^0

1. Any $f:\{0,1\}^n \to \{0,1\}$ has a depth-2 AC^0 circuit of size 2^n.

Background on AC^0

1. Any $f:\{0,1\}^n \to \{0,1\}$ has a depth-2 AC^0 circuit of size 2^n.
2. There are f such that any AC^0 circuit computing f has size $\geq 2^{n/2}$.

Background on AC^0

3. $\mathrm{PARITY}(x_1, \ldots, x_n) \equiv \sum_i x_i \pmod 2$

Background on AC^0

3. $\mathrm{PARITY}(x_1, \ldots, x_n) \equiv \sum_i x_i \pmod 2$

Property: Cannot fix it to a value w/o fixing all inputs.

Background on AC^0

3. $\text{PARITY}(x_1, \ldots, x_n) \equiv \sum_i x_i \pmod 2$

Property: Cannot fix it to a value w/o fixing all inputs.

Compare: $\wedge(x_1, x_2, 0) = 0$

$\vee(1, x_2, x_3) = 1$

Background on AC^0

3. PARITY$(x_1, \ldots, x_n) \equiv \sum_i x_i \pmod 2$

Property: Cannot fix it to a value w/o fixing all inputs.

Compare: $\wedge(x_1, x_2, 0) = 0$

$\vee(1, x_2, x_3) = 1$

[Ajtai, Furst-Saxe-Sipser, ..., Håstad 80's]

Any AC^0 depth d ckt for PARITY has size $\geq 2^{\Omega(n^{1/d-1})}$.

Håstad's theorem

Any AC^0 depth d circuit for PARITY has size $2^{\Omega(n^{1/d-1})}$

Håstad's theorem

Any AC^0 depth d circuit for PARITY has size $2^{\Omega(n^{1/d-1})}$

* Tight!

Håstad's theorem

Any AC^0 depth d circuit for PARITY has size $2^{\Omega(n^{1/d-1})}$

* Tight!

Folklore: PARITY has circuits of size $2^{O(n^{1/d-1})}$

Rossman's theorem

Rossman's theorem

Any formula of depth d for PARITY has size $\geq 2^{\Omega(dn^{1/d-1})}$

Rossman's theorem

Any formula of depth d for PARITY has size $\geq 2^{\Omega(d n^{1/d-1})}$

Fact: PARITY has depth d circuits of size $2^{O(n^{1/d-1})}$

Rossman's theorem

Any formula of depth d for PARITY has size $\geq 2^{\Omega(dn^{1/d-1})}$

Fact: PARITY has depth d circuits of size $2^{O(n^{1/d-1})}$

Corollary: For $d = O(1)$, trivial circuit to formula conversion is tight.

$AC^0[\oplus]$ - a stronger ckt class

Stronger circuit classes?

$AC^0[\oplus]$ - a stronger ckt class

Stronger circuit classes?

Larger depth?

$AC^0[\oplus]$ - a stronger ckt class

Stronger circuit classes?

Larger depth? Richer set of operations?

$AC^0[\oplus]$ - a stronger ckt class

Stronger circuit classes?
Larger depth? Richer set of operations?

$AC^0[\oplus]$ circuits / formulas -
made up of $\{\wedge, \vee, \neg, \oplus\}$ - gates.

$AC^0[\oplus]$ - a stronger ckt class

Stronger circuit classes?
Larger depth? Richer set of operations?

$AC^0[\oplus]$ circuits / formulas -
made up of $\{\wedge, \vee, \neg, \oplus\}$ - gates.

Similar result for $AC^0[\oplus]$.

Our result

There is an $f : \{0,1\}^n \rightarrow \{0,1\}$ such that

Our result

There is an $f : \{0,1\}^n \rightarrow \{0,1\}$ such that

$\rightarrow$ f has an AC^0 ckt. of depth d and size s.

Our result

There is an $f : \{0,1\}^n \to \{0,1\}$ such that

→ f has an AC^0 ckt. of depth d and size s.

→ f has no $AC^0[\oplus]$ formula of depth d and size $< s^{\Omega(d)}$.

Our result

There is an $f:\{0,1\}^n \to \{0,1\}$ such that

→ f has an AC^0 ckt. of depth d and size s.

→ f has no $AC^0[\oplus]$ formula of depth d and size $< s^{\Omega(d)}$.

<u>Corollary</u>: Trivial conversion of $AC^0[\oplus]$ circuits to formulas is tight.

Boolean functions & Polynomials

$f: \{0,1\}^n \longrightarrow \{0,1\}$ $\qquad$ $f: \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$

Boolean functions & Polynomials

$f : \{0,1\}^n \longrightarrow \{0,1\}$ $\quad$ $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$

Any f can be expressed as a polynomial $P(\bar{x}) \in \mathbb{F}_2[x_1, \dots, x_n]$ s.t.

Boolean functions & Polynomials

$f : \{0,1\}^n \longrightarrow \{0,1\}$ $\quad$ $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$

Any f can be expressed as a polynomial $P(\bar{x}) \in \mathbb{F}_2[x_1, \ldots, x_n]$ s.t.

(1) $P(\bar{x}) = f(\bar{x}) \quad \forall\, \bar{x} \in \{0,1\}^n$

Boolean functions & Polynomials

$f : \{0,1\}^n \longrightarrow \{0,1\}$ $\quad f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$

Any f can be expressed as a polynomial $P(\bar{x}) \in \mathbb{F}_2[x_1, \dots, x_n]$ s.t.

1. $P(\bar{x}) = f(\bar{x}) \quad \forall \bar{x} \in \{0,1\}^n$
2. P is multilinear (no x_i^2)

Boolean functions & Polynomials

$f : \{0,1\}^n \longrightarrow \{0,1\}$ $\quad$ $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$

Any f can be expressed as a polynomial $P(\bar{x}) \in \mathbb{F}_2[x_1, \dots, x_n]$ s.t.

1. $P(\bar{x}) = f(\bar{x}) \quad \forall \bar{x} \in \{0,1\}^n$
2. P is multilinear (no x_i^2)
3. $\deg(P) \leq n$.

Boolean functions & Polynomials

$f : \{0,1\}^n \longrightarrow \{0,1\}$ $\quad$ $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$

Any f can be expressed as a polynomial $P(\bar{x}) \in \mathbb{F}_2[x_1, \dots, x_n]$ s.t.

1. $P(\bar{x}) = f(\bar{x}) \quad \forall \bar{x} \in \{0,1\}^n$
2. P is multilinear (no x_i^2)
3. $\deg(P) \leq n$.
4. P is unique.

Boolean functions & Polynomials

$f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$

① $f = \text{PARITY}(x_1, \ldots, x_n)$

② $f = \wedge(x_1, \ldots, x_n)$

③ $f = \vee(x_1, \ldots, x_n)$

Boolean functions & Polynomials

$f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$

① $f = \text{PARITY}(x_1, \ldots, x_n)$

$= \sum_i x_i$ $\qquad \deg(f) = 1$

② $f = \wedge(x_1, \ldots, x_n)$

③ $f = \vee(x_1, \ldots, x_n)$

Boolean functions & Polynomials

$f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$

① $f = \mathrm{PARITY}(x_1, \ldots, x_n)$

$= \sum_i x_i$ $\qquad \deg(f) = 1$

② $f = \wedge(x_1, \ldots, x_n)$

$= \prod_i x_i$ $\qquad \deg(f) = n$

③ $f = \vee(x_1, \ldots, x_n)$

Boolean functions & Polynomials

$f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$

① $f = \text{PARITY}(x_1, \ldots, x_n)$

$= \sum_i x_i$ $\qquad \deg(f) = 1$

② $f = \wedge(x_1, \ldots, x_n)$

$= \prod_i x_i$ $\qquad \deg(f) = n$

③ $f = \vee(x_1, \ldots, x_n)$

$= 1 + \prod_i (1 + x_i)$ $\qquad \deg(f) = n$

Polynomials & $AC^0[\oplus]$

f has small $AC^0[\oplus]$ ckt. $\overset{?}{\Longrightarrow}$ $\deg(f)$ small

Polynomials & $AC^0[\oplus]$

f has small $AC^0[\oplus]$ ckt. $\overset{?}{\Longrightarrow}$ $\deg(f)$ small

No: $\wedge$ has an $AC^0[\oplus]$ ckt. of size 1 but $\deg(\wedge) = n$.

Polynomials & $AC^0[\oplus]$

f has small $AC^0[\oplus]$ ckt. $\overset{?}{\Longrightarrow}$ $\deg(f)$ small

No: $\wedge$ has an $AC^0[\oplus]$ ckt. of size 1 but $\deg(\wedge) = n$.

Can be salvaged by

Polynomial Approximation

Polynomial approximation

$f : \mathbb{F}_2^n \to \mathbb{F}_2, \quad P \in \mathbb{F}_2[x_1, \ldots, x_n]$

Polynomial approximation

$f : \mathbb{F}_2^n \to \mathbb{F}_2$, $P \in \mathbb{F}_2[x_1, \ldots, x_n]$

$\varepsilon \in (0,1)$.

Polynomial approximation

$f : \mathbb{F}_2^n \to \mathbb{F}_2$, $P \in \mathbb{F}_2[x_1, \ldots, x_n]$

$\varepsilon \in (0,1)$.

P ε-approximates f if

$$\Pr_{\bar{x} \in_R \{0,1\}^n} [f(\bar{x}) \neq P(\bar{x})] \leq \varepsilon$$

Polynomial approximation

$f : \mathbb{F}_2^n \to \mathbb{F}_2$, $P \in \mathbb{F}_2[x_1, \ldots, x_n]$

$\varepsilon \in (0, 1)$.

P ε-approximates f if

$$\Pr_{\bar{x} \in_R \{0,1\}^n} [f(\bar{x}) \neq P(\bar{x})] \leq \varepsilon$$

Eg: $\wedge(x_1, \ldots, x_n)$ is $1/2^n$-approximated by the zero polynomial.

Polynomial approximation lemma

[Razborov 80_s]: f computed by an $AC^0[\oplus]$ circuit of size s and depth d.

f $1/10$-approximated by a poly. p of degree $O(\log s)^{d-1}$.

Polynomial approximation lemma

[Razborov 80s]: f computed by an $AC^0[\oplus]$ circuit of size s and depth d.

f $1/10$-approximated by a poly. p of degree $O(\log s)^{d-1}$.

$s = n^{O(1)} \Longrightarrow$ deg. $O(\log n)^{d-1} \ll n$

Approximation lower bounds

$$MAJ(x_1, \ldots, x_n) = \begin{cases} 1 & \text{if } |x| > n/2 \\ 0 & \text{otherwise} \end{cases}$$

$$|x| = \left| \{ i \mid x_i = 1 \} \right|$$

Approximation lower bounds

$$MAJ(x_1, \ldots, x_n) = \begin{cases} 1 & \text{if } |x| > n/2 \\ 0 & \text{otherwise} \end{cases}$$

$$|x| = \left|\{ i \mid x_i = 1 \}\right|$$

[Razborov] Any P $1/4$-approximating MAJ must have deg $\Omega(\sqrt{n})$.

Lemma 1: f has $AC^0[\oplus]$ ckt. size s, depth d

$\Rightarrow$ f has $1/10$-approx. poly of degree

$O(\log s)^{d-1}$.

Lemma 1: f has $AC^0[\oplus]$ ckt. size s, depth d

$\Rightarrow$ f has $1/10$-approx. poly of degree

$O(\log s)^{d-1}$.

Lemma 2: MAJ has no $1/4$-approximations

of degree $< \Omega(\sqrt{n})$.

Lemma 1: f has $AC^0[\oplus]$ ckt. size s, depth d

$\Rightarrow$ f has $1/10$-approx. poly of degree

$O(\log s)^{d-1}$.

Lemma 2: MAJ has no $1/4$-approximations

of degree $< \Omega(\sqrt{n})$.

$$\Downarrow$$

Any $AC^0[\oplus]$ ckt of depth d for MAJ

has size $\geq 2^{\Omega(n^{1/2(d-1)})}$

Tightness of Razborov's theorem

Any $AC^0[\oplus]$ ckt. for MAJ has size

$\geq 2^{\Omega(n^{1/2(d-1)})}$

Tightness of Razborov's theorem

Any $AC^0[\oplus]$ ckt. for MAJ has size

$$\geq 2^{\Omega(n^{1/2(d-1)})}$$

MAJ has AC^0 ckts of size

$$2^{O\left(n^{1/d-1}(\log n)^{1-1/d-1}\right)}$$

Tightness of Razborov's theorem

Any $AC^0[\oplus]$ ckt. for MAJ has size

$\geq 2^{\Omega(n^{1/2(d-1)})}$

MAJ has AC^0 ckts of size

$$2^{O(n^{1/d-1} (\log n)^{1-1/d-1})}$$

$d=3$: lower bound $2^{\Omega(n^{1/4})}$

upper bound $2^{O(\sqrt{n}\log n)}$

Variations in our proof

Say f has an $AC^0[\oplus]$ formula of size s and depth d.

Variations in our proof

Say f has an $AC^0[\oplus]$ formula of size s and depth d.

Stronger approx. lemma: f has a $1/10$-approx. poly. of degree $O\left(\frac{\log s}{d}\right)^{d-1}$.

Variations in our proof

Say f has an $AC^0[\oplus]$ formula of size s and depth d.

Stronger approx. lemma: f has a $1/10$-approx. poly. of degree $O\left(\frac{\log s}{d}\right)^{d-1}$.

$\Downarrow$ lemma 2 from Razborov

Variations in our proof

Say f has an $AC^0[\oplus]$ formula of size s and depth d.

Stronger approx. lemma: f has a $1/10$-approx. poly. of degree $O\left(\frac{\log s}{d}\right)^{d-1}$.

$\Downarrow$ lemma 2 from Razborov

Any $AC^0[\oplus]$ formula of depth d for MAJ has size $2^{\Omega(d \cdot n^{1/2(d-1)})}$.

Variations in our proof

Defn:

Variations in our proof

Defn: f a δ-approx. Majority (δ-A.M.)

if $$\Pr_{\bar{x} \in_R \{0,1\}^n} [f(\bar{x}) \neq MAJ(\bar{x})] \leq \delta$$

Variations in our proof

Defn: f a δ-approx. Majority (δ-A.M.)

if $\Pr_{\bar{x} \in_R \{0,1\}^n} [f(\bar{x}) \neq MAJ(\bar{x})] \leq \delta$

Obs: Razborov proves a ckt. lower bound for computing any $1/10$-A.M. f.

Variations in our proof

Defn: f a δ-approx. Majority (δ-A.M.)

if $$\Pr_{\bar{x} \in_R \{0,1\}^n} [f(\bar{x}) \neq MAJ(\bar{x})] \leq \delta$$

Obs: Razborov proves a ckt. lower bound for computing any $1/10$-A.M. f.

f — $\leq 1/10$ — P Poly. approx. lemma

Variations in our proof

Defn: f a δ-approx. Majority (δ-A.M.)

if $\Pr_{\bar{x} \in_R \{0,1\}^n} [f(\bar{x}) \neq MAJ(\bar{x})] \leq \delta$

Obs: Razborov proves a ckt. lower bound for computing any $1/10$-A.M. f.

$\frac{1}{10}$-A.M. $\leq 1/10$ f $\leq 1/10$ Poly. approx. lemma

MAJ P

Variations in our proof

Defn: f a δ-approx. Majority (δ-A.M.)

if $\Pr_{\bar{x} \in_R \{0,1\}^n} [f(\bar{x}) \neq MAJ(\bar{x})] \leq \delta$

Obs: Razborov proves a ckt. lower bound for computing any $1/10$-A.M. f.

$$\begin{tikzcd}
 & f \arrow[dl, dash, "\leq 1/10"'] \arrow[dr, dash, "\leq 1/10"] & \\
MAJ \arrow[rr, dash, "\leq 1/5"'] & & P
\end{tikzcd}$$

Variations in our proof

Defn: f a δ-approx. Majority (δ-A.M.)

if $$\Pr_{\bar{x} \in_R \{0,1\}^n} [f(\bar{x}) \neq MAJ(\bar{x})] \leq \delta$$

Obs: Razborov proves a ckt. lower bound for computing any $1/10$-A.M. f.

Also: Any $AC^0[\oplus]$ formula for f

has size $\geq 2^{\Omega(d n^{1/2(d-1)})}$.

Variations in our proof

Lemma: There is a $1/10$-AM f that has an AC^0 circuit of depth d & size $2^{O(n^{1/2(d-1)})}$

Variations in our proof

Lemma: There is a $1/10$-AM f that has an AC^0 circuit of depth d & size $2^{O(n^{1/2(d-1)})}$

Builds on: Valiant; Amano; Hoory, Magen, Pitassi.

Variations in our proof

Lemma: There is a $1/10$-AM f that has an AC^0 circuit of depth d & size $2^{O(n^{1/2(d-1)})}$

Variations in our proof

Lemma: There is a $1/10$-AM f that has an AC^0 circuit of depth d & size $2^{O(n^{1/2(d-1)})}$

Lemma: Any $AC^0[\oplus]$ formula for f has size $\geq 2^{\Omega(d n^{1/2(d-1)})}$

Variations in our proof

Lemma: There is a $1/10$-AM f that has an AC^0 circuit of depth d & size $2^{O(n^{1/2(d-1)})}$

Lemma: Any $AC^0[\oplus]$ formula for f has size $\geq 2^{\Omega(d\, n^{1/2(d-1)})}$

$$\Downarrow$$

Main theorem.

Stronger approx. lemma f has $AC^0[\oplus]$ formula of size s and depth d.

$\exists P$ of deg $\Delta = O\left(\frac{\log s}{d}\right)^{d-1}$ that $1/10$-approx. f.

Probabilistic polynomials

Probabilistic polynomials

$\mathbb{P}$ a Probabilistic polynomial (PP) if it is a random polynomial from $\mathbb{F}_2[x_1, \dots, x_n]$.

Probabilistic polynomials

$\mathbb{P}$ a Probabilistic polynomial (PP) if it is a random polynomial from $\mathbb{F}_2[x_1, \dots, x_n]$.

$\mathbb{P}$ of degree d if it takes values from degree $\leq d$ polynomials.

Probabilistic polynomials

$\mathbb{P}$ a Probabilistic polynomial (PP) if it is a random polynomial from $\mathbb{F}_2[x_1, \dots, x_n]$.

$\mathbb{P}$ of degree d if it takes values from degree $\leq d$ polynomials.

$\mathbb{P}$ δ-computes $f : \mathbb{F}_2^n \to \mathbb{F}_2$ if

$$\forall x \in \mathbb{F}_2^n \qquad \Pr_{\mathbb{P}}[\mathbb{P}(x) \neq f(x)] \leq \delta.$$

Example

1. Any $P \in \mathbb{F}_2[x_1, \dots, x_n]$

Example

1. Any $P \in \mathbb{F}_2[x_1, \dots, x_n]$
2. $y_1, y_2, y_3, y_4 \in_R \mathbb{F}_2$ independently chosen.

Example

1. Any $P \in \mathbb{F}_2[x_1, \ldots, x_n]$

2. $y_1, y_2, y_3, y_4 \in_R \mathbb{F}_2$ independently chosen.

$$\mathbb{P}(x_1, x_2) = ((1+x_1)\cdot y_1 + (1+x_2)\cdot y_2 + 1)\cdot$$
$$((1+x_1)\cdot y_3 + (1+x_2)\cdot y_4 + 1)$$

Example

1. Any $P \in \mathbb{F}_2[x_1, \dots, x_n]$

2. $y_1, y_2, y_3, y_4 \in_R \mathbb{F}_2$ independently chosen.

$$\mathbb{P}(x_1, x_2) = ((1+x_1)\cdot y_1 + (1+x_2)\cdot y_2 + 1)\cdot$$
$$((1+x_1)\cdot y_3 + (1+x_2)\cdot y_4 + 1)$$

Check: For any $x_1, x_2 \in \mathbb{F}_2$

$$\Pr_{y_1, y_2}[\mathbb{P}(x_1, x_2) \neq \mathrm{AND}(x_1, x_2)] \leq 1/4$$

Probabilistic polynomials

1. $\exists\, \mathbb{P}$ of deg d δ-computing f

Probabilistic polynomials

1. $\exists \mathbb{P}$ of deg d δ-computing f

$$\Downarrow \text{ Averaging}$$

$\exists P$ of deg d δ-approximating f

Probabilistic polynomials

1. $\exists \mathbb{P}$ of deg d δ-computing f

$$\Downarrow \text{ Averaging}$$

$\exists P$ of deg d δ-approximating f

2. For $f = \mathrm{PARITY}_n$, $\exists \mathbb{P}$ of deg 1 that δ-computes it.

Probabilistic polynomials

1. $\exists \mathbb{P}$ of deg d δ-computing f

$$\Downarrow \text{ Averaging}$$

$\exists P$ of deg d δ-approximating f

2. For $f = \mathrm{PARITY}_n$, $\exists \mathbb{P}$ of deg 1 that δ-computes it.

3. For $f = \mathrm{AND}_n$, $\exists \mathbb{P}$ of deg $O(\log 1/\delta)$ that δ-computes it. [Razborov]

Probabilistic polynomials

1. $\exists \mathbb{P}$ of deg d δ-computing f

$\Downarrow$ Averaging

$\exists P$ of deg d δ-approximating f

2. For $f = \mathrm{PARITY}_n$, $\exists \mathbb{P}$ of deg 1 that δ-computes it.

3. For $f = \mathrm{AND}_n$, $\exists \mathbb{P}$ of deg $O(\log 1/\delta)$ that δ-computes it. [Razborov]

(Also true for OR_n)

Probabilistic polynomials

4. $\exists \mathbb{P}$ of deg d $\frac{1}{10}$-computing f

$$\Downarrow \text{ Error reduction}$$

$\exists \mathbb{P}'$ of deg $d \log \frac{1}{\delta}$ δ-computing f

Probabilistic polynomials

4. $\exists \mathbb{P}$ of deg d $\frac{1}{10}$-computing f

$\Downarrow$ Error reduction

$\exists \mathbb{P}'$ of deg $d \log \frac{1}{\delta}$ δ-computing f

$$\mathbb{P}' = \mathrm{Maj}_t(\underbrace{\mathbb{P}_1, \ldots, \mathbb{P}_t}_{\text{independent samples of } \mathbb{P}})$$

Probabilistic polynomials

4. $\exists\, \mathbb{P}$ of deg d $\frac{1}{10}$-computing f

$\Downarrow$ Error reduction

$\exists\, \mathbb{P}'$ of deg $d \log \frac{1}{\delta}$ δ-computing f

$$\mathbb{P}' = \mathrm{Maj}_t(\underbrace{\mathbb{P}_1, \ldots, \mathbb{P}_t}) \longrightarrow \log \frac{1}{\delta}$$

independent samples

of $\mathbb{P}$

Probabilistic polynomials

4. $\exists \mathbb{P}$ of deg d $\frac{1}{10}$-computing f

$\Downarrow$ Error reduction

$\exists \mathbb{P}'$ of deg $d \log \frac{1}{\delta}$ δ-computing f

$$\mathbb{P}' = \mathrm{Maj}_t(\underbrace{\mathbb{P}_1, \ldots, \mathbb{P}_t}) \rightarrow \log \frac{1}{\delta}$$

$\swarrow$ independent samples

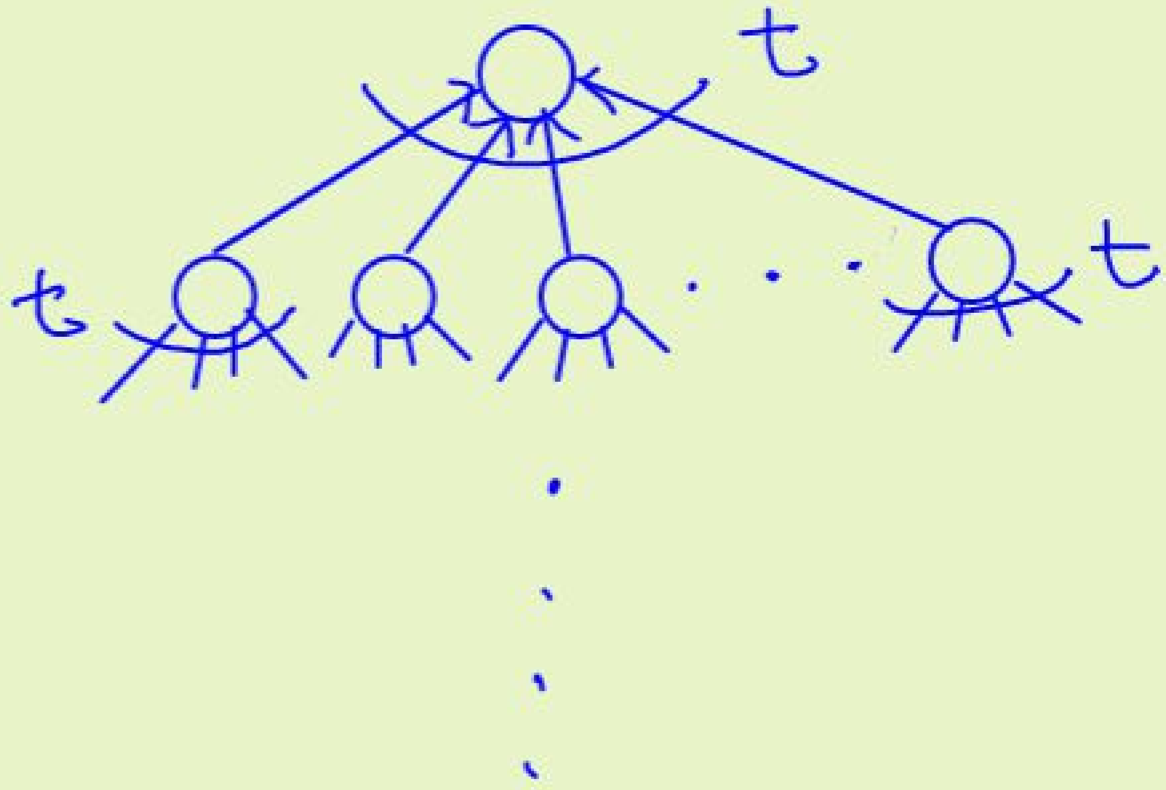
$\deg \le t$ of $\mathbb{P}$

Stronger approx. lemma f has $AC^0[\oplus]$ formula of size s and depth d.
$\exists \mathbb{P}$ of deg $\Delta = O\left(\frac{\log s}{d}\right)^{d-1}$ that $1/10$-computes f.

Stronger approx. lemma f has $AC^0[\oplus]$ formula of size s and depth d.

$\exists \mathbb{P}$ of deg $\Delta = O\left(\frac{\log s}{d}\right)^{d-1}$ that $1/10$-computes f.

Simpler case:



t - Regular formula

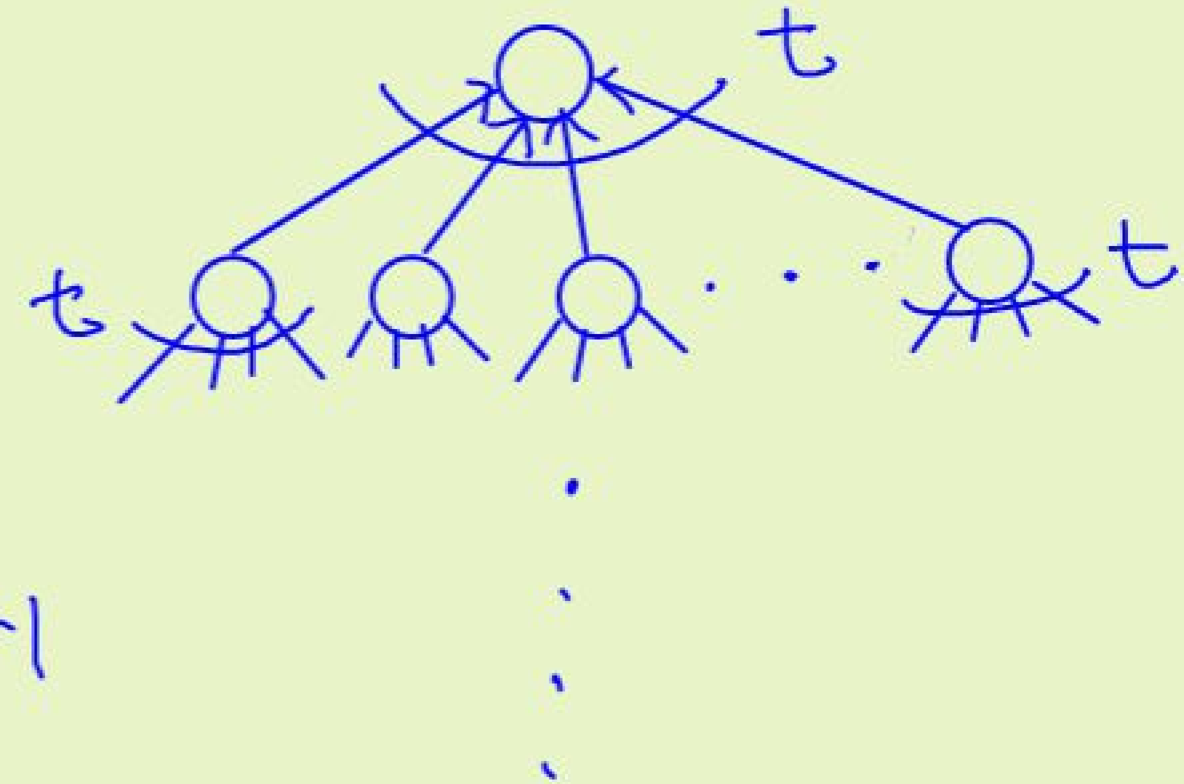
Stronger approx. lemma

f has $AC^0[\oplus]$ formula of size s and depth d.

$\exists \mathbb{P}$ of deg $\Delta = O\left(\frac{\log s}{d}\right)^{d-1}$ that $\frac{1}{10}$-computes f.

Simpler case:

t-Regular formula



$\deg \Delta = O(\log t)^{d-1}$

Stronger approx. lemma f has $AC^0[\oplus]$

t-regular formula of depth d.

$\exists\ \mathbb{P}$ of deg $\Delta = O(\log t)^{d-1}$ $1/10$-computing f.

Stronger approx. lemma f has $AC^0[\oplus]$

t-regular formula of depth d.

$\exists$ $\mathbb{P}$ of deg $\Delta = O(\log t)^{d-1}$ $1/10$-computing f.

Pf: Induction on d

Stronger approx. lemma

f has $AC^0[\oplus]$ t-regular formula of depth d.

$\exists \mathbb{P}$ of deg $\Delta = O(\log t)^{d-1}$ $1/10$-computing f.

<u>Pf</u>: Induction on d

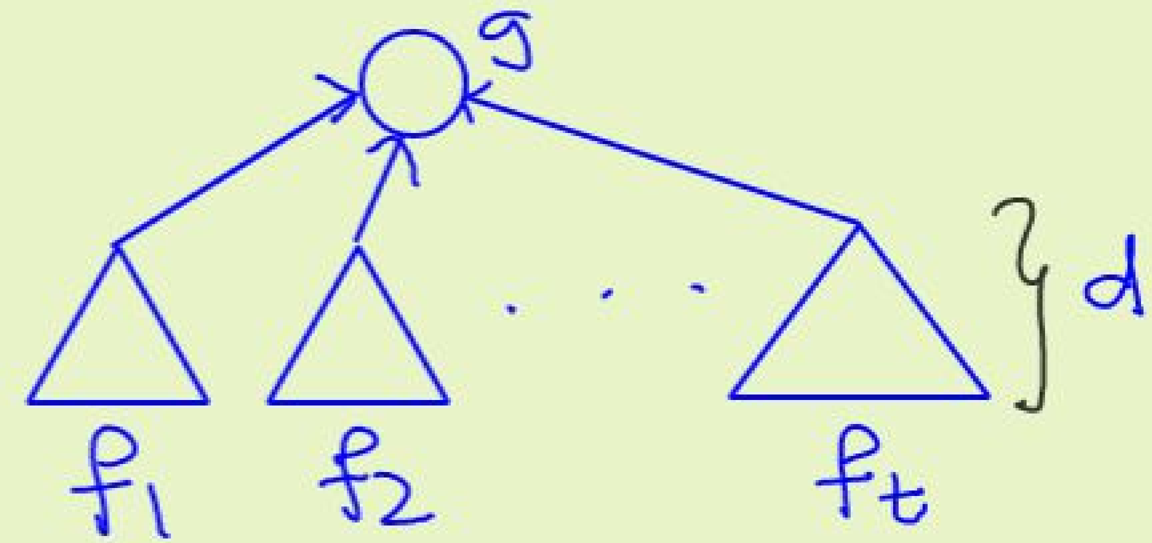
$d=1$: Razborov's construction of probabilistic polys for OR_t / AND_t of deg $O(1)$.

Stronger approx. lemma f has $AC^0[\oplus]$

t-regular formula of depth d.

$\exists$ $\mathbb{P}$ of deg $\Delta = O(\log t)^{d-1}$ $1/10$-computing f.

Pf: $d \to d+1$



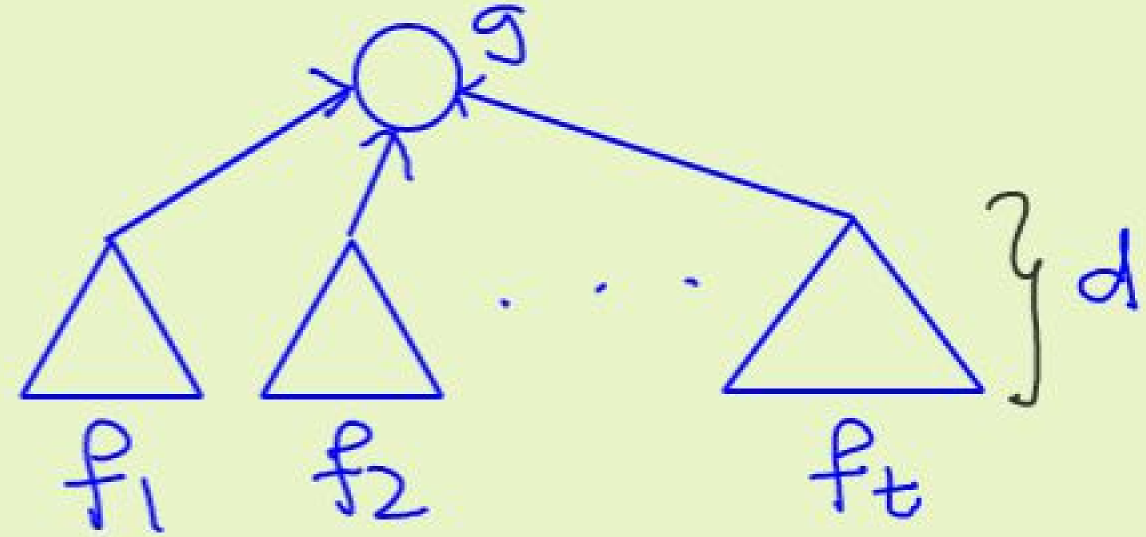
Stronger approx. lemma

f has $AC^0[\oplus]$ t-regular formula of depth d.

$\exists\, \mathbb{P}$ of deg $\Delta = O(\log t)^{d-1}$ $1/10$-computing f.

Pf: $d \to d+1$

$\mathbb{P}_i$ $1/10$-computing f_i of deg $O(\log t)^{d-1}$

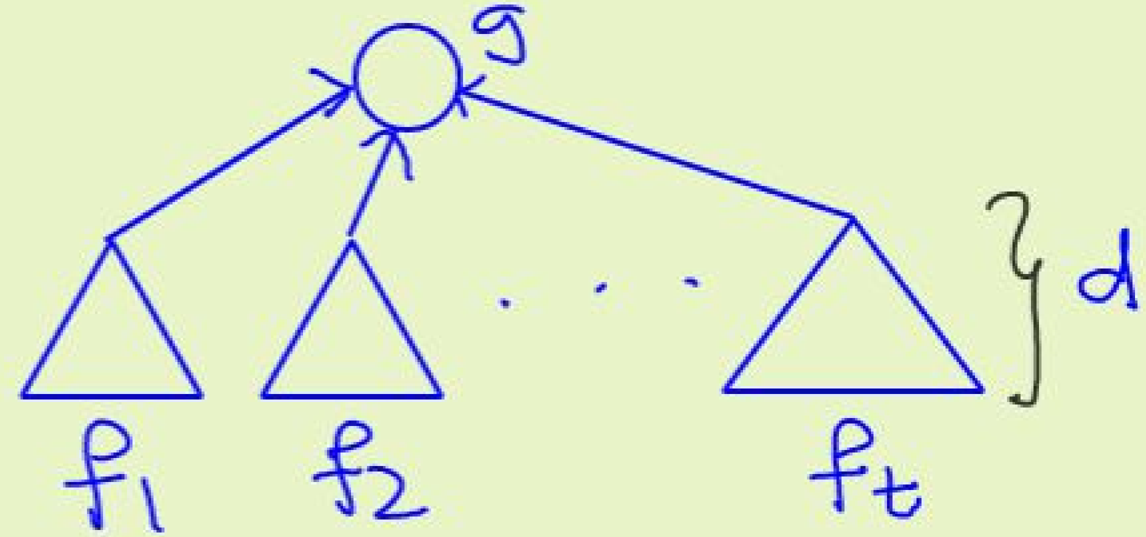


Stronger approx. lemma

f has $AC^0[\oplus]$ t-regular formula of depth d.

$\exists \mathbb{P}$ of deg $\Delta = O(\log t)^{d-1}$ $1/10$-computing f.

Pf: $d \to d+1$



$\mathbb{P}_i$ $1/10$-computing f_i

of deg $O(\log t)^{d-1}$

$\Downarrow$ Error reduction

$\mathbb{P}_i'$ $1/20t$-computing f_i

of deg $O(\log t)^d$

Stronger approx. lemma

f has $AC^0[\oplus]$

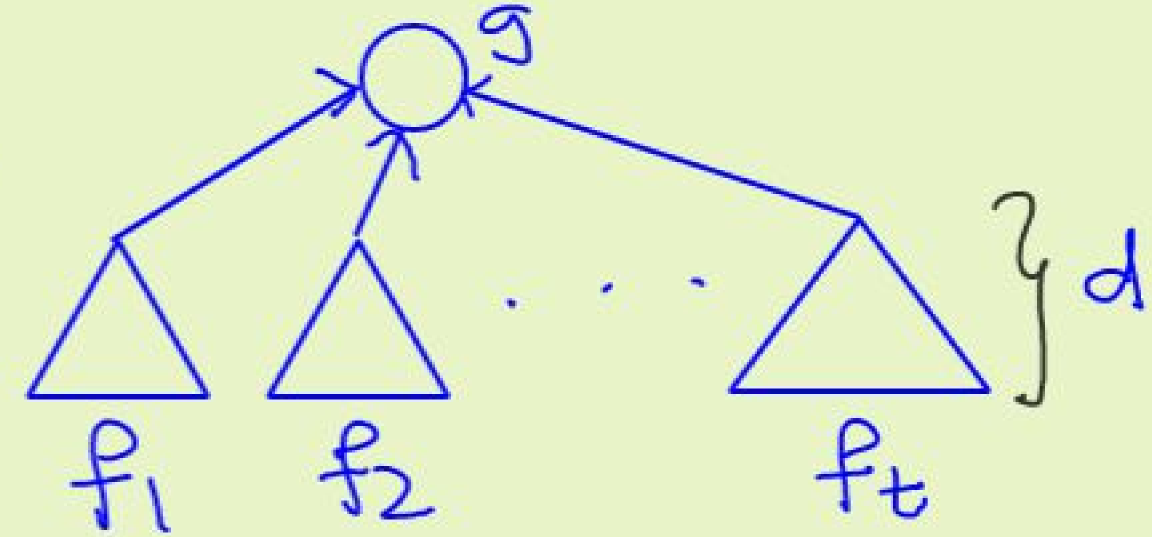
t-regular formula of depth d.

$\exists\, \mathbb{P}$ of deg $\Delta = O(\log t)^{d-1}$ $1/10$-computing f.

Pf: $d \longrightarrow d+1$

$\mathbb{P}_i'$ $1/20t$-computing f_i

of deg $O(\log t)^d$

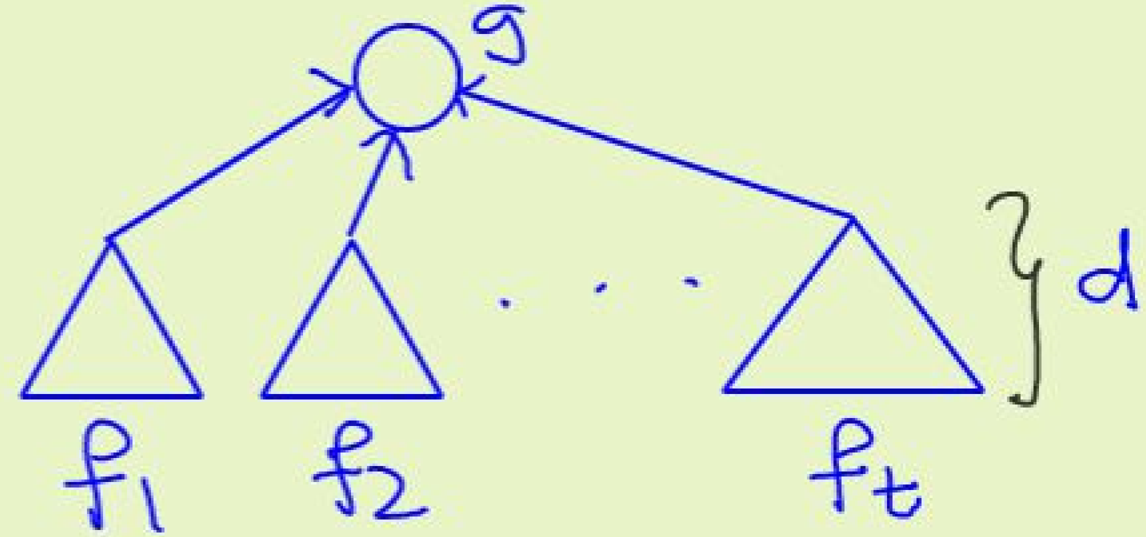


Stronger approx. lemma f has $AC^0[\oplus]$

t-regular formula of depth d.

$\exists\, \mathbb{P}$ of deg $\Delta = O(\log t)^{d-1}$ $1/10$-computing f.

Pf: $d \to d+1$



$\mathbb{P}_i'$ $1/20t$-computing f_i

of deg $O(\log t)^d$

$\tilde{\mathbb{P}}$ $1/20$-computing g

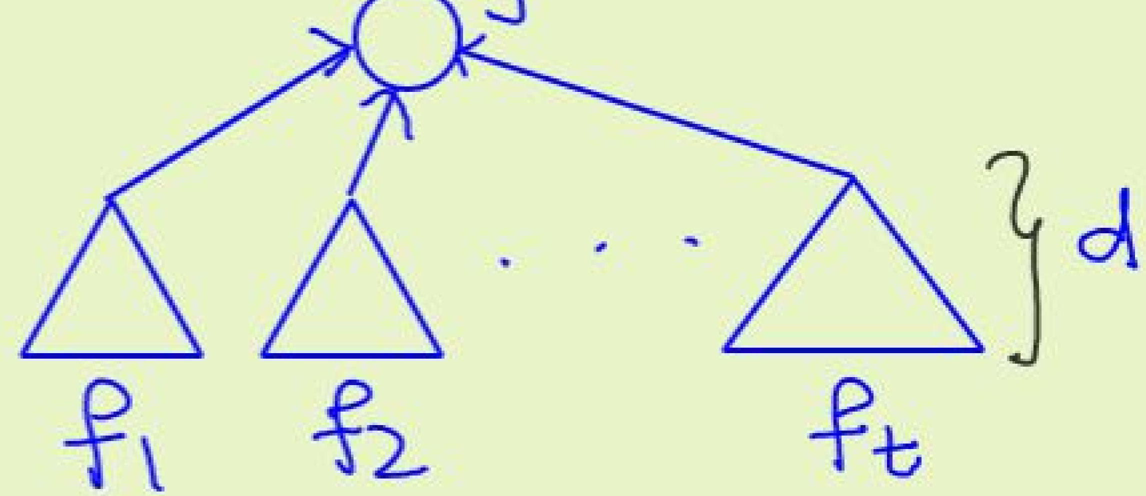
of deg $O(1)$

Stronger approx. lemma

f has $AC^0[\oplus]$ t-regular formula of depth d.

$\exists\, \mathbb{P}$ of deg $\Delta = O(\log t)^{d-1}$ $\frac{1}{10}$-computing f.

Pf: $d \to d+1$



$\mathbb{P}'_i$ $\frac{1}{20t}$-computing f_i

of deg $O(\log t)^d$

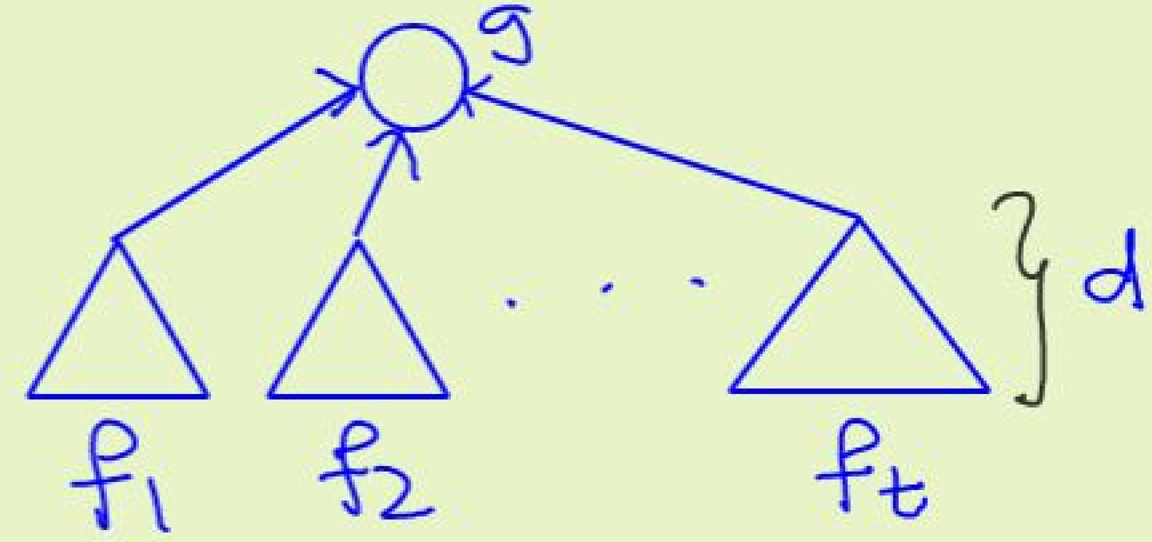
$\tilde{\mathbb{P}}$ $\frac{1}{20}$-computing g

of deg $O(1)$

$\mathbb{P} = \tilde{\mathbb{P}}(\mathbb{P}'_1, \dots, \mathbb{P}'_t)$

deg $O(\log t)^d$

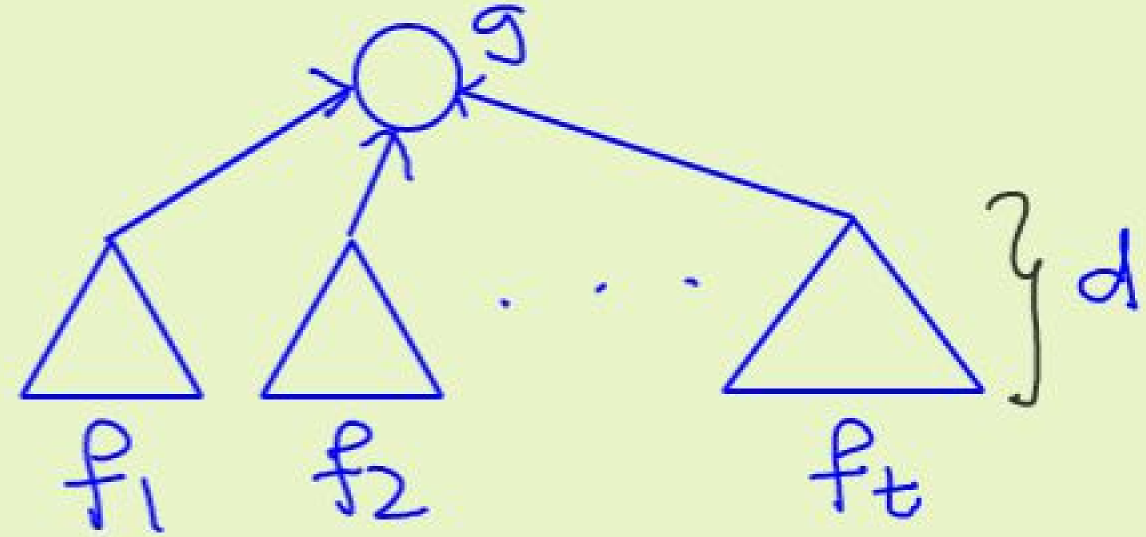
Irregular case



$\text{Size}(f_i) = s_i$

Irregular case

Π_i $\frac{1}{10}$ - computes f_i. of deg. Δ_i

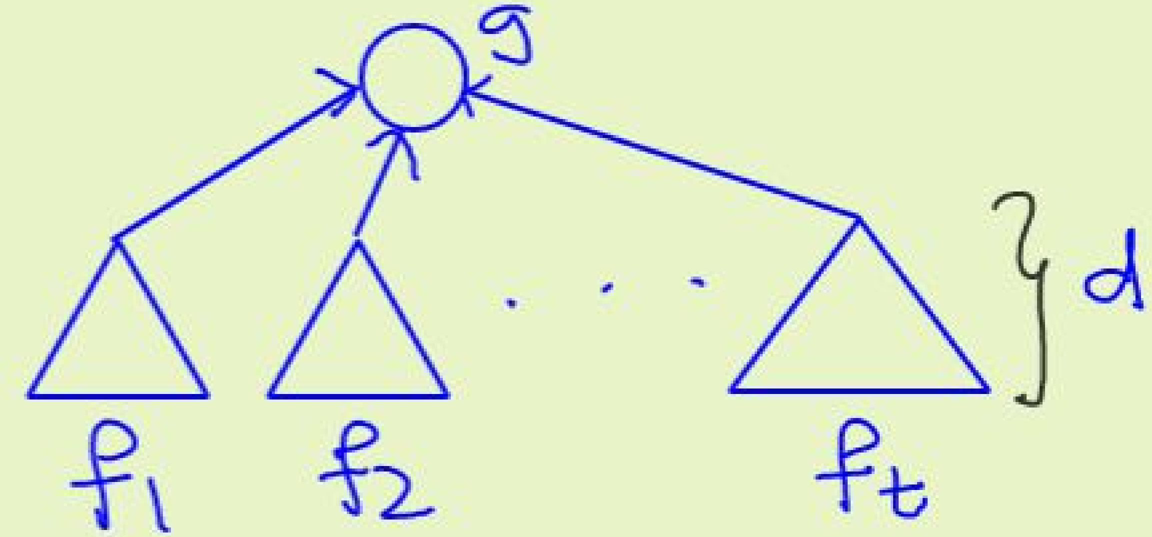


$\text{Size}(f_i) = s_i$

Irregular case

$\mathbb{P}_i$ $1/10$ - computes f_i of deg Δ_i

$\mathbb{P}_i'$ $\frac{s_i}{20s}$ - computes f_i of deg $O(\Delta_i \log \frac{s}{s_i})$



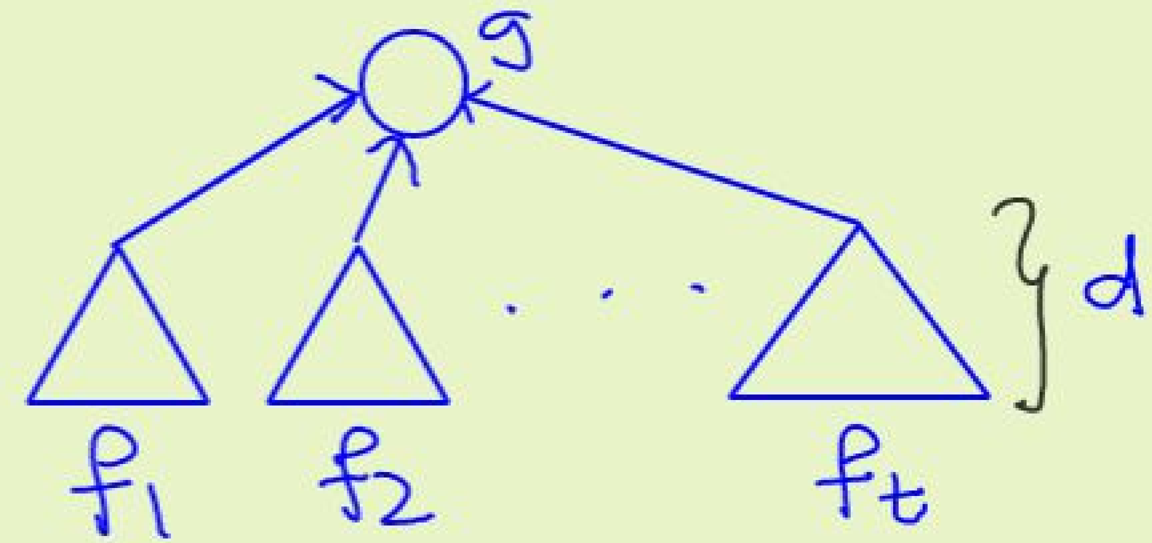
$\mathrm{Size}(f_i) = s_i$

Irregular case

$\mathbb{P}_i$ $1/10$ - computes f_i of deg Δ_i

$\mathbb{P}_i'$ $\frac{s_i}{20s}$ - computes f_i of deg $O(\Delta_i \log \frac{s}{s_i})$

$\tilde{\mathbb{P}}$ $1/20$ - computes g of deg $O(1)$



$\mathrm{Size}(f_i) = s_i$

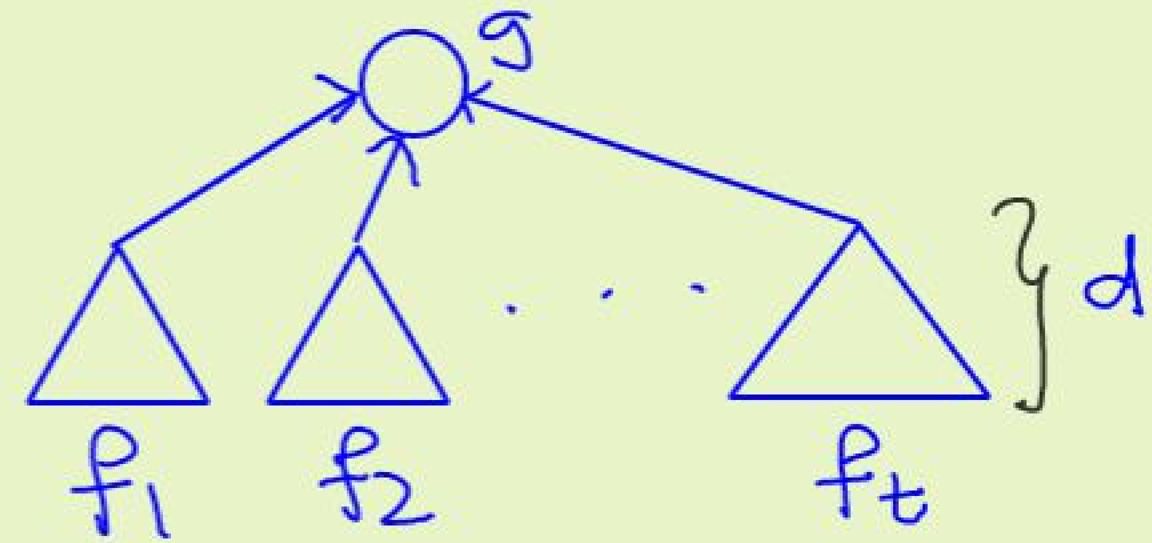
Irregular case

$\mathbb{P}_i$ $\frac{1}{10}$-computes f_i of deg Δ_i

$\mathbb{P}_i'$ $\frac{s_i}{20s}$-computes f_i of deg $O(\Delta_i \log \frac{s}{s_i})$

$\tilde{\mathbb{P}}$ $\frac{1}{20}$-computes g of deg $O(1)$

$\mathbb{P} = \tilde{\mathbb{P}}(\mathbb{P}_1', \dots, \mathbb{P}_t')$



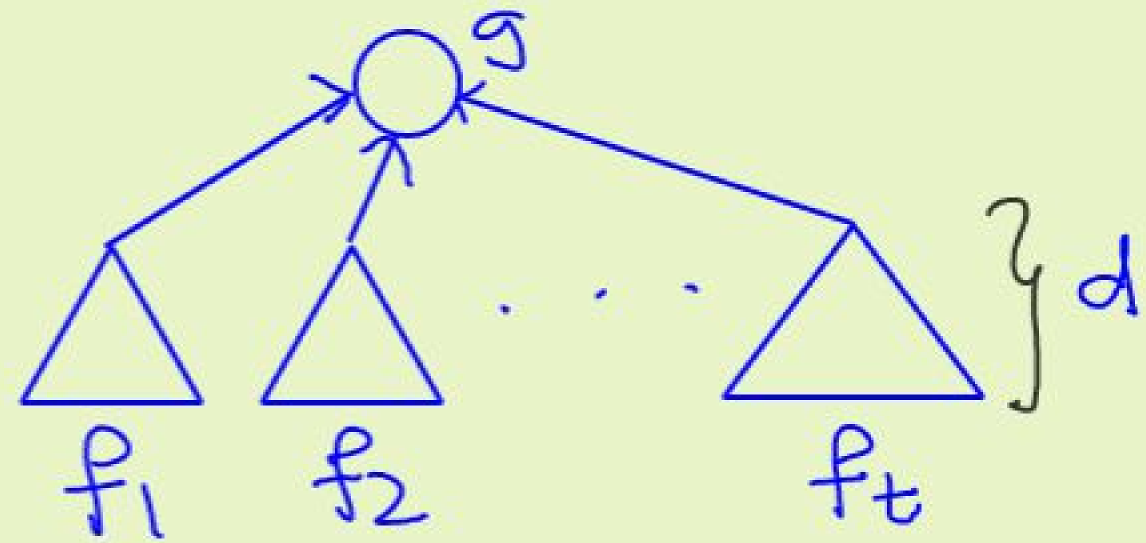
$\mathrm{Size}(f_i) = s_i$

Irregular case

$\mathbb{P}_i$ $\frac{1}{10}$-computes f_i of deg Δ_i

$\mathbb{P}_i'$ $\frac{s_i}{20s}$-computes f_i of deg $O(\Delta_i \log \frac{s}{s_i})$

$\tilde{\mathbb{P}}$ $\frac{1}{20}$-computes g of deg $O(1)$



$\mathbb{P} = \tilde{\mathbb{P}}(\mathbb{P}_1', \dots, \mathbb{P}_t')$

$\text{Size}(f_i) = s_i$

$\deg(\mathbb{P}) = \deg(\tilde{\mathbb{P}}) \cdot \max_i \deg(\mathbb{P}_i')$

Questions

Questions

① Optimal AC^0 circuit for MAJ

Questions

1. Optimal AC^0 circuit for MAJ
2. Our AMs are constructed probabilistically. Explicit AM with small AC^0 circuits?

Questions

① Optimal AC^0 circuit for MAJ

② Our AMs are constructed probabilistically. Explicit AM with small AC^0 circuits?

Thanks!