THE COIN PROBLEM & $AC^{\circ}[\oplus]$

SRIKANTH SRINIVASAN
IITB MATH.

JOINT WITH:

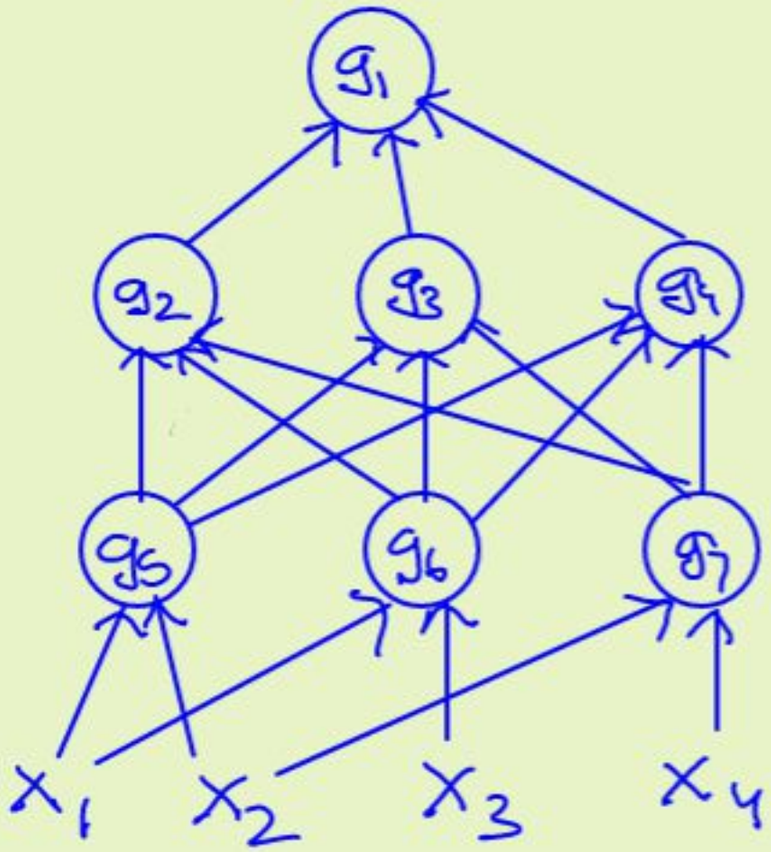
NUTAN LIMAYE (IITB CSE)

KARTEEK SREENIVASAIAH (IITH CSE)

UTKARSH TRIPATHI (IITB MATH)

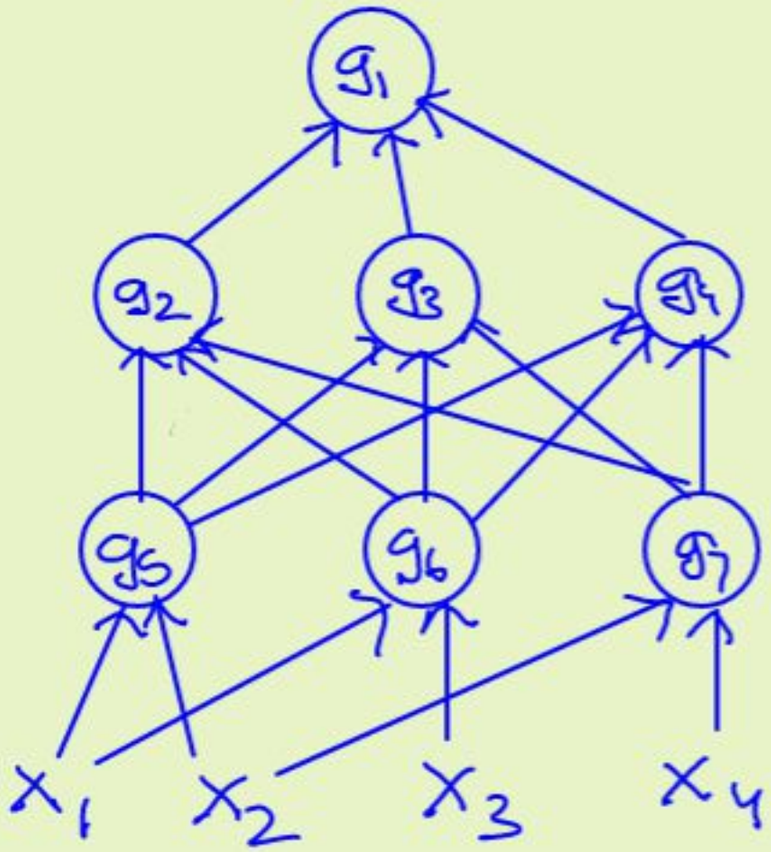
S VENKITESH (IITB MATH)

Boolean Circuits



→ Directed Acyclic Graph

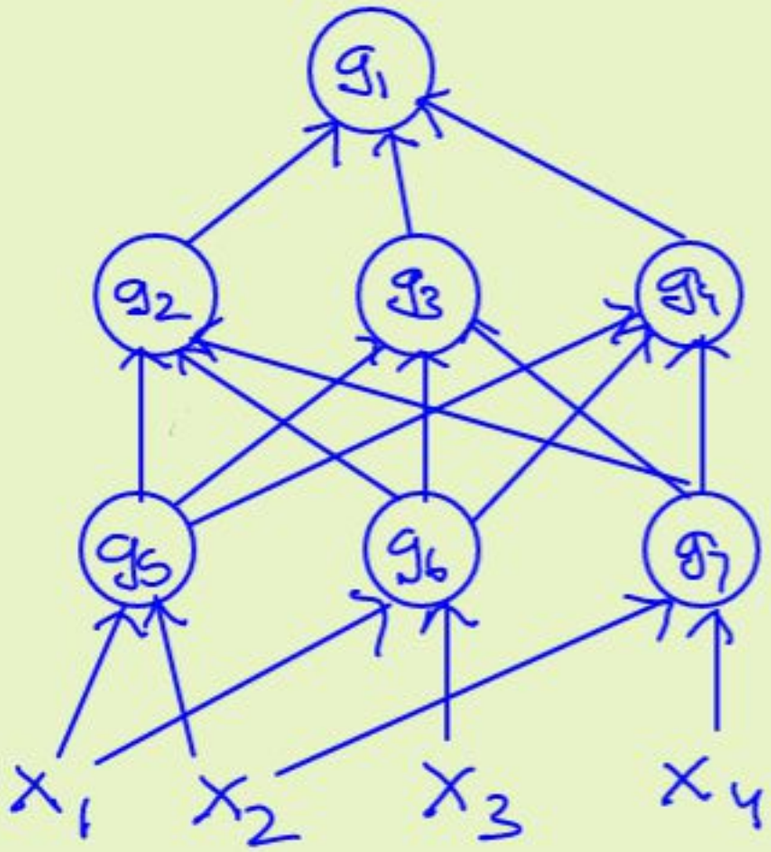
Boolean Circuits



→ Directed Acyclic Graph

↪ $g_i \in$ "Simple Ops"

Boolean Circuits



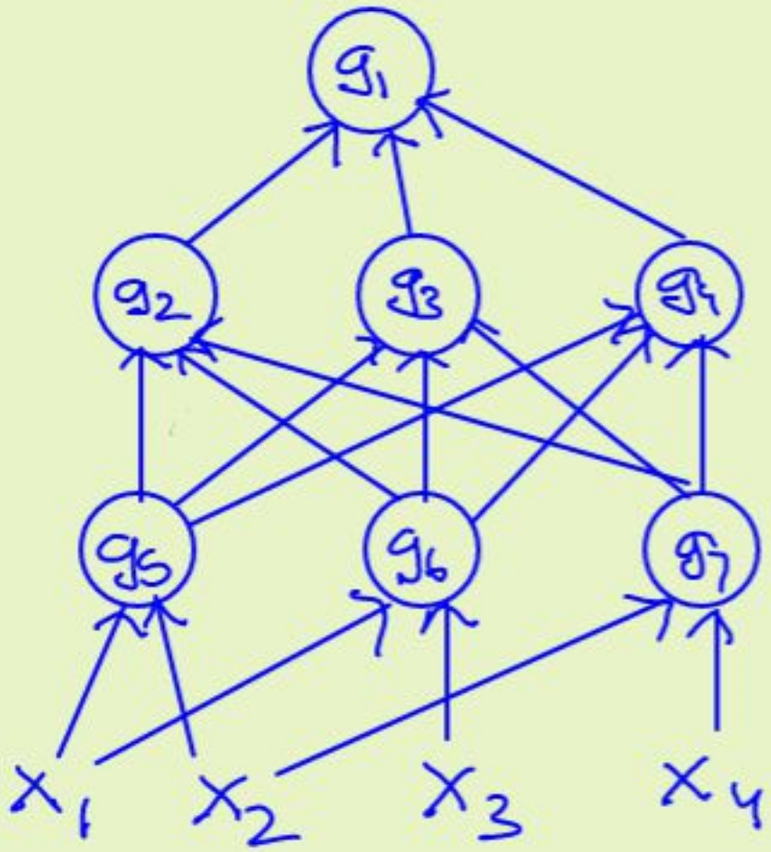
→ Directed Acyclic Graph

⟶ $g_i \in$ "Simple Ops"

⟶ Computes

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

Boolean Circuits



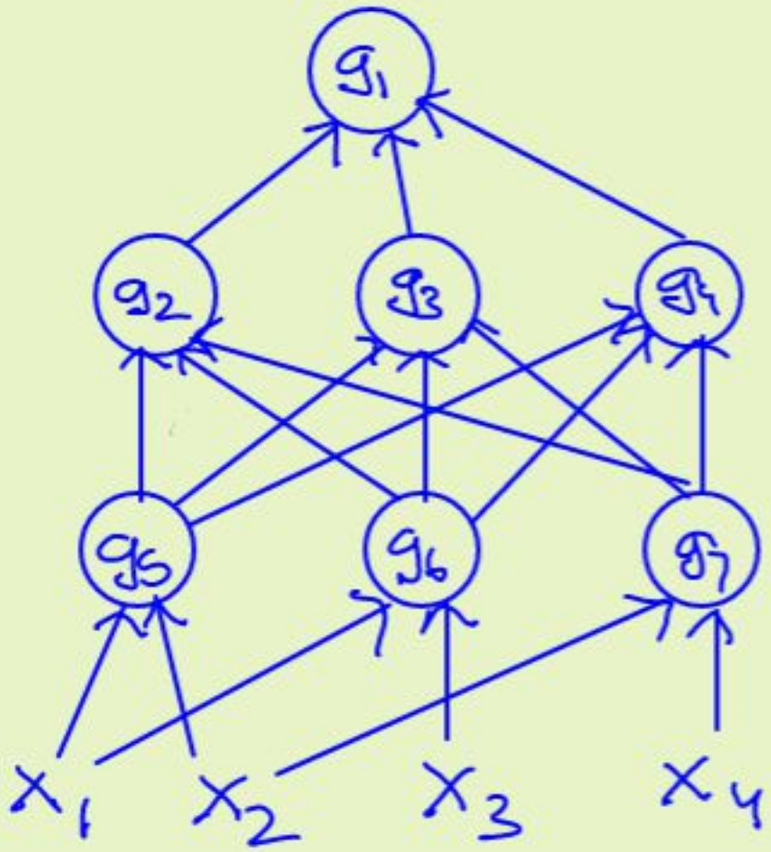
→ Directed Acyclic Graph

⟶ $g_i \in$ "Simple Ops"

⟶ Computes $f: \{0,1\}^n \to \{0,1\}$

⟶ Formula : Tree

Boolean Circuits



→ Directed Acyclic Graph

⟶ $g_i \in$ "Simple Ops"

⟶ Computes $f: \{0,1\}^n \to \{0,1\}$

⟶ Formula : Tree

Size = # of ops = 4

Depth = length of longest path = 3

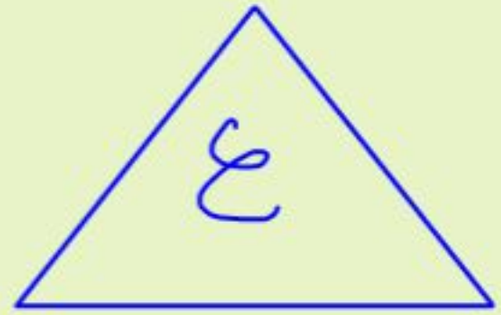
The Big Questions

→ $\mathcal{E}$ - a class of ckts

The Big Questions

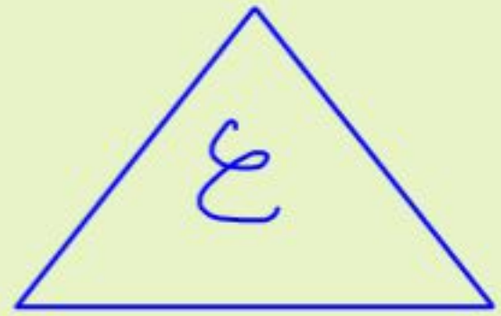
→ $\mathcal{C}$ - a class of ckts

→ Lower bounds



Explicit $f: \{0,1\}^n \to \{0,1\} \notin \mathcal{C}$

The Big Questions



→ $\mathcal{C}$ - a class of ckts

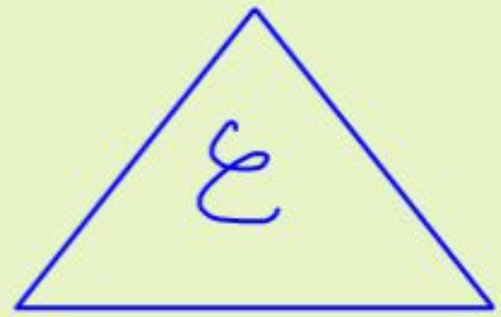
→ Lower bounds

Explicit $f: \{0,1\}^n \to \{0,1\}$ $\notin \mathcal{C}$

→ Average case lbds

The Big Questions

→ $\mathcal{C}$ - a class of ckts



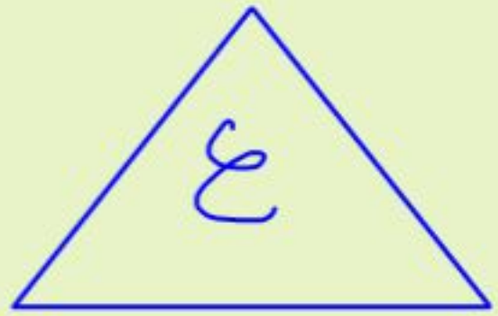
→ Lower bounds

Explicit $f: \{0,1\}^n \to \{0,1\} \notin \mathcal{C}$

→ Average case lbds

→ Pseudorandom Generators (PRGs)

The Big Questions



→ $\mathcal{C}$ - a class of ckts

→ Lower bounds

Explicit $f: \{0,1\}^n \to \{0,1\}$ $\notin \mathcal{C}$

→ Average case lbds

→ Pseudorandom Generators (PRGs)

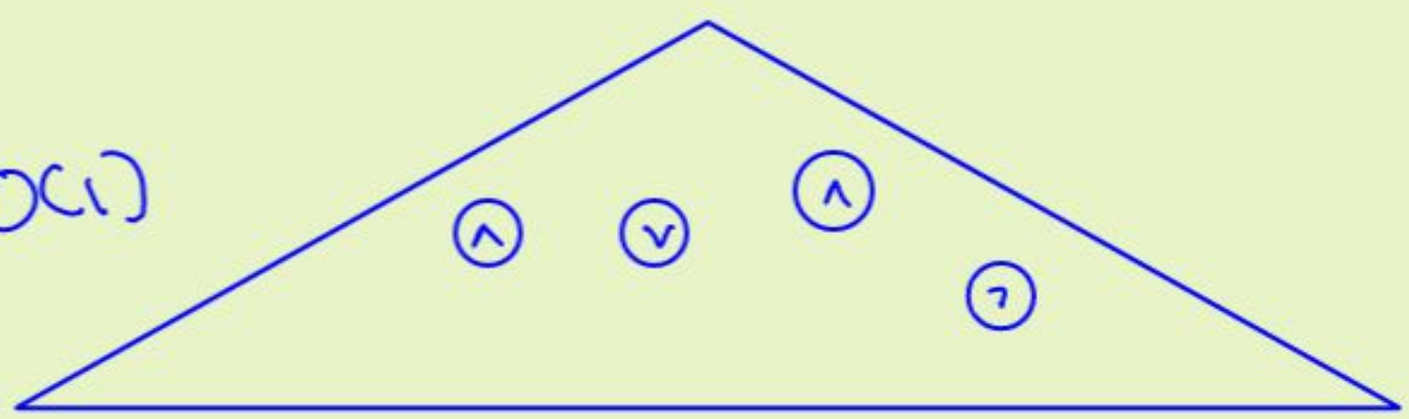
→ Hierarchy theorems

AC^0 & $AC^0[\oplus]$

AC^0:

$\wedge, \vee, \neg$ gates

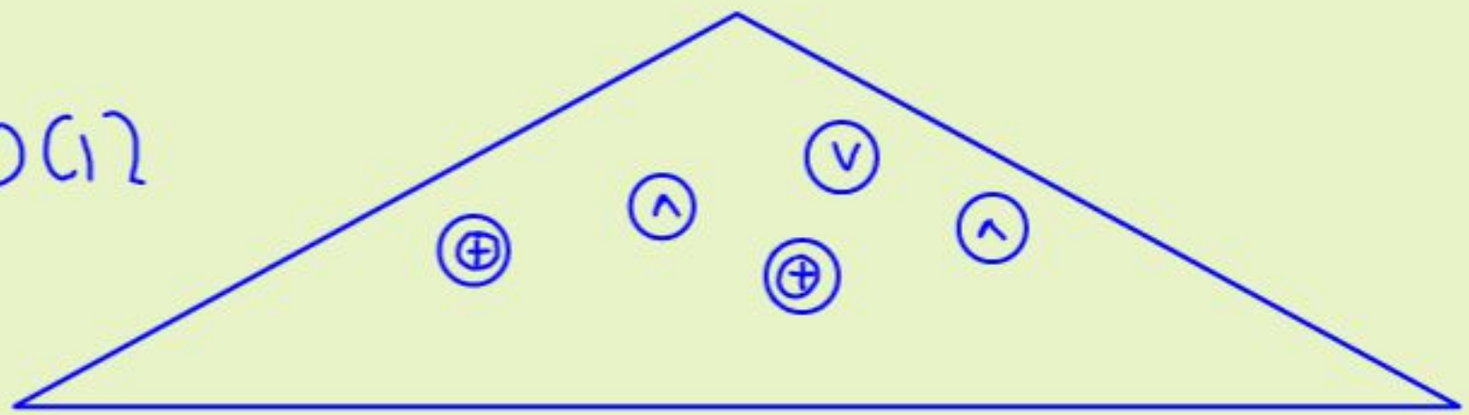
$d = O(1)$



$AC^0[\oplus]$:

$\wedge, \vee, \neg, \oplus$ gates

$d = O(1)$



AC^0 & $AC^0[\oplus]$

AC^0	$AC^0[\oplus]$
Exponential lower bounds [A, FSS, ..., H]	Exponential lower bounds [R, S]

AC^0 & $AC^0[\oplus]$

AC^0	$AC^0[\oplus]$
Exponential lower bounds [A, FSS, ..., H]	Exponential lower bounds [R, S]
Strong average-case lbds [H]	Weak average-case lbds [R, S]

AC^0 & $AC^0[\oplus]$

AC^0	$AC^0[\oplus]$
Exponential lower bounds [A, FSS, ..., H]	Exponential lower bounds [R, S]
Strong average-case lbds [H]	Weak average-case lbds [R, S]
Strong PRGs [N]	Weak PRGs [FSUV]
⋮	⋮

Size hierarchy theorems

Size hierarchy theorems

$\mathcal{C}$: circuit class

$$\mathcal{C}\text{-SIZE}[s] \overset{?}{\subsetneq} \mathcal{C}\text{-SIZE}[s^2]$$

Size hierarchy theorems

$\mathcal{C}$: circuit class

$$\mathcal{C}\text{-SIZE}[s] \overset{?}{\subsetneq} \mathcal{C}\text{-SIZE}[s^2]$$

→ Non-explicitly: Trivial

Size hierarchy theorems

$\mathcal{C}$: circuit class

$$\mathcal{C}\text{-SIZE}[s] \overset{?}{\subsetneq} \mathcal{C}\text{-SIZE}[s^2]$$

→ Non-explicitly: Trivial

→ Explicit separations?

AC^0

Thm [Håstad]: Any AC^0_d ckt. for $\oplus_n$ must have size $\exp(\Omega(n^{1/(d-1)}))$.

AC^0

Thm [Håstad]: Any AC^0_d ckt. for $\oplus_n$ must have size $\exp(\Omega(n^{1/(d-1)}))$.

Tight!: Ubd. of $\exp(O(n^{1/(d-1)}))$

AC^0

Thm [Håstad]: Any AC^0_d ckt. for $\oplus_n$ must have size $\exp(\Omega(n^{1/(d-1)}))$.

Tight!: Ubd. of $\exp(O(n^{1/(d-1)}))$

$d=3$: AC^0_3 complexity: $\exp(\Theta(\sqrt{n}))$. of $\oplus_n$

AC^0

Thm [Håstad]: Any AC^0_d ckt. for $\oplus_n$ must have size $\exp(\Omega(n^{1/(d-1)}))$.

Tight!: Ubd. of $\exp(O(n^{1/(d-1)}))$

$d=3$: AC^0_3 complexity: $\exp(\Theta(\sqrt{n}))$ of $\oplus_n$

$$AC^0_3\text{-SIZE}[s] \subsetneq AC^0_3\text{-SIZE}[s^{O(1)}]$$

if $s < \exp(o(\sqrt{n}))$

AC^0

$\forall d:\quad AC^0_d\text{-SIZE}[s] \subsetneq AC^0_d\text{-SIZE}[s^{O(1)}]$

AC^0

$\forall d$: $AC^0_d\text{-SIZE}[s] \subsetneq AC^0_d\text{-SIZE}[s^{O(1)}]$

Fixed-Depth Size Hierarchy thm

AC^0

$\forall d$: $AC^0_d\text{-SIZE}[s] \subsetneq AC^0_d\text{-SIZE}[s^{O(1)}]$

Fixed-Depth Size Hierarchy thm

Thm [Rossman; Amano] $\forall s = n^{O(1)}$

$AC^0\text{-SIZE}[s] \subsetneq AC^0\text{-SIZE}[s^{1+\varepsilon}]$

AC^0

$\forall d$: $AC^0_d\text{-SIZE}[s] \subsetneq AC^0_d\text{-SIZE}[s^{O(1)}]$

Fixed-Depth Size Hierarchy thm

Thm [Rossman; Amano] $\forall s = n^{O(1)}$

$AC^0\text{-SIZE}[s] \subsetneq AC^0\text{-SIZE}[s^{1+\varepsilon}]$

$\exists F \in AC^0_2\text{-SIZE}[n^k]$ s.t.

$\forall d \quad F \notin AC^0_d\text{-SIZE}[n^{k-\varepsilon}]$

$AC^0[\oplus]$

Thm [Razborov; Smolensky]: Any $AC^0_3[\oplus]$ ckt. for $MOD_{3,n}$, MAJ_n has size $\exp(\Omega(n^{1/4}))$.

$AC^0[\oplus]$

Thm [Razborov; Smolensky]: Any $AC^0_3[\oplus]$ ckt. for $MOD_{3,n}$, MAJ_n has size $\exp(\Omega(n^{1/4}))$.

$[AC^0 : \exp(\Omega(\sqrt{n}))]$

$AC^0[\oplus]$

Thm [Razborov; Smolensky]: Any $AC^0_3[\oplus]$ ckt. for $MOD_{3,n}$, MAJ_n has size $\exp(\Omega(n^{1/4}))$.

$$\left[AC^0 : \exp(\Omega(\sqrt{n}))\right]$$

Best ubd: $> \exp(O(\sqrt{n}))$

$AC^0[\oplus]$

Thm [Razborov; Smolensky]: Any $AC^0_3[\oplus]$ ckt. for $MOD_{3,n}$, MAJ_n has size $\exp(\Omega(n^{1/4}))$.

$[AC^0 : \exp(\Omega(\sqrt{n}))]$

Best ubd: $> \exp(O(\sqrt{n}))$

$AC^0_3[\oplus]\text{-SIZE}[s] \subsetneq AC^0_3[\oplus]\text{-SIZE}[s^{\log s}]$

Quasipoly. Size Hierarchy theorem

Our result

Thm: $\forall s \leq \exp(n^{o(1)})$, $d = O(1)$

$$AC^0_d[\oplus]\text{-SIZE}[s] \subsetneq AC^0_d[\oplus]\text{-SIZE}[s^{O(1)}]$$

explicitly.

Our result

Thm: $\forall s \leq \exp(n^{o(1)})$, $d = O(1)$

$$AC^0_d[\oplus]\text{-SIZE}[s] \subsetneq AC^0_d[\oplus]\text{-SIZE}[s^{O(1)}]$$

explicitly.

Explicit hard functions chosen to solve the Coin Problem.

δ-Coin Problem

Coin with bias $\frac{1}{2}+\delta$ or $\frac{1}{2}-\delta$.

δ-Coin Problem

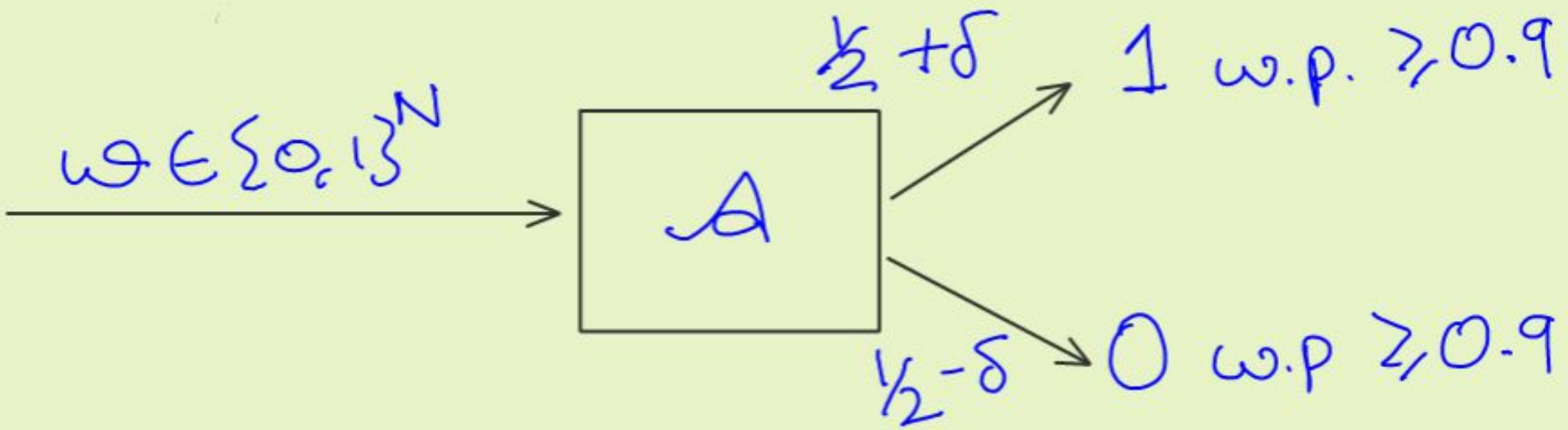
Coin with bias $1/2+\delta$ or $1/2-\delta$.

Given: N ind. tosses of coin.

δ-Coin Problem

Coin with bias $\frac{1}{2}+\delta$ or $\frac{1}{2}-\delta$.

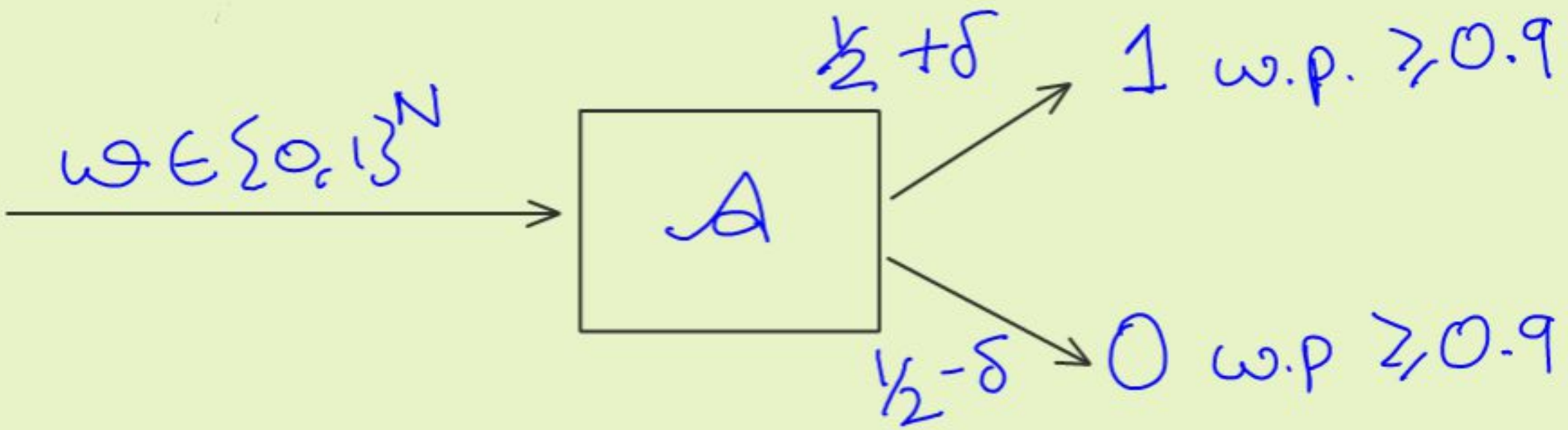
Given: N ind. tosses of coin.



δ-Coin Problem

Coin with bias $\frac{1}{2}+\delta$ or $\frac{1}{2}-\delta$.

Given: N ind. tosses of coin.



$N =:$ Sample complexity of $\mathcal{A}$

Solving the δ-Coin Problem

→ Natural problem. Closely related to Majority.

Solving the δ-Coin Problem

→ Natural problem. Closely related to Majority.

→ Maj. of $1/\delta^2$ coin tosses solves δ-C.P.

→ Sample optimal.

Solving the δ-Coin Problem

→ Natural problem. Closely related to Majority.

→ Maj. of $1/\delta^2$ coin tosses solves δ-C.P.

→ Sample optimal.

→ Circuit complexity?

[ABO, Val., Bop., SV, OW, Ama., Aar., BV, CGR, LV.]

ABO: 80's

Aar.: formal defn. [2010]

LV.: 2017.

$AC^0[\oplus]$ & δ- Coin Problem

→ Majority of $N = 1/\delta^2$ coin tosses.

→ $AC^0_3[\oplus]$ ckt. of size $\exp(1/\delta)$.

$AC^0[\oplus]$ & δ-Coin Problem

→ Majority of $N = 1/\delta^2$ coin tosses.

→ $AC^0_3[\oplus]$ ckt. of size $\exp(1/\delta)$.

→ Can do better!

$AC^0[\oplus]$ & δ-Coin Problem

→ Majority of $N = 1/\delta^2$ coin tosses.

→ $AC^0_3[\oplus]$ ckt. of size $\exp(1/\delta)$.

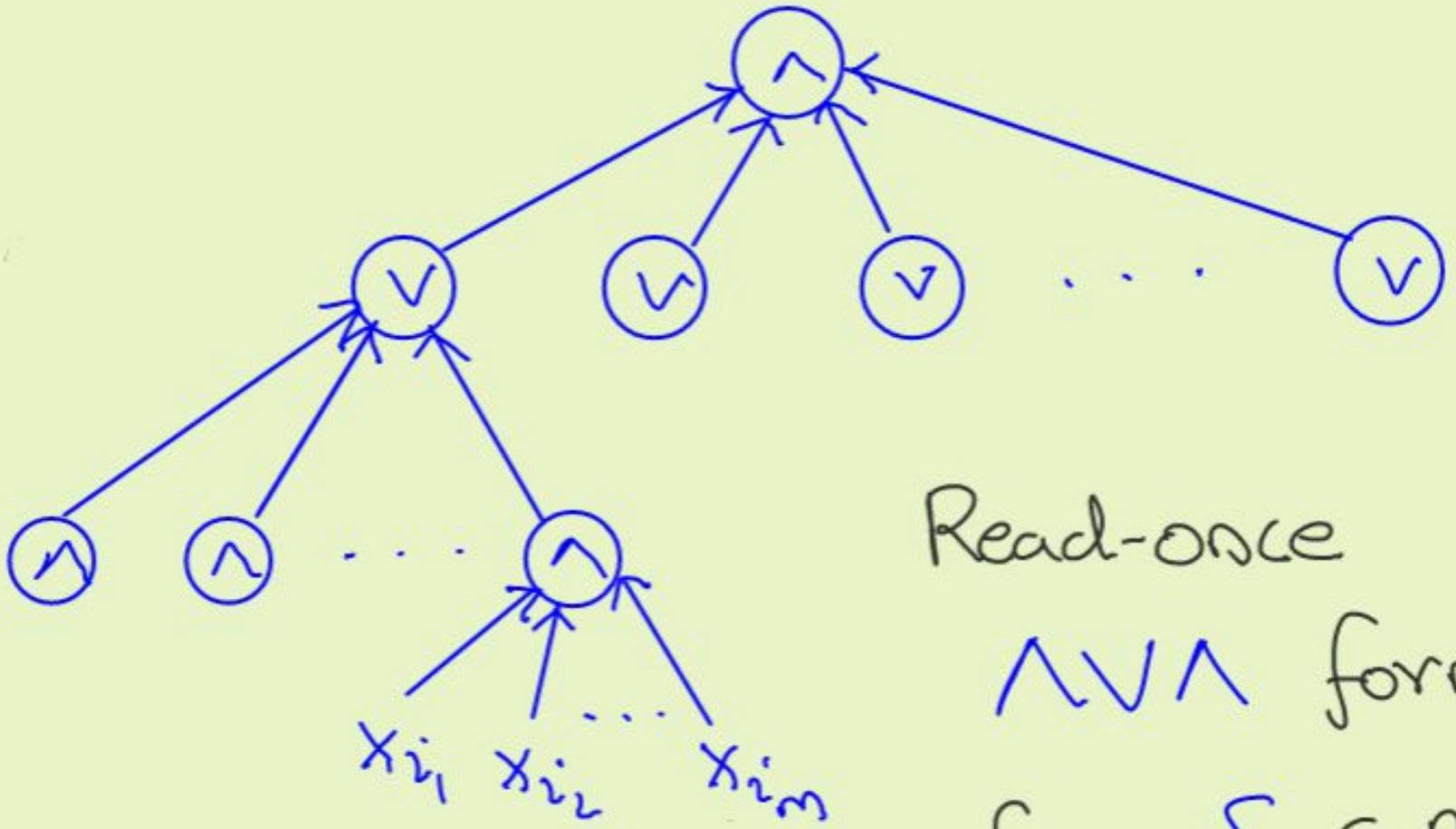
→ Can do better!

→ [O'Donnell-Wimmer, Amano]:

AC^0_3 ckt. of size $\exp(\sqrt{1/\delta})$.

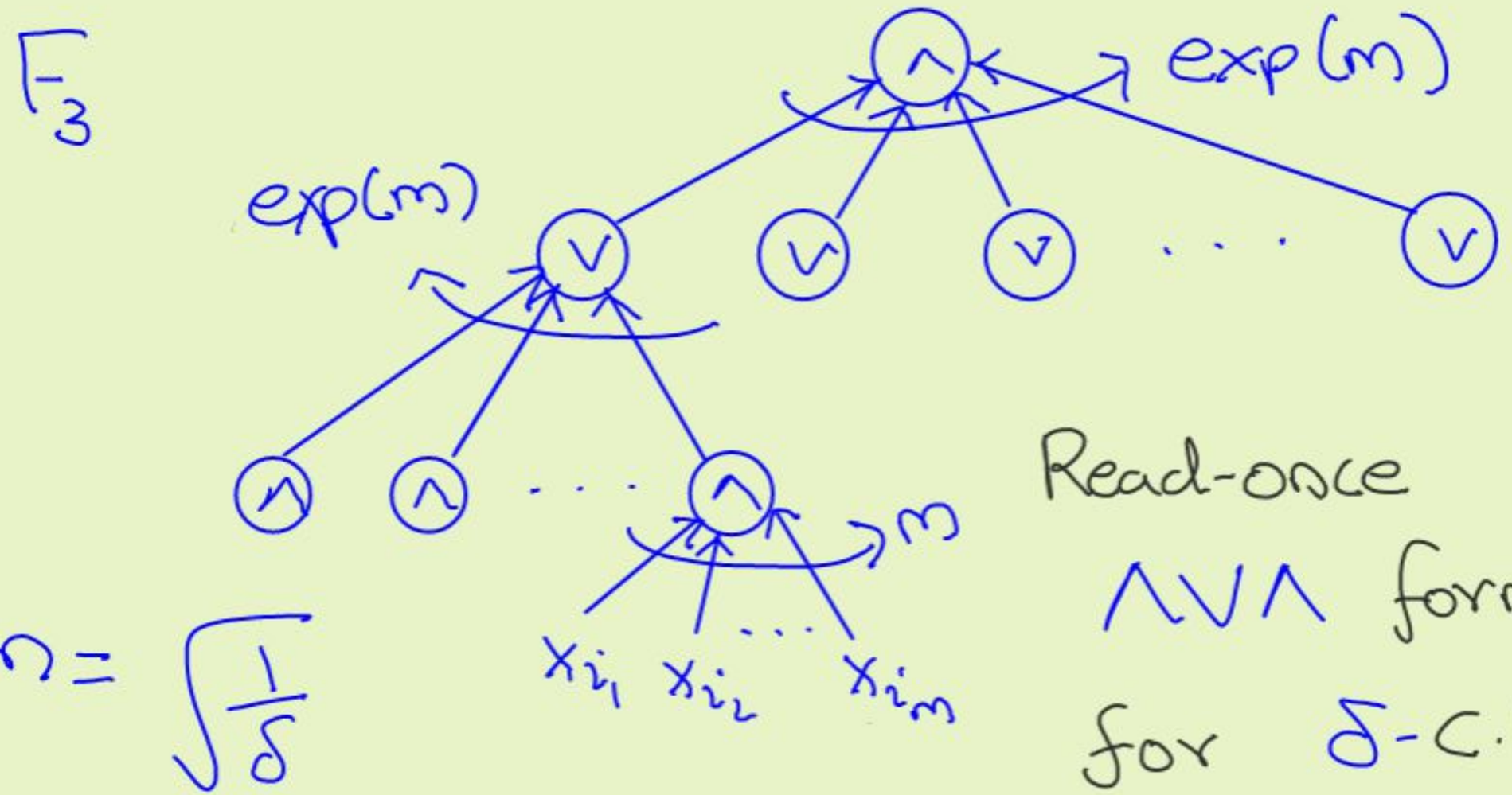
The O'Donnell-Wimmer-Amano construction

F_3



Read-once $\wedge\vee\wedge$ formula for δ-C.P.

The O'Donnell-Wimmer-Amano construction



Read-once $\wedge\vee\wedge$ formula for δ-C.P.

Back to Size hierarchy thms

→ Want: explicit tight lbds for $AC^0_d[\oplus]$

→ Standard lbds. (e.g. Maj) not tight.

Back to Size hierarchy thms

→ Want: explicit tight lbds for $AC^0_d[\oplus]$

→ Standard lbds. (e.g. Maj) not tight.

→ Do have tight lower bounds for (non-explicit) Approximate Majorities.

Back to Size hierarchy thms

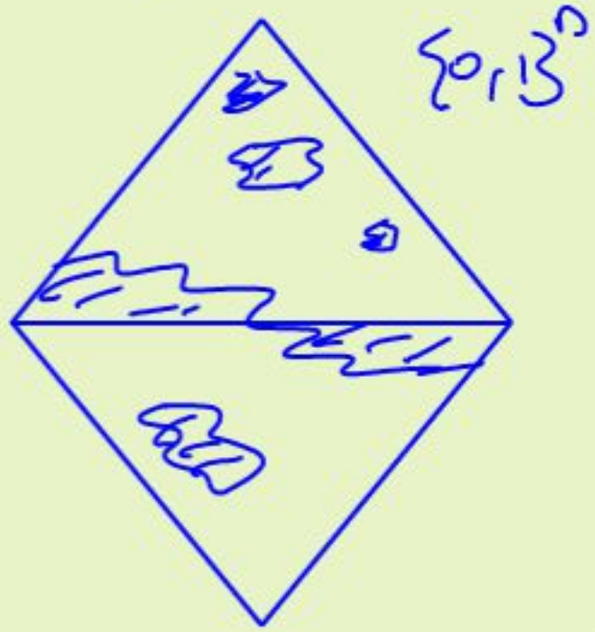
→ Want: explicit tight lbds for $AC^0_d[\oplus]$

→ Standard lbds. (e.g. Maj) not tight.

→ Do have tight lower bounds for (non-explicit) Approximate Majorities.

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

$$\Pr_x [f(x) = Maj_n(x)] \geq 0.9$$



$AC^0[\oplus]$ complexity of Approx. Majority

$AC^0[\oplus]$ complexity of Approx. Majority

→ [OW, Amano]: ∃ A.M. $f : \{0,1\}^n \to \{0,1\}$

AC^0_3-complexity $(f) \leq \exp(n^{1/4})$

$AC^0[\oplus]$ complexity of Approx. Majority

→ [OW, Amano]: ∃ A.M. $f : \{0,1\}^n \to \{0,1\}$

AC^0_3-complexity $(f) \leq \exp(n^{1/4})$

→ Tight, even with $\oplus$ gates!

$AC^0[\oplus]$ complexity of Approx. Majority

→ [OW, Amano]: ∃ A.M. $f : \{0,1\}^n \to \{0,1\}$

AC^0_3-complexity $(f) \leq \exp(n^{1/4})$

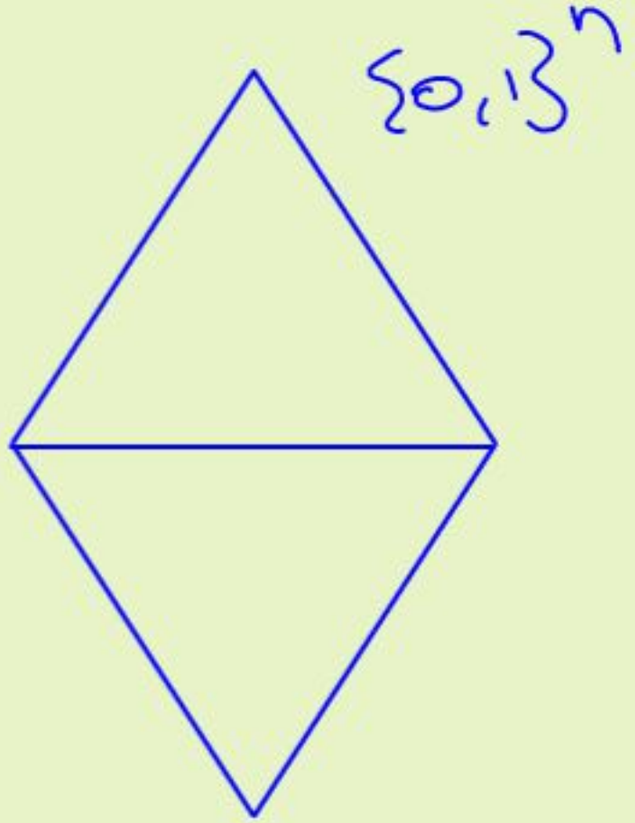
→ Tight, even with $\oplus$ gates!

→ [Razborov; Smolensky]

$AC^0_3[\oplus]$-complexity $(f) \geq \exp(n^{1/4})$

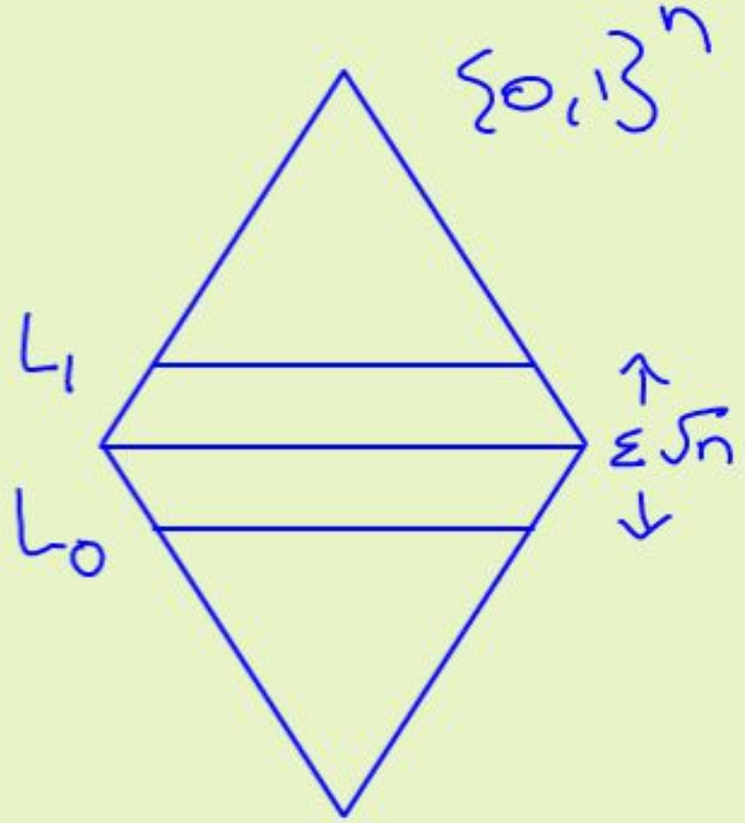
Constructing AM's in AC^0

Want: AM $f: \{0,1\}^n \to \{0,1\}$



Constructing AM's in AC^0

Want: AM $f: \{0,1\}^n \to \{0,1\}$

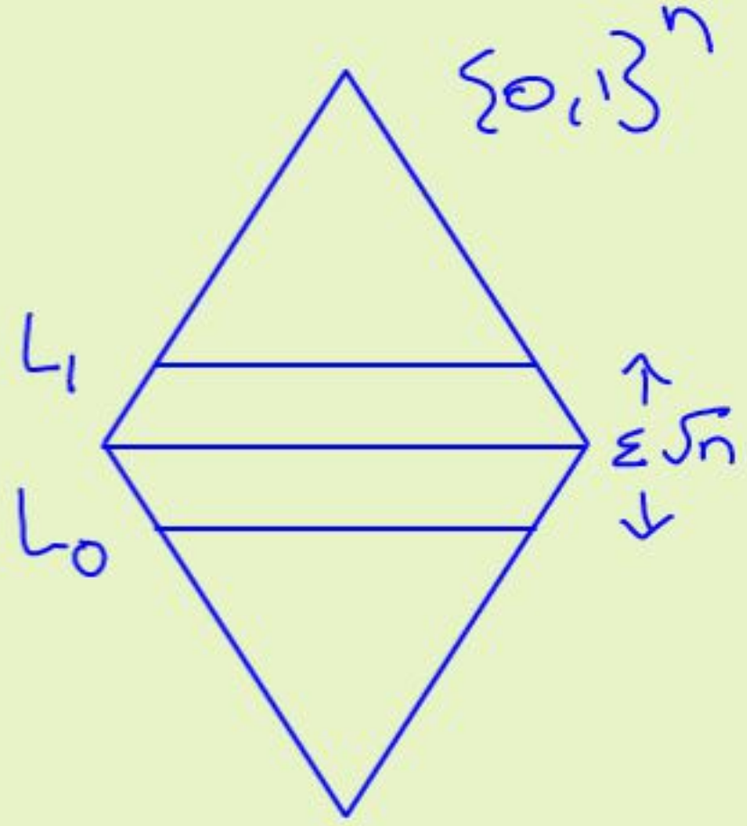


Constructing AM's in AC^0

Want: AM $f: \{0,1\}^n \to \{0,1\}$

$x \in L_1$: $\Pr_{i \in [n]}[x_i = 1] = \frac{1}{2} + \frac{\varepsilon}{\sqrt{n}}$

$x \in L_0$: $\Pr_{i \in [n]}[x_i = 1] = \frac{1}{2} - \frac{\varepsilon}{\sqrt{n}}$

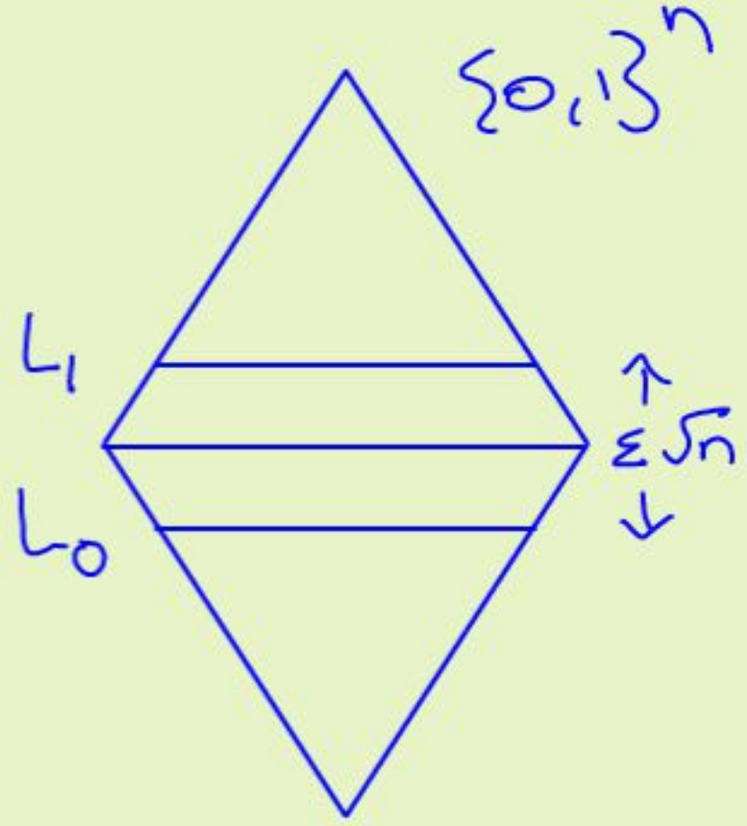


Constructing AM's in AC^0

Want: AM $f: \{0,1\}^n \to \{0,1\}$

$x \in L_1$: $\Pr_{i \in [n]}[x_i = 1] = \frac{1}{2} + \frac{\varepsilon}{\sqrt{n}}$

$x \in L_0$: $\Pr_{i \in [n]}[x_i = 1] = \frac{1}{2} - \frac{\varepsilon}{\sqrt{n}}$



Obs: $C: \{0,1\}^N \to \{0,1\}$ solves $\delta = \varepsilon/\sqrt{n}$ - C.P.

$\Rightarrow$ $\Pr_{i_1,\ldots,i_N \in [n]}[C(x_{i_1},\ldots,x_{i_N}) \neq Maj_n(x)] < 0.1.$

Constructing AM's in AC^0

$C(y_1, \ldots, y_N)$ solves δ-C.P. size $\exp\left(\frac{1}{\sqrt{\delta}}\right)$

$\Downarrow$ $\delta \approx 1/\sqrt{n}$

$C(x_{i_1}, \ldots, x_{i_N})$ computes AM size $\exp(n^{1/4})$

Constructing AM's in AC^0

$C(y_1, \ldots, y_N)$ solves δ-C.P. size $\exp\left(\frac{1}{\sqrt{\delta}}\right)$

$\Downarrow$ $\delta \approx 1/\sqrt{n}$

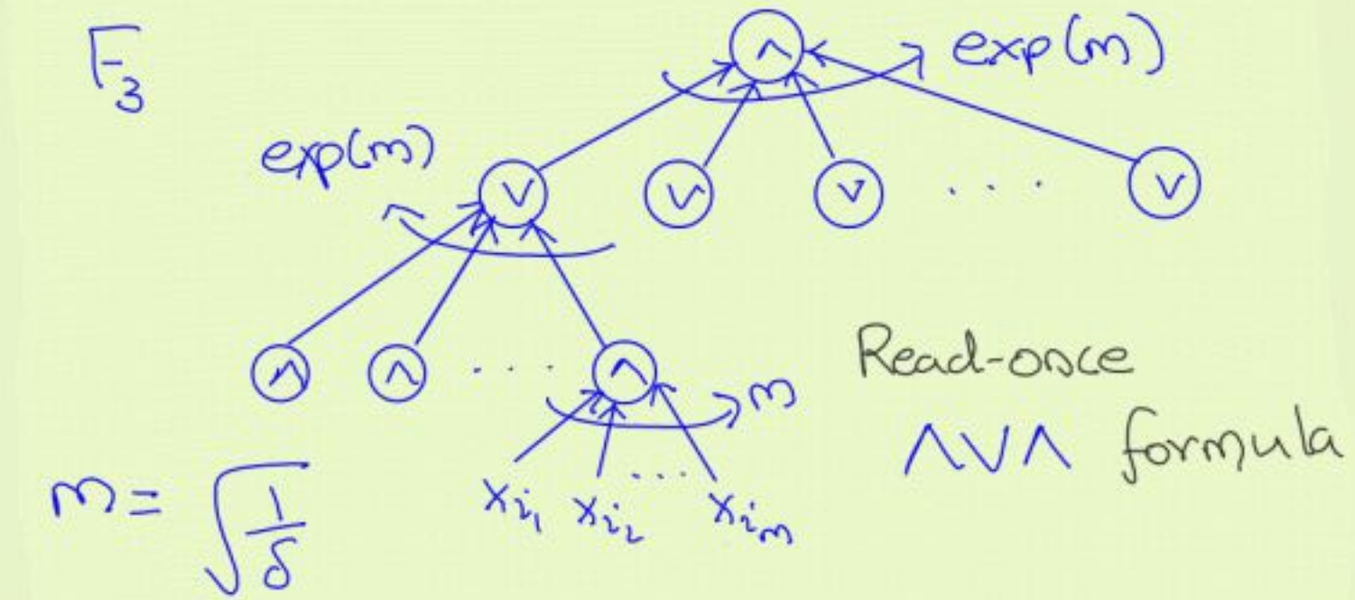
$C(x_{i_1}, \ldots, x_{i_N})$ computes AM size $\exp(n^{1/4})$

$\rightarrow$ Not explicit.

Formulas solving the coin problem

→ Computes

$f: \{0,1\}^N \to \{0,1\}$

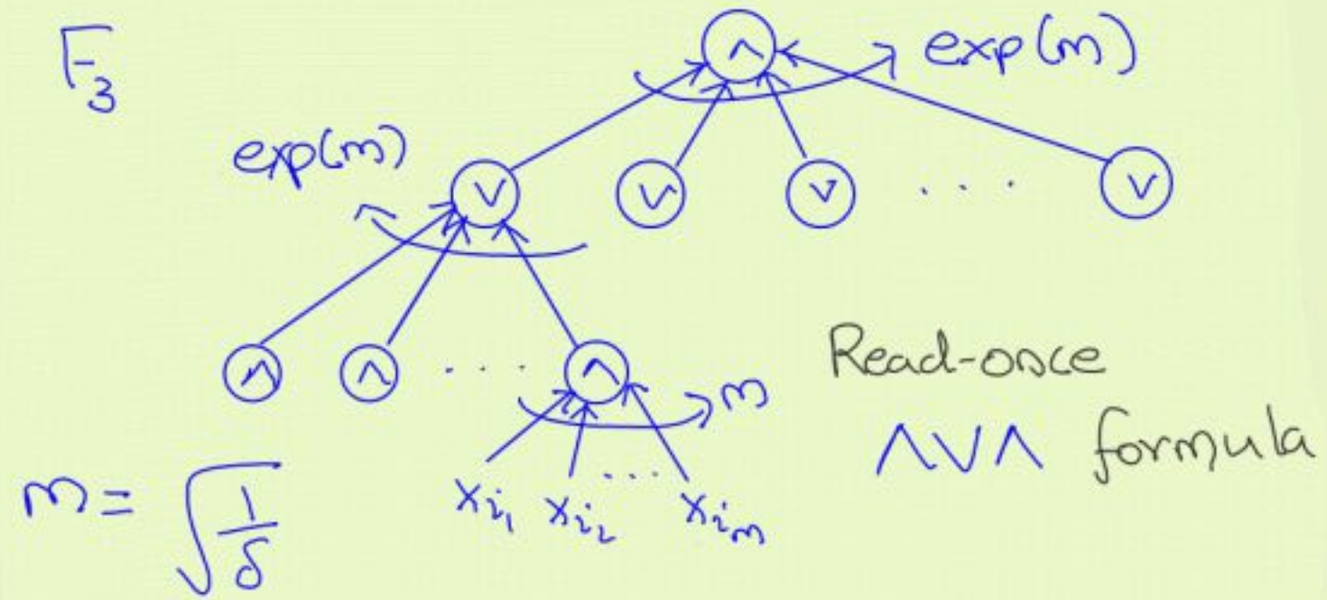


Formulas solving the coin problem

→ Computes

$f: \{0,1\}^N \to \{0,1\}$

→ Size-optimal!

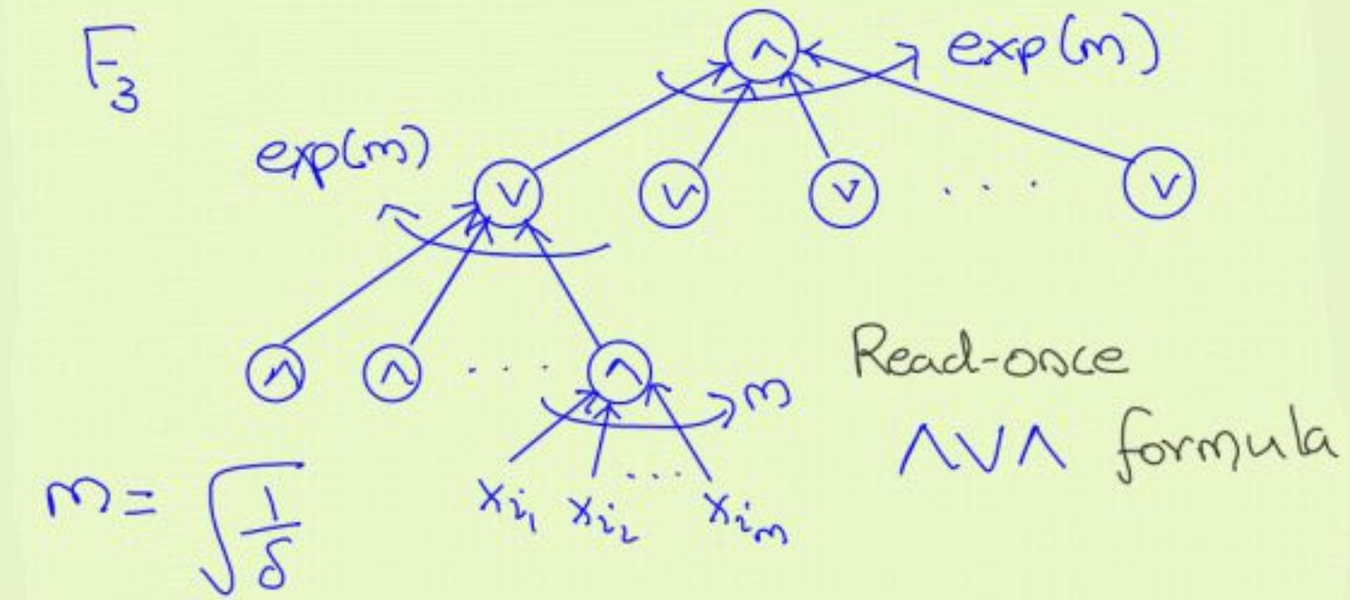


Formulas solving the coin problem

→ Computes

$f: \{0,1\}^N \to \{0,1\}$

→ Size-optimal!



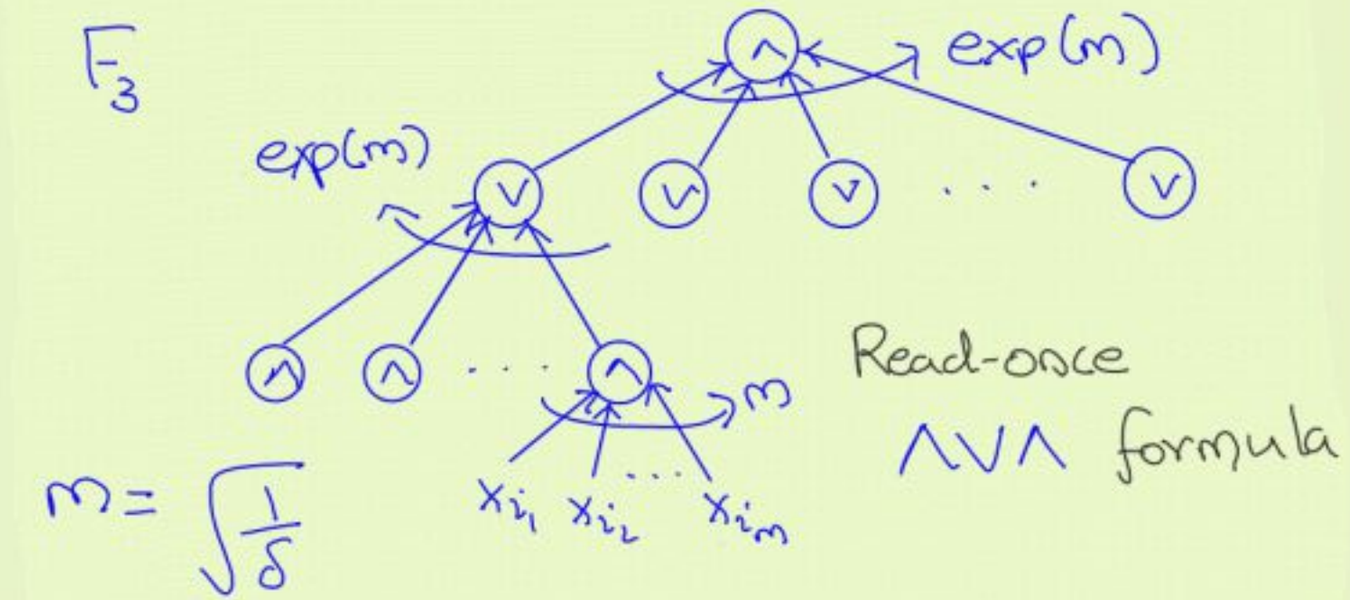
→ $AC^0_3[\oplus]\text{-SIZE}[<<N] \subsetneq AC^0_3[\oplus]\text{-SIZE}[N]$

Formulas solving the coin problem

→ Computes

$f: \{0,1\}^N \to \{0,1\}$

→ Size-optimal!



→ $AC^0_3[\oplus]\text{-SIZE}[<<N] \subsetneq AC^0_3[\oplus]\text{-SIZE}[N]$

→ Idea: Reduce N while fixing size.

Main Result

Thm 1: δ-C.P. solved by explicit $\wedge\vee\wedge$ formulas of size $\exp(1/\delta)$ & sample complexity $\text{poly}(1/\delta)$.

Main Result

Thm 1: δ-C.P. solved by explicit $\wedge\vee\wedge$ formulas of size $\exp(1/5\delta)$ & sample complexity $\text{poly}(1/\delta)$.

Thm 2: Any $AC^0_3[\oplus]$ ckt. for δ-C.P. must have size $\exp(1/5\delta)$.

Main Result

Thm 1: δ-C.P. solved by explicit $\wedge\vee\wedge$ formulas of size $\exp(1/s\delta)$ & sample complexity $\text{poly}(1/\delta)$.

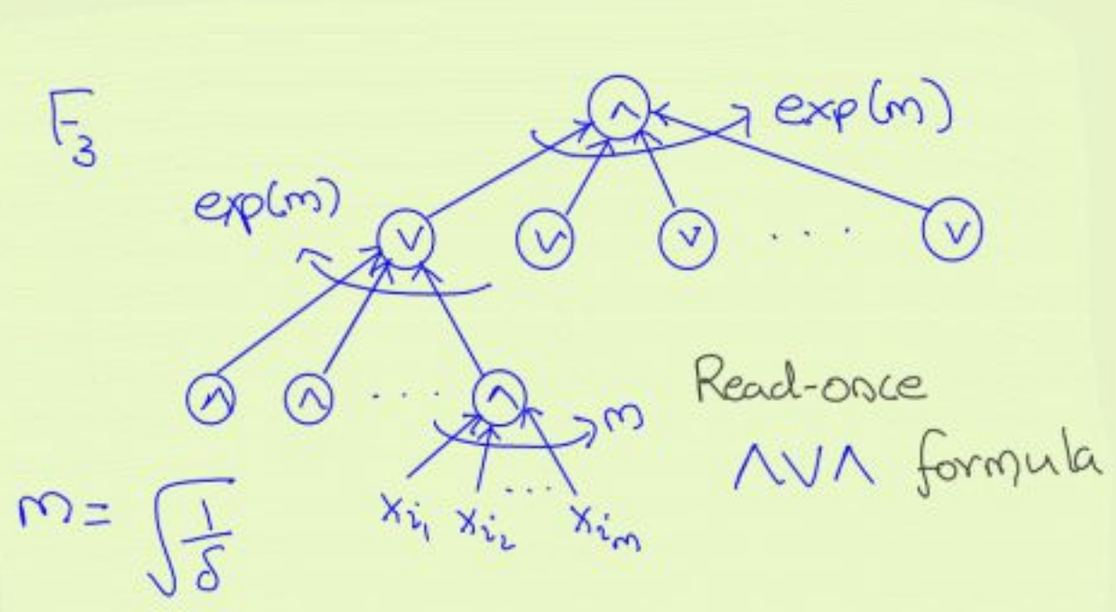
Thm 2: Any $AC^0_3[\oplus]$ ckt. for δ-C.P. must have size $\exp(1/s\delta)$.

$\Updownarrow$

Level-1 Fourier coeff. bound of CHLT'18

Proof of Thm 1

$$P_i^{(1)} := \Pr_{(1/2+\delta)}[\text{ht. } i \text{ formula accepts}]$$

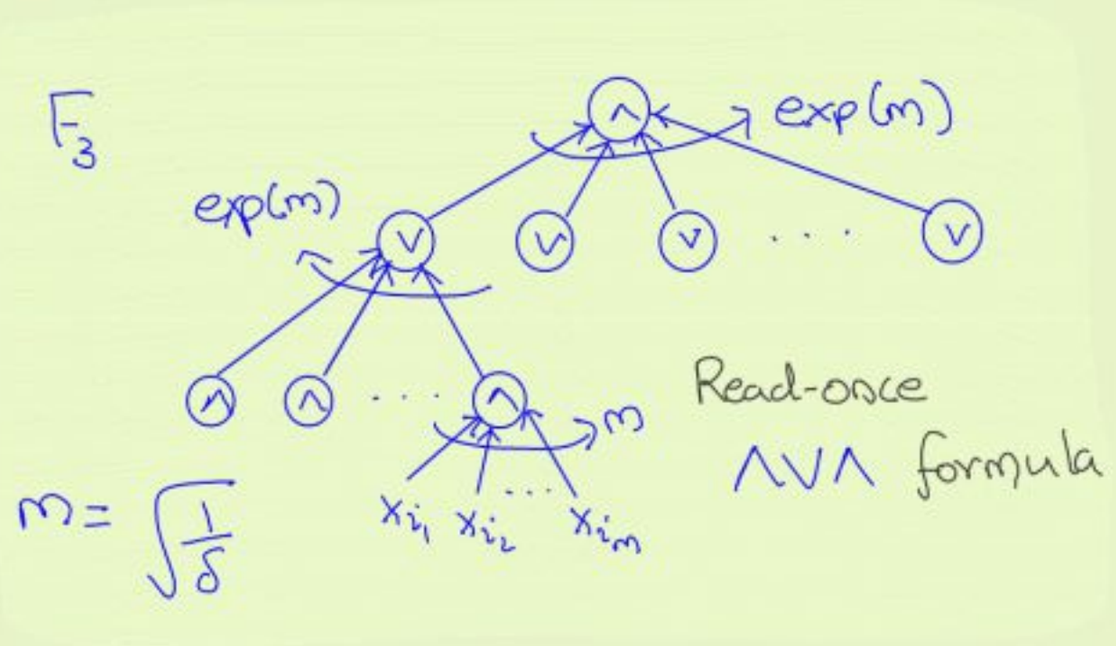


Proof of Thm 1

$$P_i^{(1)} := \Pr_{(\frac{1}{2}+\delta)}[\text{ht. } i \text{ formula accepts}]$$

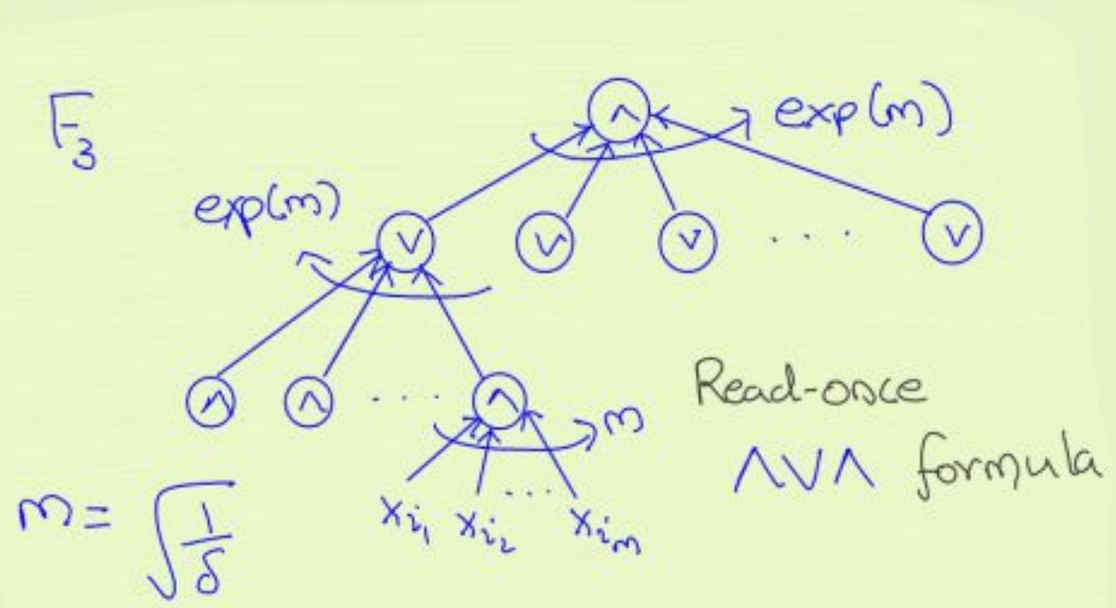
$$P_0^{(1)} = \frac{1}{2}+\delta$$

$$P_1^{(1)} = \left(\frac{1}{2}+\delta\right)^m \approx \frac{1}{2^m}(1+\delta m)$$



Proof of Thm 1

$$P_i^{(1)} := \Pr_{(\frac{1}{2}+\delta)}[\text{ht. } i \text{ formula accepts}]$$



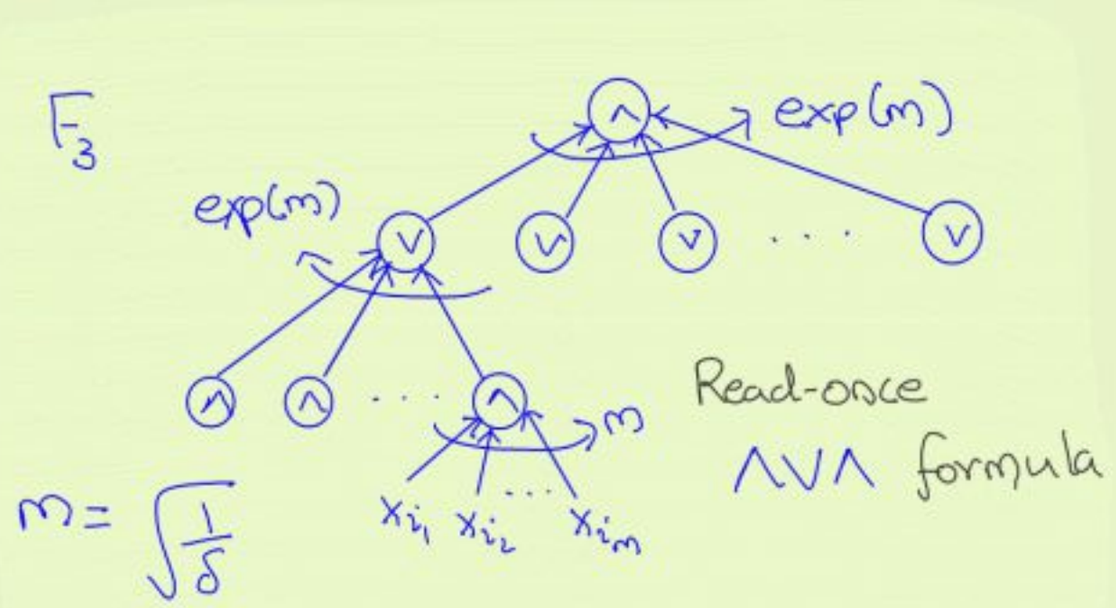
$$P_0^{(1)} = \frac{1}{2} + \delta$$

$$P_1^{(1)} = \left(\frac{1}{2}+\delta\right)^m \approx \frac{1}{2^m}(1+\delta m)$$

$$q_i^{(1)} := 1 - P_i^{(1)}$$

Proof of Thm 1

$$P_i^{(1)} := \Pr_{(\frac{1}{2}+\delta)}[\text{ht. } i \text{ formula accepts}]$$



$$P_0^{(1)} = \frac{1}{2} + \delta$$

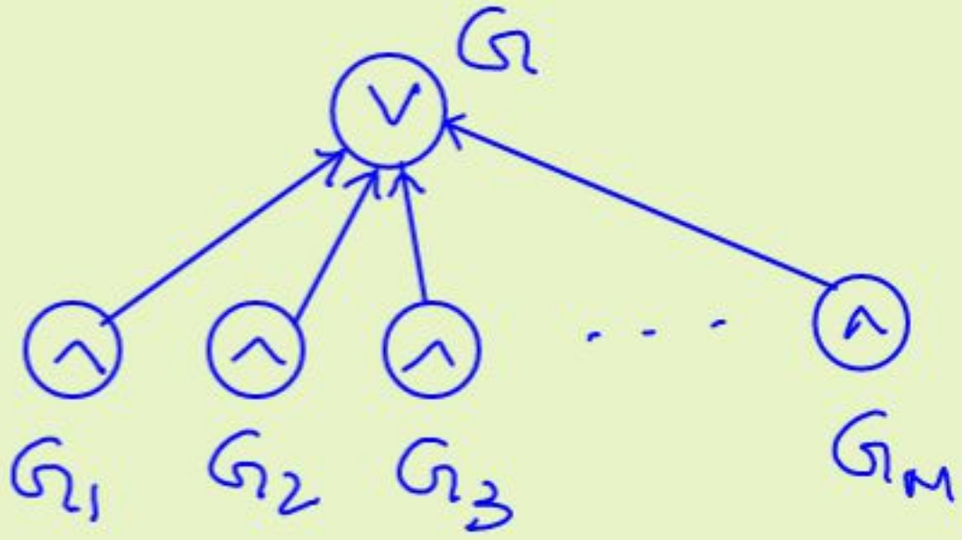
$$P_1^{(1)} = \left(\frac{1}{2}+\delta\right)^m \approx \frac{1}{2^m}(1+\delta m)$$

$$q_i^{(1)} := 1 - p_i^{(1)}$$

Key quantity: $\dfrac{\min\{p_i^{(1)}, q_i^{(1)}\}}{\min\{p_i^{(0)}, q_i^{(0)}\}}$

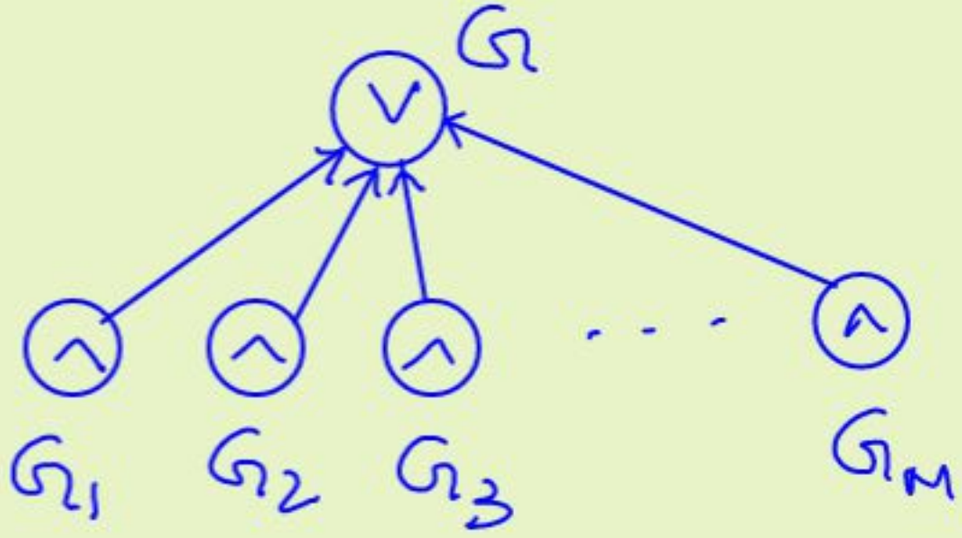
Janson's Inequality

G - monotone formula



Jansen's Inequality

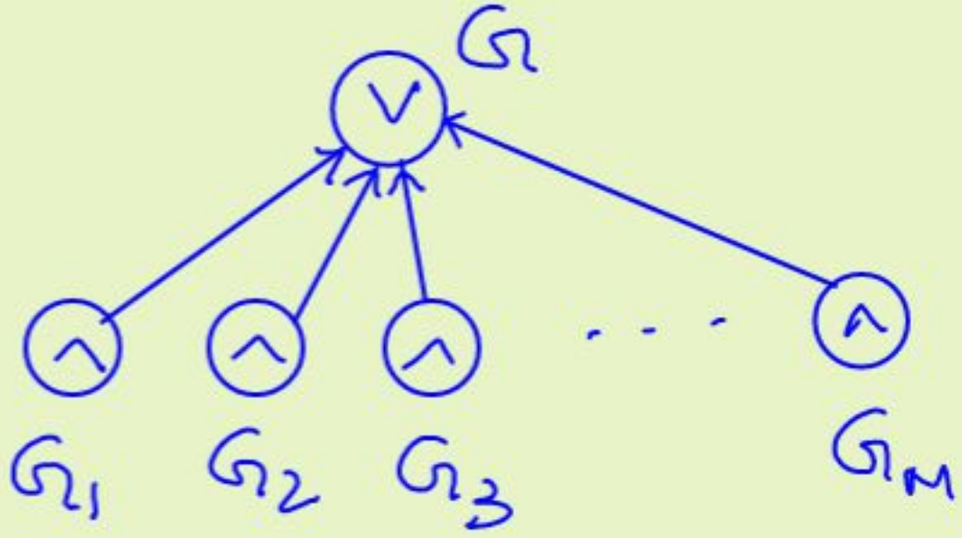
G - monotone formula



$$\prod_i \Pr[G_i = 0] \leq \Pr[G = 0]$$

Janson's Inequality

G - monotone formula

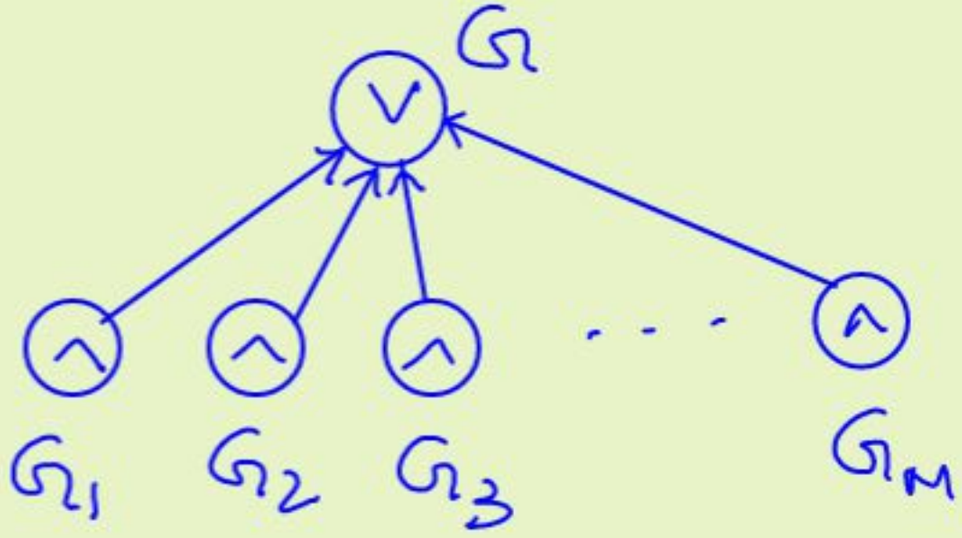


$$\prod_i \Pr[G_i = 0] \le \Pr[G = 0] \le \prod_i \Pr[G_i = 0] \cdot (1+\alpha)$$

↓ Janson

Janson's Inequality

G - monotone formula

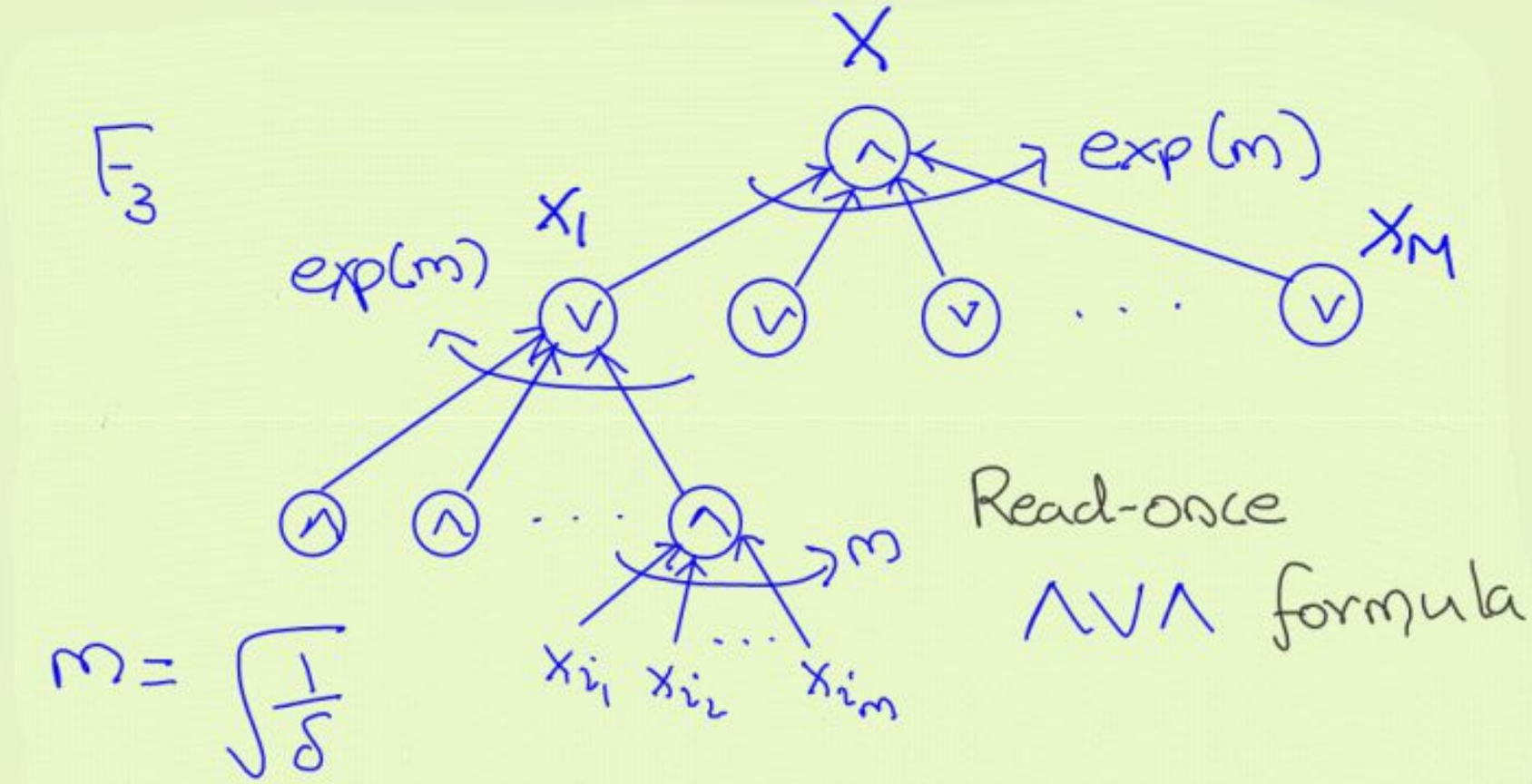


$$\prod_i \Pr[G_i = 0] \le \Pr[G = 0] \le \prod_i \Pr[G_i = 0] \cdot (1+\alpha)$$

↓ Janson

α small if most pairs G_i, G_j variable disjoint

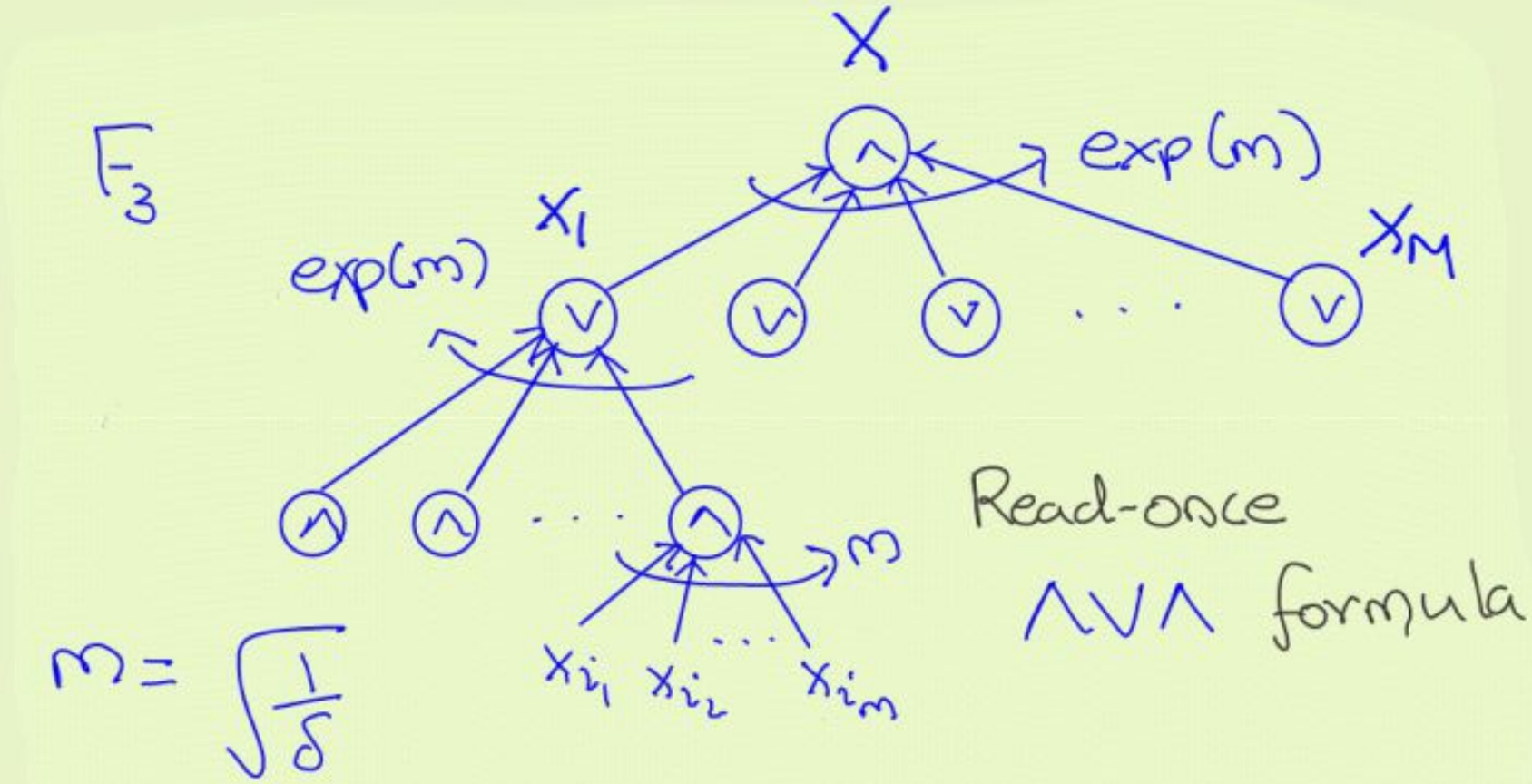
Formula construction



Read-once

$\wedge\vee\wedge$ formula

Formula construction

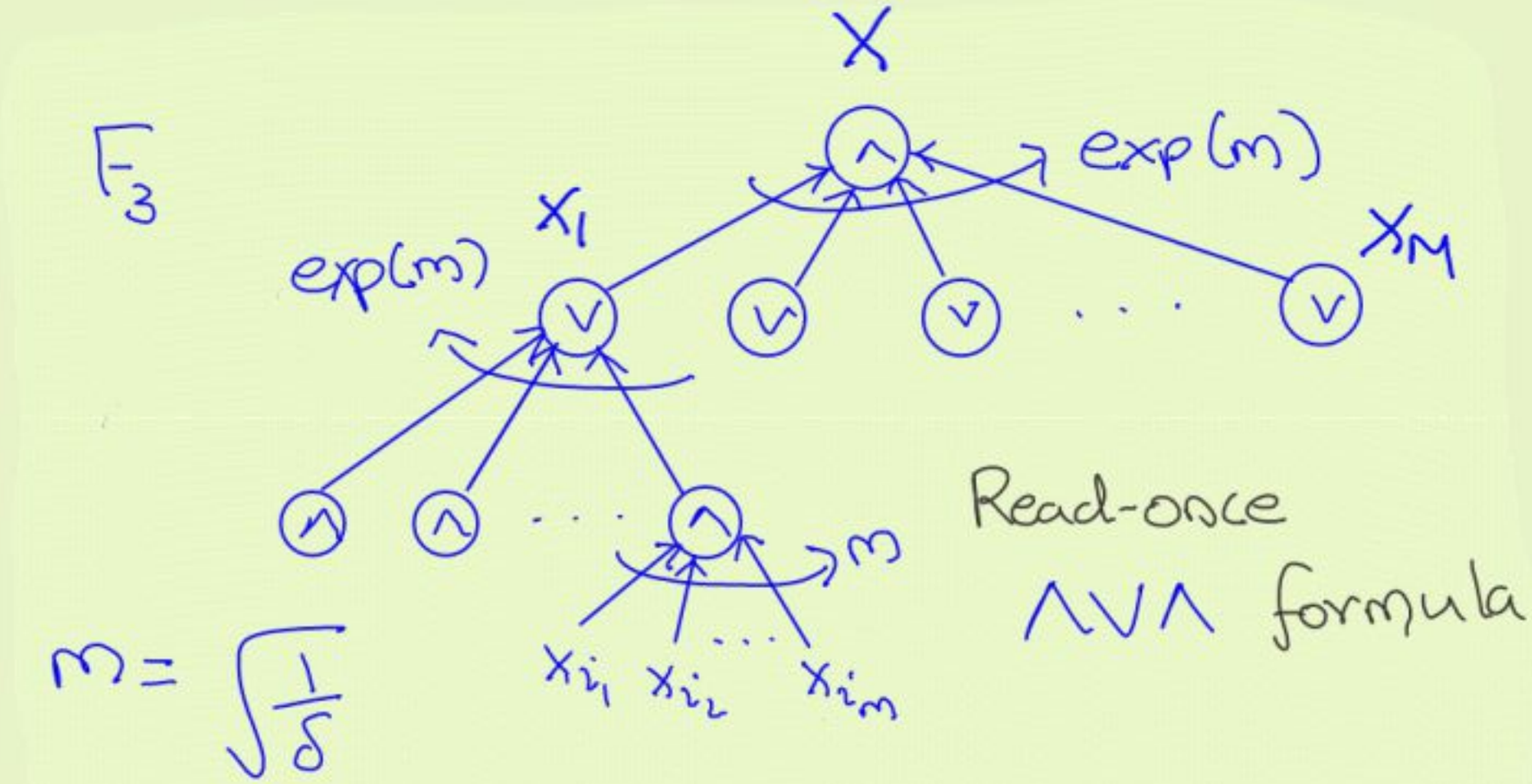


Read-once

$\wedge\vee\wedge$ formula

$X \longmapsto X_1 \cup \dots \cup X_M$: most $X_i \cap X_j = \emptyset$

Formula construction



Read-once

$\wedge\vee\wedge$ formula

$X \longmapsto X_1 \vee \cdots \vee X_M$: most $X_i \cap X_j = \emptyset$

Use an NW-design!

NW-design

$\rightarrow \mathcal{F} \subseteq \binom{[N_1]}{N_2}$

NW-design

$\rightarrow \mathcal{F} \subseteq \binom{[N]}{N_2}$ s.t. $\forall X \neq Y \in \mathcal{F}$

$|X \cap Y|$ small

NW-design

→ $\mathcal{F} \subseteq \binom{[N_1]}{N_2}$ s.t. $\forall\, X \neq Y \in \mathcal{F}$

$|X \cap Y|$ small

→ Standard designs are better:

Most $X \cap Y = \emptyset$.

NW-design

→ $\mathcal{F} \subseteq \binom{[N_1]}{N_2}$ s.t. $\forall\, X \neq Y \in \mathcal{F}$

$|X \cap Y|$ small

→ Standard designs are better:

Most $X \cap Y = \emptyset$.

→ $X = [N_1]$

$\mathcal{F} = \{X_1, \ldots, X_M\}$

Questions

1. Tight $AC^0[\oplus]$ lower bounds for MOD_3 or MAJ ?

2. Optimal sample complexity $1/\delta^2$ for δ-C.P. ?

Questions

1. Tight $AC^0[\oplus]$ lower bounds for MOD_3 or MAJ ?

2. Optimal sample complexity $1/\delta^2$ for δ-C.P. ?

Thanks !