Lower bounds based on restrictions

Restrictions

- A (**random**) **restriction** is a (random) subset R of $\{0,1\}^n$
- When R is a subcube of $\{0,1\}^n$, identify with a function $\{x_1,\ldots,x_n\} \to \{0,1,\star\}$ (each coordinate fixed to 0 or 1 or free)
- For $0 \le p \le 1$, let $\mathbf{R}_p$ denotes the p-**random restriction**

$$\mathbf{R}_p(x_i) = \begin{cases} \star & \text{with prob. } p \\ 0 & \text{with prob. } (1-p)/2 \\ 1 & \text{with prob. } (1-p)/2 \end{cases}$$

independently for each variable x_i

Lower Bounds from Restrictions

- A restriction $R \subseteq \{0,1\}^n$ can be applied to both
  - Boolean functions $f : \{0,1\}^n \to \{0,1\}$
  - Boolean circuits C (by syntactic simplification)

- Recipe for lower bounds:

  Show that $C \restriction R$ becomes "simple", while $f \restriction R$ remains "complex" (with high prob. if R is random)

Types of Restrictions $R \subseteq \{0,1\}^n$
(increasing order of generality)

- subcube $x_i = 0,\ x_i = 1$
- mon. projection $x_i = 0,\ x_i = 1,\ x_i = x_j$
- projection $x_i = 0,\ x_i = 1,\ x_i = x_j,\ x_i \neq x_j$
- affine $x_{i\_1} \oplus \cdots \oplus x_{i\_k} = 0,$

  $x_{i\_1} \oplus \cdots \oplus x_{i\_k} = 1$
- low-degree variety $P(x_1,\ldots,x_n) = 0$ where $\deg(P) \leq d$

Circuit Complexity

Circuit Complexity

- Studies the complexity of specific problems (e.g. PARITY, MATRIX MULTIPLICATION, etc.) in ***combinatorial models of computation***, most importantly Boolean circuits
- Goal is to prove ***unconditional lower bounds***, which do not rely on any unproven assumptions

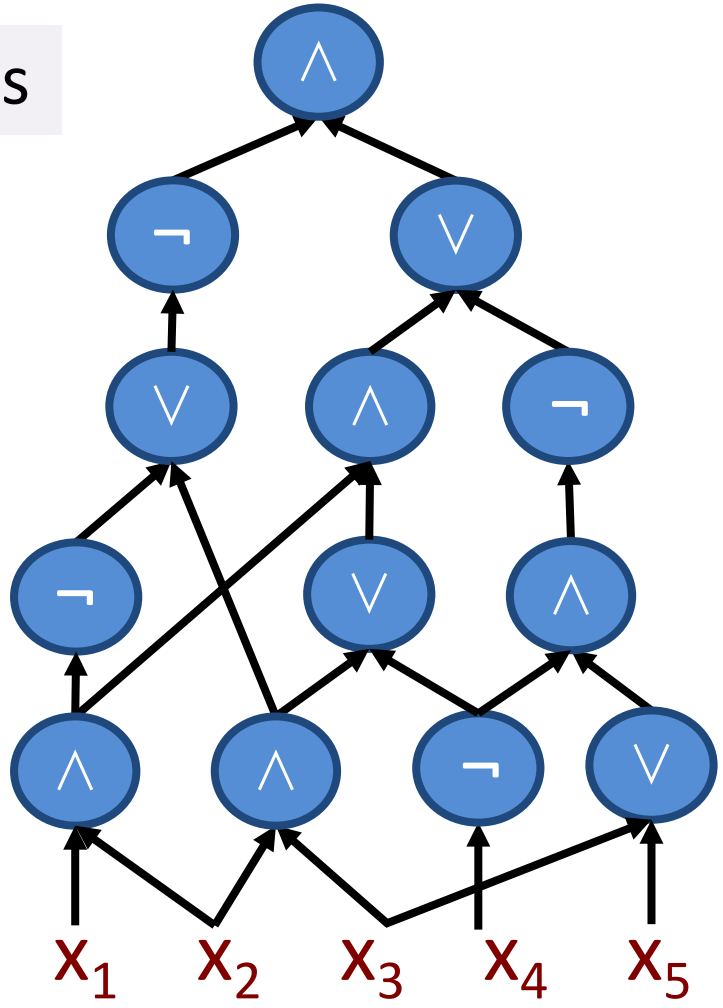
Circuit Complexity

- Studies the complexity of specific **problems** (e.g. PARITY, MATRIX MULTIPLICATION, etc.) in ***combinatorial models of computation***, most importantly Boolean circuits
- Go

a **problem** (i.e. decision problem) is represented by a sequence of boolean functions $f_n : \{0,1\}^n \rightarrow \{0,1\}$

Boolean Circuits

size = # of AND and OR gates



Boolean Circuits

- An n-variable Boolean circuit computes an n-variable Boolean function $\{0,1\}^n \rightarrow \{0,1\}$
- A problem is "solved" by a sequence of Boolean circuits $C_1, C_2, \ldots, C_n, \ldots$ if C_n computes the appropriate function $\{0,1\}^n \rightarrow \{0,1\}$

Boolean Circuits

- An n-variable Boolean circuit computes an n-variable Boolean function $\{0,1\}^n \rightarrow \{0,1\}$
- A problem is "solved" by a **sequence** of Boolean circuits $C_1, C_2, \ldots, C_n, \ldots$ if C_n computes the appropriate function $\{0,1\}^n \rightarrow \{0,1\}$

in contrast to *uniform* models of computation (e.g. Turing machines) where a single algorithm solves the problem on all instances

Circuit Size

- The **circuit size** of a function $f : \{0,1\}^n \to \{0,1\}$ is the minimum # of AND/OR gates in a circuit computing f
- Theorem [Shannon 1949, Lupanov 1958]

  Almost all Boolean functions have circuit size $\Theta(2^n/n)$
- The goal in Circuit Complexity is proving lower bounds for ***explicit*** Boolean functions (e.g. k-CLIQUE)

Circuit Size

- Theorem [Schnorr 1976, Fischer-Pippenger 1979]

  Turing mach. time $T(n)$ $\Longrightarrow$ circuit size $O(T(n)*\log T(n))$

- Corollary

  A ***super-polynomial lower bound*** on the circuit size of any function in NP (i.e. $NP \not\subseteq P/poly$) implies $P \neq NP$

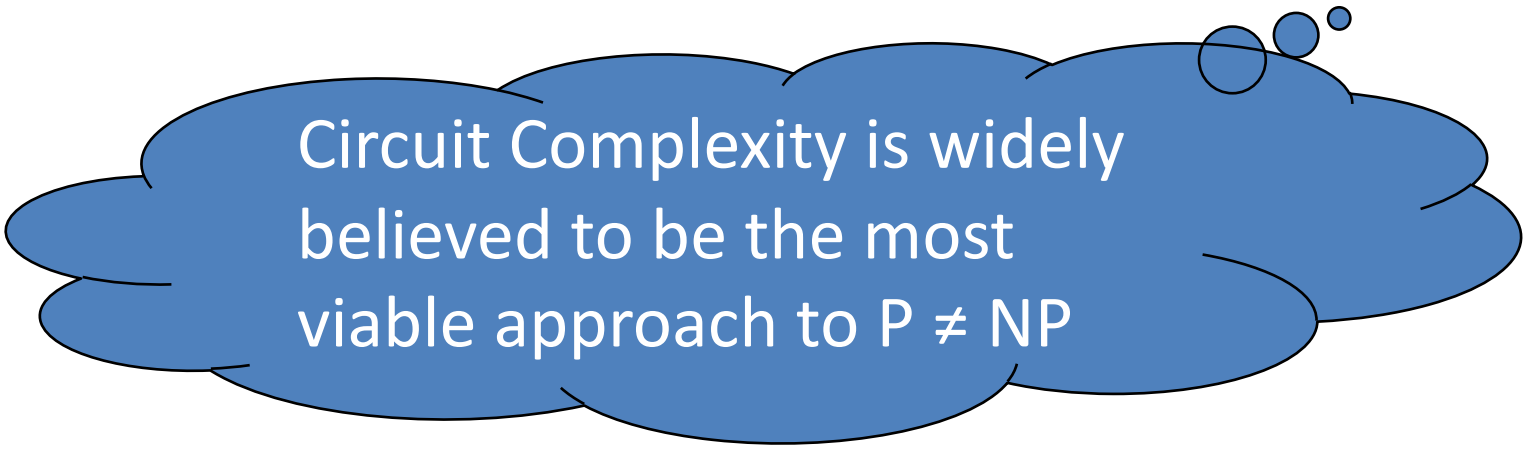
Circuit Size

- Theorem [Schnorr 1976, Fischer-Pippenger 1979]

  Turing mach. time $T(n)$ $\Longrightarrow$ circuit size $O(T(n)*\log T(n))$

- Corollary

  A ***super-polynomial lower bound*** on the circuit size of any function in NP (i.e. $NP \not\subseteq P/poly$) implies $P \neq NP$



Circuit Size

- Holy Grail ($P \neq NP$)

  Prove a ***super-polynomial lower bound*** on the circuit size of any problem in NP

Circuit Size

- Holy Grail ($P \neq NP$)

  Prove a ***super-polynomial lower bound*** on the circuit size of any problem in NP

- Best known lower bound

$3n - O(1)$	1976	[Schnorr]
$4n - O(1)$	1991	[Zwick]
$4.5n - o(n)$	2001	[Lachish-Raz]
$5n - o(n)$	2002 - today	[Iwama-Morizumi]

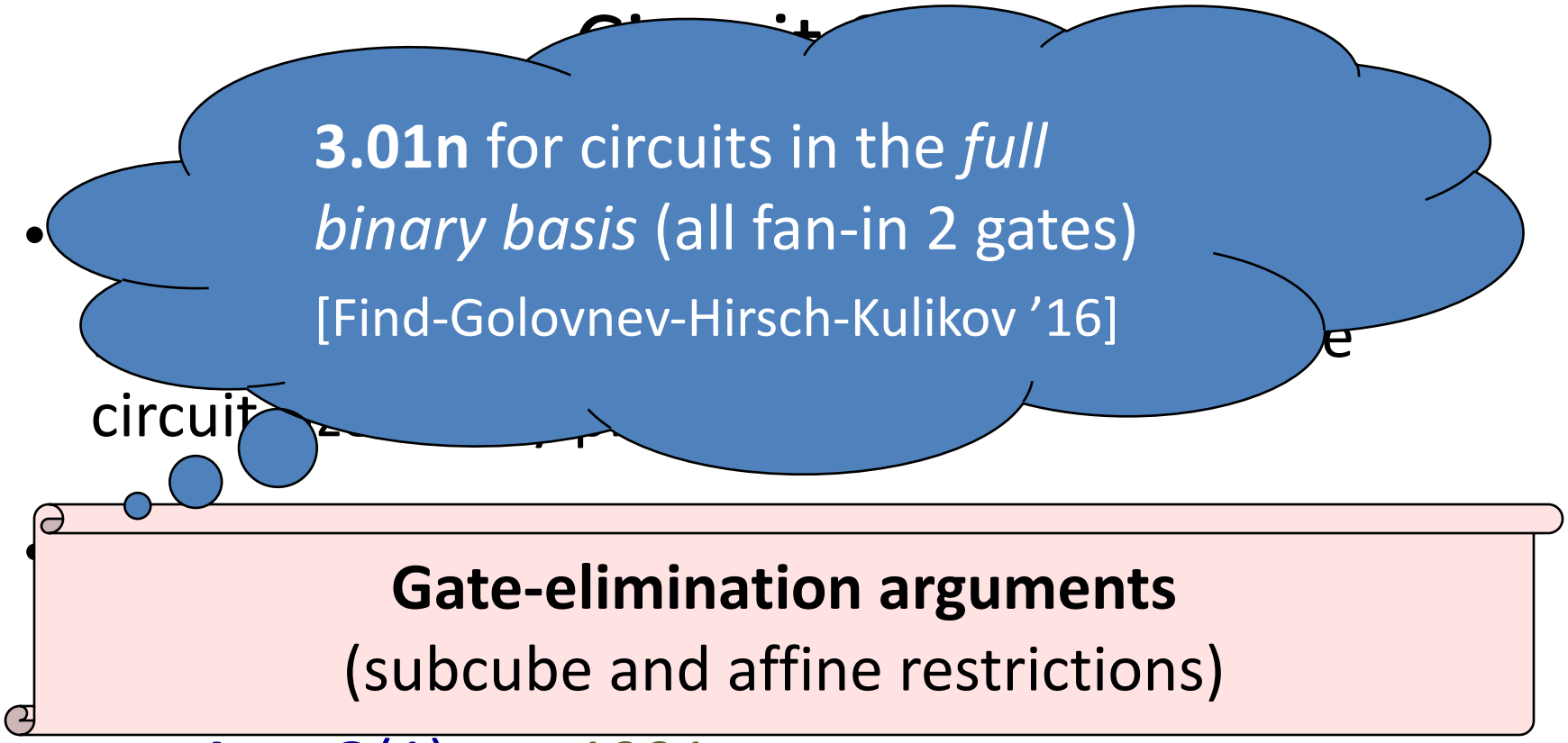
- Circuit
- e
circuit

3.01n for circuits in the *full binary basis* (all fan-in 2 gates)

[Find-Golovnev-Hirsch-Kulikov '16]

- Best known lower bound

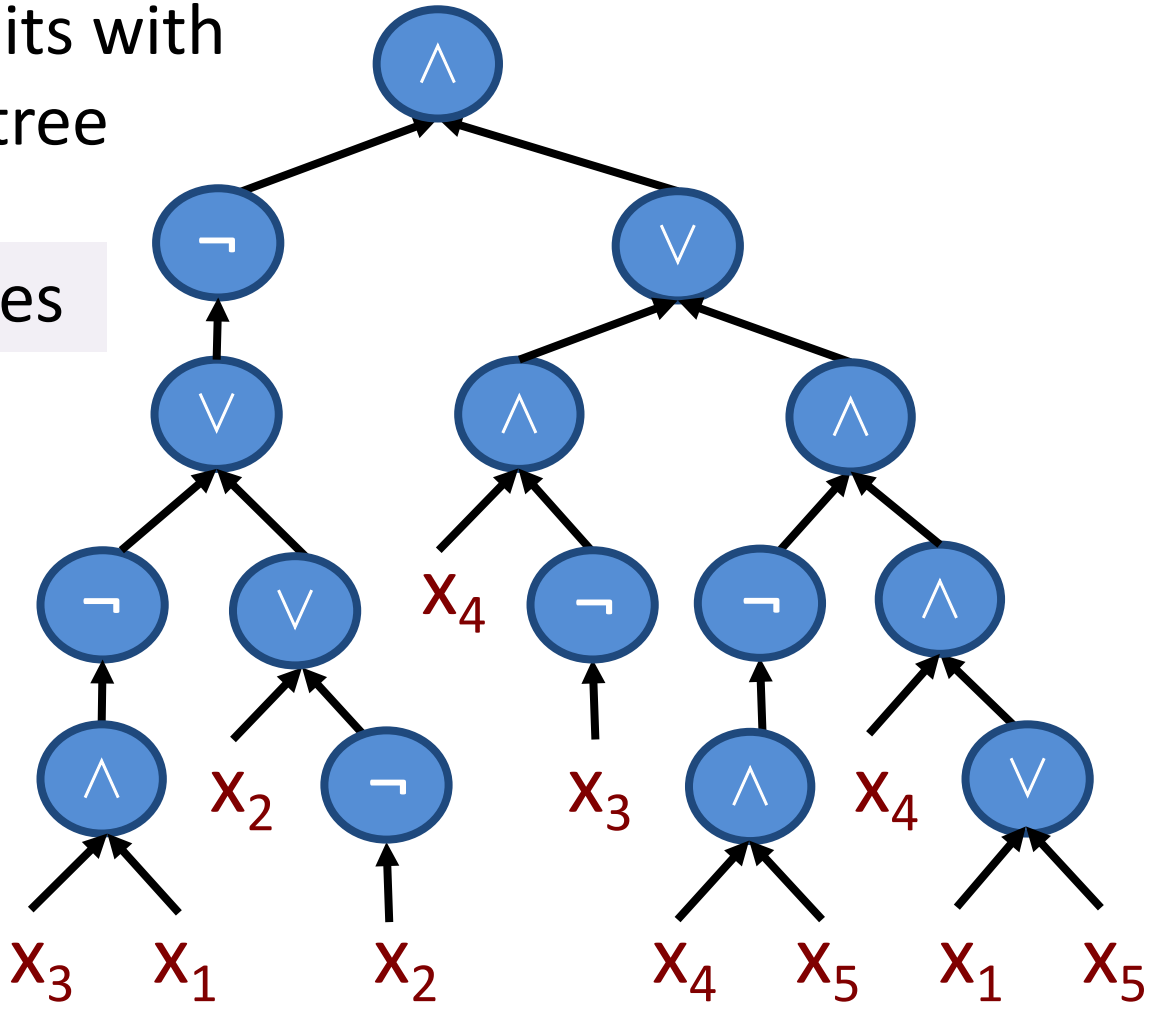
3n – O(1)	1976	[Schnorr]
4n – O(1)	1991	[Zwick]
4.5n – o(n)	2001	[Lachish-Raz]
5n – o(n)	2002 - today	[Iwama-Morizumi]


3.01n for circuits in the *full binary basis* (all fan-in 2 gates)
[Find-Golovnev-Hirsch-Kulikov '16]
Gate-elimination arguments
(subcube and affine restrictions)
4n – O(1) 1991 [Zwick]
4.5n – o(n) 2001 [Lachish-Raz]
5n – o(n) 2002 - today [Iwama-Morizumi]

(DeMorgan) Formulas

Formulas are circuits with the structure of a tree

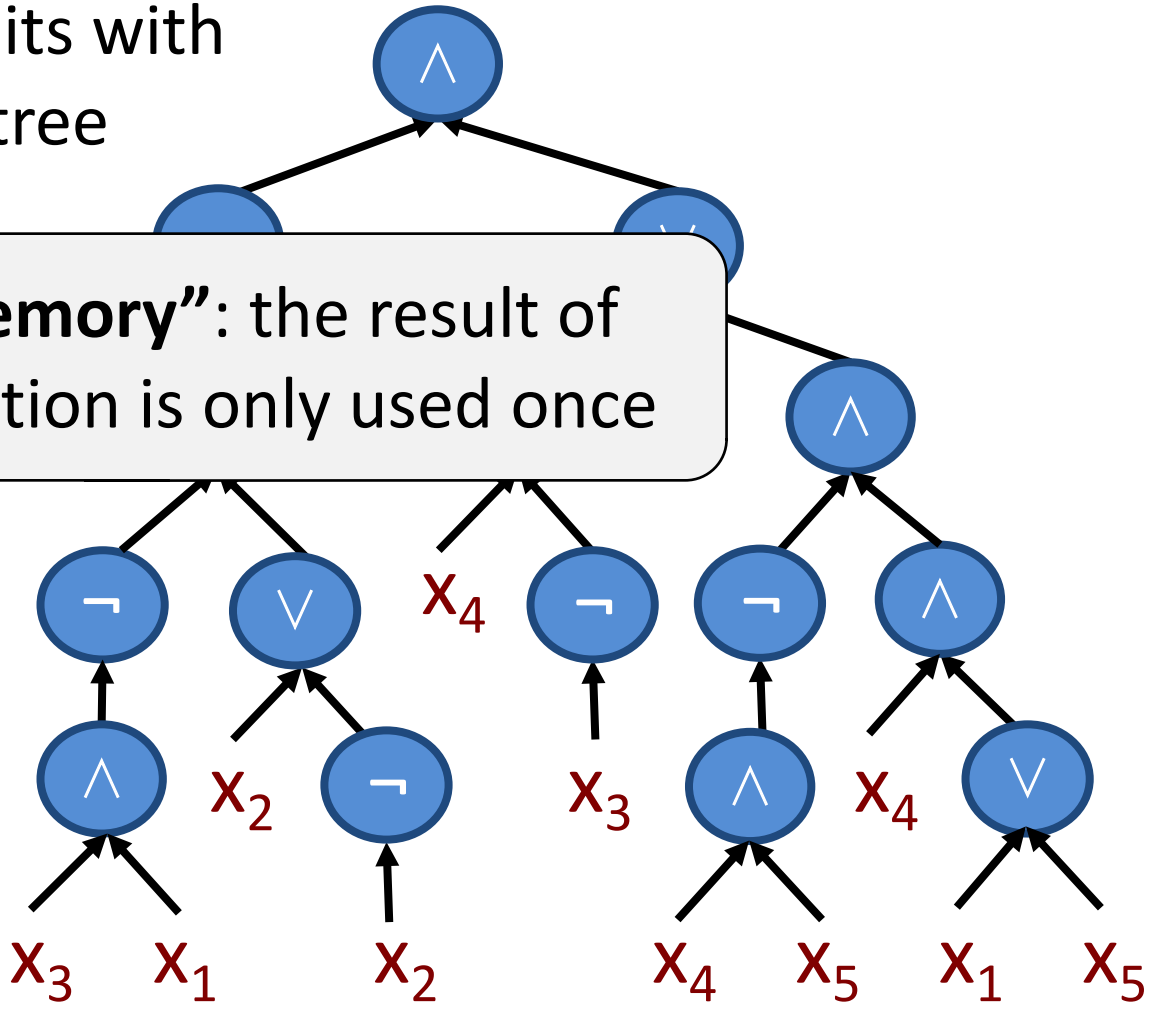
leafsize = # of leaves



(DeMorgan) Formulas

Formulas are circuits with the structure of a tree

Formulas lack "memory": the result of each sub-computation is only used once

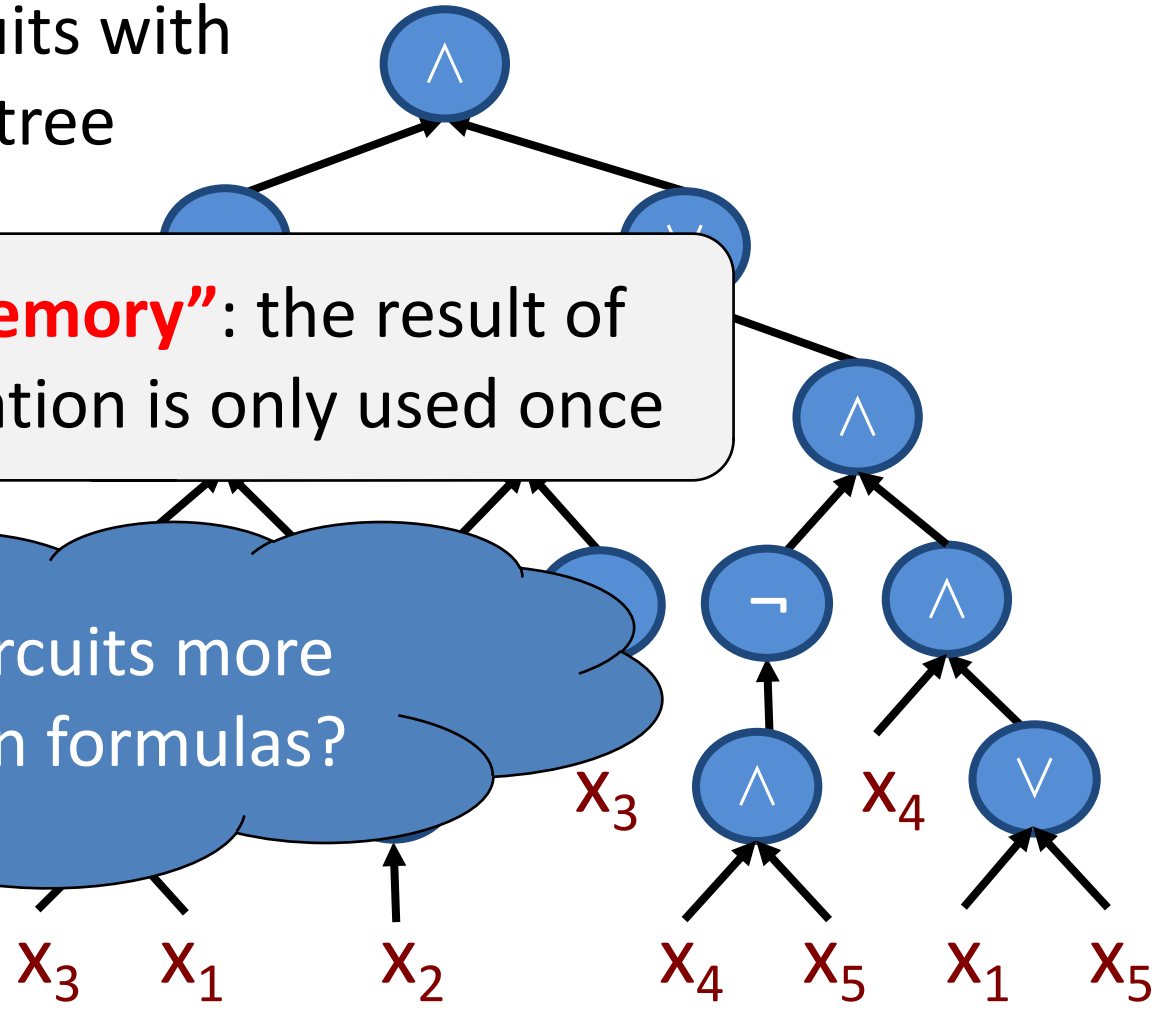


(DeMorgan) Formulas

Formulas are circuits with the structure of a tree

Formulas lack "memory": the result of each sub-computation is only used once

Open: Are circuits more powerful than formulas?



Formulas vs. Circuits

- A Pret-ty Holy Grail ($NC^1 \neq P$)

  Prove that **poly-size circuits** are strictly more powerful than **poly-size formulas**

Formulas vs. Circuits

- A Pret-ty Holy Grail ($NC^1 \neq P$)

  Prove that **poly-size circuits** are strictly more powerful than **poly-size formulas**

- Best known formula size lower bound

$n^{1.5 - o(1)}$	1961	[Subbotovskaya]
n^2	1971	[Khrapchenko]
$n^{2.5 - o(1)}$	1991	[Andreev]
$n^{3 - o(1)}$	1998 - today	[Hastad]

(log-factor improvement [Tal'14])

Formulas vs. Circuits

- A Pret-ty Holy Grail ($NC^1 \neq P$)

  Prove that **poly-size circuits** are strictly more powerful than **poly-size formulas**

Shrinkage of DeMorgan formulas
(simplification under p-random restrictions)

n^2	1971	[Khrapchenko]
$n^{2.5 - o(1)}$	1991	[Andreev]
$n^{3 - o(1)}$	1998 - today	[Hastad]

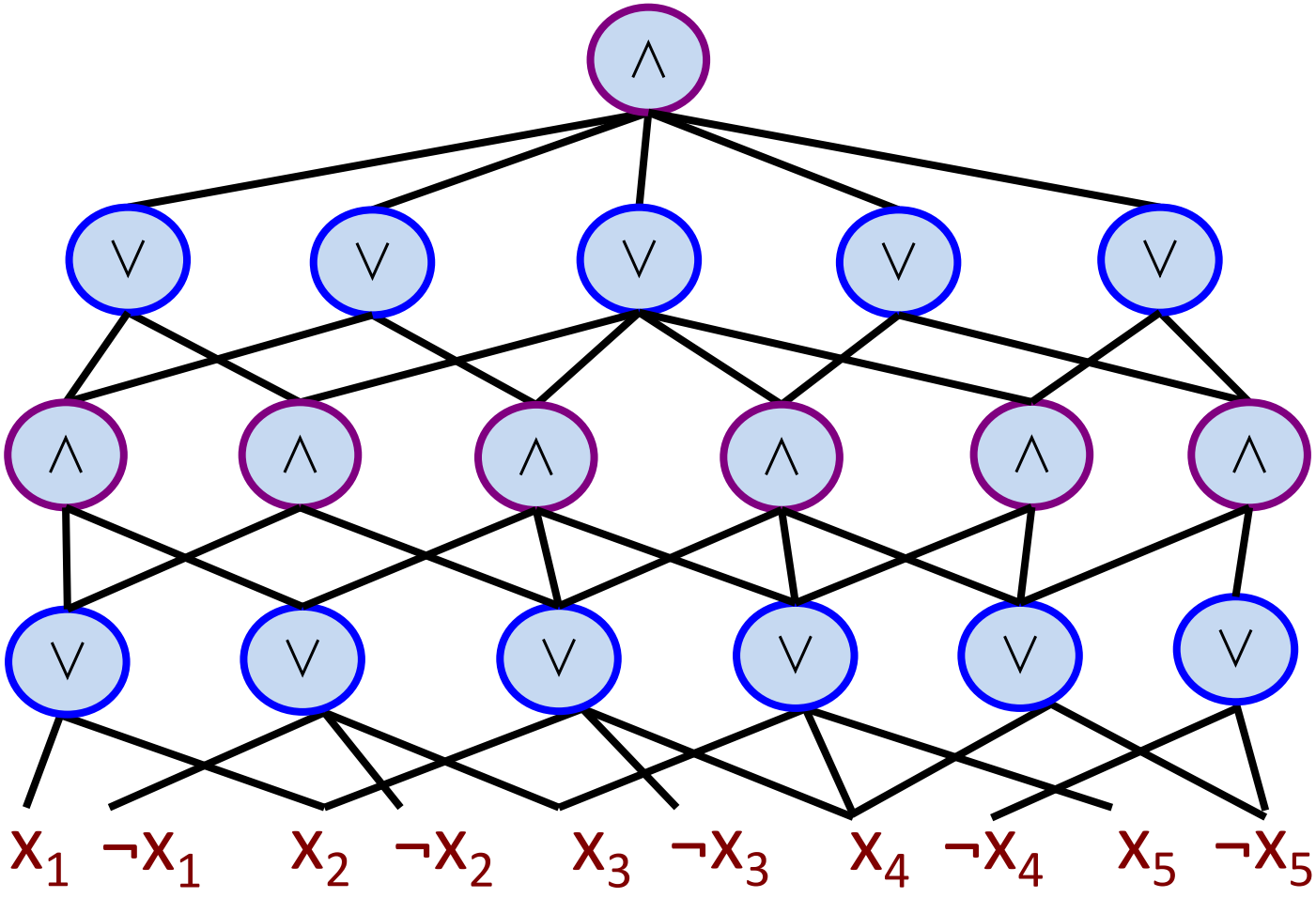
(log-factor improvement [Tal'14])

Restricted Classes (AC^0, monotone, etc.)

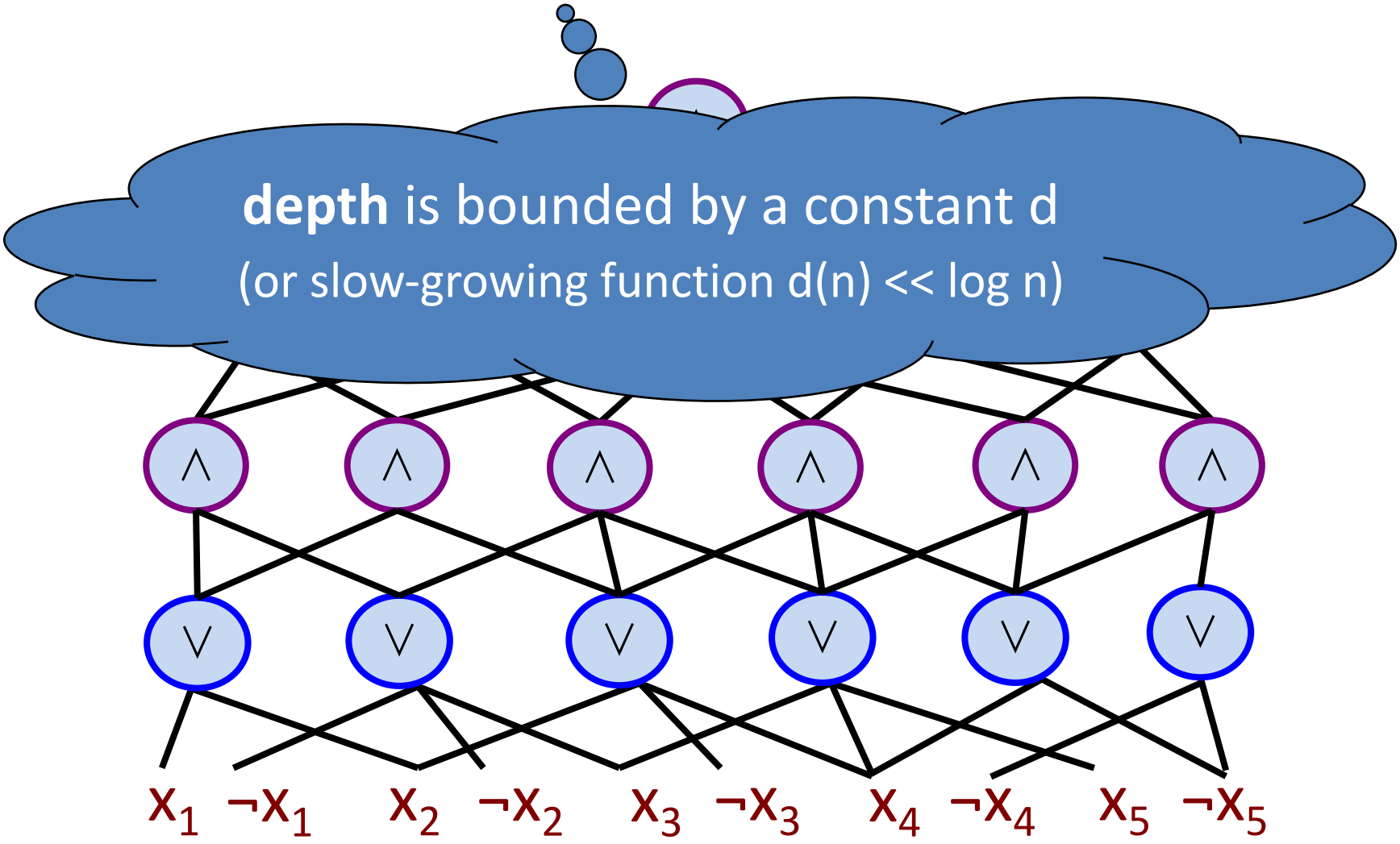
Restricted Classes

- **AC^0 setting** (fast parallel computation)
  constant-depth, unbounded fan-in AND/OR gates
- **monotone setting**
  negation-free (no NOT gates)
- **arithmetic (+, ×), tropical (min, +), …**

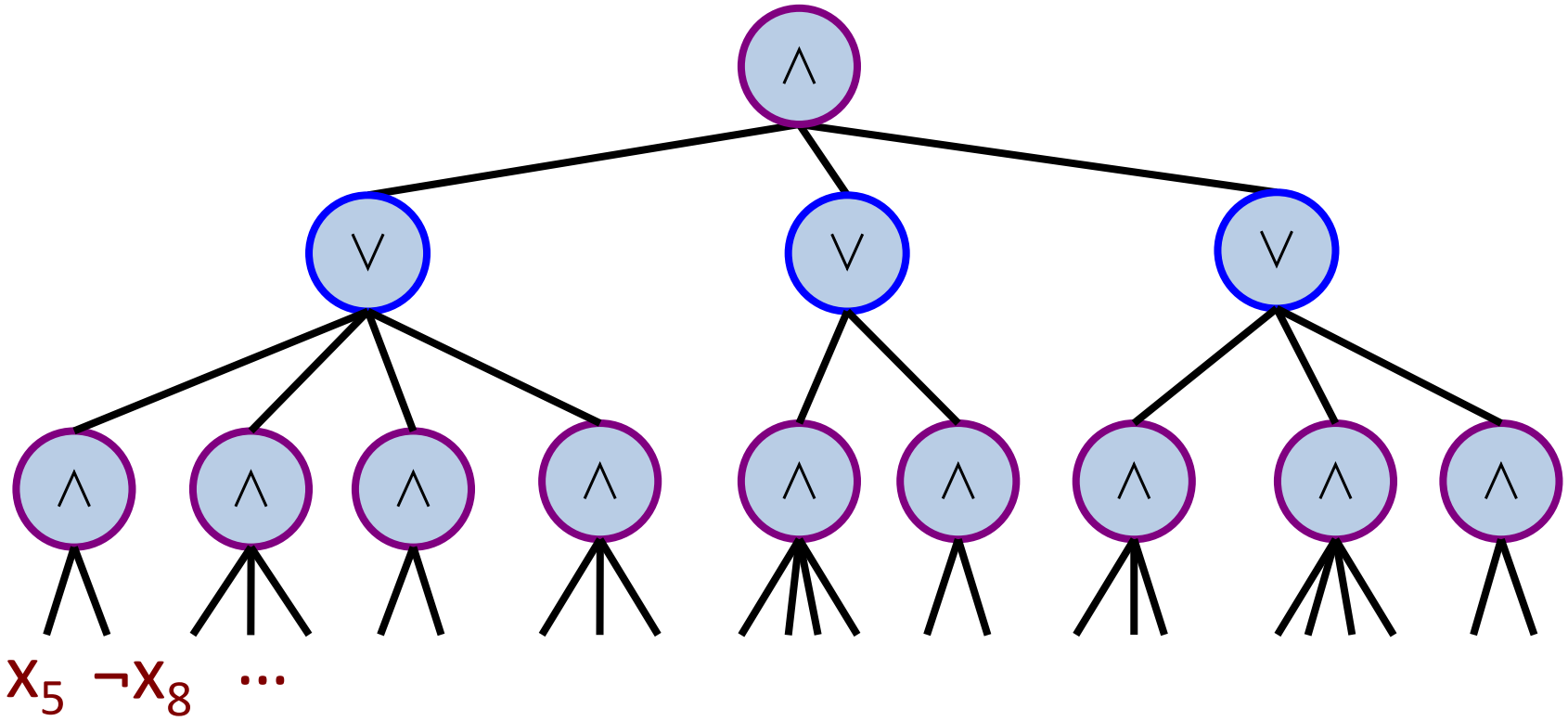
AC^0 Circuits



AC^0 Circuits



AC^0 Formulas



AC^0 Lower Bounds

- **Exponential lower bounds** known since the 1980's: the depth-d AC^0 circuit size $PARITY_n$ is $2^{\Theta(n^{1/(d-1)})}$

[Ajtai, Furst-Saxe-Sipser, Yao, Hastad]

AC^0 Lower Bounds

- **Exponential lower bounds** known since the 1980's: the depth-d AC^0 circuit size $PARITY_n$ is $2^{\Theta(n^{1/(d-1)})}$

[Ajtai, Furst-Saxe-Sipser, Yao, Hastad]

Switching Lemma
(simplification under p-random restrictions)

Lower Bound Techniques

- **counting**
  - almost all Boolean functions are complex
  - circuit size hierarchy theorem
- **gate-elimination arguments [restriction based]**
  - best lower bounds for *unrestricted* circuits and formulas
- **switching lemmas [restriction based]**
  - best lower bounds against AC^0
- **polynomial method**
  - best lower bounds against $AC^0[\oplus]$

Monotone Lower Bounds

$$mAC^0 \subset mNC^1 \subset mL \subset mNL \subset mNC \subset mP \subset mNP \subset \cdots$$

- We know essentially all separations among interesting monotone classes, via a multitude of techniques

Gate Elimination Arguments & Shrinkage

Restrictions

- Consider a Boolean function

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

- A **restriction** (on the variables of f) is a function

$$R : \{x_1,\ldots,x_n\} \rightarrow \{0,1,\star\}$$

Restrictions

- Consider a Boolean function

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

- A **restriction** (on the variables of f) is a function

$$R : \{x_1,\ldots,x_n\} \rightarrow \{0,1,\star\}$$

equivalently, a **partial function** from $\{x_1,\ldots,x_n\}$ to $\{0,1\}$

Restrictions

- Consider a Boolean function

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

- A **restriction** (on the variables of f) is a function

$$R : \{x_1,\ldots,x_n\} \to \{0,1,\star\}$$

- Applying R to f, we get a Boolean function

$$f \restriction R : \{0,1\}^{Stars(R)} \to \{0,1\}$$

Restrictions

- Consider a Boolean function

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

- A **restriction** (on the variables of f) is a function

$$R : \{x_1,\ldots,x_n\} \rightarrow \{0,1,\star\}$$

- Applying R to f, we get a Boolean function

$$f \restriction R : \{0,1\}^{Stars(R)} \rightarrow \{0,1\}$$

$$R \quad \star 1 \star \star 1\,0 \star 1 \star 1\,0\,0 \star \star 0 \star 0 \star \star \star 0 \star 0$$

$$f \restriction R\,(0 \quad 1\,0 \quad\quad 0 \quad 0 \quad\quad\quad 1\,1 \quad 1 \quad 1\,0\,1 \quad 1 \quad)$$

$$f(0\,1\,1\,0\,1\,0\,0\,1\,0\,1\,0\,0\,1\,1\,0\,1\,0\,1\,0\,1\,0)$$

Restrictions

- Consider a Boolean function

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

- A **restriction** (on the variables of f) is a function

$$R : \{x_1,\ldots,x_n\} \to \{0,1,\star\}$$

- Applying R to f, we get a Boolean function

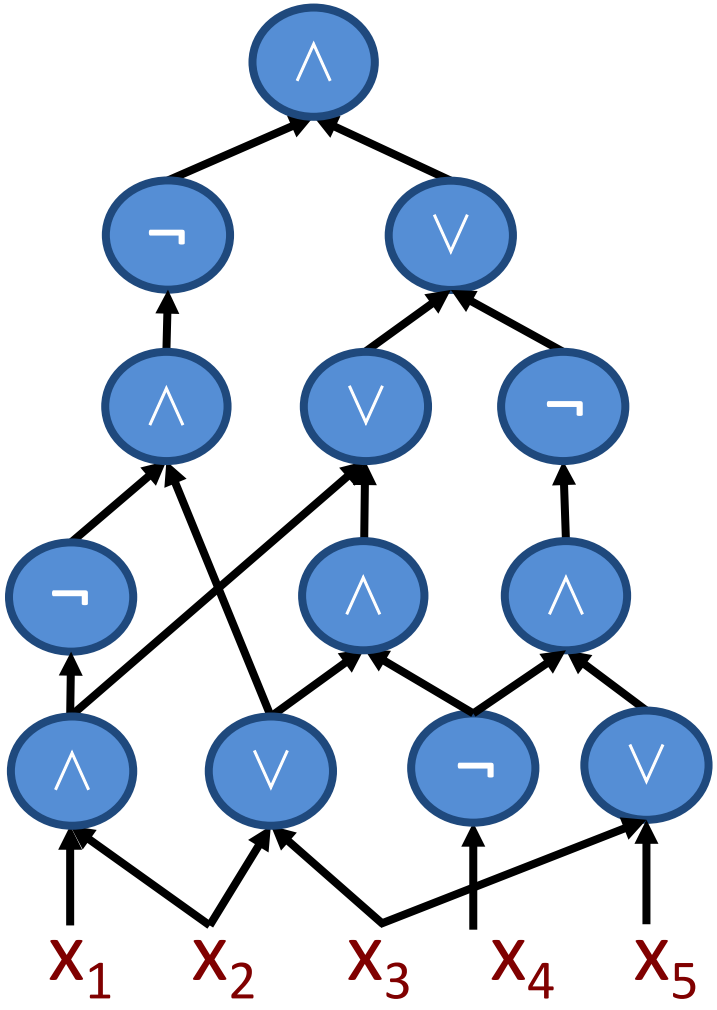
$$f \restriction R : \{0,1\}^{\mathrm{Stars}(R)} \to \{0,1\}$$

- Can also apply R *syntactically* to circuits (and other objects)

Restricting a Circuit

- Consider the 1-bit restriction

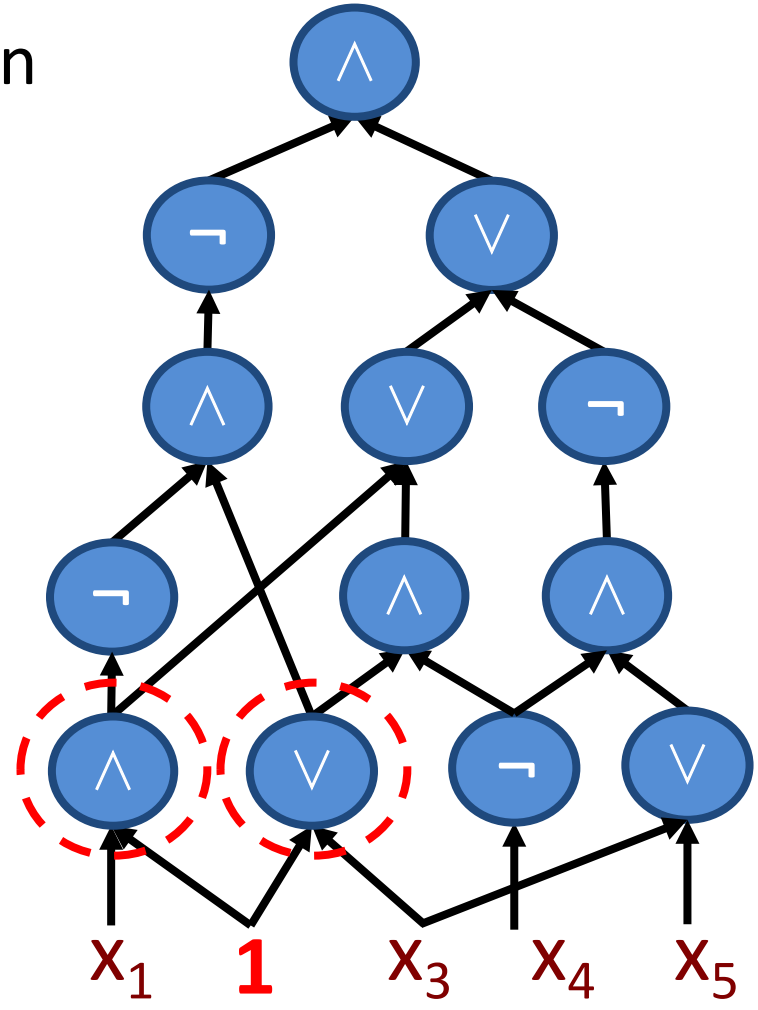
  $R = \{ x_2 \mapsto 1 \}$



Restricting a Circuit

- Consider the 1-bit restriction

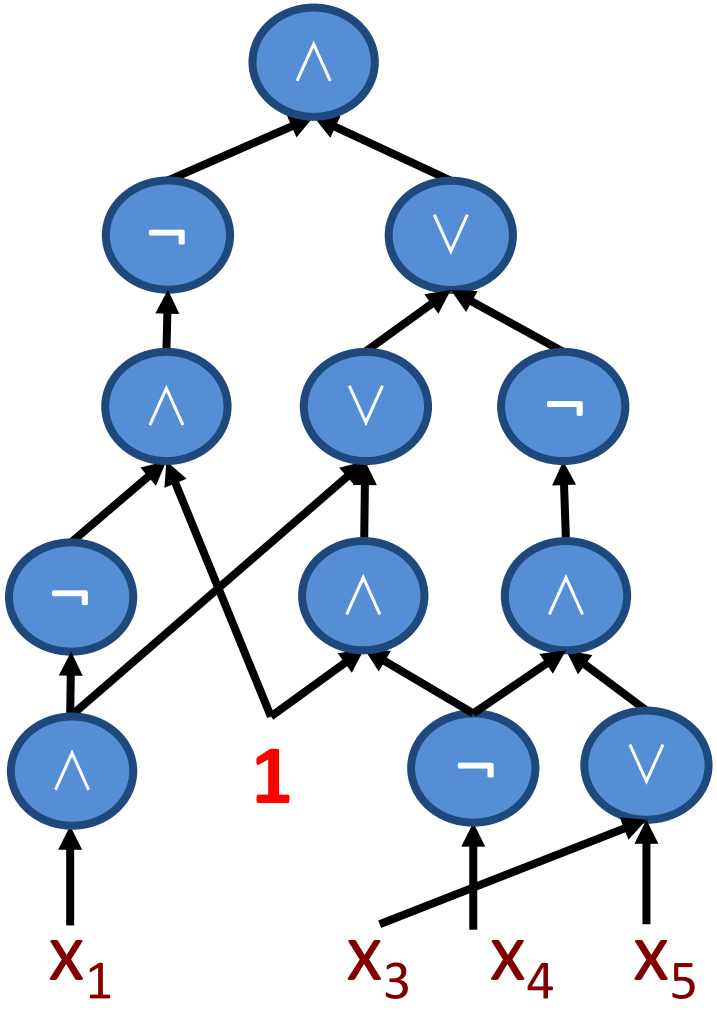
  $R = \{ x_2 \mapsto 1 \}$



Restricting a Circuit

- Consider the 1-bit restriction

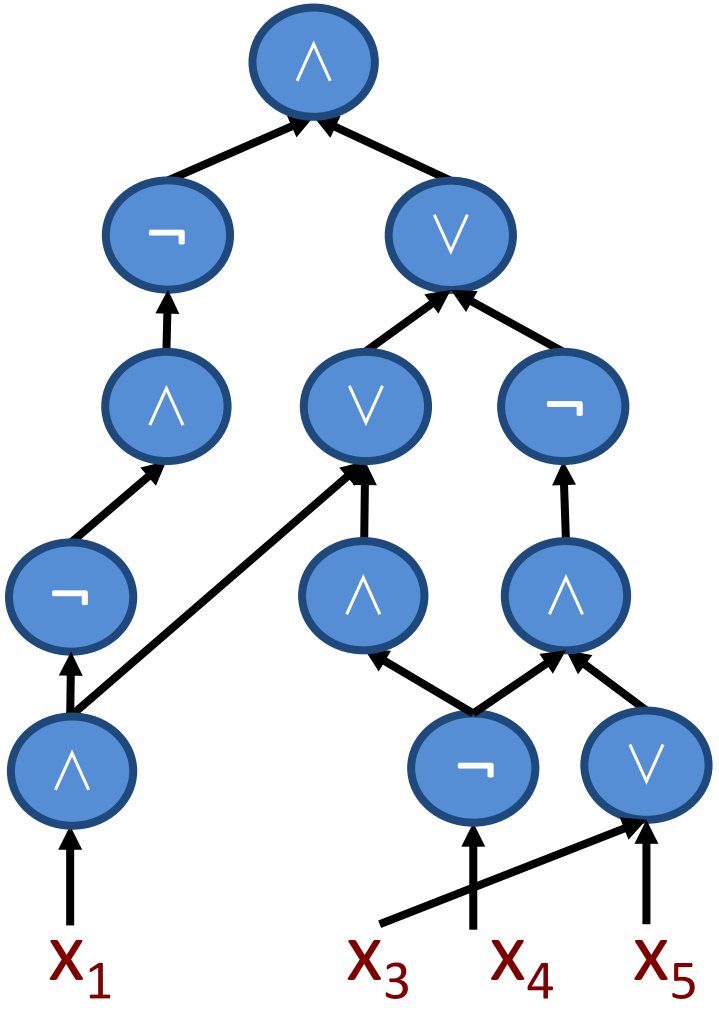
  $R = \{ x_2 \mapsto 1 \}$



Restricting a Circuit

- Consider the 1-bit restriction

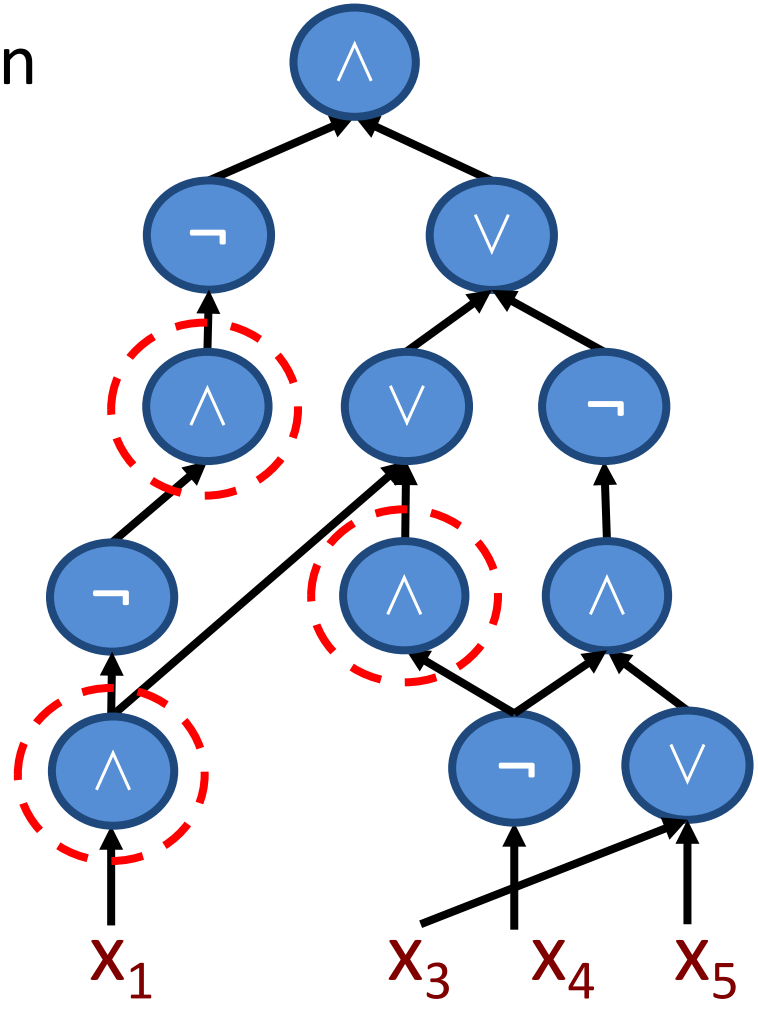
  $R = \{ x_2 \mapsto 1 \}$



Restricting a Circuit

- Consider the 1-bit restriction

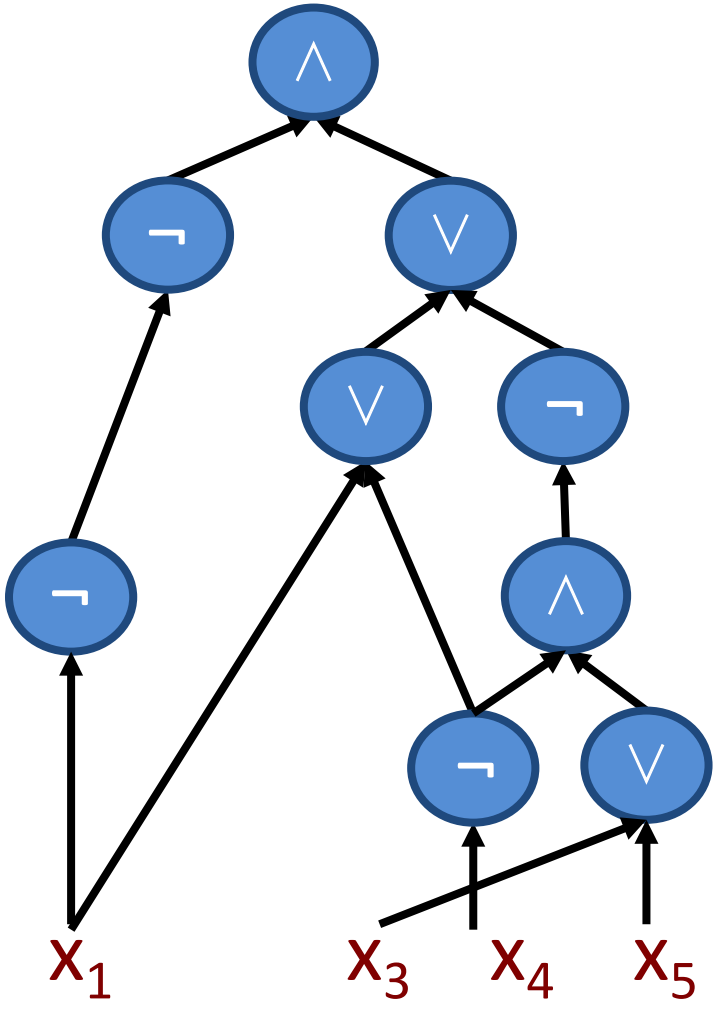
  $R = \{ x_2 \mapsto 1 \}$



Restricting a Circuit

- Consider the 1-bit restriction

  $R = \{ x_2 \mapsto 1 \}$



Gate Elimination

- Lemma [Schnorr '76]

  If a circuit C (in basis $\{AND_2, OR_2, NOT\}$) computes $PARITY_n$ ($n \geq 2$), then there exists a 1-bit restriction R killing at least 3 AND/OR gates of C (i.e. $size(C \restriction R) \leq size(C) - 3$)

- Corollary

  $PARITY_n$ has circuit size at least $3n - 3$. Moreover, matching upper bound.

Gate Elimination

- More sophisticated gate elimination arguments give the best lower bounds:

  $5n - o(n)$ $\{AND_2, OR_2, NOT\}$ basis

  [Iwama-Lachish-Morizumi-Raz '02]

  $\approx 3.01n$ full binary basis

  [Find-Golovnev-Hirsch-Kulikov '16]

Gate Elimination

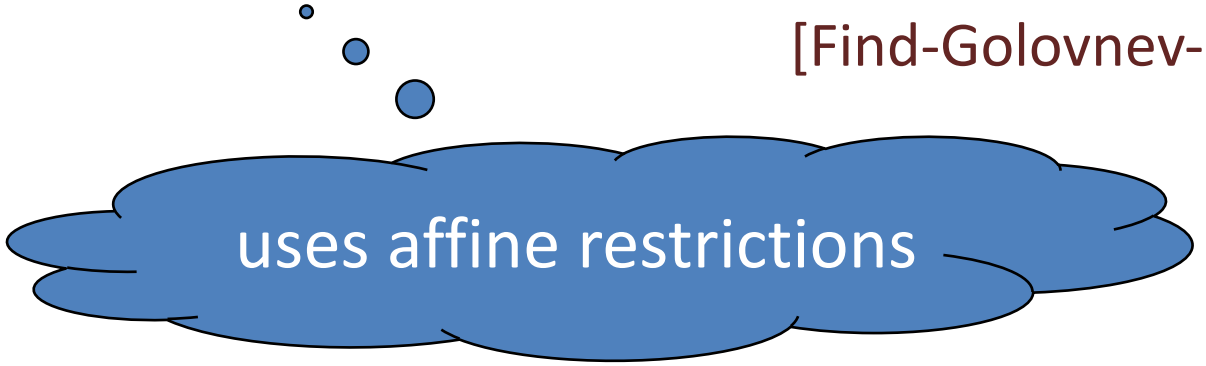
- More sophisticated gate elimination arguments give the best lower bounds:

$5n - o(n)$ $\{AND_2, OR_2, NOT\}$ basis

[Iwama-Lachish-Morizumi-Raz '02]

$\approx 3.01n$ full binary basis

[Find-Golovnev-Hirsch-Kulikov '16]



Gate Elimination

- Theorem [Chaudhuri-Radhakrishnan '96]

  $n^{1 + 1/\exp(d)}$ lower bound on the depth-d AC^0 circuit size of APPROX-MAJORITY via ***deterministic restrictions*** (greedily apply the best 1-bit restriction)

Gate Elimination

- Theorem [Chaudhuri-Radhakrishnan '96]

  $n^{1 + 1/\exp(d)}$ lower bound on the depth-d AC^0 circuit size of APPROX-MAJORITY via ***deterministic restrictions*** (greedily apply the best 1-bit restriction)

- Theorem [Koppary-Srinivasan '12]

  Similar lower bound for $AC^0[\oplus]$ circuits via ***deterministic low-degree-variety restrictions*** (method of "certifying polynomials")

p-Random Restriction $\mathbf{R}_p$

- For $0 \le p \le 1$, let $\mathbf{R}_p$ denotes the p**-random restriction**

$$\mathbf{R}_p(x_i) = \begin{cases} \star & \text{with prob. } p \\ 0 & \text{with prob. } (1-p)/2 \\ 1 & \text{with prob. } (1-p)/2 \end{cases}$$

  independently for each variable index $i \in [n]$

p-Random Restriction $\mathbf{R}_p$

- For $0 \le p \le 1$, let $\mathbf{R}$

$\mathbf{R}_p(x_i) = \{$

1 with prob. $(1-p)/2$

independently for each variable index $i \in [n]$

<u>Convention</u>:

Random objects written in **boldface**

Effect of $\mathbf{R}_p$

- $\mathbf{R}_p$ simplifies Boolean functions computed by small:
  - DeMorgan formulas
  - decision trees
  - AC^0 circuits
- Certain Boolean functions, like $PARITY_n$, maintain their complexity under $\mathbf{R}_p$
- Ergo, *lower bounds!*

Effect of $\mathbf{R}_p$ on DeMorgan Formulas

- Subbotovskaya '61

  If F is an n-variable DeMorgan formula, then

  $$\mathrm{Ex}[\ \mathrm{leafsize}(F \restriction \textbf{random 1-bit rest.})\ ] \leq (1-n)^{1.5}\,\mathrm{leafsize}(F)$$

- As a consequence,

  $$\mathrm{Ex}[\ \mathrm{leafsize}(F \restriction \mathbf{R}_p)\ ] \leq O(p^{1.5}\,\mathrm{leafsize}(F) + 1)$$

Effect of $\mathbf{R}_p$ on DeMorgan Formulas

- Subbotovskaya '61

  If F is an n-variable DeMorgan formula, then

  $$\mathrm{Ex}[\ \mathrm{leafsize}(F \restriction \textbf{random 1-bit rest.})\ ] \leq (1-n)^{1.5}\,\mathrm{leafsize}(F)$$

- As a consequence,

  $$\mathrm{Ex}[\ \mathrm{leafsize}(F \restriction \mathbf{R}_p)\ ] \leq O(p^{1.5}\,\mathrm{leafsize}(F) + 1)$$

- Hastad '98, Tal '14

  $$\mathrm{Ex}[\ \mathrm{leafsize}(F \restriction \mathbf{R}_p)\ ] \leq O(p^{2}\,\mathrm{leafsize}(F) + 1)$$

Effect of $\mathbf{R}_p$ on DeMorgan Formulas

- Subbotovskaya ‘61

  If F is an n-variable DeMorgan formula, then

  Ex[leafsize(F ↾ **random 1-bit rest.**)]

  Known as the ***shrinkage exponent*** of DeMorgan formulas

  leafsize(F) + 1)

- Hastad ‘98, Tal ‘14

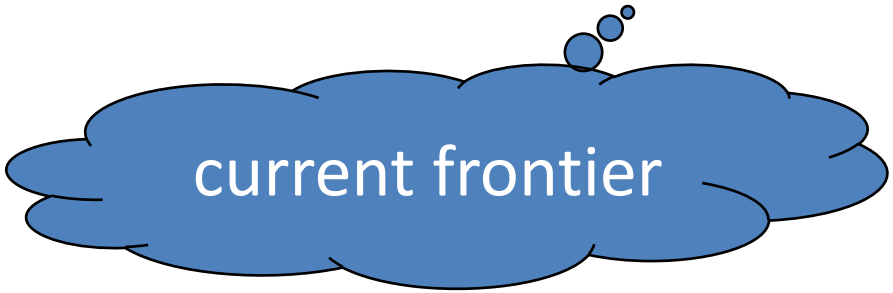
  $\mathrm{Ex}[\ \mathrm{leafsize}(F \restriction \mathbf{R}_p)\ ] \leq O(p^2\ \mathrm{leafsize}(F) + 1)$

Effect of $\mathbf{R}_p$ on DeMorgan Formulas

- Implies lower bounds:

$$\text{leafsize}(\text{PARITY}_n) = \Omega(n^2)$$

$$\text{leafsize}(\text{ANDREEV}_n) = \tilde{\Omega}(n^3)$$



- Hastad '98, Tal '14

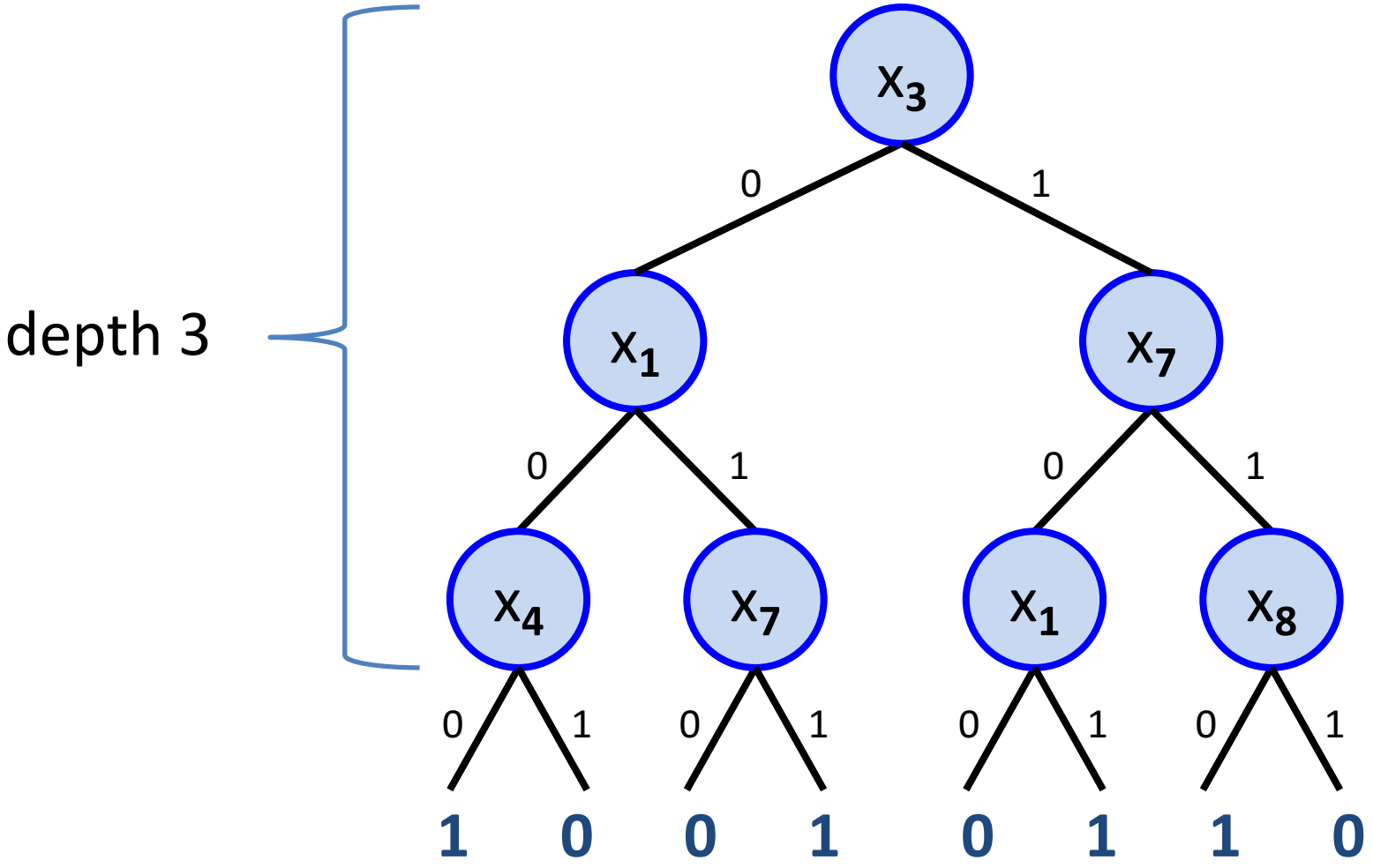
$$\text{Ex}[\ \text{leafsize}(F \restriction \mathbf{R}_p)\ ] \leq O(p^2\, \text{leafsize}(F) + 1)$$

Effect of $\mathbf{R}_p$ on *Monotone* Formulas

- Open Question What is the shrinkage exponent of **monotone formulas** (basis $\{AND_2, OR_2\}$)?
- Conjecture Equals the shrinkage exponent of **read-once formulas** (≈ 3.27) [Hastad-Razborov-Yao '97]

The Switching Lemma

Decision Trees



Decision Trees

The ***decision-tree depth*** of a Boolean function

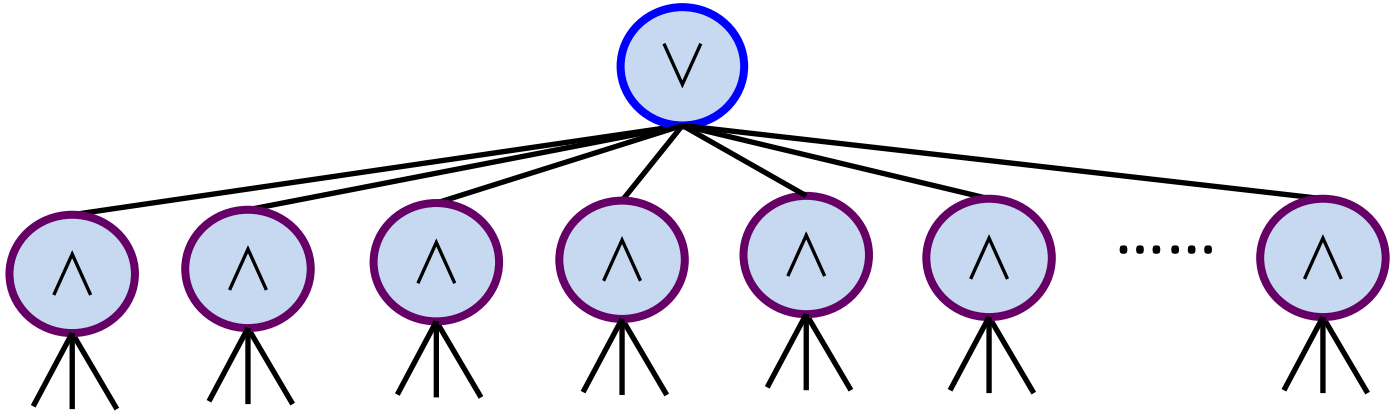
$$f : \{0,1\}^n \rightarrow \{0,1\}$$

is the minimum depth of a decision tree that computes f.

- $DT_{depth}(PARITY_n) = DT_{depth}(AND_n) = n$
- $DT_{depth}(f) = 0 \Leftrightarrow$ f is constant

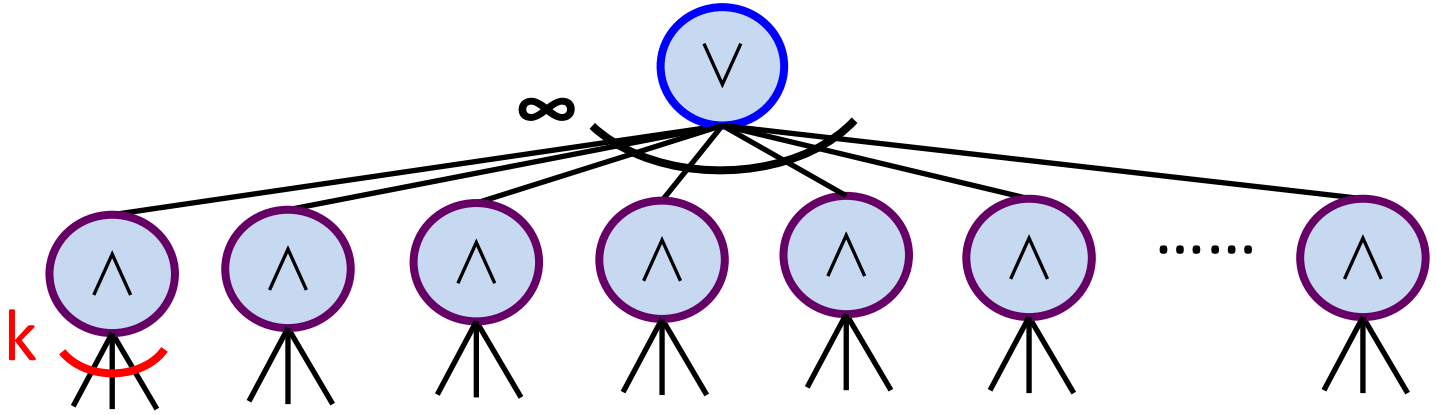
Depth-2 Formulas (DNFs and CNFs)

- **DNF** = disjunctive normal form (OR-AND formula)
- **CNF** = conjunctive normal form (AND-OR formula)



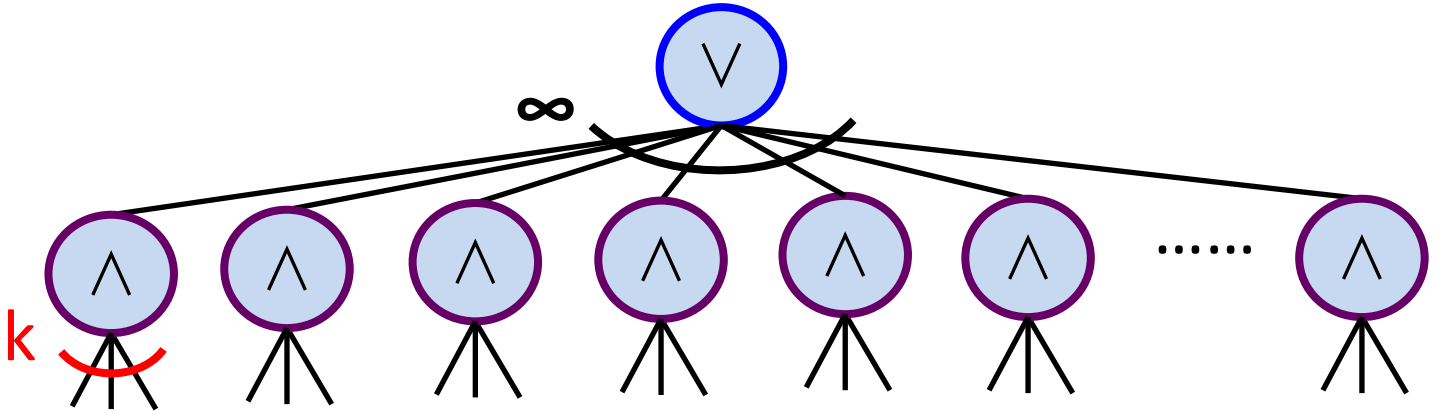
Depth-2 Formulas (DNFs and CNFs)

- **DNF** = disjunctive normal form (OR-AND formula)
- **CNF** = conjunctive normal form (AND-OR formula)
- **width** = bottom fan-in (max # of variables in a clause)



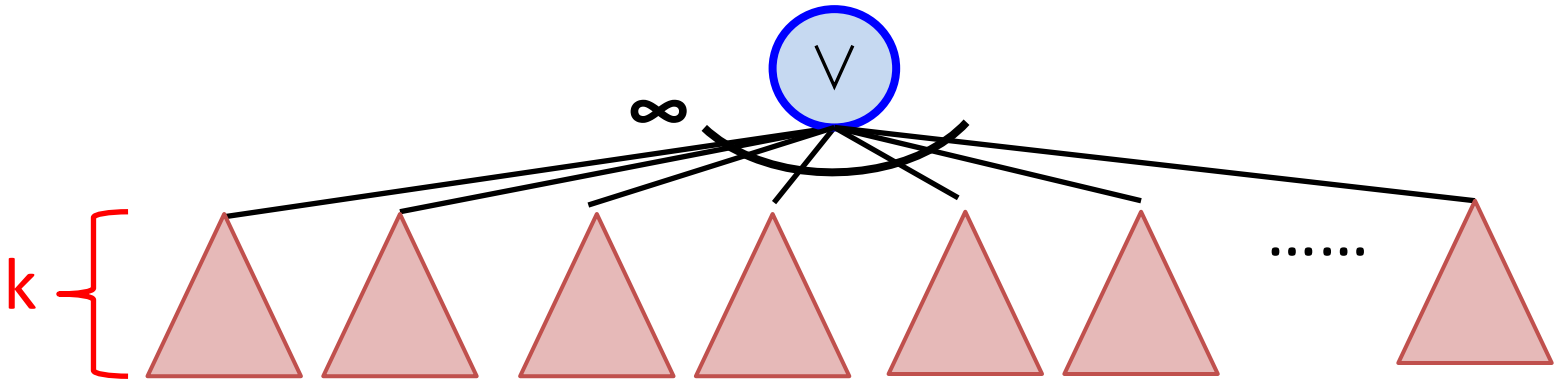
Depth-2 Formulas (DNFs and CNFs)

- **k-DNF** = width-k DNF
- **k-CNF** = width-k CNF



Depth-2 Formulas (DNFs and CNFs)

- **k-DNF** = width-k DNF = OR_∞ of depth-k DTs
- **k-CNF** = width-k CNF = AND_∞ of depth-k DTs



Depth-2 Formulas (DNFs and CNFs)

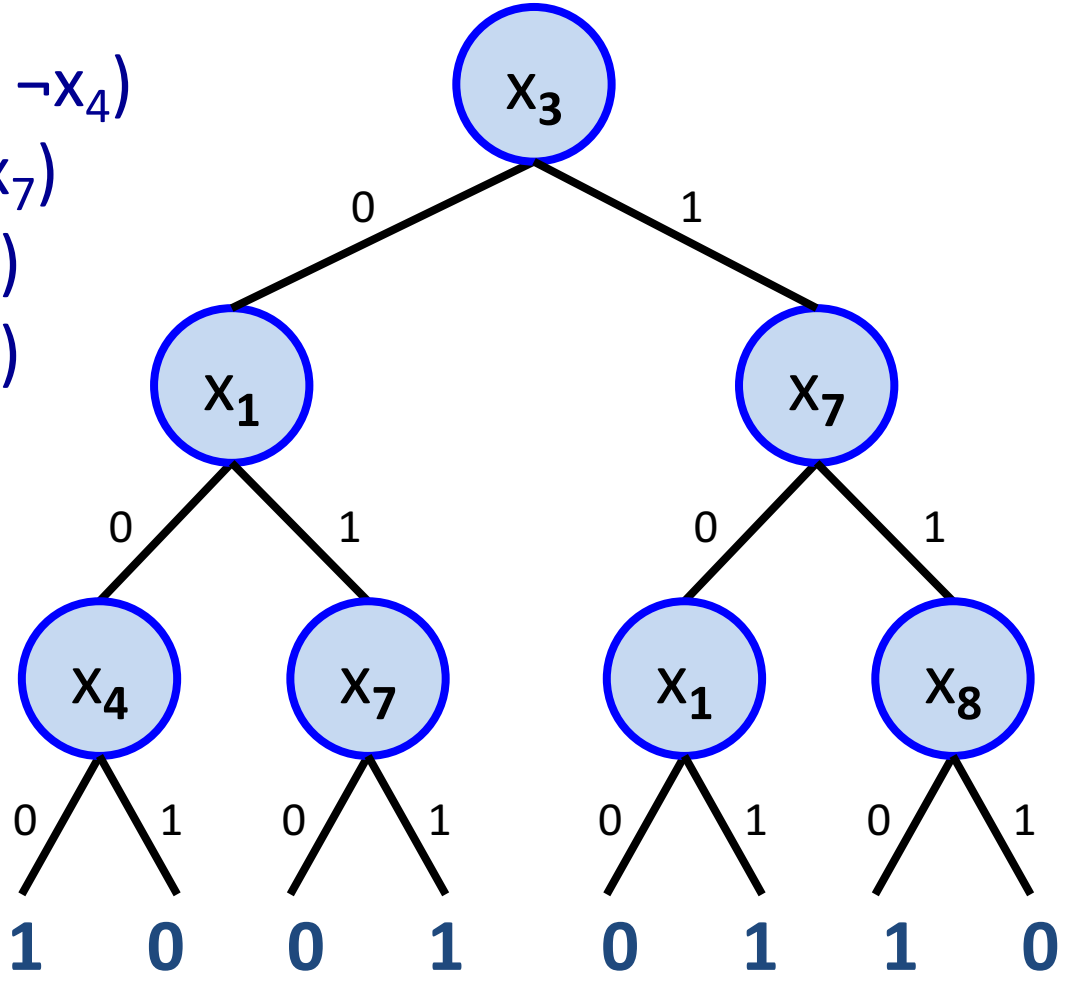
- **k-DNF** = width-k DNF = OR_∞ of depth-k DTs
- **k-CNF** = width-k CNF = AND_∞ of depth-k DTs

- Every depth-k DT is equivalent to a k-DNF and a k-CNF

- Weak converse: If a Boolean function is equivalent to a k-DNF and an ℓ-CNF, then it is equivalent to a DT of depth $k\ell$

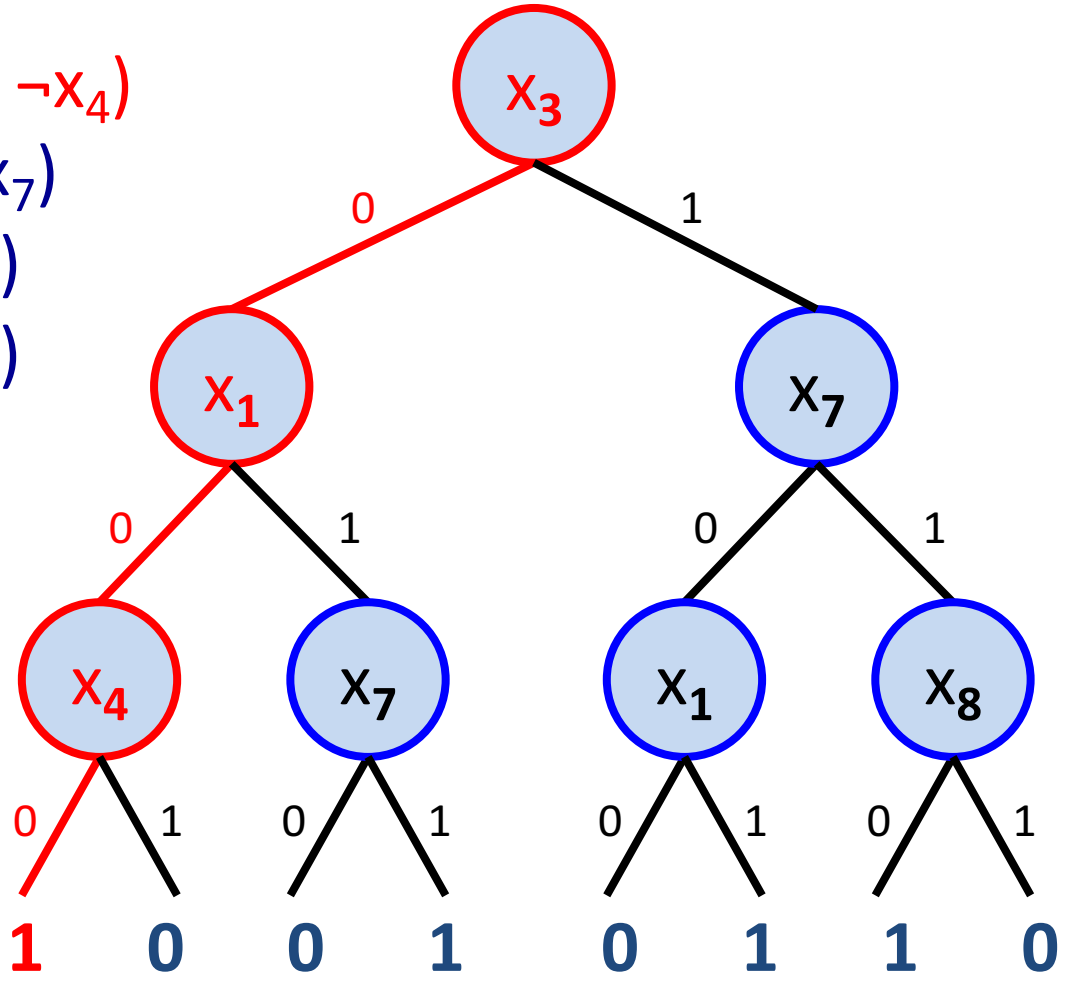
Decision Tree to DNF

$$(\neg x_3 \wedge \neg x_1 \wedge \neg x_4) \vee (\neg x_3 \wedge x_1 \wedge x_7) \vee (x_3 \wedge x_7 \wedge x_1) \vee (x_3 \wedge x_7 \wedge x_8)$$



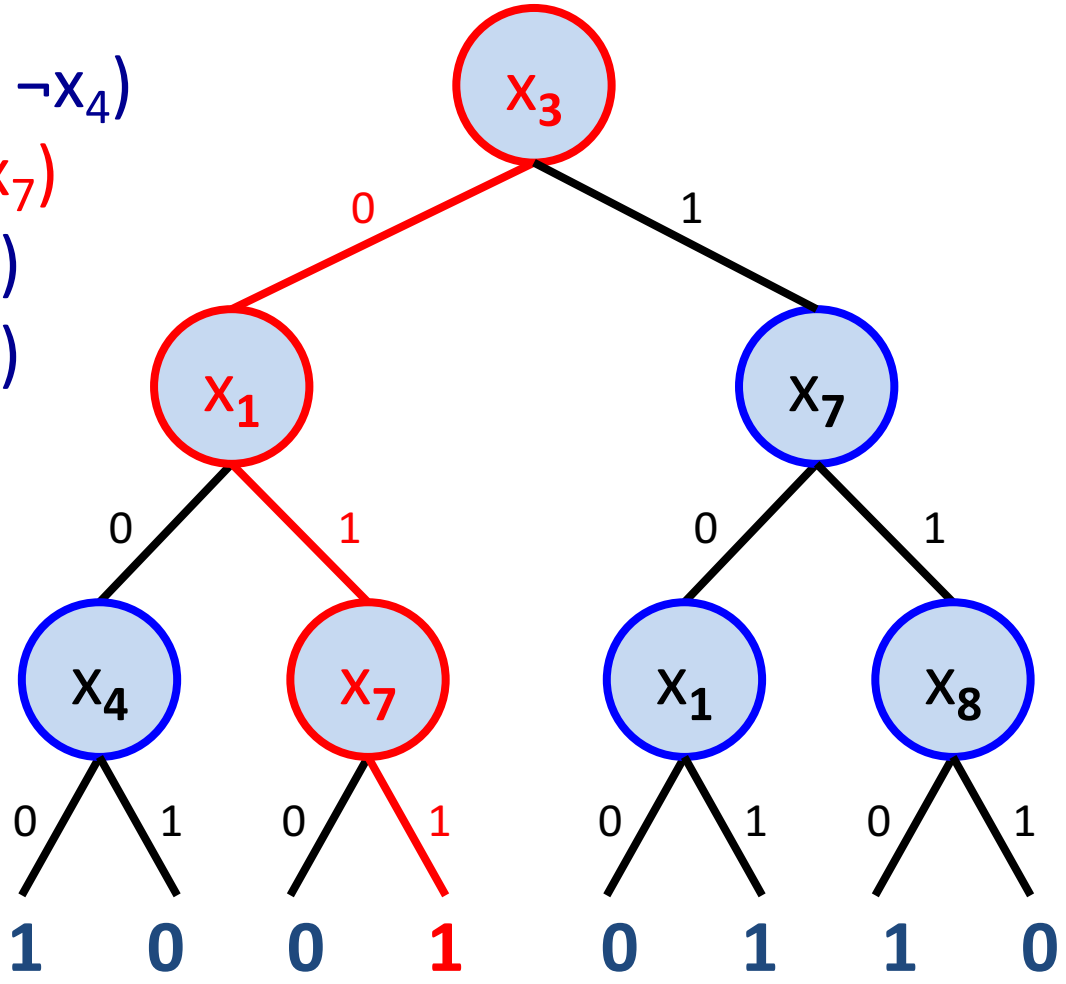
Decision Tree to DNF

$$(\neg x_3 \wedge \neg x_1 \wedge \neg x_4) \vee (\neg x_3 \wedge x_1 \wedge x_7) \vee (x_3 \wedge x_7 \wedge x_1) \vee (x_3 \wedge x_7 \wedge x_8)$$



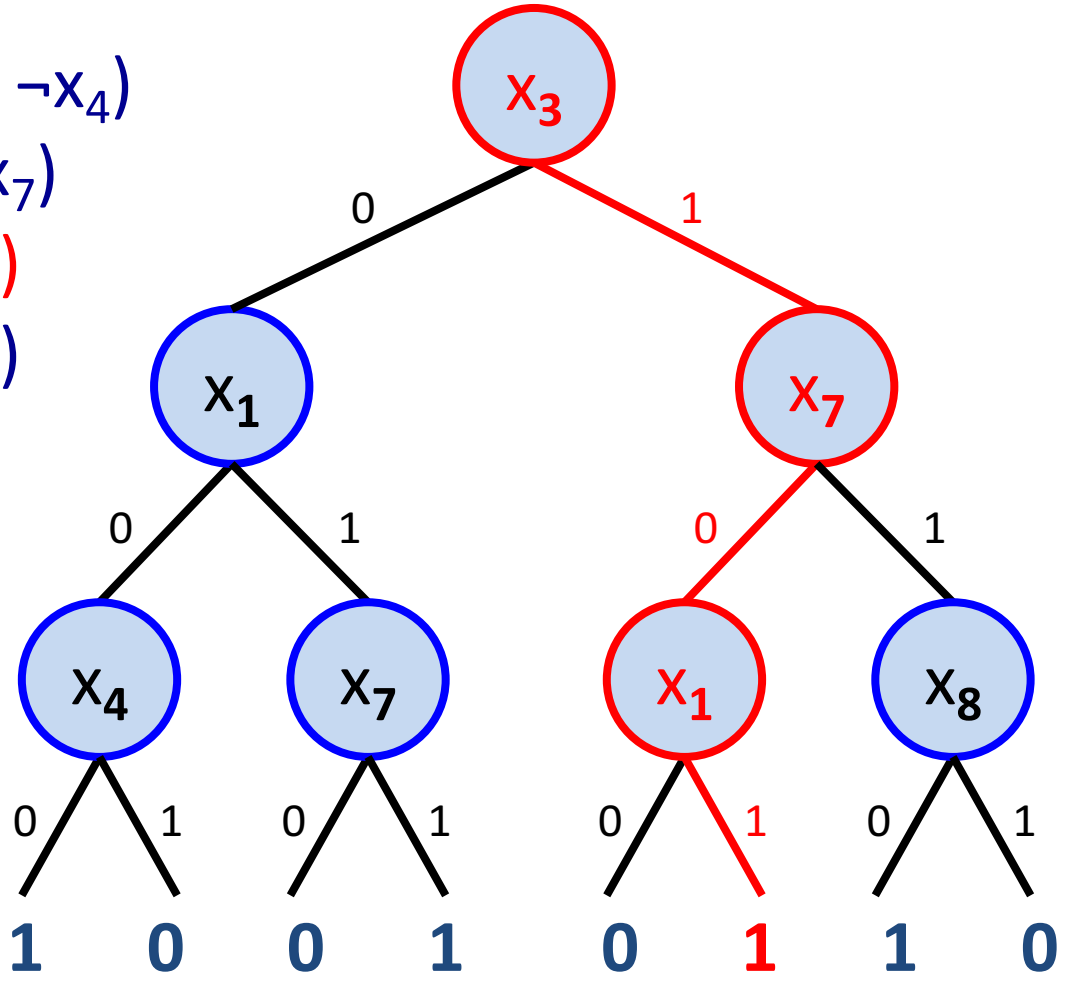
Decision Tree to DNF

$$(\neg x_3 \wedge \neg x_1 \wedge \neg x_4)$$
$$\vee\ (\neg x_3 \wedge x_1 \wedge x_7)$$
$$\vee\ (x_3 \wedge x_7 \wedge x_1)$$
$$\vee\ (x_3 \wedge x_7 \wedge x_8)$$



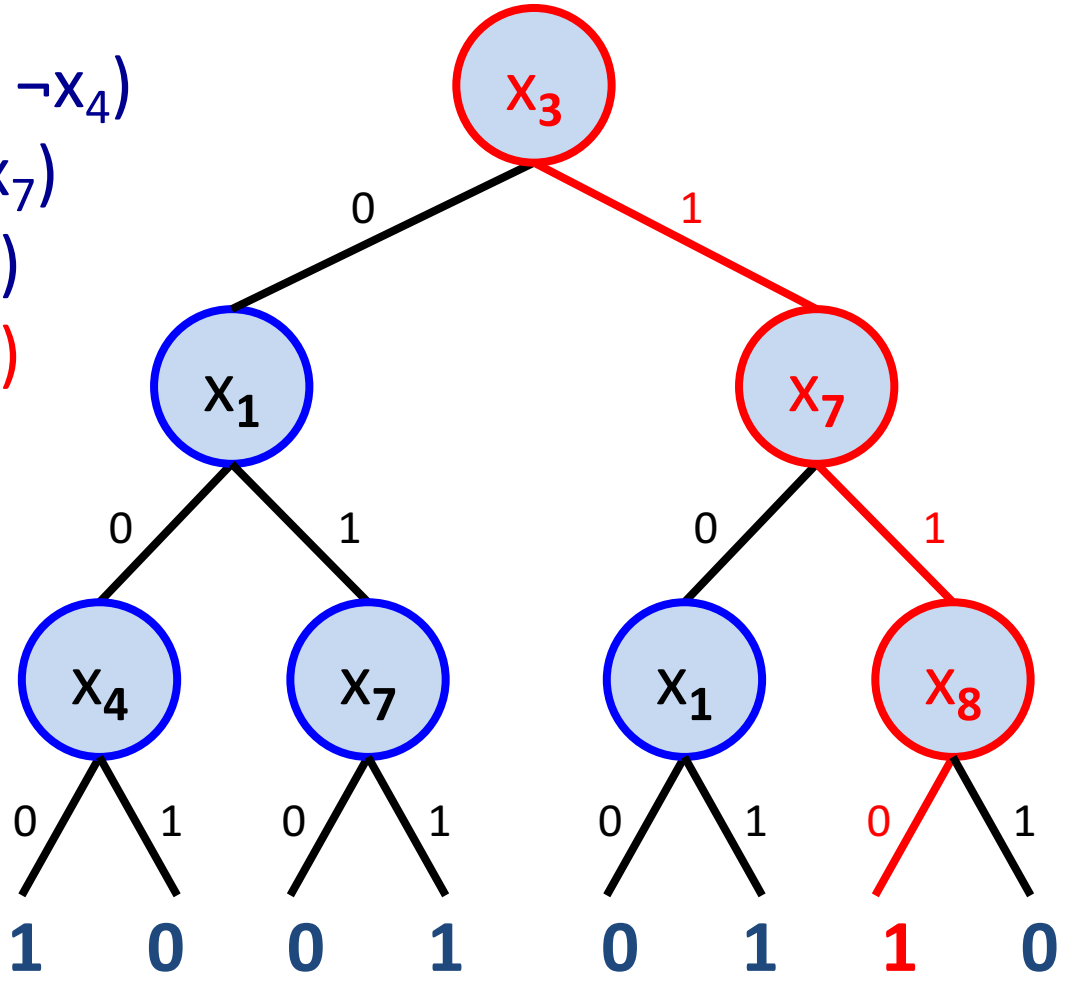
Decision Tree to DNF

$$(\neg x_3 \wedge \neg x_1 \wedge \neg x_4)$$
$$\vee\ (\neg x_3 \wedge x_1 \wedge x_7)$$
$$\vee\ (x_3 \wedge x_7 \wedge x_1)$$
$$\vee\ (x_3 \wedge x_7 \wedge x_8)$$



Decision Tree to DNF

$$(\neg x_3 \wedge \neg x_1 \wedge \neg x_4)$$
$$\vee\ (\neg x_3 \wedge x_1 \wedge x_7)$$
$$\vee\ (x_3 \wedge x_7 \wedge x_1)$$
$$\vee\ (x_3 \wedge x_7 \wedge x_8)$$



k-DNF Switching Lemma

Hastad's Switching Lemma (1986)

If F is a k-DNF (i.e. OR_∞ of depth-k decision trees), then

$$\Pr[\, DT_{depth}(F \restriction \mathbf{R}_p) \geq t \,] \leq (5pk)^t$$

k-DNF Switching Lemma

Hastad's Switching Lemma (1986)

If F is a k-DNF (i.e. OR_∞ of depth-k decision trees), then

$$\Pr[\, DT_{depth}(F \restriction \mathbf{R}_p) \geq t \,] \leq (5pk)^t$$

$\leq 2^{-t}$ when $p = 1 / 10k$

k-DNF Switching Lemma

Hastad's Switching Lemma (1986)

If F is a k-DNF (i.e. OR_∞ of depth-k decision trees), then

$$\Pr[\, DT_{depth}(F \restriction \mathbf{R}_p) \geq t \,] \leq (5pk)^t$$

Dual CNF version

If F is a k-CNF (i.e. AND_∞ of depth-k decision trees), then

$$\Pr[\, DT_{depth}(F \restriction \mathbf{R}_p) \geq t \,] \leq (5pk)^t$$

k-DNF Switching Lemma

Hastad's Switching Lemma (1986)

If F is a k-DNF (i.e. OR_∞ of depth-k decision trees), then

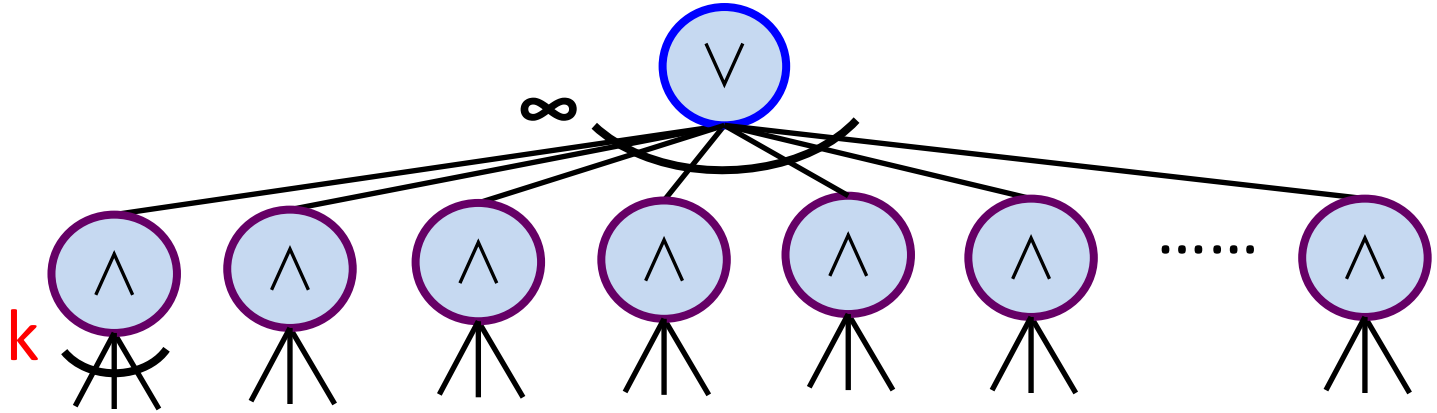
$$\Pr[\, DT_{depth}(F \restriction \mathbf{R}_p) \geq t \,] \leq (5pk)^t$$

Corollary (usual statement of the S.L.)

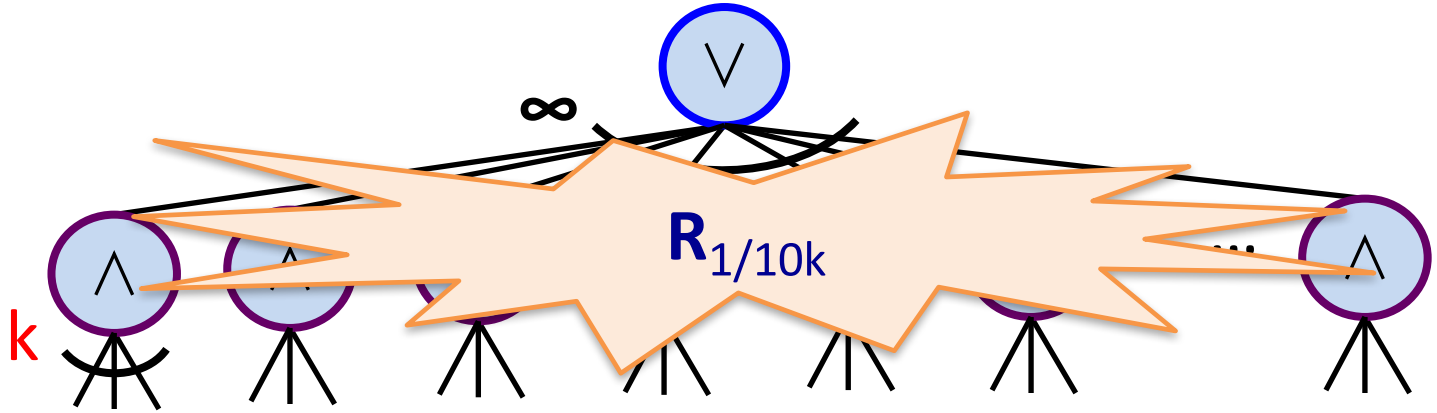
If F is a k-DNF, then

$$\Pr[\, F \restriction \mathbf{R}_p \text{ is not equivalent to a } t\text{-CNF} \,] \leq (5pk)^t$$

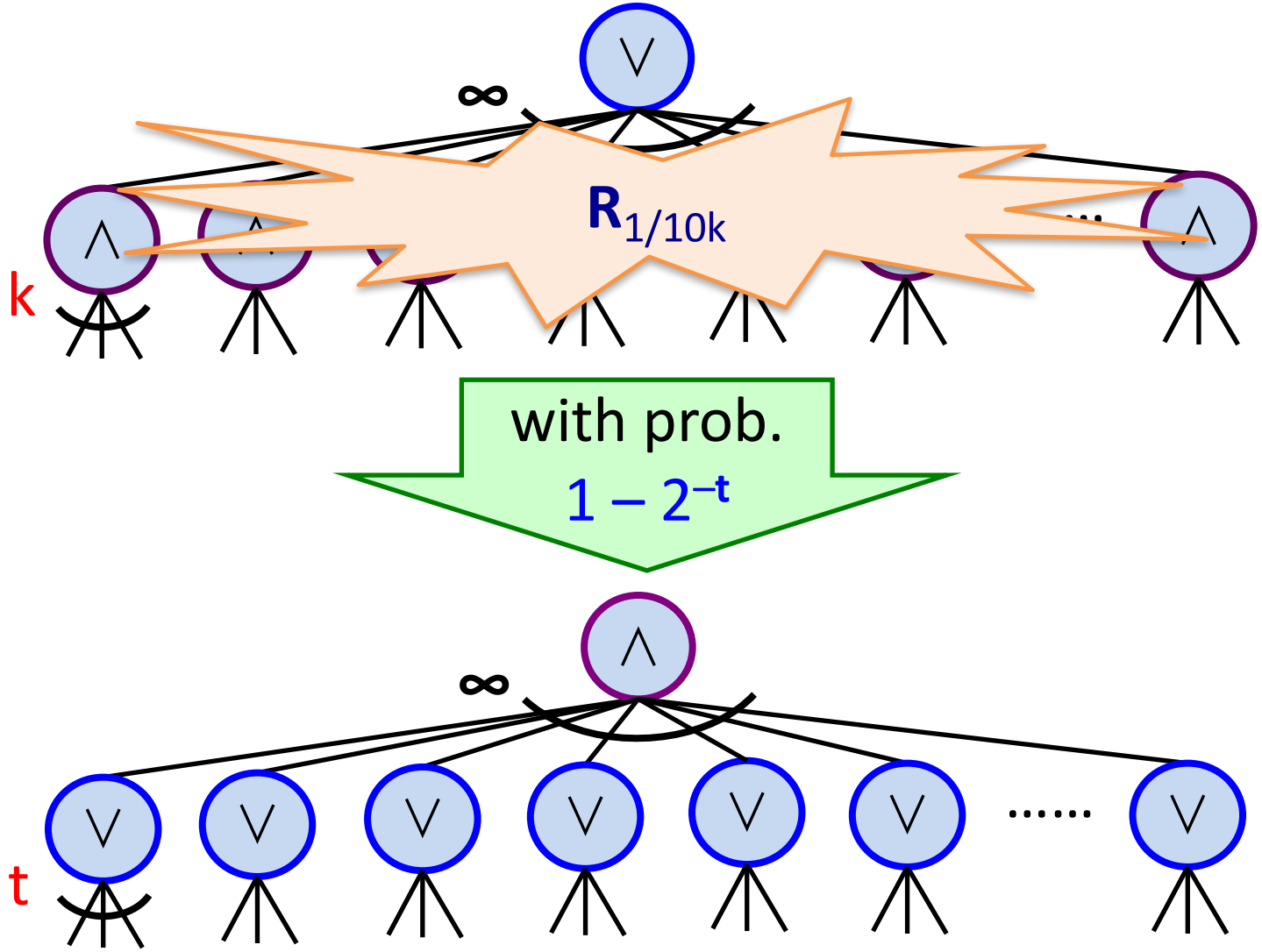
k-DNF Switching Lemma



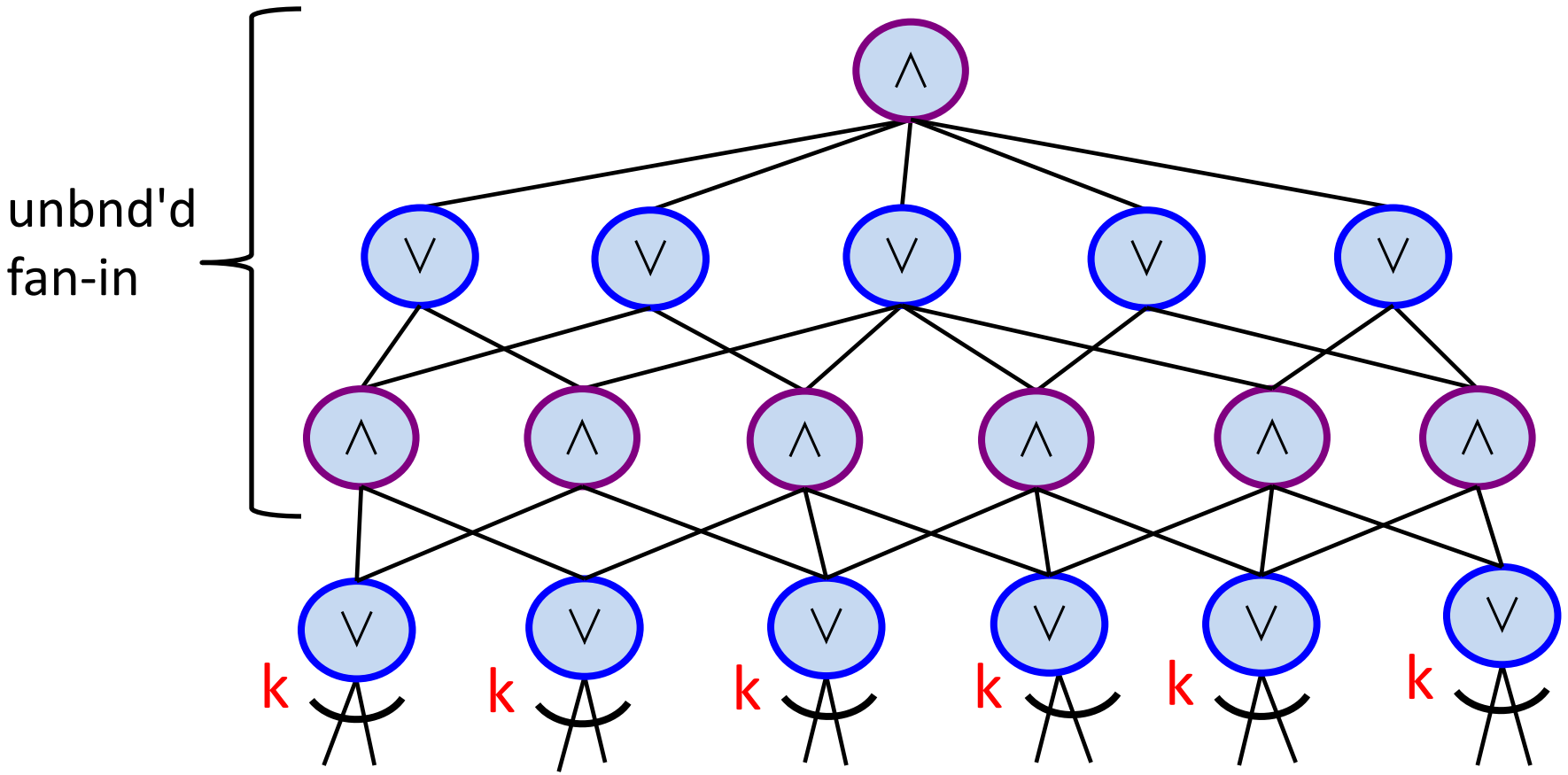
k-DNF Switching Lemma



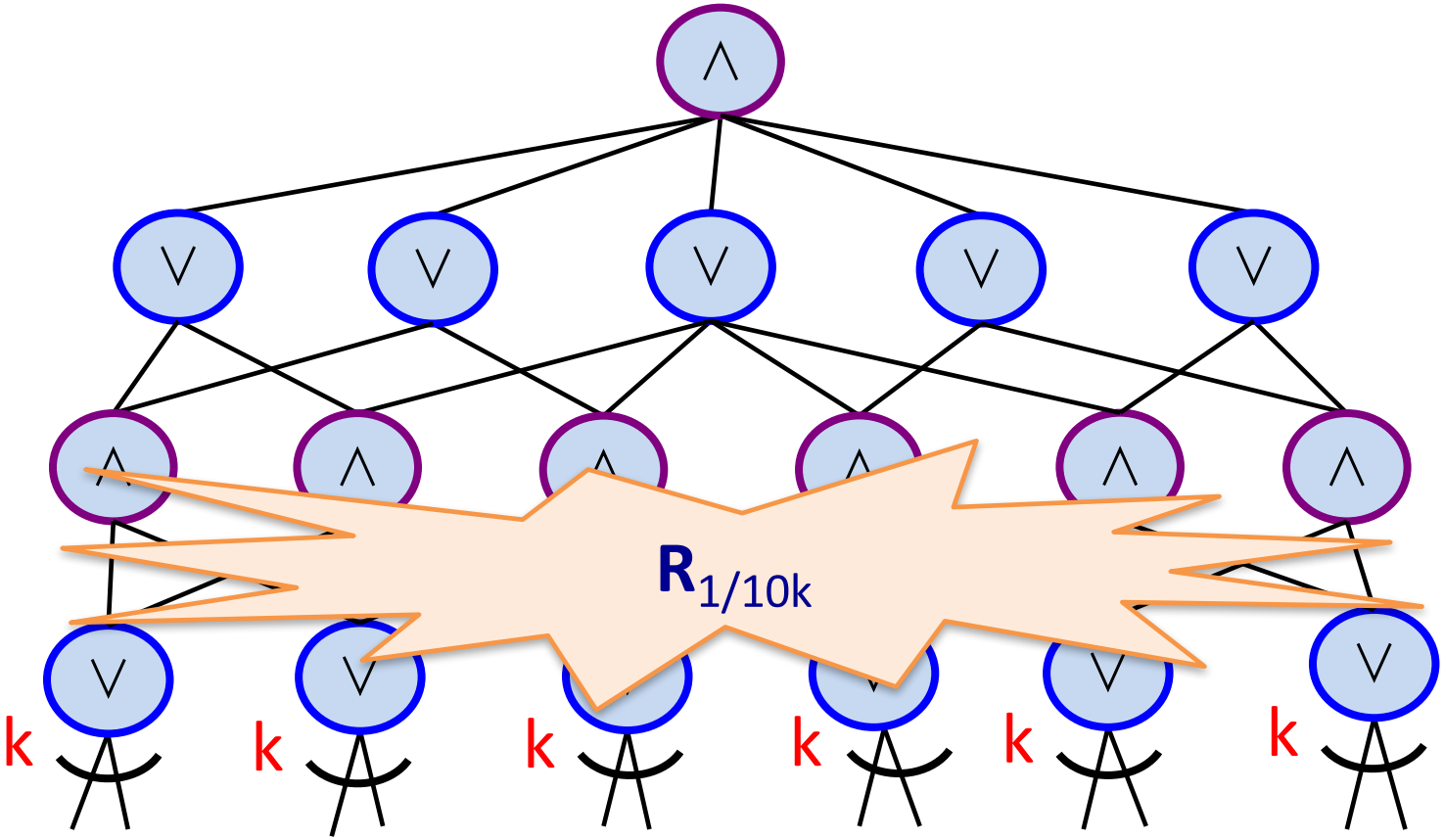
k-DNF Switching Lemma



Depth Reduction

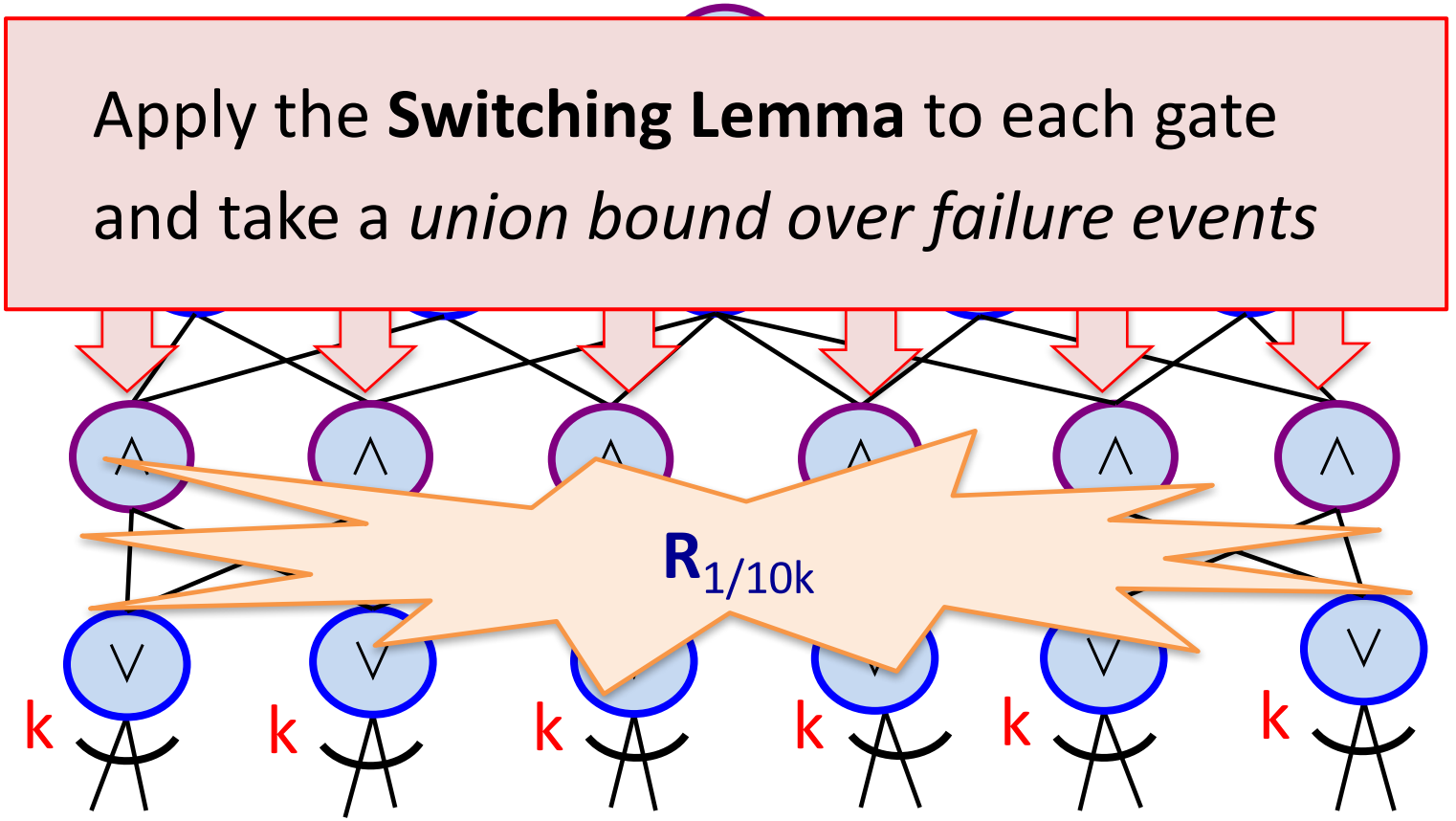


Depth Reduction

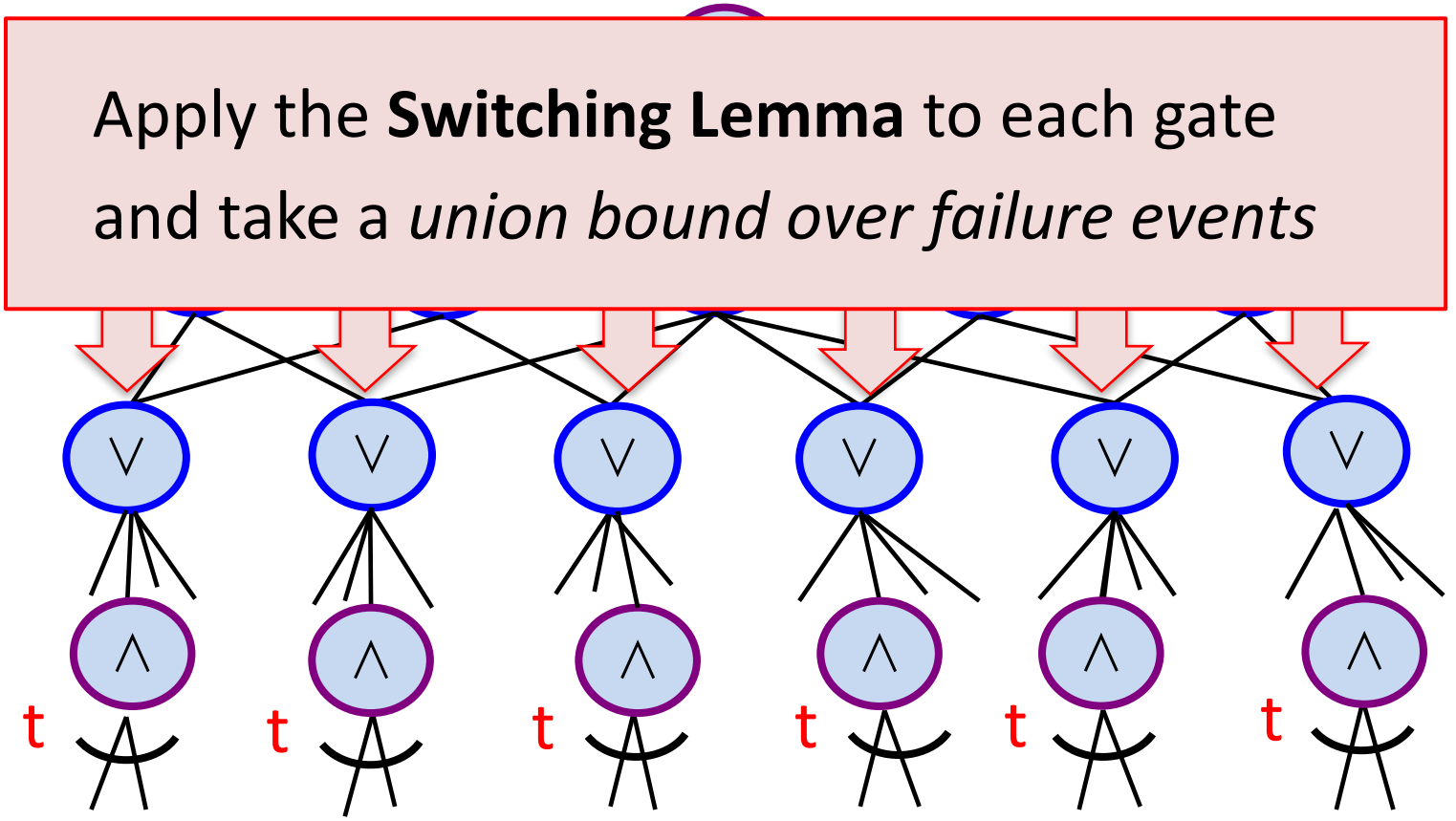


Depth Reduction

Apply the **Switching Lemma** to each gate and take a *union bound over failure events*



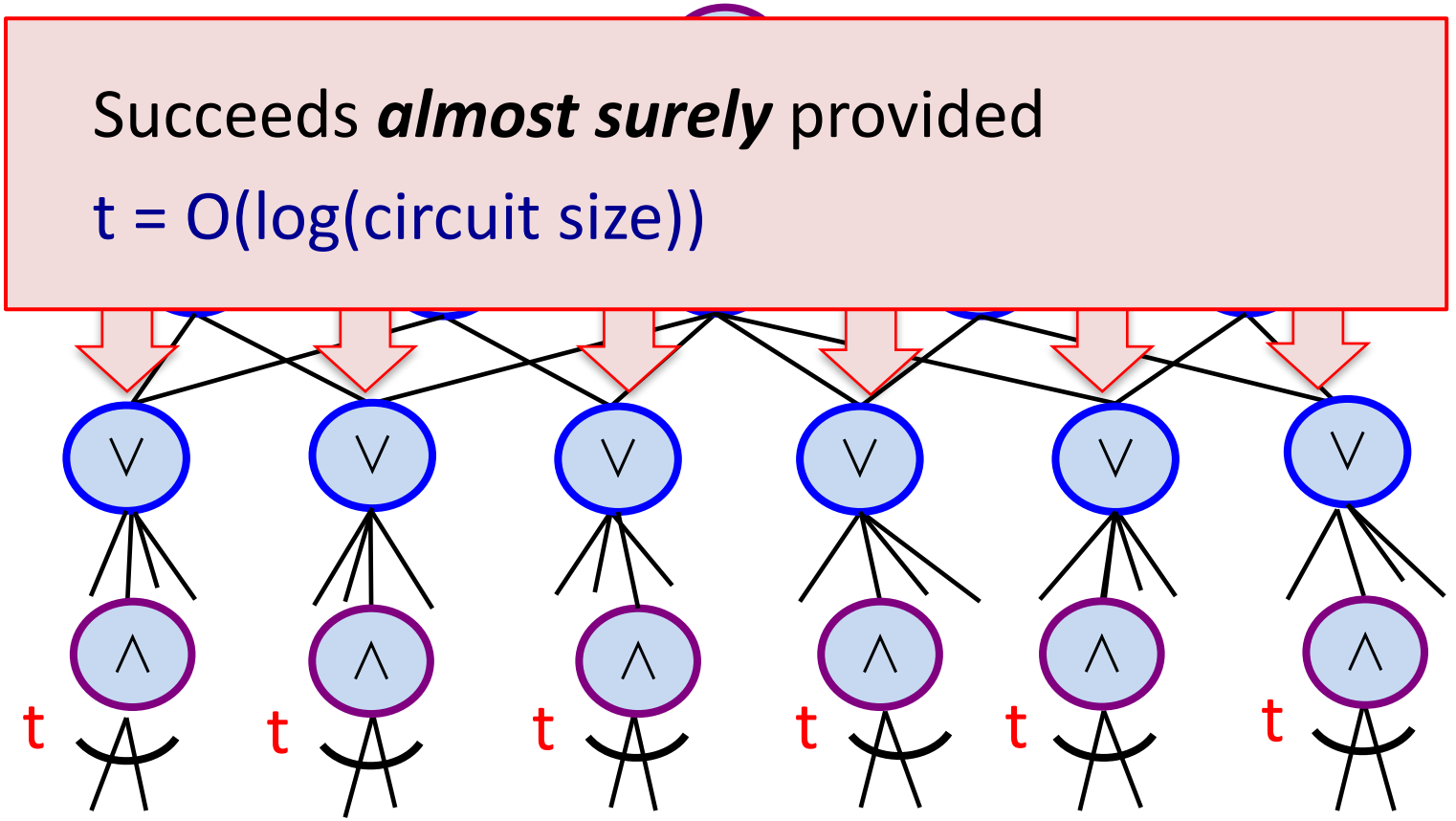
Depth Reduction



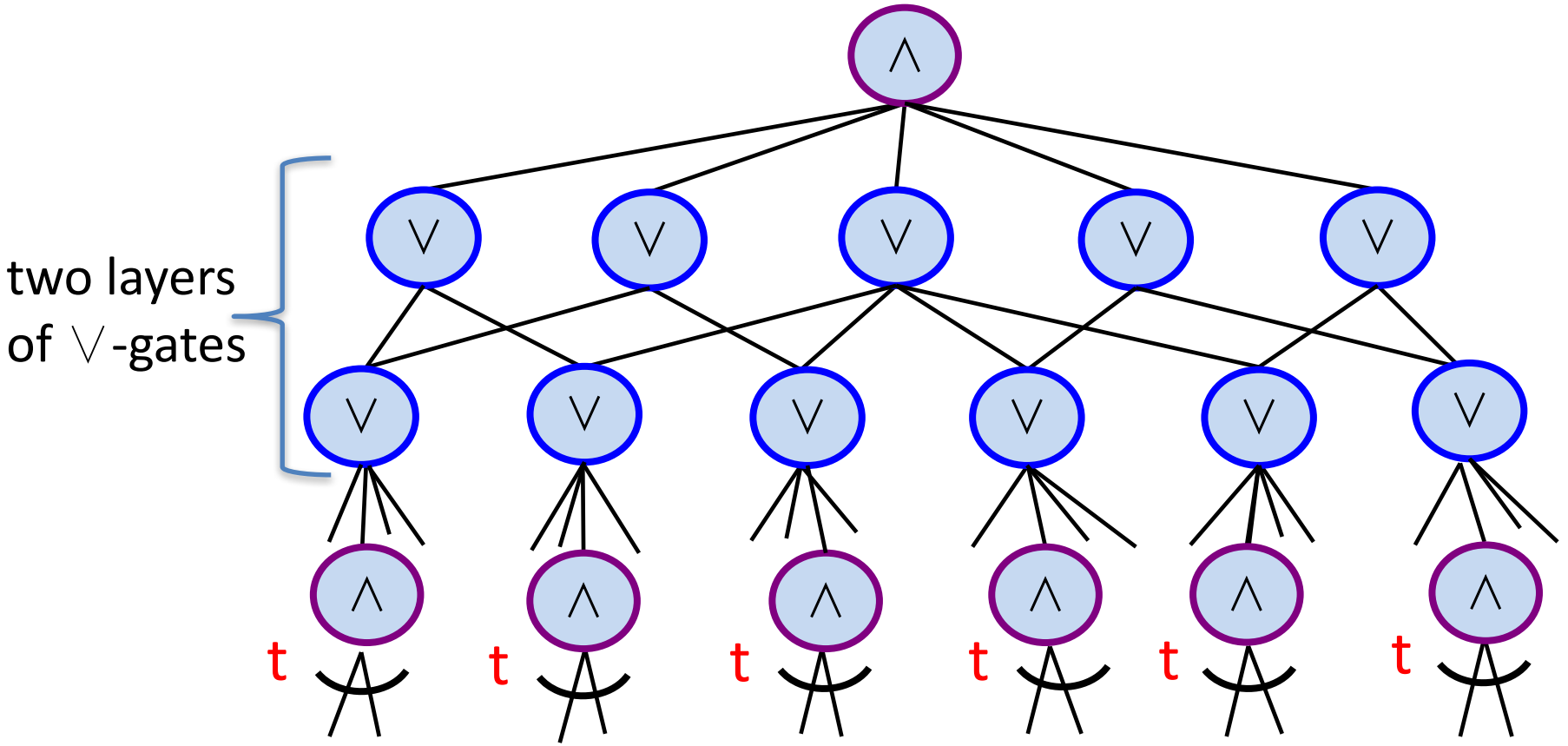
Depth Reduction

Succeeds ***almost surely*** provided

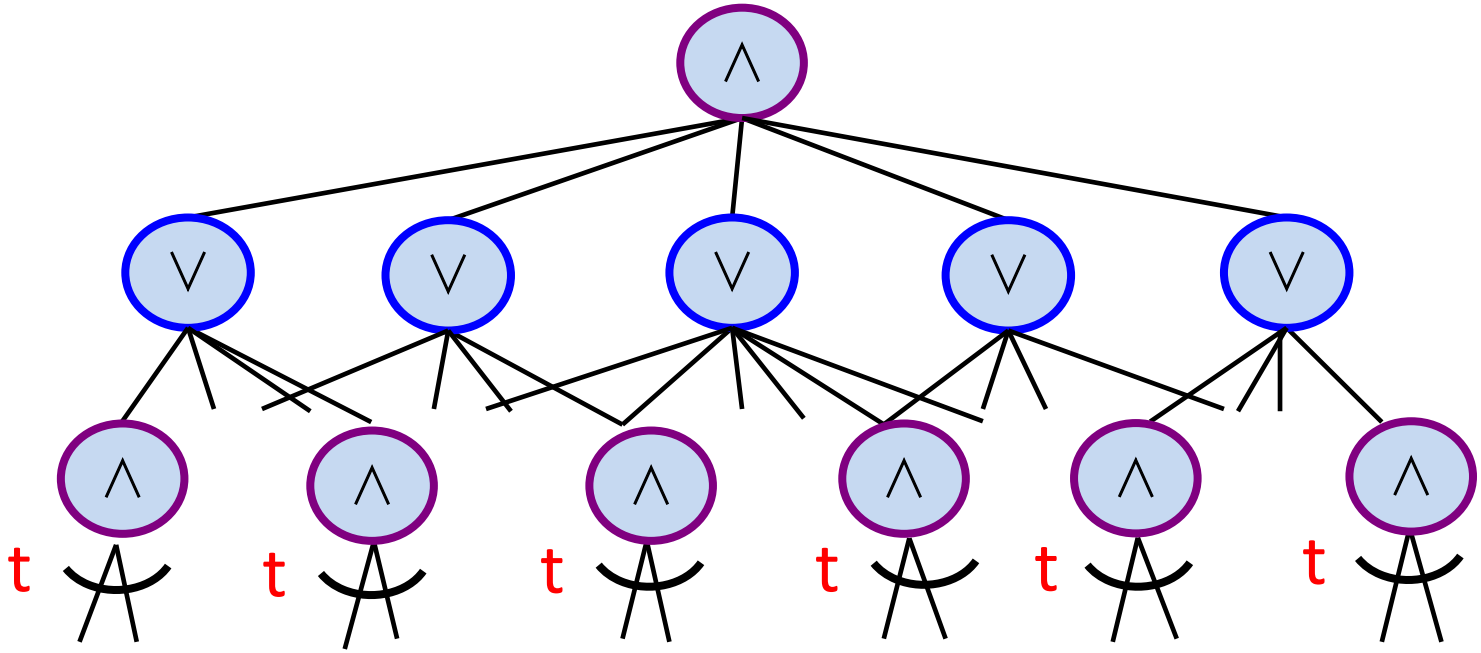
t = O(log(circuit size))



Depth Reduction



Depth Reduction



PARITY Lower Bound

Theorem [Hastad '86]

Depth d+1 **circuits** for $PARITY_n$ have size $\exp(\Omega(n^{1/d}))$

Matching Upper Bound

$PARITY_n$ has depth d+1 **circuits** of size $\exp(O(n^{1/d}))$

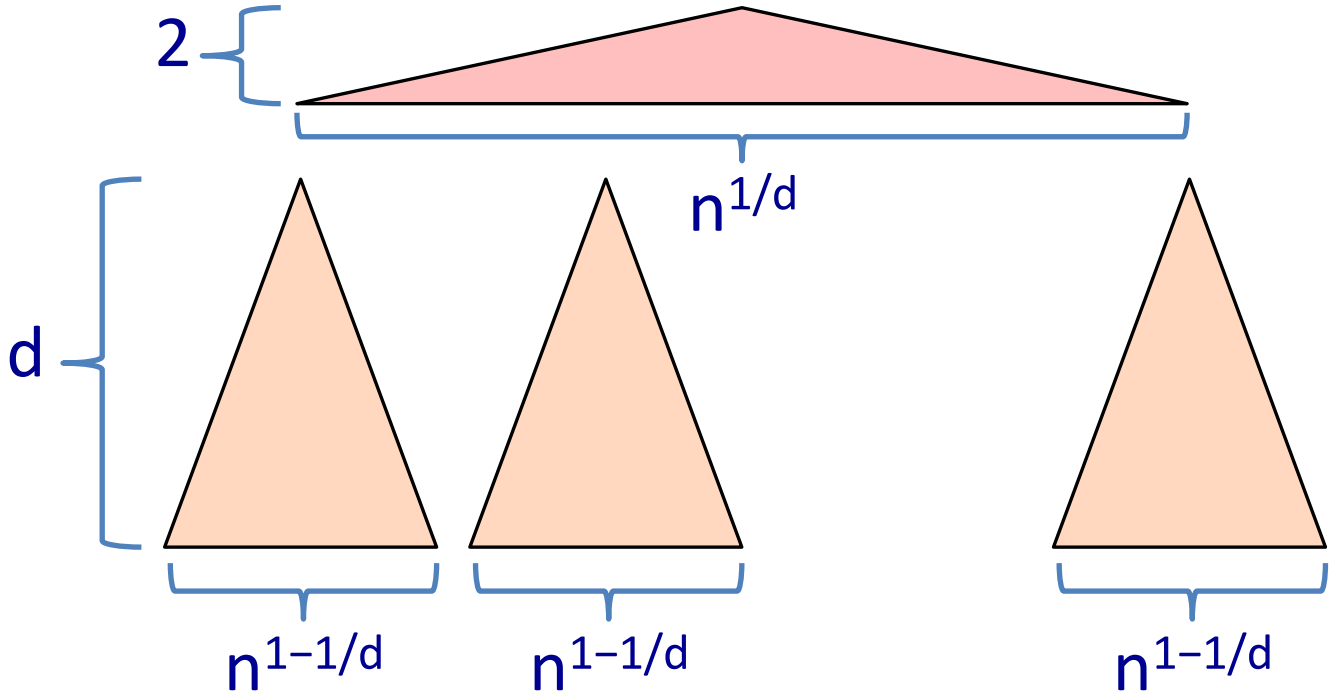
Theorem [Hastad '86]

Depth d+1 **circuits** for $PARITY_n$ have size $\exp(\Omega(n^{1/d}))$

Matching Upper Bound

$PARITY_n$ has depth $d+1$ **circuits** of size $\exp(O(n^{1/d}))$

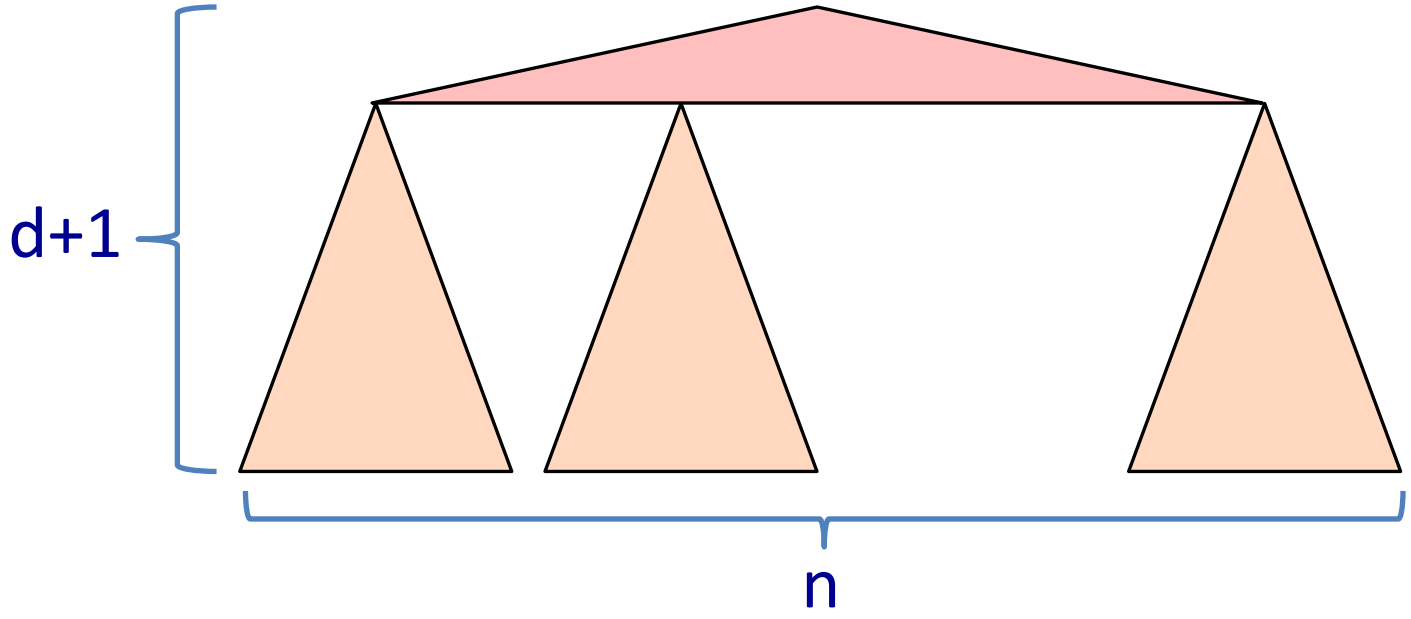
- depth 2 circuits of size $O(2^n)$ (brute-force CNF/DNF)
- for $d+1 \geq 3$, divide and conquer:



Matching Upper Bound

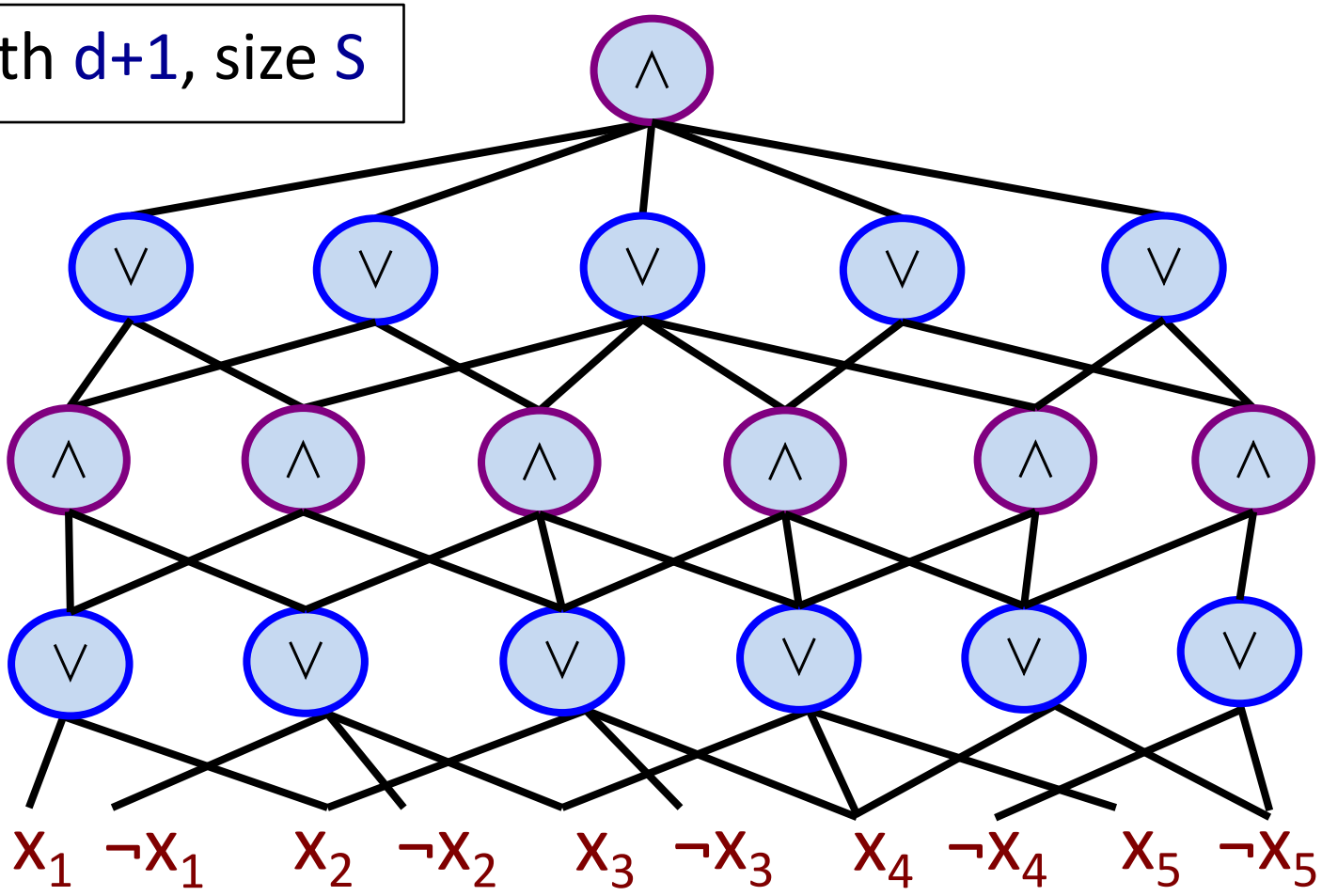
$PARITY_n$ has depth $d+1$ **circuits** of size $\exp(O(n^{1/d}))$

- depth 2 circuits of size $O(2^n)$ (brute-force CNF/DNF)
- for $d+1 \geq 3$, divide and conquer:

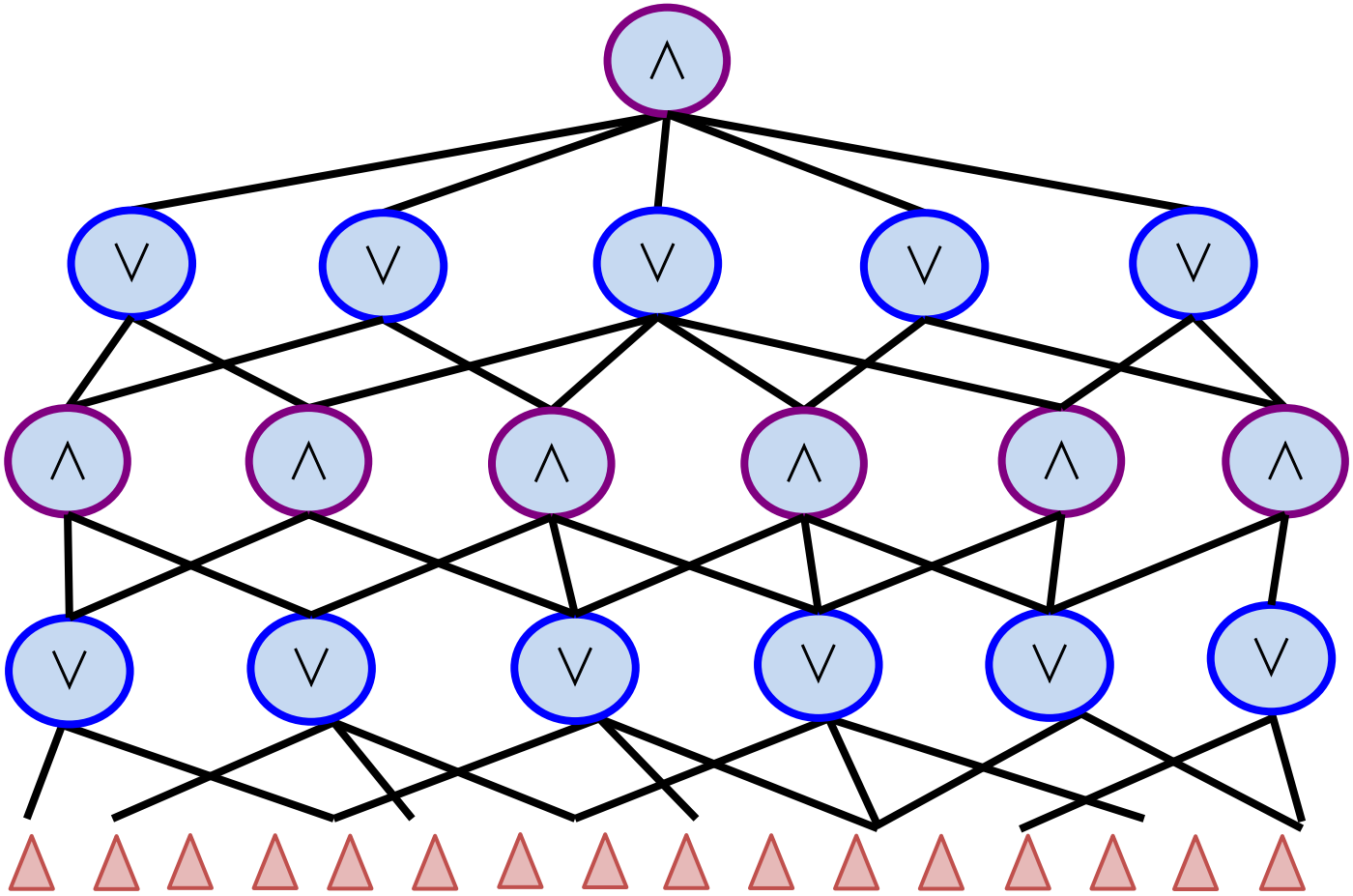


PARITY Lower Bound

depth d+1, size S

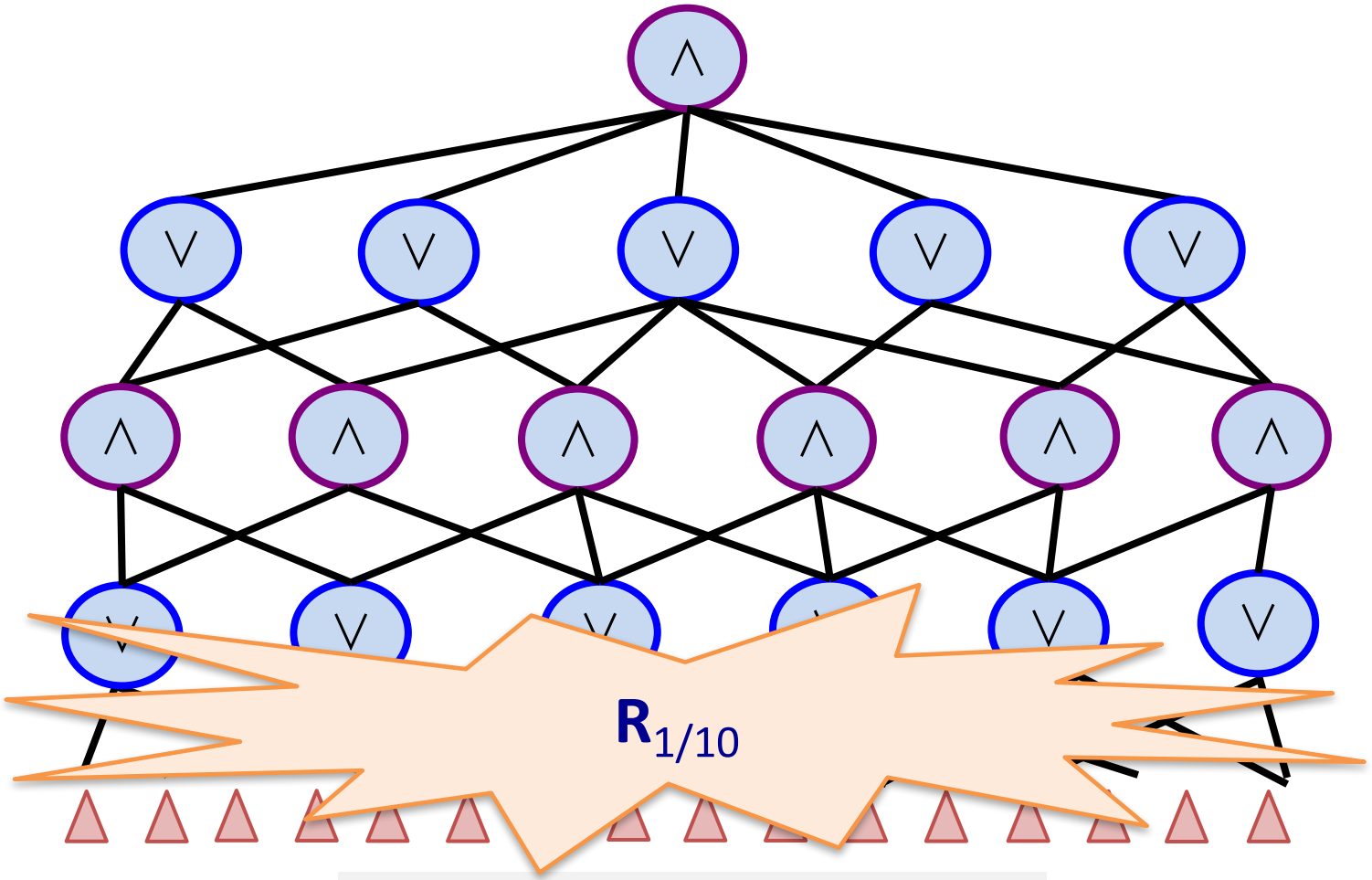


PARITY Lower Bound



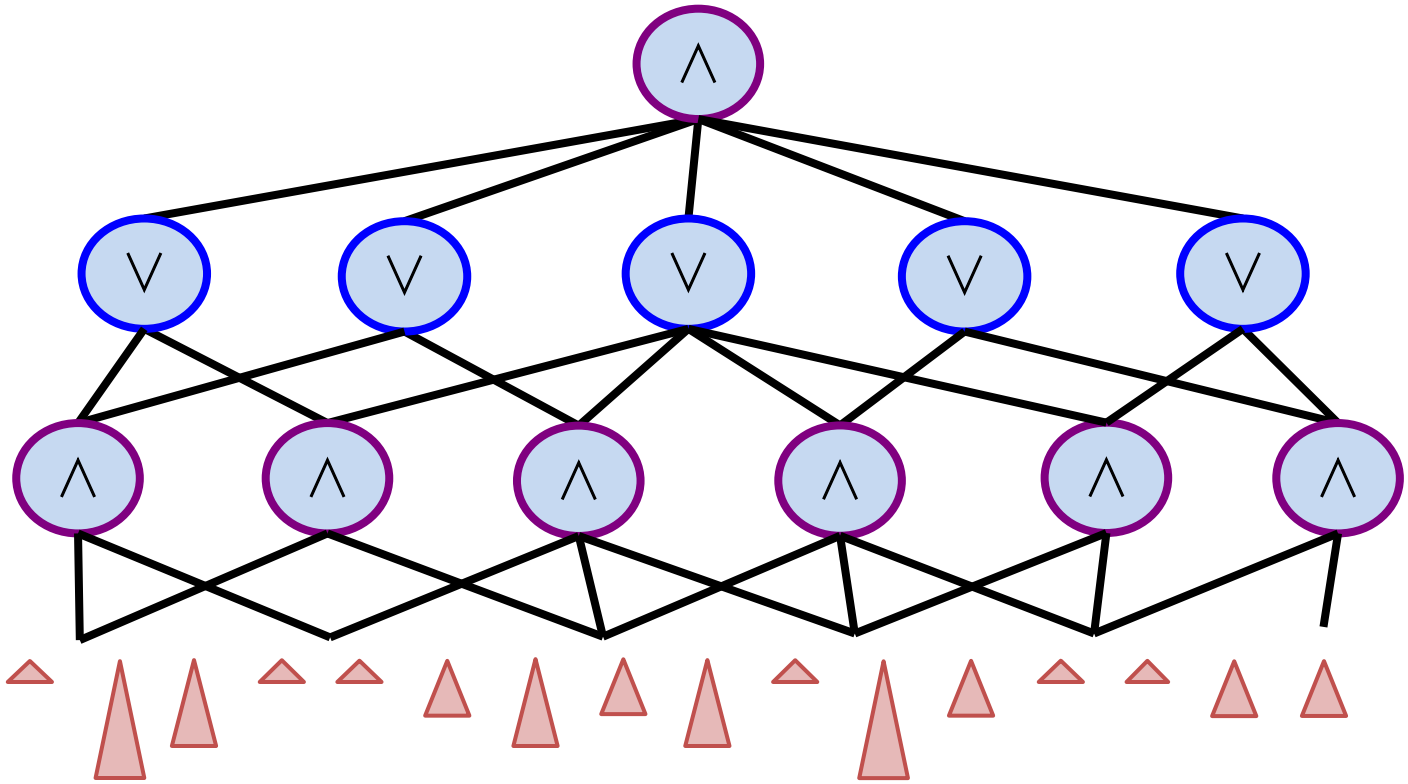
depth-1 decision trees

PARITY Lower Bound



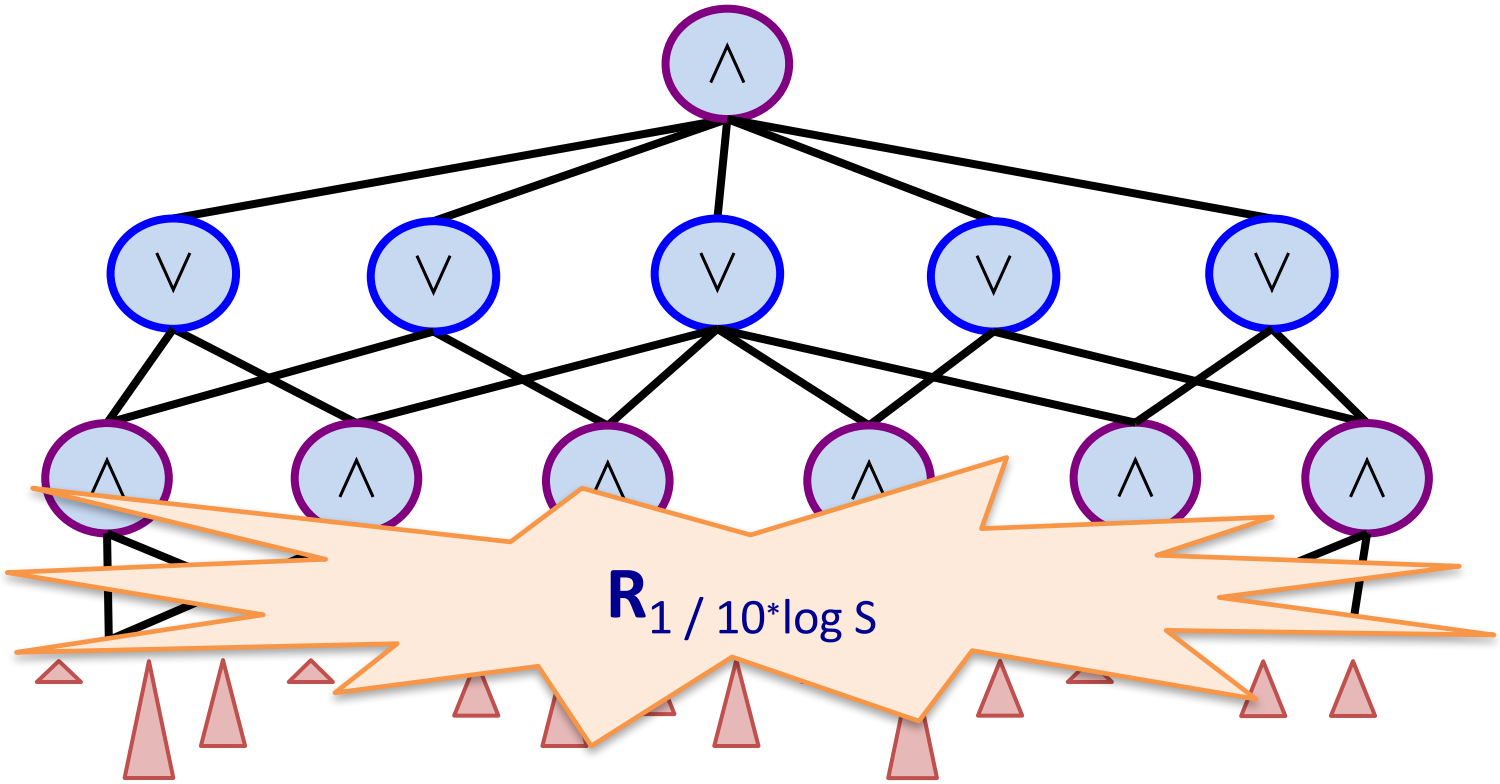
depth-1 decision trees

PARITY Lower Bound



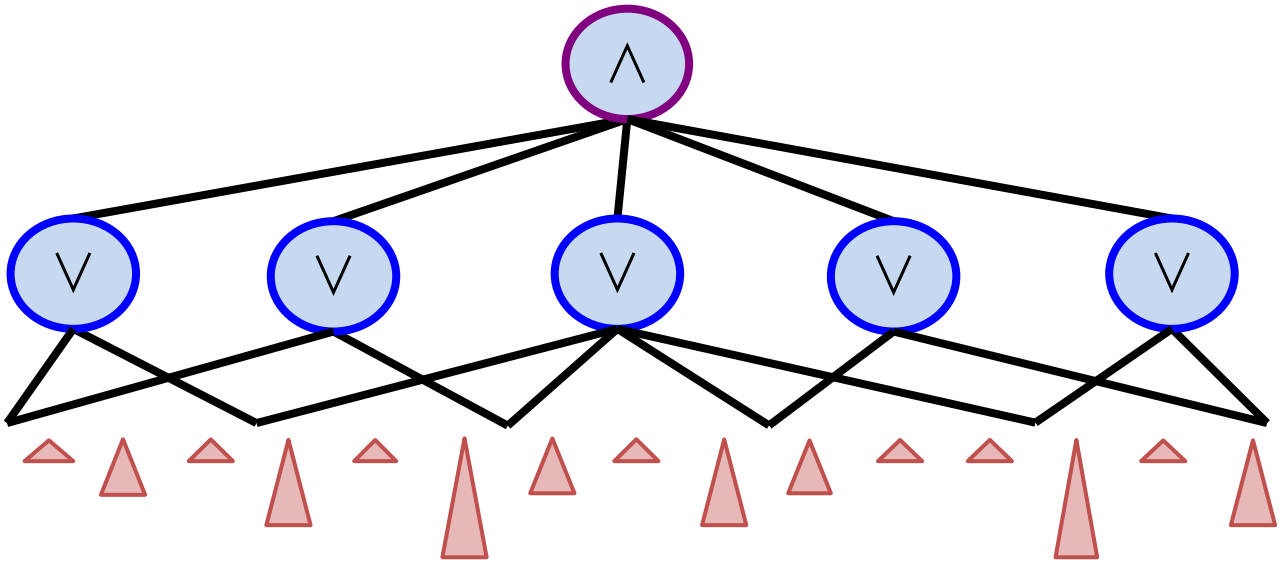
depth O(log S) decision trees (w.h.p.)

PARITY Lower Bound



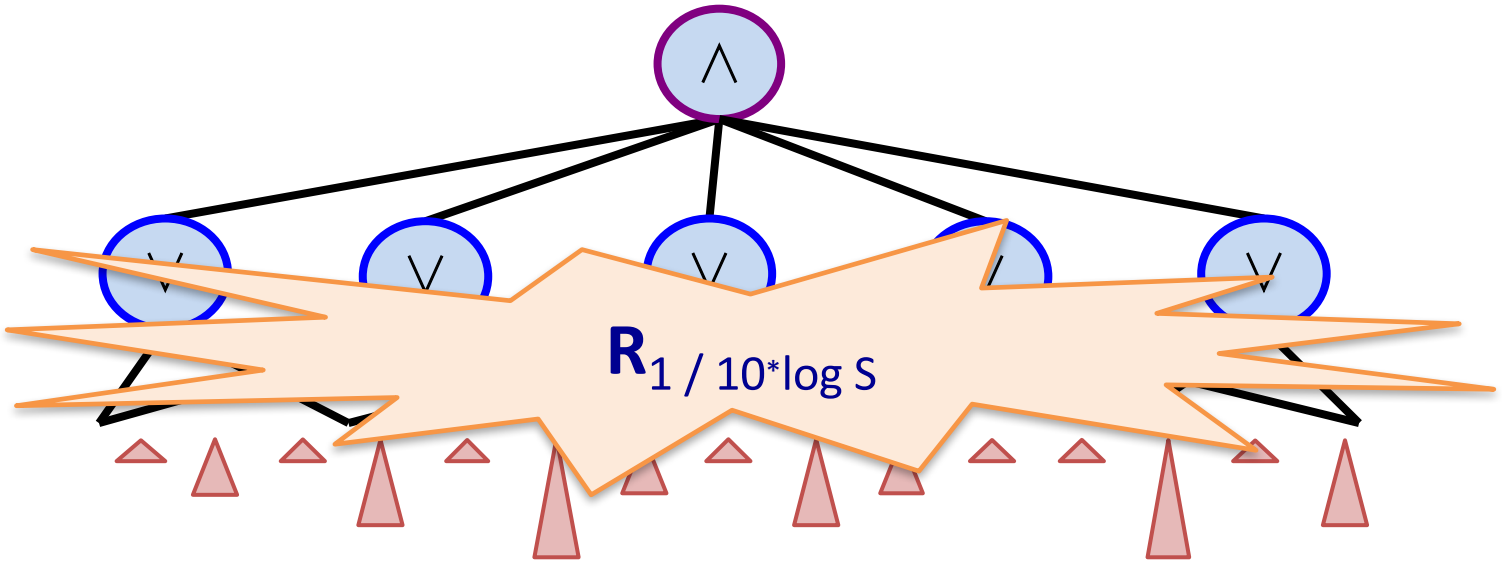
depth O(log S) decision trees (w.h.p.)

PARITY Lower Bound



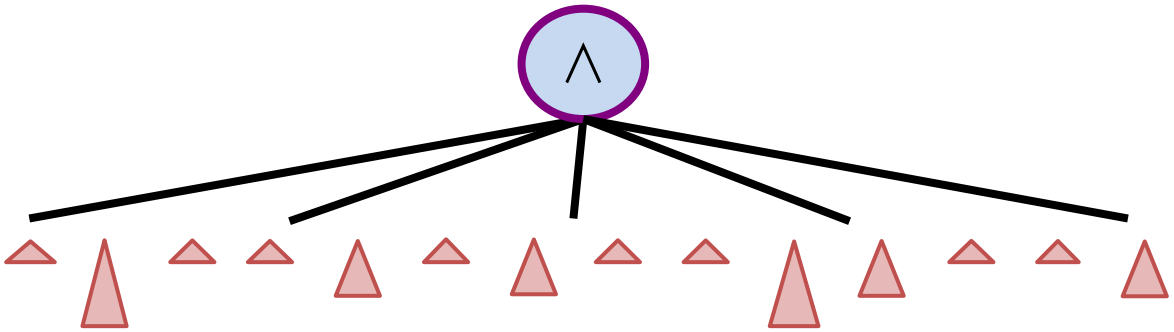
depth O(log S) decision trees (w.h.p.)

PARITY Lower Bound



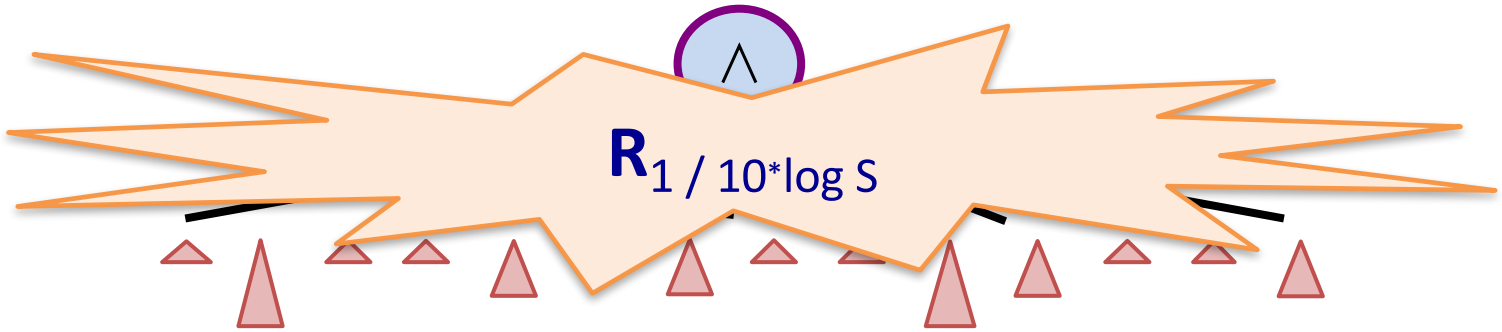
depth O(log S) decision trees (w.h.p.)

PARITY Lower Bound



depth O(log S) decision trees (w.h.p.)

PARITY Lower Bound



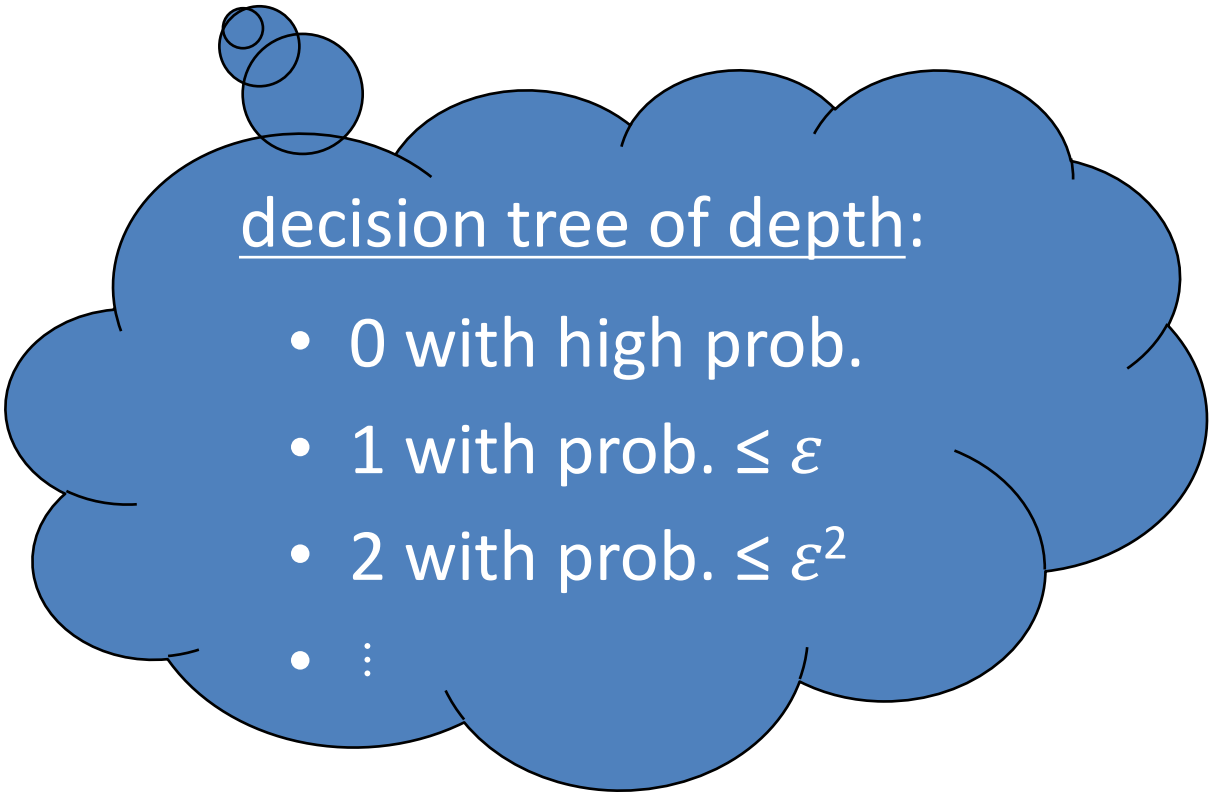
depth O(log S) decision trees (w.h.p.)

PARITY Lower Bound

constant function (w.h.p.)

PARITY Lower Bound

constant function (w.h.p.)



PARITY Lower Bound

- Started with AC^0 circuit of depth $d+1$ and size S
- Applied a sequence of restrictions

$$\mathbf{R}_{1/10}, \underbrace{\mathbf{R}_{1/(10^*\log S)}, \mathbf{R}_{1/(10^*\log S)}, \ldots, \mathbf{R}_{1/(10^*\log S)}}_{d \text{ times}}$$

  Combined restriction: $\mathbf{R}_{1/O(\log S)^d}$

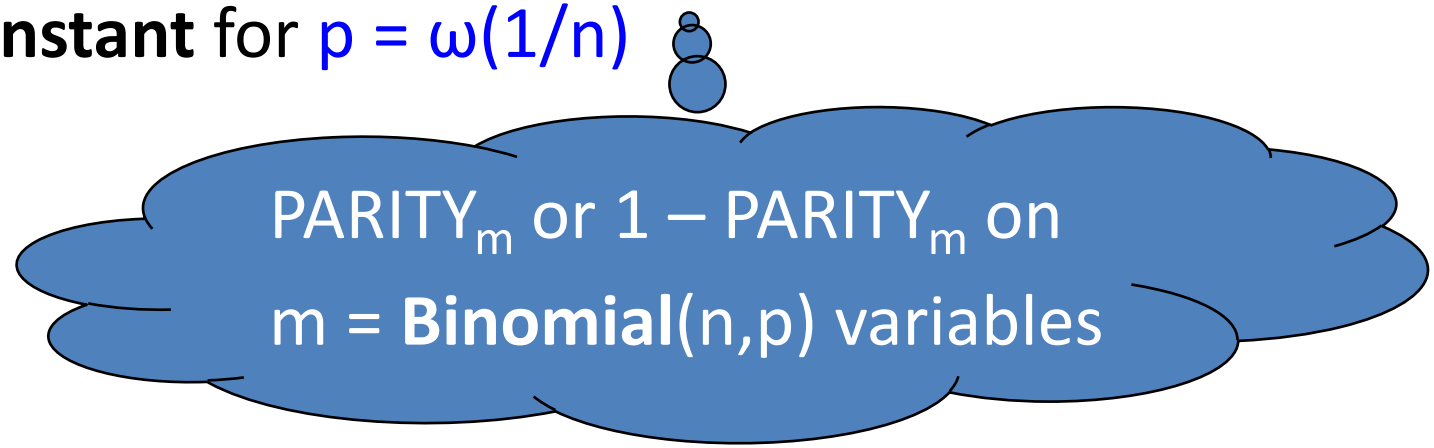
- Circuit reduces to a **constant** (0 or 1) with high prob.

PARITY Lower Bound

- (AC^0 circuit of depth $d+1$ and size S) $\upharpoonright$ $\mathbf{R}_{1/O(\log S)^d}$ is almost surely **constant**
- On the other hand, $PARITY_n \upharpoonright \mathbf{R}_p$ is almost surely **non-constant** for $p = \omega(1/n)$

PARITY Lower Bound

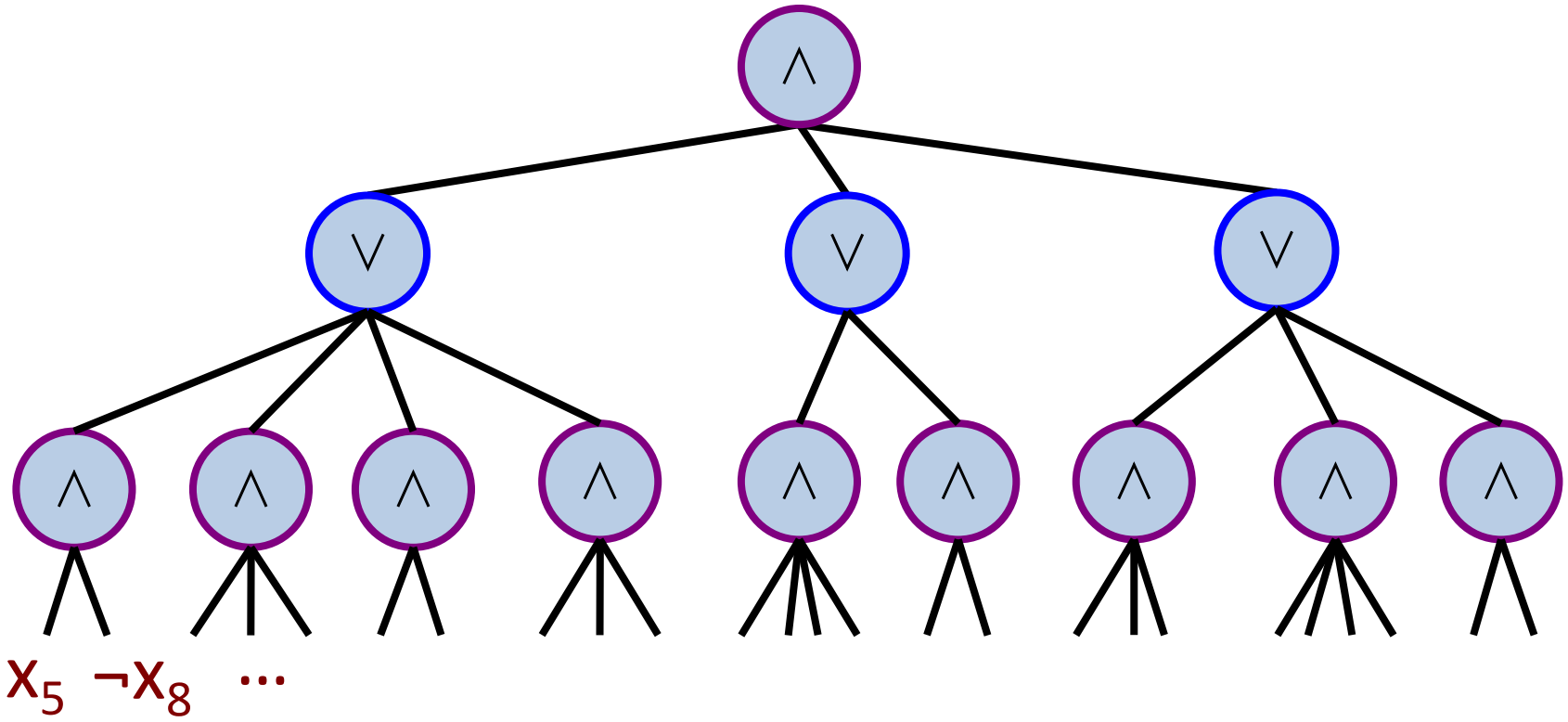
- (AC^0 circuit of depth $d+1$ and size S) $\restriction$ $\mathbf{R}_{1/O(\log S)^d}$ is almost surely **constant**
- On the other hand, $PARITY_n \restriction \mathbf{R}_p$ is almost surely **non-constant** for $p = \omega(1/n)$



PARITY Lower Bound

- (AC^0 circuit of depth $d+1$ and size S) $\not\upharpoonright$ $\mathbf{R}_{1/O(\log S)^d}$ is almost surely **constant**
- On the other hand, $PARITY_n \not\upharpoonright \mathbf{R}_p$ is almost surely **non-constant** for $p = \omega(1/n)$
- Therefore, depth $d+1$ circuits for $PARITY_n$ require size $\exp(n^{1/d})$

Recall: AC^0 Formulas

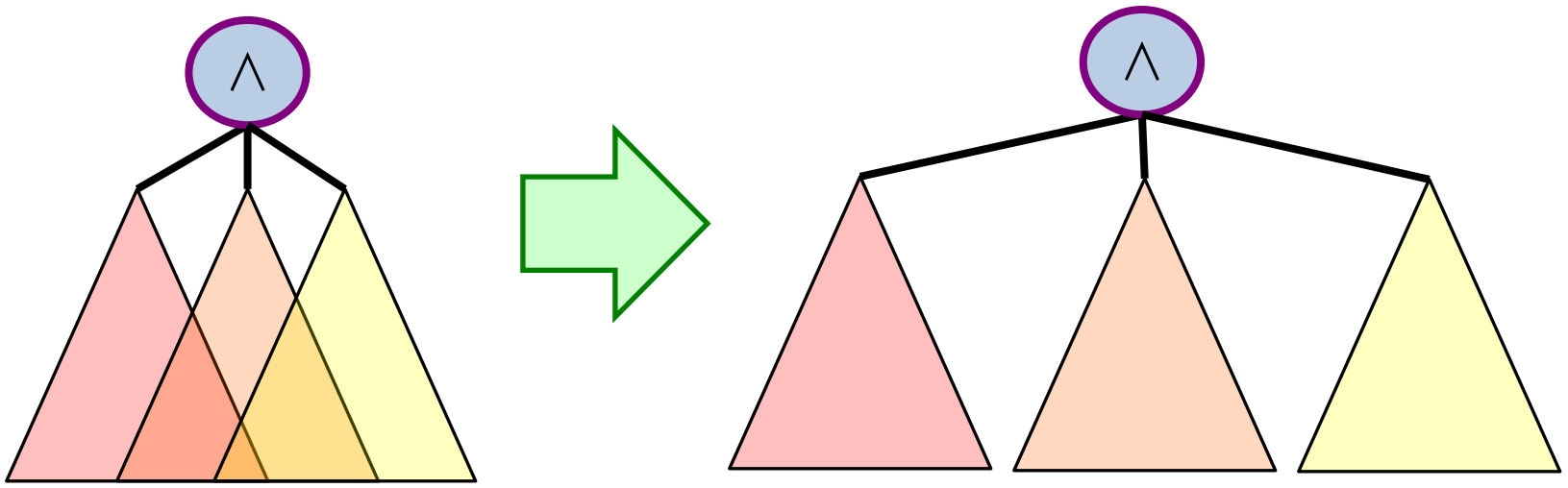


Upper Bound

PARITY has depth d+1 **circuits** of size $\exp(O(n^{1/d}))$

Upper Bound

PARITY has depth d+1 **circuits** of size $\exp(O(n^{1/d}))$
and depth d+1 **formulas** of size $\exp(O(dn^{1/d}))$



Upper Bound

PARITY has depth d+1 **circuits** of size $\exp(O(n^{1/d}))$
and depth d+1 **formulas** of size $\exp(O(dn^{1/d}))$

Theorem [Hastad '86]

Depth d+1 **circuits** for PARITY have size $\exp(\Omega(n^{1/d}))$

Upper Bound

PARITY has depth d+1 **circuits** of size $\exp(O(n^{1/d}))$
and depth d+1 **formulas** of size $\exp(O(dn^{1/d}))$

Theorem [Hastad '86]

Depth d+1 **circuits** for PARITY have size $\exp(\Omega(n^{1/d}))$

Theorem [R.'15]

Depth d+1 **formulas** for PAR. have size $\exp(\Omega(dn^{1/d}))$

Proof of the Switching Lemma

Canonical Decision Tree

- For a DNF formula F and restriction R, we define the **canonical decision tree** of F↾R, denoted CanDT(F↾R), as follows:

1. If F↾R is identically 0 or 1, then CanDT(F↾R) outputs 0 or 1 without making any queries.
2. Otherwise, let C be the first term (conjunction of literals) in F such that C↾R is not fixed to 0 or 1.

   Query all free variables of C↾R. Then proceed as CanDT(F↾R') where R' is the extension of R that includes answers to the queried variables.

- Fix a k-DNF F and $\ell \geq 1$

Switching Lemma:

$$\Pr[\ \mathrm{depth}(\mathrm{CanDT}(F \restriction \mathbf{R}_p)) \geq \ell\ ] = O(pk)^{\ell}$$

- Fix a k-DNF F and $\ell \geq 1$

Switching Lemma:

$$\Pr[\ \text{depth}(\text{CanDT}(F \restriction \mathbf{R}_p)) \geq \ell\ ] = O(pk)^{\ell}$$

Obs: $\text{depth}(\text{CanDT}(F \restriction \mathbf{R}_p)) < \ell$

Implies $\text{DT}_{\text{depth}}(F \restriction \mathbf{R}_p) < \ell$

- Fix a k-DNF F and $\ell \geq 1$
- BAD := { restrictions R | depth(CanDT(F $\restriction$ R)) $\geq \ell$ }

Switching Lemma:

$$\Pr[\ \text{depth}(\text{CanDT}(F \restriction \mathbf{R}_p)) \geq \ell\ ] = O(pk)^{\ell}$$

- Fix a k-DNF F and $\ell \geq 1$
- BAD := { restrictions R | depth(CanDT(F $\restriction$ R)) $\geq \ell$ }
- Goal. Pr[$\mathbf{R}_p \in$ BAD] = $O(pk)^{\ell}$

Switching Lemma:

$$\Pr[\ \text{depth}(\text{CanDT}(F \restriction \mathbf{R}_p)) \geq \ell\ ] = O(pk)^{\ell}$$

- Fix a k-DNF F and $\ell \geq 1$
- BAD := { restrictions R | depth(CanDT(F $\restriction$ R)) $\geq \ell$ }
- Goal. Pr[$\mathbf{R}_p \in$ BAD] = $O(pk)^{\ell}$

Key idea. We associate each R $\in$ BAD with a restriction R* such that

- Fix a k-DNF F and $\ell \geq 1$
- BAD := { restrictions R | depth(CanDT(F ↾ R)) ≥ ℓ }
- Goal. Pr[$\mathbf{R}_p \in$ BAD] = $O(pk)^{\ell}$

Key idea. We associate each R ∈ BAD with a restriction R* such that

① |Stars(R*)| = |Stars(R)| − ℓ

R ⋆ 1 ⋆ ⋆ 1 0 ⋆ 1 ⋆ 1 0 0 ⋆ ⋆ 0 ⋆ 0 ⋆ ⋆ ⋆ 0 ⋆ 0

R* ⋆ 1 ⋆ 0 1 0 ⋆ 1 ⋆ 1 0 0 1 ⋆ 0 ⋆ 0 ⋆ 0 ⋆ 0 ⋆ 0

(ℓ = 3)

- Fix a k-DNF F and $\ell \geq 1$
- BAD := { restrictions R | depth(CanDT(F ↾ R)) ≥ ℓ }
- Goal. Pr[$\mathbf{R}_p \in$ BAD] = $O(pk)^{\ell}$

Key idea. We associate each R ∈ BAD with a restriction R* such that

① |Stars(R*)| = |Stars(R)| − ℓ

in particular, Pr[$\mathbf{R}_p$ = R*] / Pr[$\mathbf{R}_p$ = R] = $((1-p)/2p)^{\ell}$

- Fix a k-DNF F and $\ell \geq 1$
- BAD := { restrictions R | depth(CanDT($F \restriction R$)) $\geq \ell$ }
- Goal. Pr[$\mathbf{R}_p \in$ BAD] = $O(pk)^\ell$

Key idea. We associate each $R \in$ BAD with a restriction R* such that

① $|\text{Stars}(R^*)| = |\text{Stars}(R)| - \ell$

in particular, $\Pr[\mathbf{R}_p = R^*] / \Pr[\mathbf{R}_p = R] = ((1-p)/2p)^\ell$

for any restriction ρ with s stars,

$\Pr[\mathbf{R}_p = \rho] = p^s (1-p)^{n-s}$

- Fix a k-DNF F and $\ell \geq 1$
- BAD := { restrictions R | depth(CanDT(F $\restriction$ R)) $\geq \ell$ }
- Goal. Pr[$\mathbf{R}_p \in$ BAD] = $O(pk)^{\ell}$

Key idea. We associate each R $\in$ BAD with a restriction R* such that

① |Stars(R*)| = |Stars(R)| − ℓ

② the map R $\mapsto$ R* is $(4k)^{\ell}$-to-1

- Fix a k-DNF F and $\ell \geq 1$
- BAD := { restrictions R | depth(CanDT(F $\restriction$ R)) $\geq \ell$ }
- Goal. Pr[$\mathbf{R}_p \in$ BAD] = $O(pk)^\ell$

Key idea. We associate each R $\in$ BAD with a restriction R* such that

① |Stars(R*)| = |Stars(R)| – ℓ

② the map R $\mapsto$ R* is $(4k)^\ell$-to-1

any restriction ρ equals R* for at most $(4k)^\ell$ distinct R $\in$ BAD

Key idea. We associate each $R \in \text{BAD}$ with a restriction R^* such that

① $|\text{Stars}(R^*)| = |\text{Stars}(R)| - \ell$

② the map $R \mapsto R^*$ is $(4k)^{\ell}$-to-1

Key idea. We associate each $R \in \text{BAD}$ with a restriction R^* such that

① $|\text{Stars}(R^*)| = |\text{Stars}(R)| - \ell$

② the map $R \mapsto R^*$ is $(4k)^{\ell}$-to-1

$$\Pr[\, \mathbf{R}_p \in \text{BAD} \,] = \sum_{R \in \text{BAD}} \Pr[\, \mathbf{R}_p = R \,]$$

Key idea. We associate each $R \in BAD$ with a restriction R^* such that

① $|Stars(R^*)| = |Stars(R)| - \ell$

② the map $R \mapsto R^*$ is $(4k)^\ell$-to-1

$$\Pr[\, \mathbf{R}_p \in BAD \,]$$

$$= \sum_{R \in BAD} \Pr[\, \mathbf{R}_p = R \,]$$

$$= \sum_{R \in BAD} (2p/(1-p))^\ell \Pr[\, \mathbf{R}_p = R^* \,]$$

$$\Pr[\, \mathbf{R}_p = R \,] = (2p/(1-p))^\ell \Pr[\, \mathbf{R}_p = R^* \,]$$

Key idea. We associate each $R \in \text{BAD}$ with a restriction R^* such that

① $|\text{Stars}(R^*)| = |\text{Stars}(R)| - \ell$

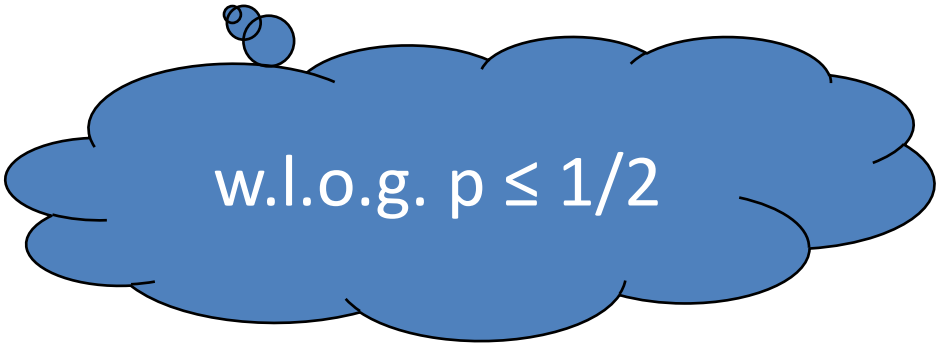
② the map $R \mapsto R^*$ is $(4k)^\ell$-to-1

$$\Pr[\, \mathbf{R}_p \in \text{BAD} \,]$$

$$= \sum_{R \in \text{BAD}} \Pr[\, \mathbf{R}_p = R \,]$$

$$= \sum_{R \in \text{BAD}} (2p/(1-p))^\ell \Pr[\, \mathbf{R}_p = R^* \,]$$

$$\leq (4p)^\ell \sum_{R \in \text{BAD}} \Pr[\, \mathbf{R}_p = R^* \,]$$



Key idea. We associate each $R \in \text{BAD}$ with a restriction R^* such that

① $|\text{Stars}(R^*)| = |\text{Stars}(R)| - \ell$

② the map $R \mapsto R^*$ is $(4k)^\ell$-to-1

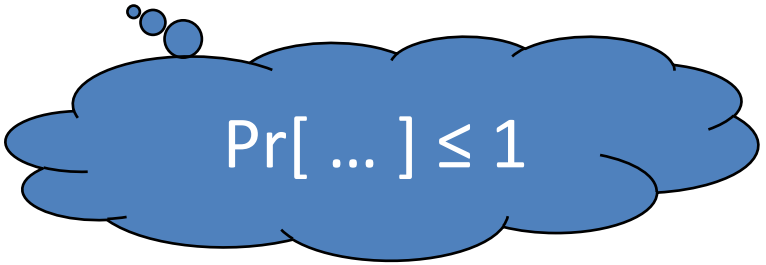
$$\begin{aligned}
&\Pr[\, \mathbf{R}_p \in \text{BAD} \,] \\
&\quad = \textstyle\sum_{R \in \text{BAD}} \Pr[\, \mathbf{R}_p = R \,] \\
&\quad = \textstyle\sum_{R \in \text{BAD}} (2p/(1-p))^\ell \Pr[\, \mathbf{R}_p = R^* \,] \\
&\quad \le (4p)^\ell \textstyle\sum_{R \in \text{BAD}} \Pr[\, \mathbf{R}_p = R^* \,] \\
&\quad \le (4p)^\ell \, (4k)^\ell \Pr[\, \mathbf{R}_p \in \{R^* \mid R \in \text{BAD}\} \,]
\end{aligned}$$

Key idea. We associate each $R \in \text{BAD}$ with a restriction R^* such that

① $|\text{Stars}(R^*)| = |\text{Stars}(R)| - \ell$

② the map $R \mapsto R^*$ is $(4k)^\ell$-to-1

$$\begin{aligned}
&\Pr[\, \mathbf{R}_p \in \text{BAD} \,] \\
&\quad = \textstyle\sum_{R \in \text{BAD}} \Pr[\, \mathbf{R}_p = R \,] \\
&\quad = \textstyle\sum_{R \in \text{BAD}} (2p/(1-p))^\ell \Pr[\, \mathbf{R}_p = R^* \,] \\
&\quad \le (4p)^\ell \textstyle\sum_{R \in \text{BAD}} \Pr[\, \mathbf{R}_p = R^* \,] \\
&\quad \le (4p)^\ell (4k)^\ell \Pr[\, \mathbf{R}_p \in \{R^* \mid R \in \text{BAD}\} \,]
\end{aligned}$$



Key idea. We associate each $R \in \text{BAD}$ with a restriction R^* such that

① $|\text{Stars}(R^*)| = |\text{Stars}(R)| - \ell$

② the map $R \mapsto R^*$ is $(4k)^\ell$-to-1

$$\begin{aligned}
&\Pr[\, \mathbf{R}_p \in \text{BAD} \,] \\
&\quad = \textstyle\sum_{R \in \text{BAD}} \Pr[\, \mathbf{R}_p = R \,] \\
&\quad = \textstyle\sum_{R \in \text{BAD}} (2p/(1-p))^\ell \Pr[\, \mathbf{R}_p = R^* \,] \\
&\quad \le (4p)^\ell \textstyle\sum_{R \in \text{BAD}} \Pr[\, \mathbf{R}_p = R^* \,] \\
&\quad \le (4p)^\ell (4k)^\ell \Pr[\, \mathbf{R}_p \in \{R^* \mid R \in \text{BAD}\} \,] \\
&\quad \le (16pk)^\ell
\end{aligned}$$

Q.E.D.

Switching Lemma:

$$\Pr[\ \text{depth}(\text{CanDT}(F \restriction \mathbf{R}_p)) \geq \ell\ ] = O(pk)^{\ell}$$

$$\begin{aligned}
&\Pr[\ \mathbf{R}_p \in \text{BAD}\ ] \\
&\quad = \textstyle\sum_{R \in \text{BAD}} \Pr[\ \mathbf{R}_p = R\ ] \\
&\quad = \textstyle\sum_{R \in \text{BAD}} (2p/(1-p))^{\ell} \Pr[\ \mathbf{R}_p = R^*\ ] \\
&\quad \leq (4p)^{\ell} \textstyle\sum_{R \in \text{BAD}} \Pr[\ \mathbf{R}_p = R^*\ ] \\
&\quad \leq (4p)^{\ell} (4k)^{\ell} \Pr[\ \mathbf{R}_p \in \{R^* \mid R \in \text{BAD}\}\ ] \\
&\quad \leq (16pk)^{\ell}
\end{aligned}$$

Q.E.D.

Switching Lemma:

$$\Pr[\ \text{depth}(\text{CanDT}(F \restriction \mathbf{R}_p)) \geq \ell\ ] = O(pk)^{\ell}$$

$$\Pr[\ \mathbf{R}_p \in \text{BAD}\ ]$$

$$= \sum_{R \in \text{BAD}} \Pr[\ \mathbf{R}_p = R\ ]$$

$$= \sum_{R \in \text{BAD}} (2p/(1-p))^{\ell} \Pr[\ \mathbf{R}_{1-p} = R^*\ ]$$

$$\leq (4p)^{\ell} \Pr[\ \mathbf{R}_{1-p} \in \{R^* \mid R \in \text{BAD}\}\ ]$$

$$\leq (16pk)^{\ell}$$

more careful analysis gives $(5pk)^{\ell}$

Q.E.D.

Key idea. We associate each $R \in \text{BAD}$ with a restriction R^* such that

① $|\text{Stars}(R^*)| = |\text{Stars}(R)| - \ell$

② the map $R \mapsto R^*$ is $(4k)^{\ell}$-to-1

Key idea. We associate each $R \in$ BAD with a pair (R*,Code(R)) such that

① $|\text{Stars}(R^*)| = |\text{Stars}(R)| - \ell$

② the map $R \mapsto R^*$ is $(4k)^{\ell}$-to-1

③

④

Key idea. We associate each $R \in \mathrm{BAD}$ with a pair $(R^*, \mathrm{Code}(R))$ such that

① $|\mathrm{Stars}(R^*)| = |\mathrm{Stars}(R)| - \ell$

② the map $R \mapsto R^*$ is $(4k)^\ell$-to-1

③ $\mathrm{Code}(R) \in (\{0,1\}^2 \times [k])^\ell$

④

Key idea. We associate each $R \in$ BAD with a pair (R*,Code(R)) such that

① $|\text{Stars}(R^*)| = |\text{Stars}(R)| - \ell$

② the map $R \mapsto R^*$ is $(4k)^\ell$-to-1

③ $\text{Code}(R) \in (\{0,1\}^2 \times [k])^\ell$

④

in particular, Code(R) has $(4k)^\ell$ possible values

Key idea. We associate each $R \in \mathrm{BAD}$ with a pair $(R^*, \mathrm{Code}(R))$ such that

① $|\mathrm{Stars}(R^*)| = |\mathrm{Stars}(R)| - \ell$

② the map $R \mapsto R^*$ is $(4k)^\ell$-to-1

③ $\mathrm{Code}(R) \in (\{0,1\}^2 \times [k])^\ell$

④ the map $R \mapsto (R^*, \mathrm{Code}(R))$ is 1-to-1

Key idea. We associate each $R \in$ BAD with a pair (R*,Code(R)) such that

① $|\text{Stars}(R^*)| = |\text{Stars}(R)| - \ell$

② the map $R \mapsto R^*$ is $(4k)^\ell$-to-1

③ $\text{Code}(R) \in (\{0,1\}^2 \times [k])^\ell$

④ the map $R \mapsto (R^*, \text{Code}(R))$ is 1-to-1

③ & ④ imply ②

Key idea. We associate each $R \in \mathrm{BAD}$ with a pair $(R^*, \mathrm{Code}(R))$ such that

① $|\mathrm{Stars}(R^*)| = |\mathrm{Stars}(R)| - \ell$

② the map $R \mapsto R^*$ is $(4k)^\ell$-to-1

③ $\mathrm{Code}(R) \in (\{0,1\}^2 \times [k])^\ell$

④ the map $R \mapsto (R^*, \mathrm{Code}(R))$ is 1-to-1

intuitively, Code(R) is a "recipe" for inverting $R \mapsto (R^*, \mathrm{Code}(R))$ given knowledge of R^*

$R \mapsto (R^*, \mathrm{Code}(R))$

k = 3, $\ell = 4$

$R \mapsto (R^*, \mathrm{Code}(R))$

$$F = x_1 x_2 \neg x_3 \vee \neg x_1 x_3 x_5 \vee x_2 \neg x_4 x_5 \vee x_3 x_4 \neg x_6 \vee x_1 \neg x_4 \neg x_7$$

$k = 3,\ \ell = 4$

$R \mapsto (R^*, \mathrm{Code}(R))$

$$F = x_1\, x_2\, \neg x_3 \vee \neg x_1\, x_3\, x_5 \vee x_2\, \neg x_4\, x_5 \vee x_3\, x_4\, \neg x_6 \vee x_1\, \neg x_4\, \neg x_7$$

$R = \{\, x_1 \mapsto 1,\ x_4 \mapsto 0 \,\}$

$k = 3,\ \ell = 4$

$R \mapsto (R^*, \mathrm{Code}(R))$

$$F\restriction R \quad \overset{1}{x_1}\ x_2\ \neg x_3 \ \vee\ \neg x_1\ x_3\ x_5 \ \overset{0}{\vee}\ x_2\ \neg x_4\ x_5 \ \overset{1}{\vee}\ x_3\ x_4\ \neg x_6 \ \overset{0}{\vee}\ x_1\ \neg x_4\ \neg x_7 \quad \overset{1\ \ 1}{}$$

$R = \{\, x_1 \mapsto 1,\ x_4 \mapsto 0 \,\}$

k = 3, $\ell = 4$

$R \mapsto (R^*, \mathrm{Code}(R))$

1 0 1 0 1 1

$F \restriction R \; x_1 \; x_2 \; \neg x_3 \vee \neg x_1 \; x_3 \; x_5 \vee x_2 \; \neg x_4 \; x_5 \vee x_3 \; \neg x_6 \vee x_1 \; \neg x_4 \; \neg x_7$

$R = \{ x_1 \mapsto 1, x_4 \mapsto 0 \}$

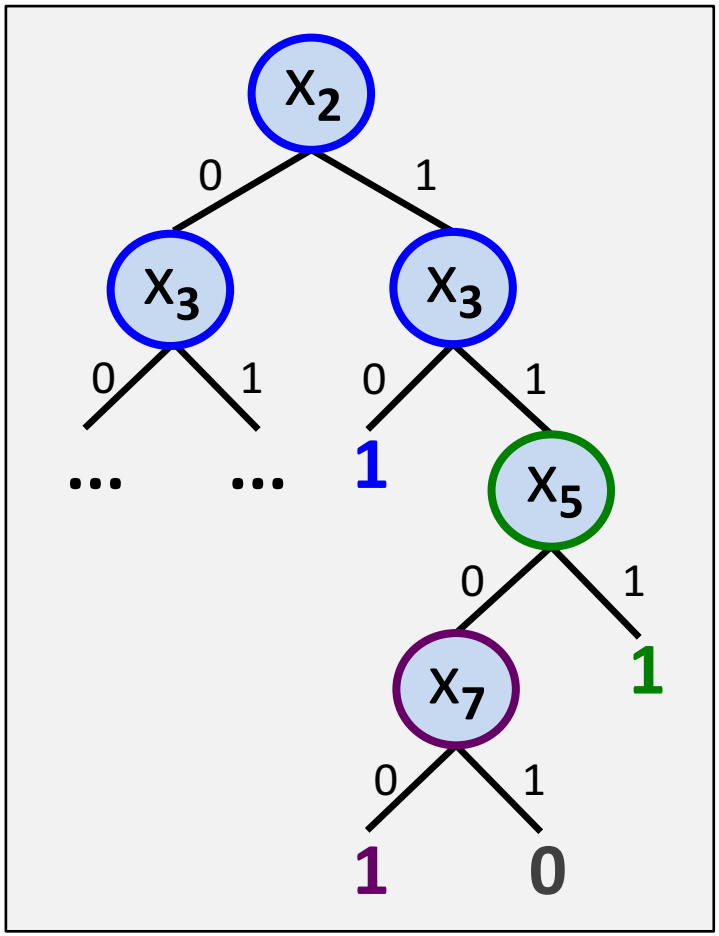
$k = 3,\ \ell = 4$

$R \mapsto (R^*, \mathrm{Code}(R))$

$F \restriction R$ $x_1\ x_2\ \neg x_3 \vee \neg x_1\ x_3\ x_6 \vee x_2\ \neg x_4\ x_5 \vee x_3\ x_5\ \neg x_6 \vee x_1\ \neg x_4\ \neg x_7$

$R = \{ x_1 \mapsto 1, x_4 \mapsto 0 \}$

CanDT($F \restriction R$) =



k = 3, $\ell = 4$

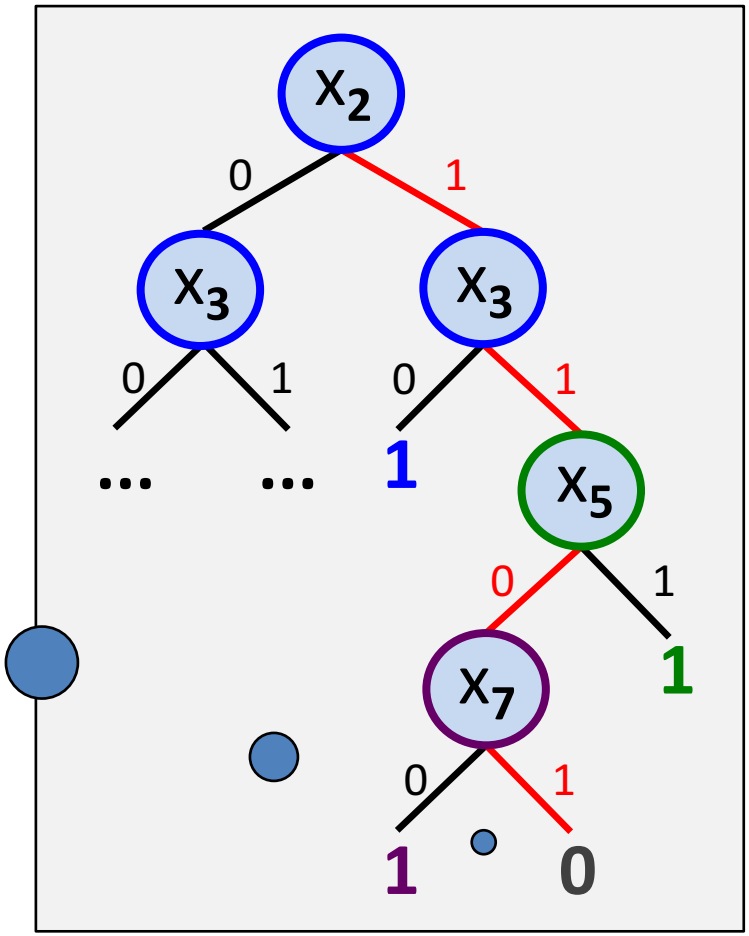
$R \mapsto (R^*, \mathrm{Code}(R))$

$F \restriction R$ $x_1\ x_2\ \neg x_3 \vee \neg x_1\ x_3\ x_6 \vee x_2\ \neg x_4\ x_5 \vee x_3\ \neg x_5\ \neg x_6 \vee x_1\ \neg x_4\ \neg x_7$

=

$R = \{ x_1 \mapsto 1, x_4 \mapsto 0 \}$

$R \in$ BAD, since
$\mathrm{CanDT}(F \restriction R) \geq \ell$



k = 3, $\ell = 4$

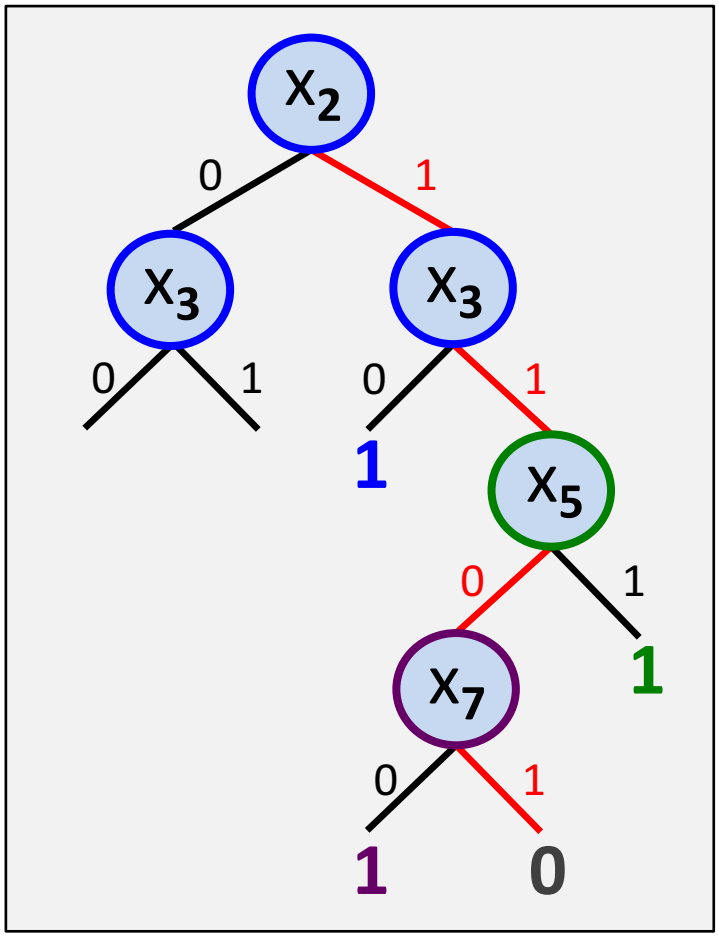
$R \mapsto (R^*, \mathrm{Code}(R))$

$F \upharpoonright R$ $x_1\ x_2\ \neg x_3 \vee$ [illegible] $\vee\ x_2\ \neg x_4\ x_5 \vee$ [illegible] $\vee\ x_1\ \neg x_4\ \neg x_7$

=

$R = \{ x_1 \mapsto 1, x_4 \mapsto 0 \}$

$R^{\sim} = \{ x_1 \mapsto 1, x_4 \mapsto 0,$
$x_2 \mapsto 1, x_3 \mapsto 1,$
$x_5 \mapsto 0, x_7 \mapsto 1 \}$



k = 3, $\ell = 4$

$R \mapsto (R^*, \mathrm{Code}(R))$

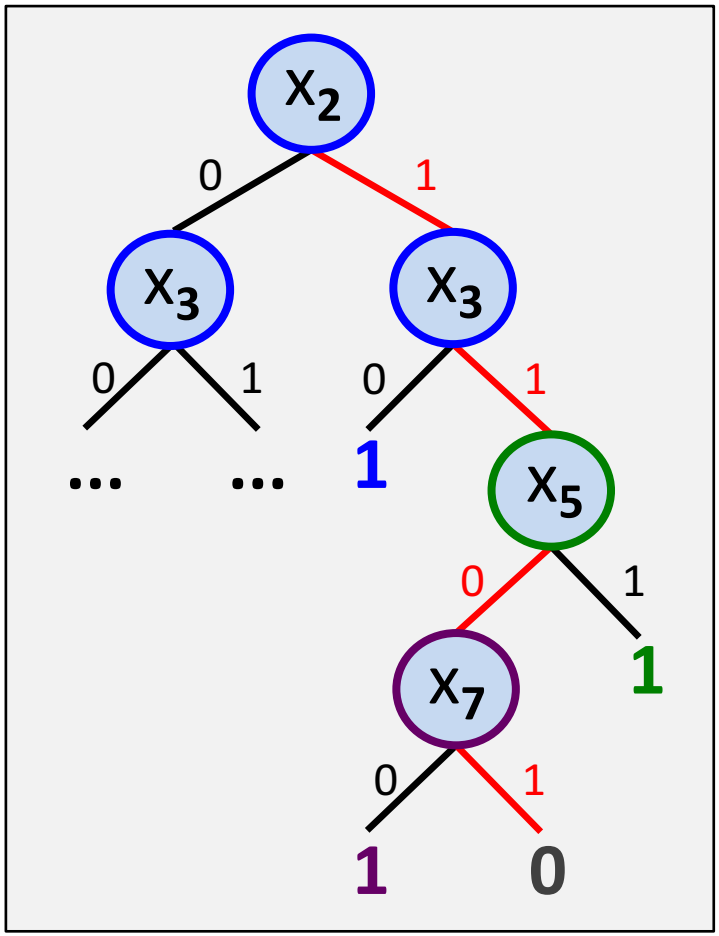
$F \upharpoonright R$ $x_1\ x_2\ \neg x_3 \vee \neg x_1\ x_3\ x_6 \vee x_2\ \neg x_4\ x_5 \vee x_3\ \neg x_5\ \neg x_6 \vee x_1\ \neg x_4\ \neg x_7$

=

$R = \{ x_1 \mapsto 1, x_4 \mapsto 0 \}$

$R\sim = \{ x_1 \mapsto 1, x_4 \mapsto 0,$
$x_2 \mapsto 1, x_3 \mapsto 1,$
$x_5 \mapsto 0, x_7 \mapsto 1 \}$

$R^* = \{ x_1 \mapsto 1, x_4 \mapsto 0,$
$x_2 \mapsto 1, x_3 \mapsto 0,$
$x_5 \mapsto 1, x_7 \mapsto 0 \}$



k = 3, $\ell = 4$

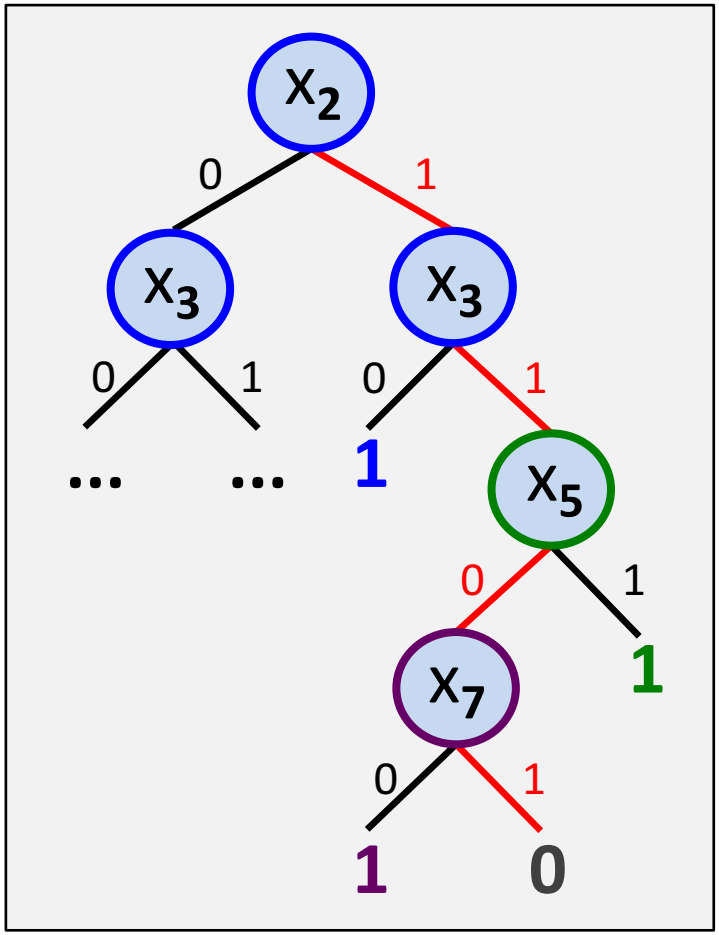
$R \mapsto (R^*, \mathrm{Code}(R))$

$F \upharpoonright R = x_1\, x_2\, \neg x_3 \vee \neg x_1\, x_3\, x_6 \vee x_2\, \neg x_4\, x_5 \vee x_3\, \neg x_5\, \neg x_6 \vee x_1\, \neg x_4\, \neg x_7$

$R = \{ x_1 \mapsto 1, x_4 \mapsto 0 \}$

$R^{\sim} = \{ x_1 \mapsto 1, x_4 \mapsto 0, x_2 \mapsto \quad x_3 \mapsto \quad x_5 \mapsto \quad x_7 \mapsto \quad \}$

$R^* = \{ x_1 \mapsto 1, x_4 \mapsto 0, x_2 \mapsto \quad x_3 \mapsto \quad x_5 \mapsto \quad x_7 \mapsto \quad \}$



k = 3, ℓ = 4

R ↦ (R*,Code(R))

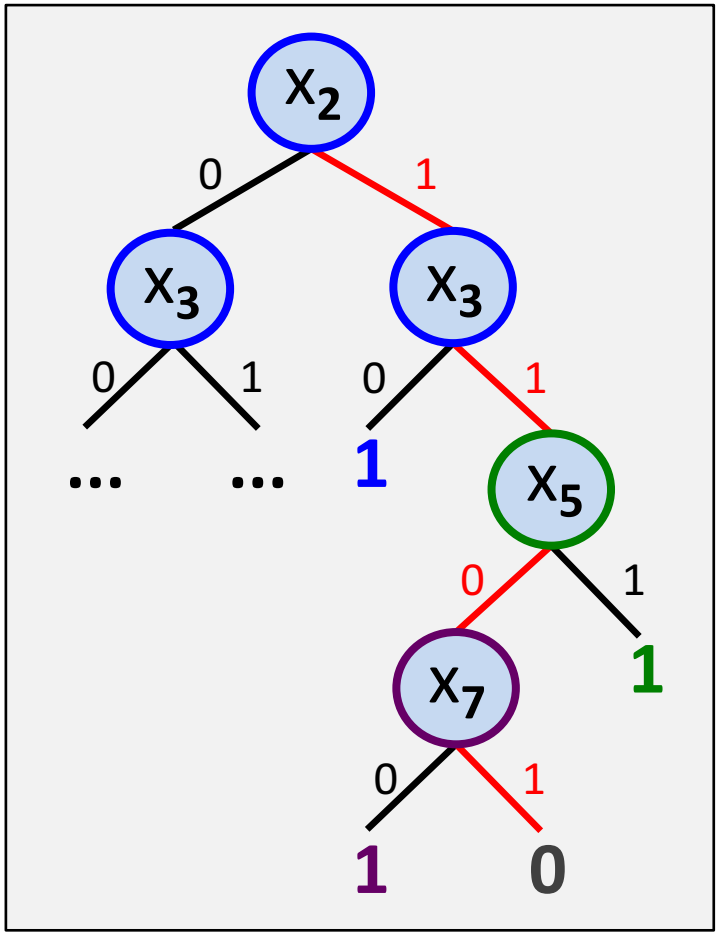
F ⊢ R $x_1\ x_2\ \neg x_3 \vee \neg x_1\ x_3\ x_6 \vee x_2\ \neg x_4\ x_5 \vee x_3\ x_5\ \neg x_6 \vee x_1\ \neg x_4\ \neg x_7$

=

$R = \{ x_1 \mapsto 1, x_4 \mapsto 0 \}$

$R^{\sim} = \{ x_1 \mapsto 1, x_4 \mapsto 0,$
$x_2 \mapsto \quad x_3 \mapsto$
$x_5 \mapsto \quad x_7 \mapsto \quad \}$

$R^* = \{ x_1 \mapsto 1, x_4 \mapsto 0,$
$x_2 \mapsto \quad x_3 \mapsto$
$x_5 \mapsto \quad x_7 \mapsto \quad \}$



k = 3, $\ell = 4$

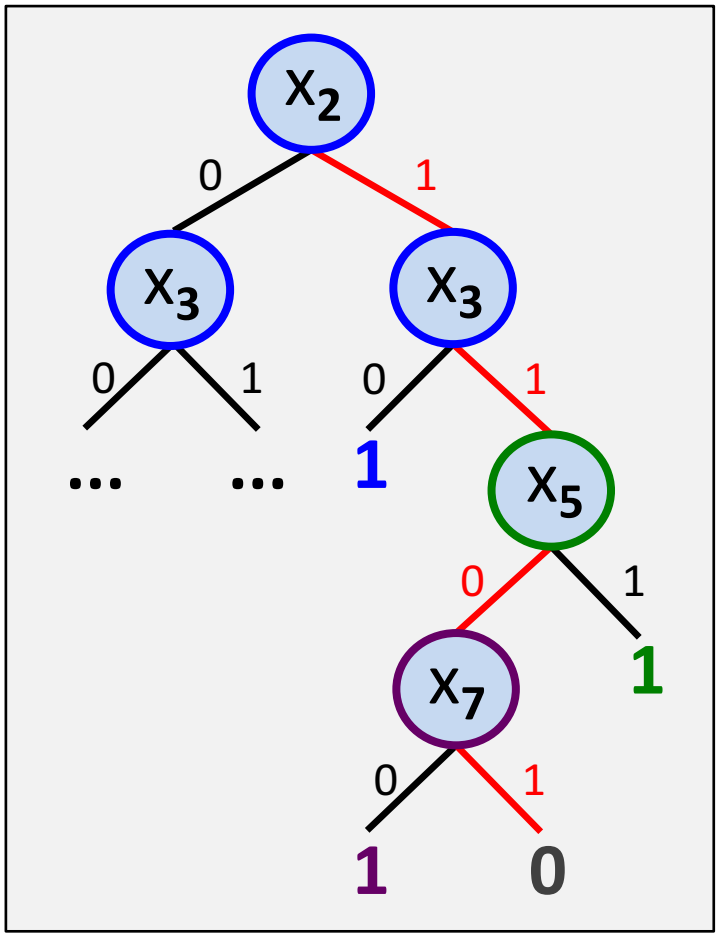
$R \mapsto (R^*, \mathrm{Code}(R))$

$F \upharpoonright R = x_1\, x_2\, \neg x_3 \vee \neg x_1\, x_3\, x_6 \vee x_2\, \neg x_4\, x_5 \vee x_3\, x_5\, \neg x_6 \vee x_1\, \neg x_4\, \neg x_7$

$R = \{ x_1 \mapsto 1, x_4 \mapsto 0 \}$

$R\sim = \{ x_1 \mapsto 1, x_4 \mapsto 0,$
$x_2 \mapsto \quad x_3 \mapsto$
$x_5 \mapsto \quad x_7 \mapsto \quad \}$

$R^* = \{ x_1 \mapsto 1, x_4 \mapsto 0,$
$x_2 \mapsto 1, x_3 \mapsto 0,$
$x_5 \mapsto \quad x_7 \mapsto \quad \}$



k = 3, $\ell = 4$

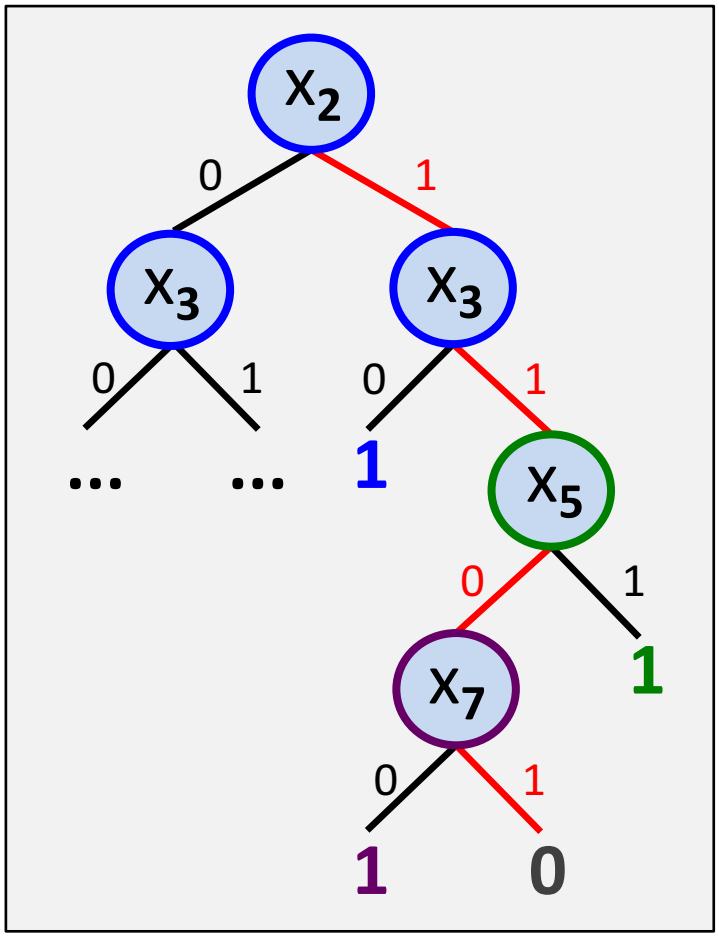
$R \mapsto (R^*, \mathrm{Code}(R))$

$F \upharpoonright R = x_1\, x_2\, \neg x_3 \vee \neg x_1\, x_3\, x_6 \vee x_2\, \neg x_4\, x_5 \vee x_3\, \neg x_5\, \neg x_6 \vee x_1\, \neg x_4\, \neg x_7$

$R = \{ x_1 \mapsto 1, x_4 \mapsto 0 \}$

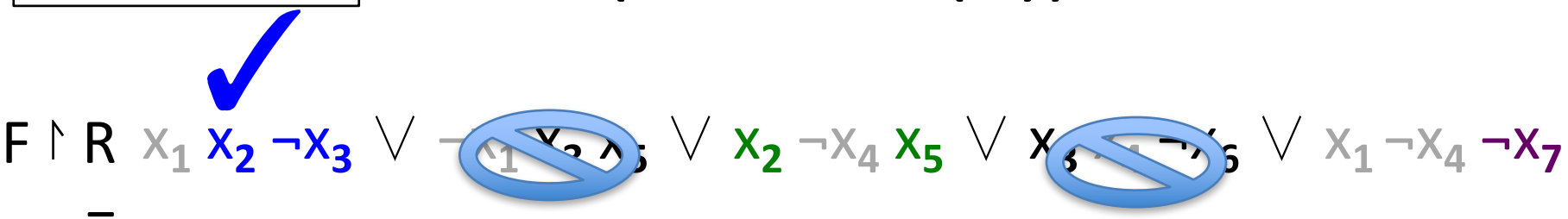
$R^{\sim} = \{ x_1 \mapsto 1, x_4 \mapsto 0, x_2 \mapsto 1, x_3 \mapsto 1, x_5 \mapsto \quad x_7 \mapsto \quad \}$

$R^* = \{ x_1 \mapsto 1, x_4 \mapsto 0, x_2 \mapsto 1, x_3 \mapsto 0, x_5 \mapsto \quad x_7 \mapsto \quad \}$



k = 3, $\ell = 4$

$R \mapsto (R^*, \mathrm{Code}(R))$



$R = \{ x_1 \mapsto 1, x_4 \mapsto 0 \}$

$R\sim = \{ x_1 \mapsto 1, x_4 \mapsto 0, x_2 \mapsto 1, x_3 \mapsto 1, x_5 \mapsto \quad x_7 \mapsto \quad \}$

$R^* = \{ x_1 \mapsto 1, x_4 \mapsto 0, x_2 \mapsto 1, x_3 \mapsto 0, x_5 \mapsto \quad x_7 \mapsto \quad \}$

Code(R) says:

- find the first satisfied term of F ⊦ R*
- the "long path" begins with

  $x_2 \mapsto 1, x_3 \mapsto 1$

  (i.e. var_2 of term ↦ 1 and var_3 of term ↦ 1)
- …

$k = 3,\ \ell = 4$

$R \mapsto (R^*, \mathrm{Code}(R))$

1 0 1

$F \restriction R$ $x_1\ x_2\ \neg x_3 \vee \neg x_1\ x_3\ x_6 \vee x_2\ \neg x_4\ x_5 \vee x_3\ \neg x_5\ \neg x_6 \vee x_1\ \neg x_4\ \neg x_7$

=

$R = \{ x_1 \mapsto 1, x_4 \mapsto 0 \}$

$R\sim = \{ x_1 \mapsto 1, x_4 \mapsto 0,$
$x_2 \mapsto 1, x_3 \mapsto 1,$
$x_5 \mapsto \quad x_7 \mapsto \ \}$

$R^* = \{ x_1 \mapsto 1, x_4 \mapsto 0,$
$x_2 \mapsto 1, x_3 \mapsto 0,$
$x_5 \mapsto \quad x_7 \mapsto \ \}$

Fix variables according to the beginning of the long path

k = 3, $\ell = 4$

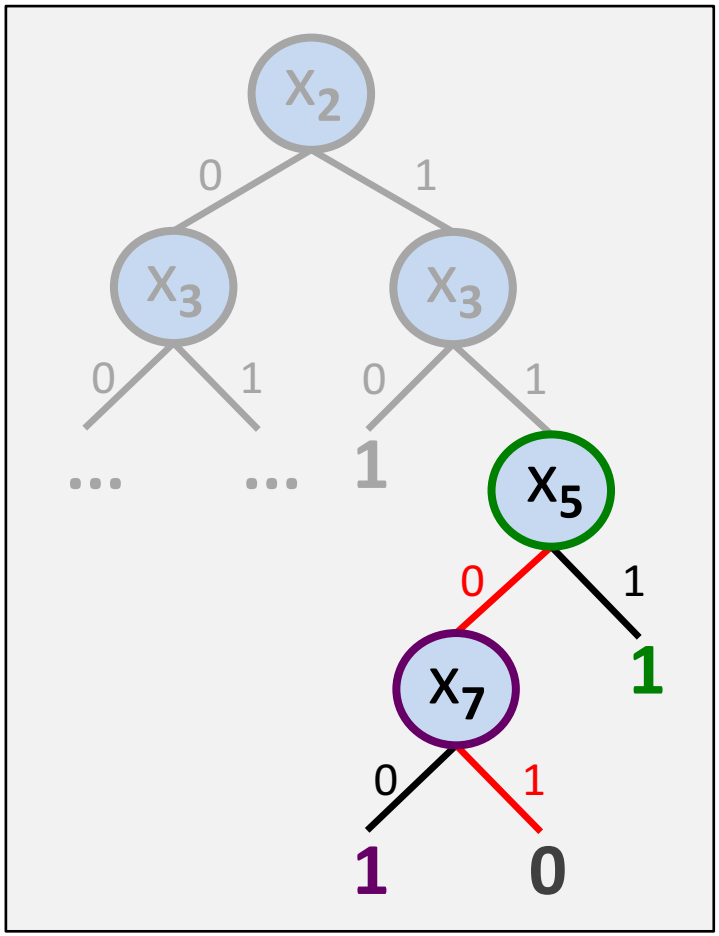
$R \mapsto (R^*, \mathrm{Code}(R))$

$F \upharpoonright R = \; \cdots \vee x_2 \neg x_4 x_5 \vee \cdots \vee x_1 \neg x_4 \neg x_7$

$R = \{ x_1 \mapsto 1, x_4 \mapsto 0 \}$

$R^{\sim} = \{ x_1 \mapsto 1, x_4 \mapsto 0,$
$x_2 \mapsto 1, x_3 \mapsto 1,$
$x_5 \mapsto \quad x_7 \mapsto \quad \}$

$R^* = \{ x_1 \mapsto 1, x_4 \mapsto 0,$
$x_2 \mapsto 1, x_3 \mapsto 0,$
$x_5 \mapsto \quad x_7 \mapsto \quad \}$



k = 3, ℓ = 4

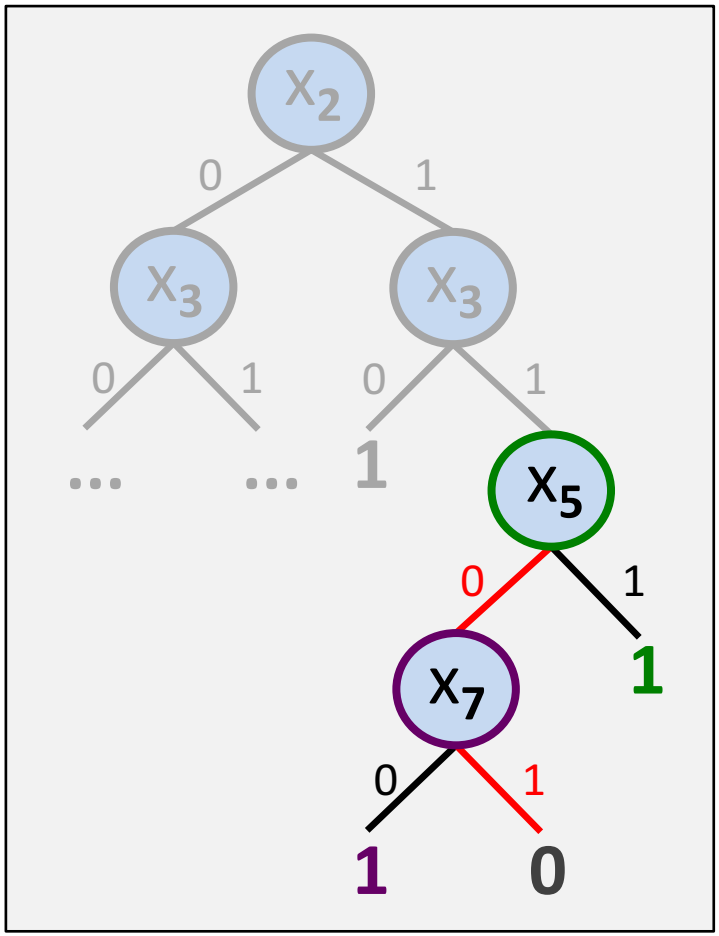
$R \mapsto (R^*, \mathrm{Code}(R))$

$F \upharpoonright R$ = $\bigvee \bigvee x_2\, \neg x_4\, x_5 \bigvee \bigvee x_1\, \neg x_4\, \neg x_7$

$R = \{ x_1 \mapsto 1, x_4 \mapsto 0 \}$

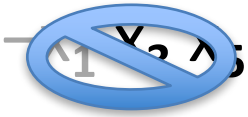
$R\sim = \{ x_1 \mapsto 1, x_4 \mapsto 0,$
$x_2 \mapsto 1, x_3 \mapsto 1,$
$x_5 \mapsto \quad x_7 \mapsto \quad \}$

$R^* = \{ x_1 \mapsto 1, x_4 \mapsto 0,$
$x_2 \mapsto 1, x_3 \mapsto 0,$
$x_5 \mapsto \quad x_7 \mapsto \quad \}$



k = 3, $\ell = 4$

$R \mapsto (R^*, \mathrm{Code}(R))$



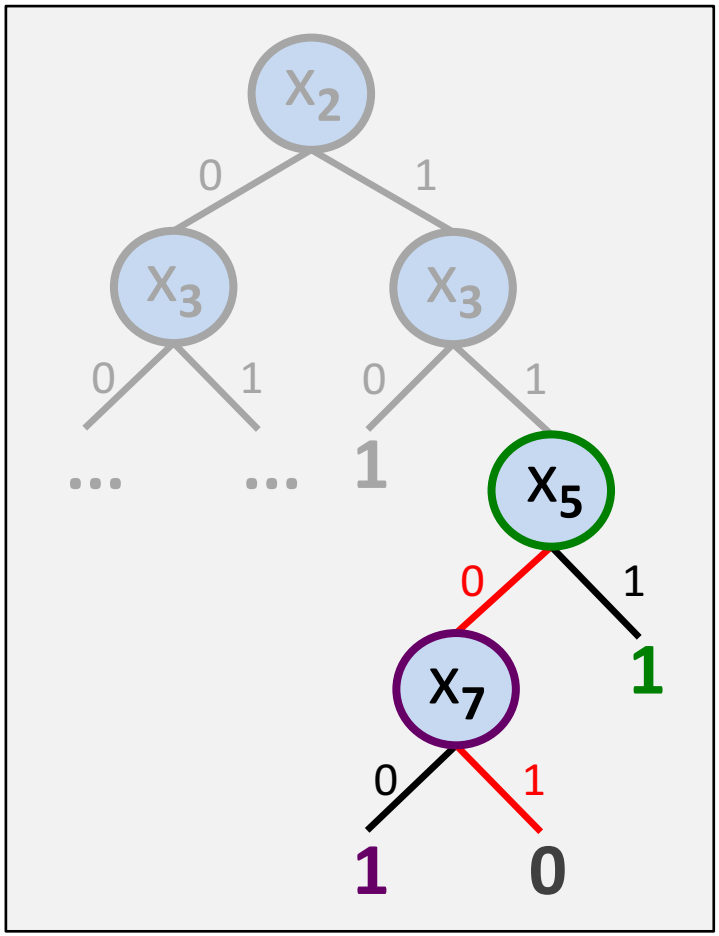
$F \restriction R \quad \ldots \vee \neg x_1 \ldots \vee x_2\ \neg x_4\ x_5 \vee \ldots \neg x_6 \vee x_1\ \neg x_4\ \neg x_7$

=

$R = \{ x_1 \mapsto 1, x_4 \mapsto 0 \}$

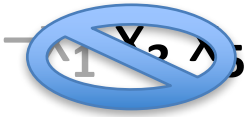
$R\sim = \{ x_1 \mapsto 1, x_4 \mapsto 0,$
$x_2 \mapsto 1, x_3 \mapsto 1,$
$x_5 \mapsto \quad x_7 \mapsto \quad \}$

$R^* = \{ x_1 \mapsto 1, x_4 \mapsto 0,$
$x_2 \mapsto 1, x_3 \mapsto 0,$
$x_5 \mapsto 1 \quad x_7 \mapsto \quad \}$



k = 3, $\ell = 4$

$R \mapsto (R^*, \mathrm{Code}(R))$

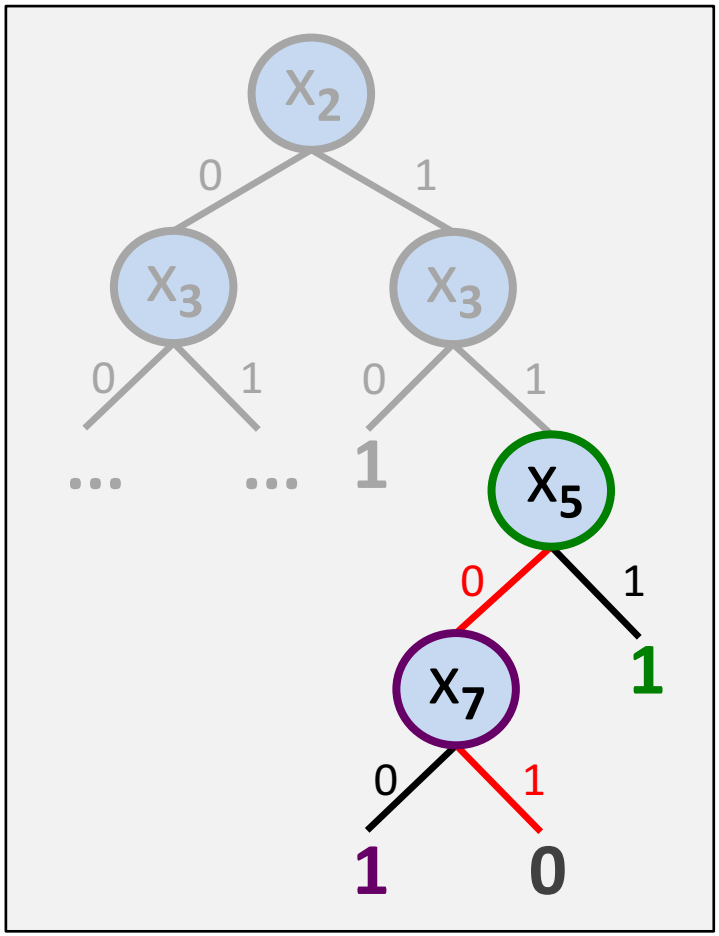




$F \restriction R = \quad \vee \quad \vee x_2 \neg x_4 x_5 \vee \quad \vee x_1 \neg x_4 \neg x_7$

$R = \{ x_1 \mapsto 1, x_4 \mapsto 0 \}$

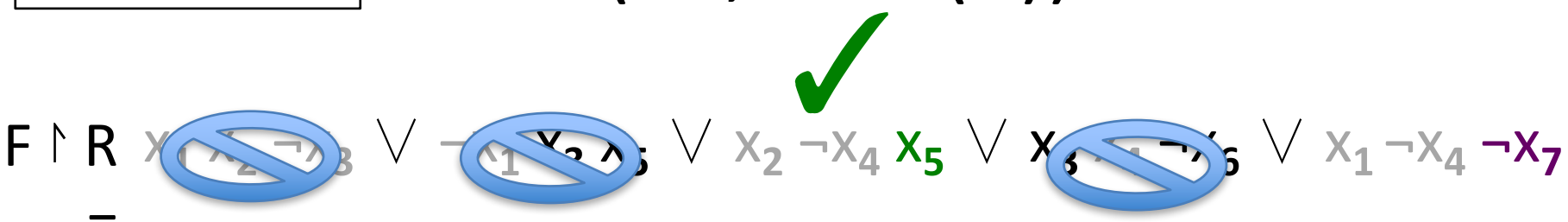
$R\sim = \{ x_1 \mapsto 1, x_4 \mapsto 0, x_2 \mapsto 1, x_3 \mapsto 1, x_5 \mapsto 0 \; x_7 \mapsto \; \}$

$R^* = \{ x_1 \mapsto 1, x_4 \mapsto 0, x_2 \mapsto 1, x_3 \mapsto 0, x_5 \mapsto 1 \; x_7 \mapsto \; \}$



k = 3, ℓ = 4

$R \mapsto (R^*, \mathrm{Code}(R))$



$R = \{ x_1 \mapsto 1, x_4 \mapsto 0 \}$

$R\sim = \{ x_1 \mapsto 1, x_4 \mapsto 0, x_2 \mapsto 1, x_3 \mapsto 1, x_5 \mapsto 0 \; x_7 \mapsto \; \}$

$R^* = \{ x_1 \mapsto 1, x_4 \mapsto 0, x_2 \mapsto 1, x_3 \mapsto 0, x_5 \mapsto 1 \; x_7 \mapsto \; \}$

Code(R) next says:

- find the next satisfied term of $F \vdash R^*$ (overwriting $x_2 \mapsto 1$, $x_3 \mapsto 1$)
- the "long path" continues

  $x_5 \mapsto 0$

  (i.e. var_3 of term $\mapsto 0$)
- …

k = 3, $\ell = 4$

$R \mapsto (R^*, \mathrm{Code}(R))$

0

$F \restriction R$ = $\neg x_1 \neg x_2 \neg x_3 \vee \neg x_1 x_3 x_5 \vee x_2 \neg x_4 x_5 \vee x_3 \neg x_5 \neg x_6 \vee x_1 \neg x_4 \neg x_7$

$R = \{ x_1 \mapsto 1, x_4 \mapsto 0 \}$

$R\sim = \{ x_1 \mapsto 1, x_4 \mapsto 0,$
$x_2 \mapsto 1, x_3 \mapsto 1,$
$x_5 \mapsto 0 \quad x_7 \mapsto \quad \}$

$R^* = \{ x_1 \mapsto 1, x_4 \mapsto 0,$
$x_2 \mapsto 1, x_3 \mapsto 0,$
$x_5 \mapsto 1, x_7 \mapsto \quad \}$

Fix variables according to the long path

k = 3, ℓ = 4

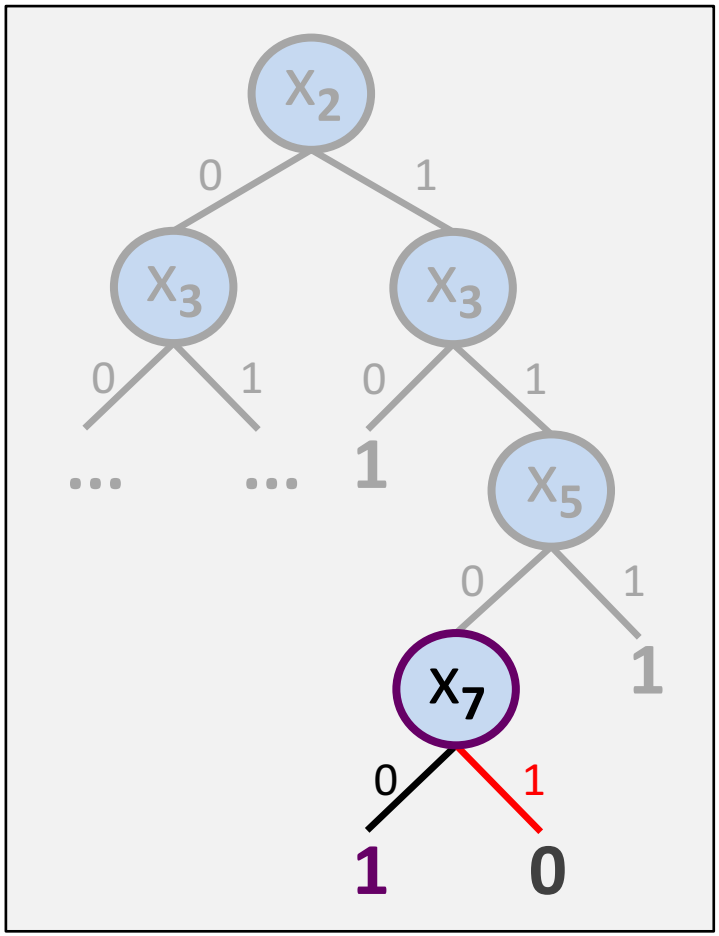
R ↦ (R*,Code(R))

F ⊢ R = $x_1 \neg x_4 \neg x_7$

$R = \{ x_1 \mapsto 1, x_4 \mapsto 0 \}$

$R\sim = \{ x_1 \mapsto 1, x_4 \mapsto 0,$
$x_2 \mapsto 1, x_3 \mapsto 1,$
$x_5 \mapsto 0, x_7 \mapsto \quad \}$

$R^* = \{ x_1 \mapsto 1, x_4 \mapsto 0,$
$x_2 \mapsto 1, x_3 \mapsto 0,$
$x_5 \mapsto 1, x_7 \mapsto \quad \}$



k = 3, $\ell = 4$

$R \mapsto (R^*, \mathrm{Code}(R))$

$$F = x_1 x_2 \neg x_3 \vee \neg x_1 x_3 x_5 \vee x_2 \neg x_4 x_5 \vee x_3 x_4 \neg x_6 \vee x_1 \neg x_4 \neg x_7$$

$R = \{ x_1 \mapsto 1, x_4 \mapsto 0 \}$

$R\sim = \{ x_1 \mapsto 1, x_4 \mapsto 0,$
$x_2 \mapsto 1, x_3 \mapsto 1,$
$x_5 \mapsto 0, x_7 \mapsto 1 \}$

$R^* = \{ x_1 \mapsto 1, x_4 \mapsto 0,$
$x_2 \mapsto 1, x_3 \mapsto 0,$
$x_5 \mapsto 1, x_7 \mapsto 0 \}$

$\mathrm{Code}(R) \in (\{0,1\}^2 \times [k])^{\ell}$
given knowledge of R^* (and F), follow these instructions to recover R (and along the way R~)

k = 3, $\ell = 4$

$R \mapsto (R^*, \text{Code}(R))$

$$F = x_1 x_2 \neg x_3 \vee \neg x_1 x_3 x_5 \vee x_2 \neg x_4 x_5 \vee x_3 x_4 \neg x_6 \vee x_1 \neg x_4 \neg x_7$$

$R = \{ x_1 \mapsto 1, x_4 \mapsto 0 \}$

$R\sim = \{ x_1 \mapsto 1, x_4 \mapsto 0,$
$x_2 \mapsto 1, x_3 \mapsto 1,$
$x_5 \mapsto 0, x_7 \mapsto 1 \}$

$R^* = \{ x_1 \mapsto 1, x_4 \mapsto 0,$
$x_2 \mapsto 1, x_3 \mapsto 0,$
$x_5 \mapsto 1, x_7 \mapsto 0 \}$

$\underline{\text{Code}(R) \in (\{0,1\}^2 \times [k])^\ell}$
given knowledge of R^* (and F), follow these instructions to recover R (and along the way R~)

- ✓ R^* has ℓ fewer stars than R
- ✓ $R \mapsto (R^*, \text{Code}(R))$ is 1-to-1