A Switching Lemma Tutorial

Benjamin Rossman

University of Toronto and NII, Tokyo

homage to Paul Beame's excellent
A Switching Lemma Primer

A Switching Lemma Tutorial*

Benjamin Rossman

University of Toronto and NII, Tokyo

Overview

1. **Basic Concepts**
   - models of computation (AC^0, DNFs/CNFs, decision trees)
   - random restriction $\mathbf{R}_p$
2. **The Classic Switching Lemma** (Hastad '86)
3. **PARITY Lower Bound**
4. **Affine Restrictions**
   - "Tseitin expander switching lemma" (joint with Pitassi, Servedio and Tan)

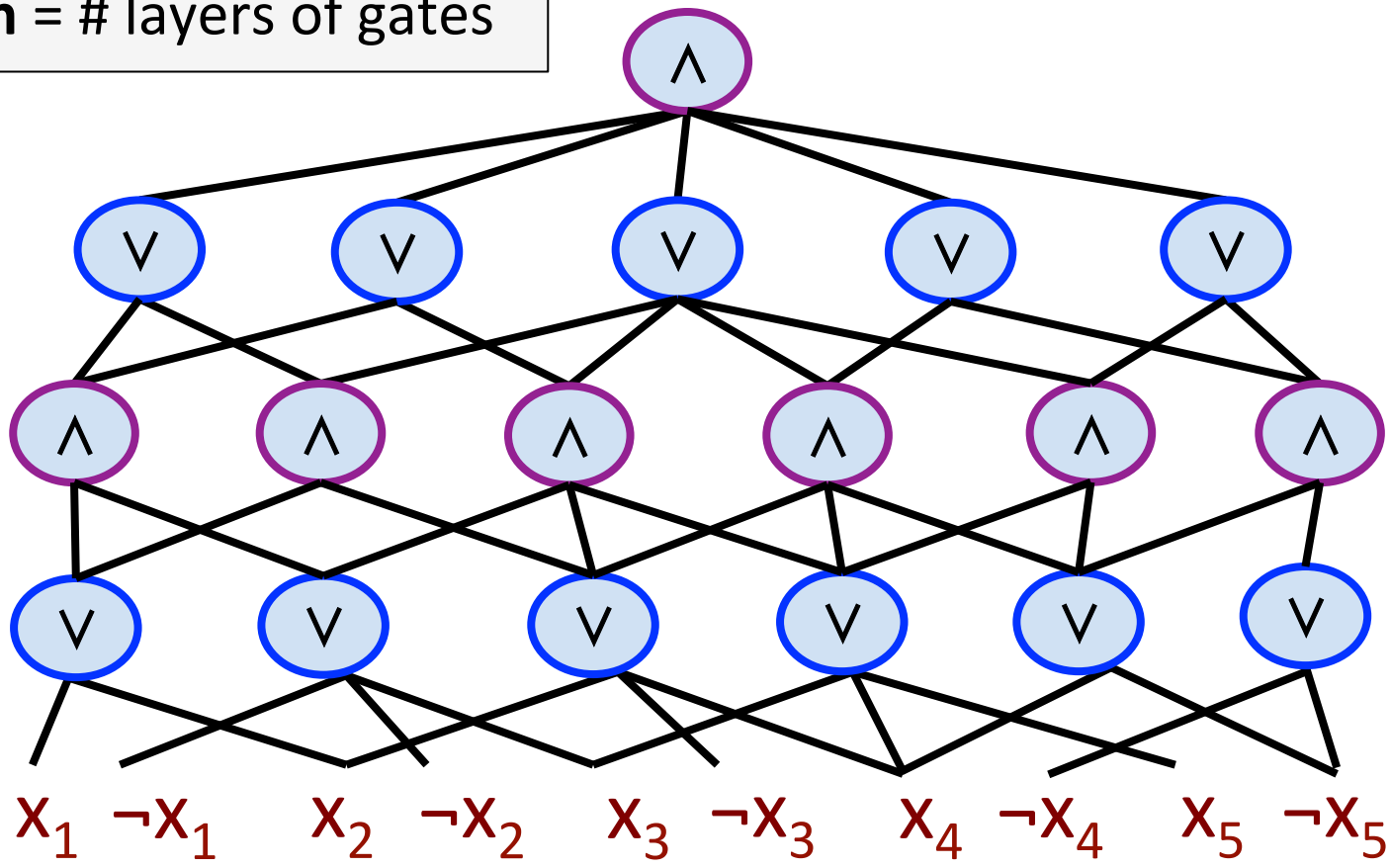
Models of Computation

- AC^0 circuits / formulas
- DNFs / CNFs (i.e. depth-2 formulas)
- Decision trees
- *Canonical decision tree of a DNF / CNF*

AC^0 Circuits

size = # of gates

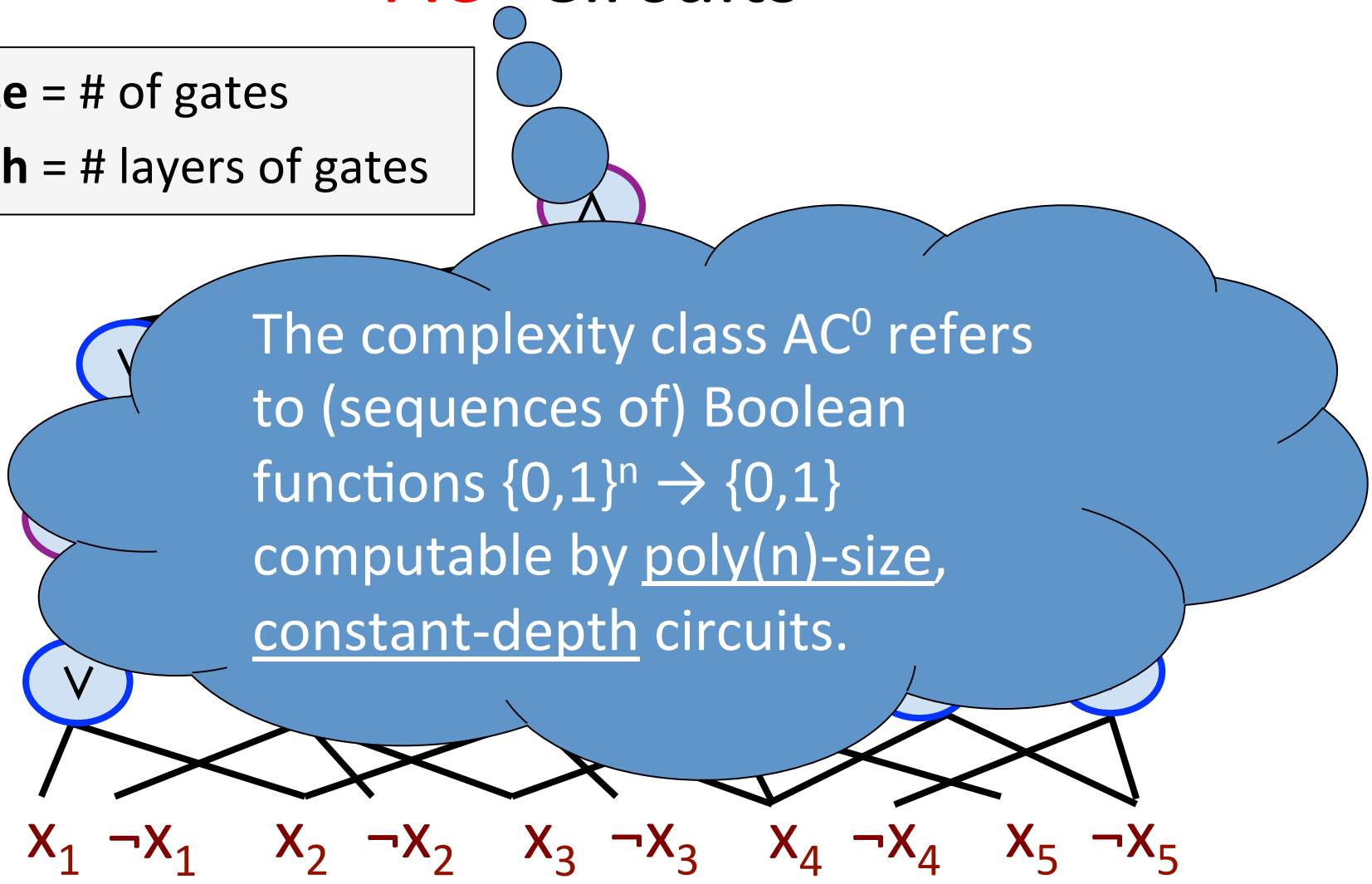
depth = # layers of gates



AC^0 Circuits

size = # of gates

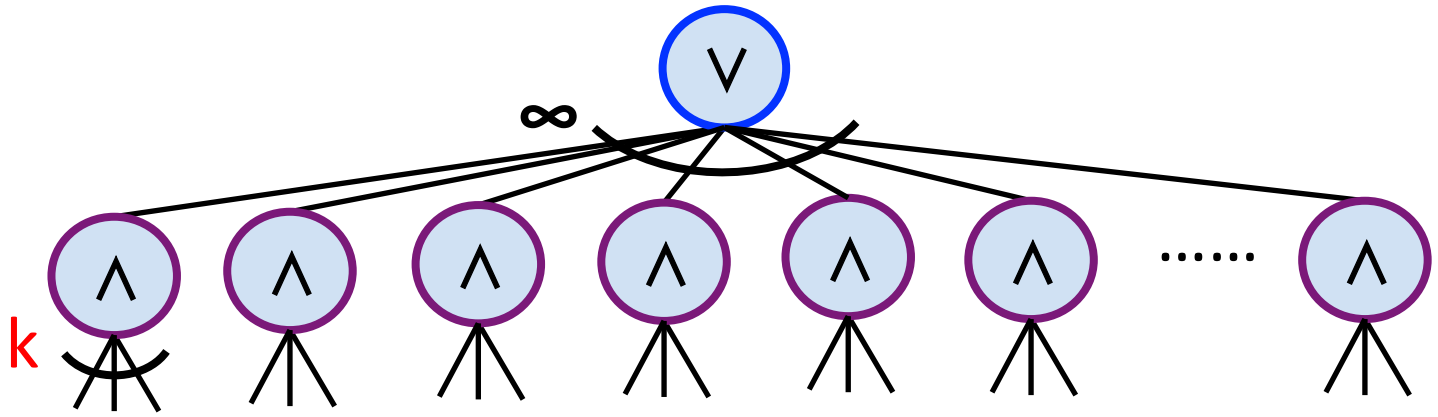
depth = # layers of gates



The complexity class AC^0 refers to (sequences of) Boolean functions $\{0,1\}^n \rightarrow \{0,1\}$ computable by poly(n)-size, constant-depth circuits.

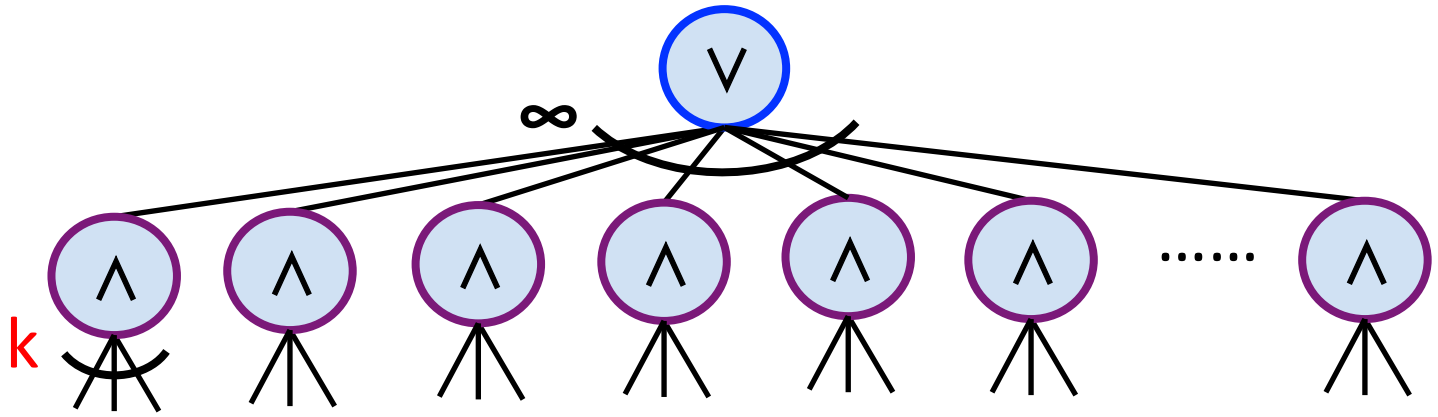
Depth-2 (DNFs and CNFs)

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

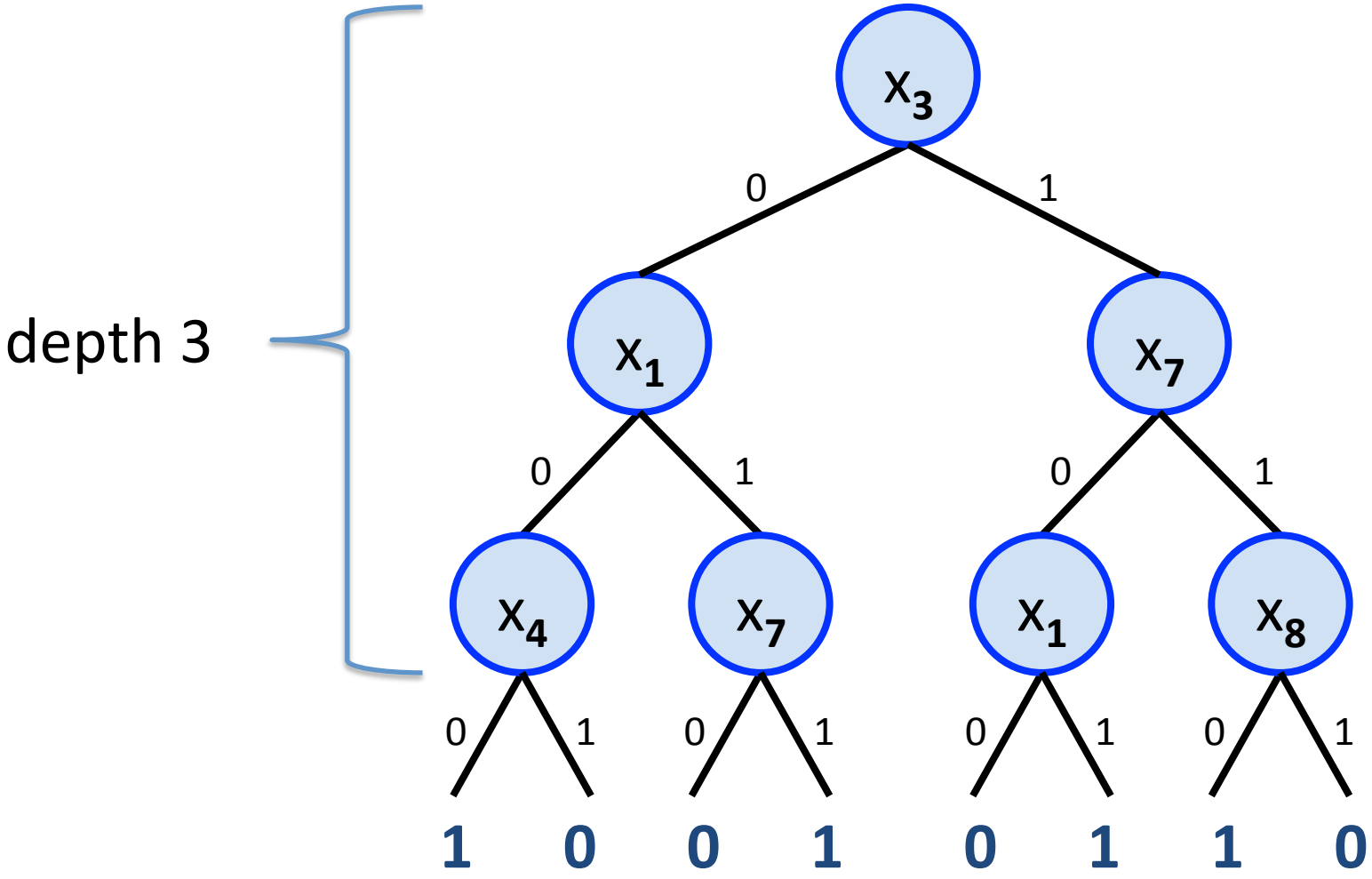


Depth-2 (DNFs and CNFs)

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



Decision Trees



Decision Trees

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

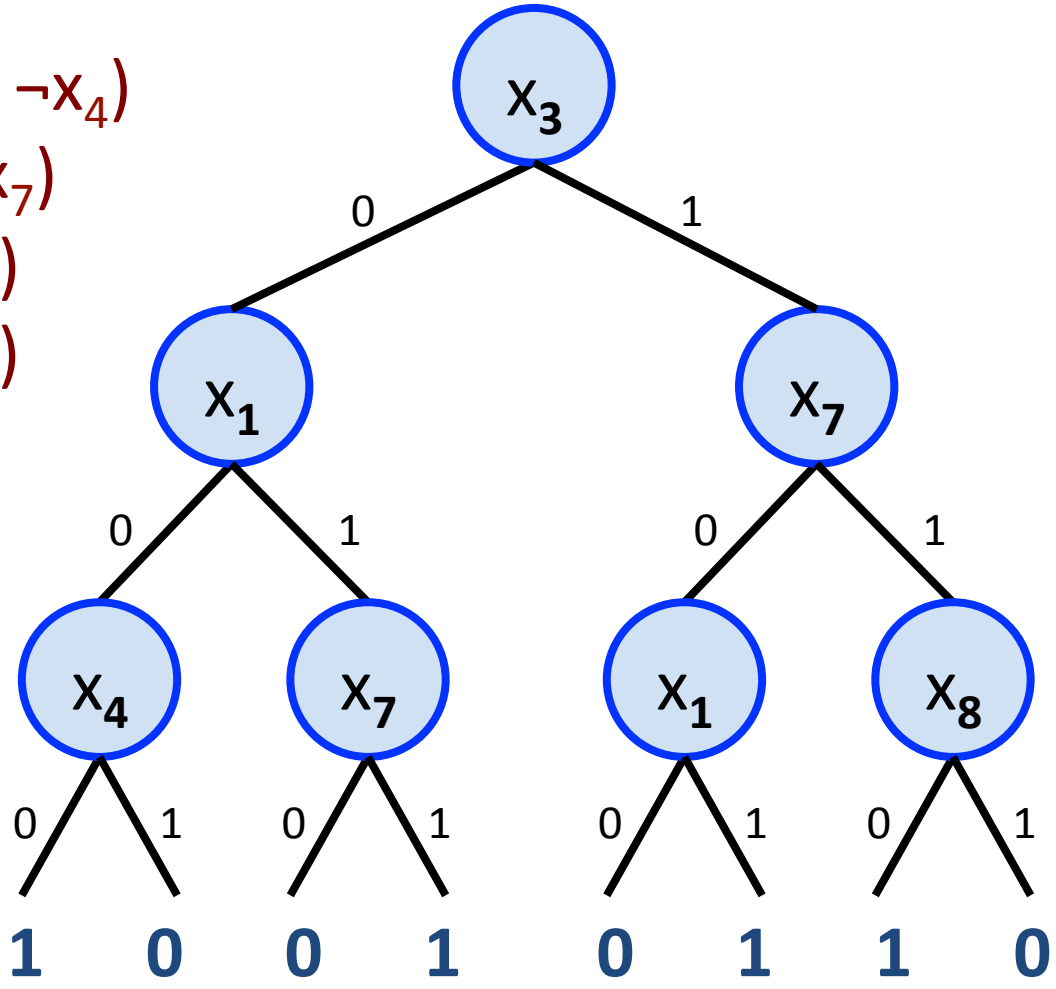
$$f : \{0,1\}^n \rightarrow \{0,1\}$$

denoted $DT_{depth}(f)$, 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

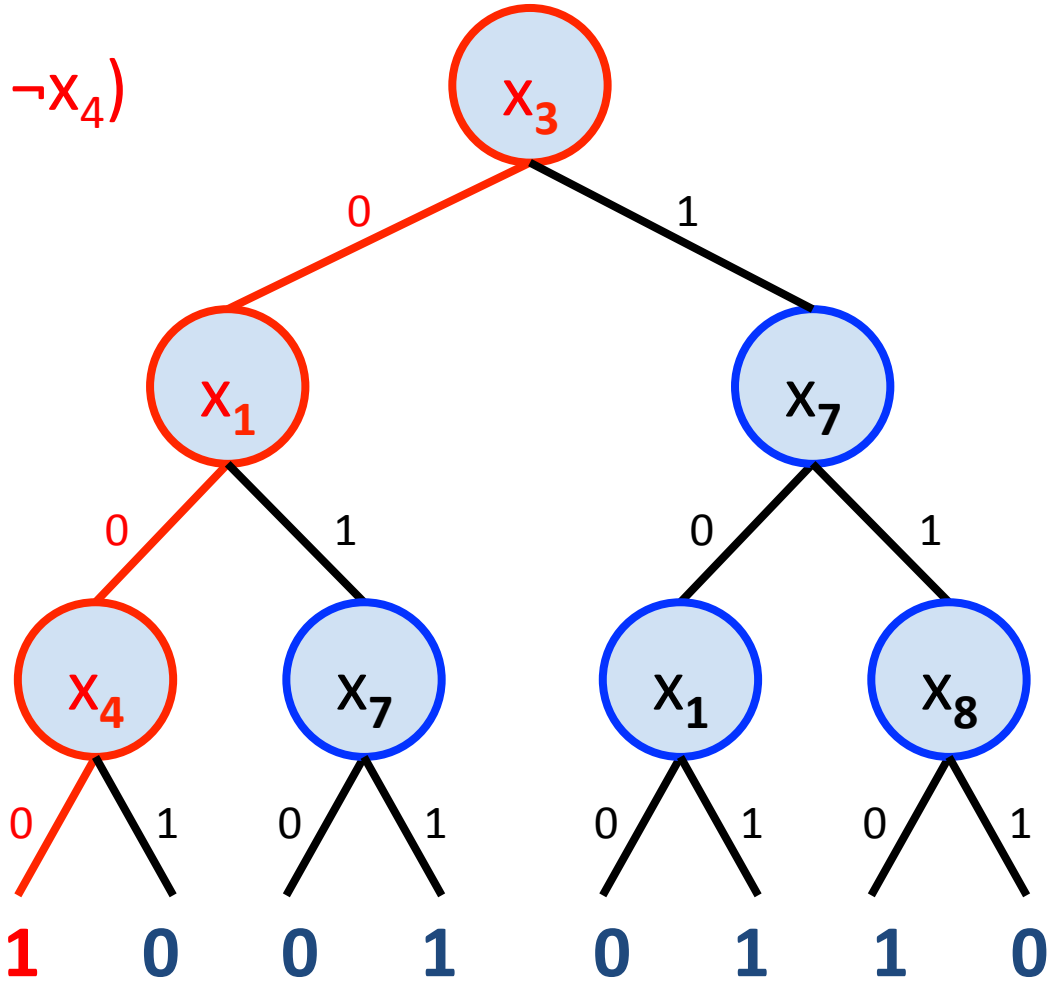
Decision Tree to DNF

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



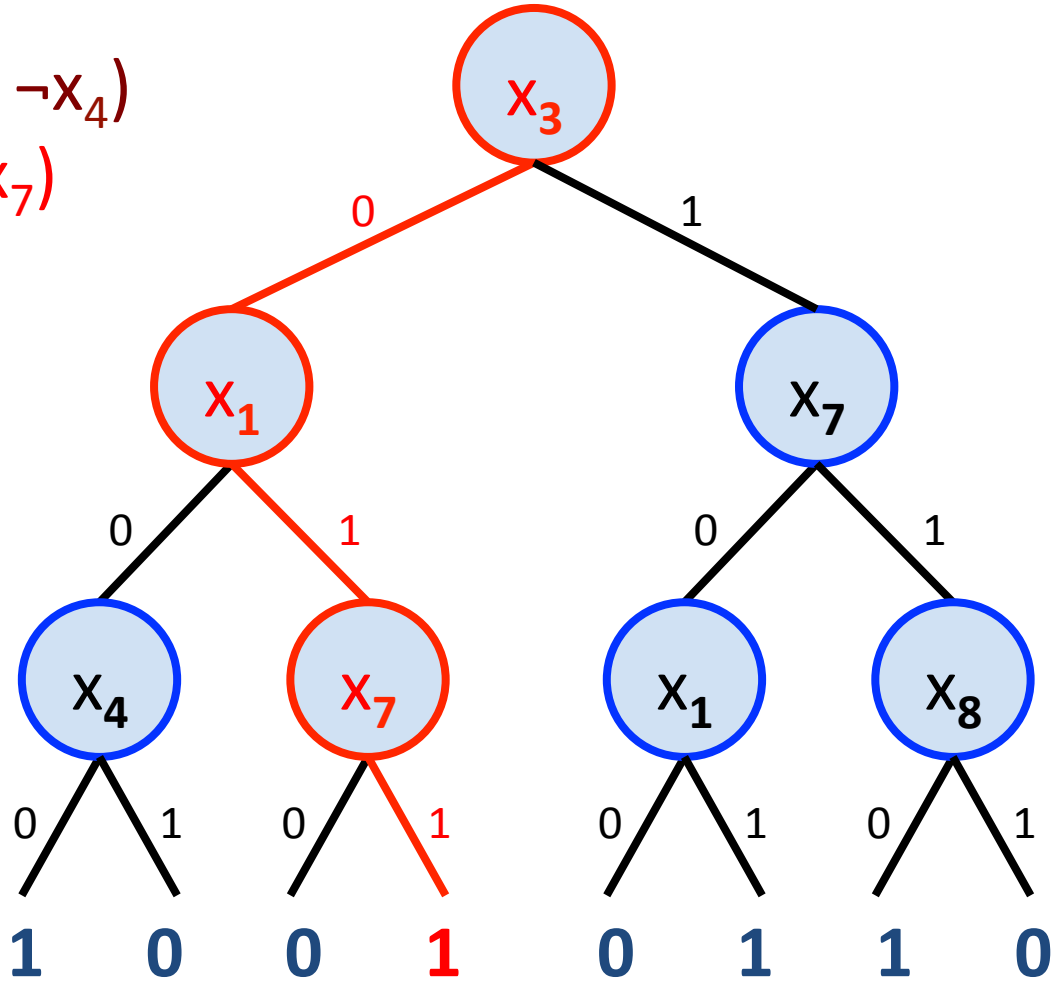
Decision Tree to DNF

$(\neg x_3 \wedge \neg x_1 \wedge \neg x_4)$



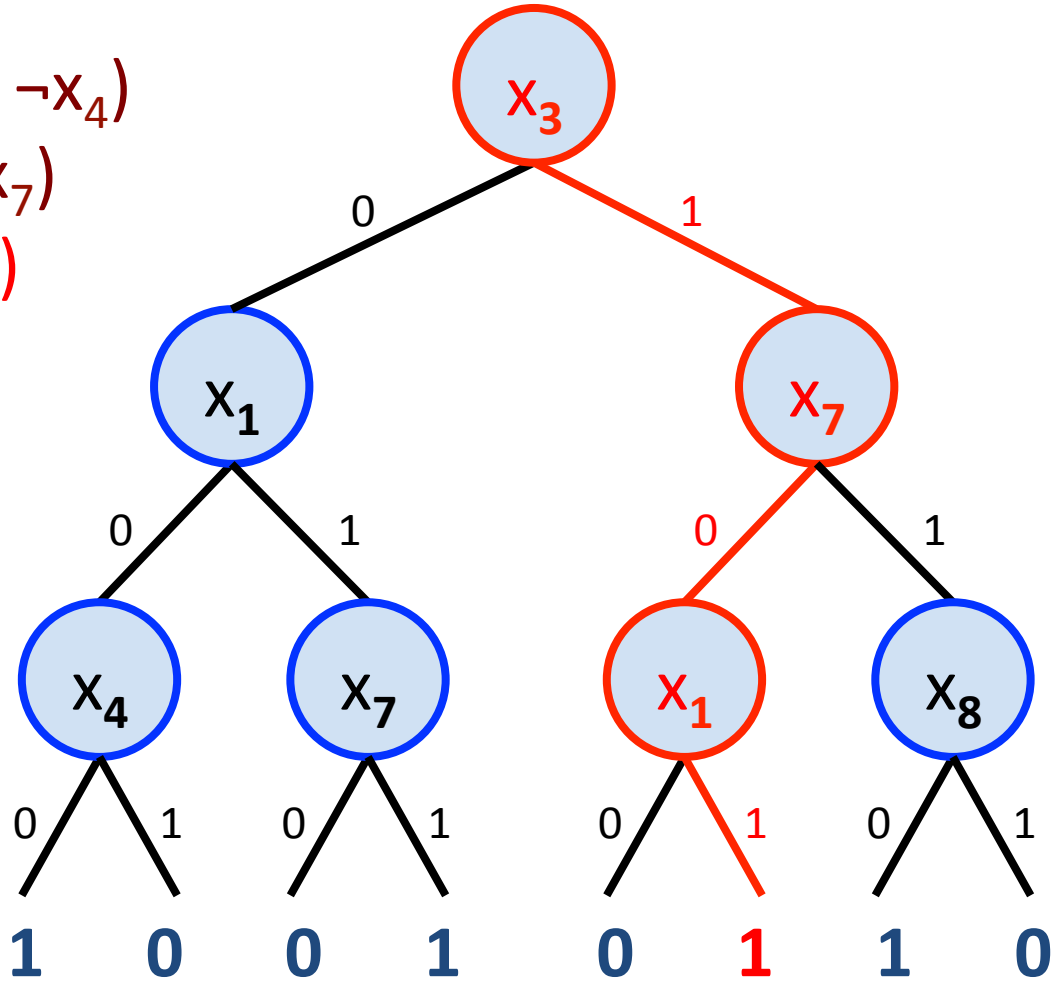
Decision Tree to DNF

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



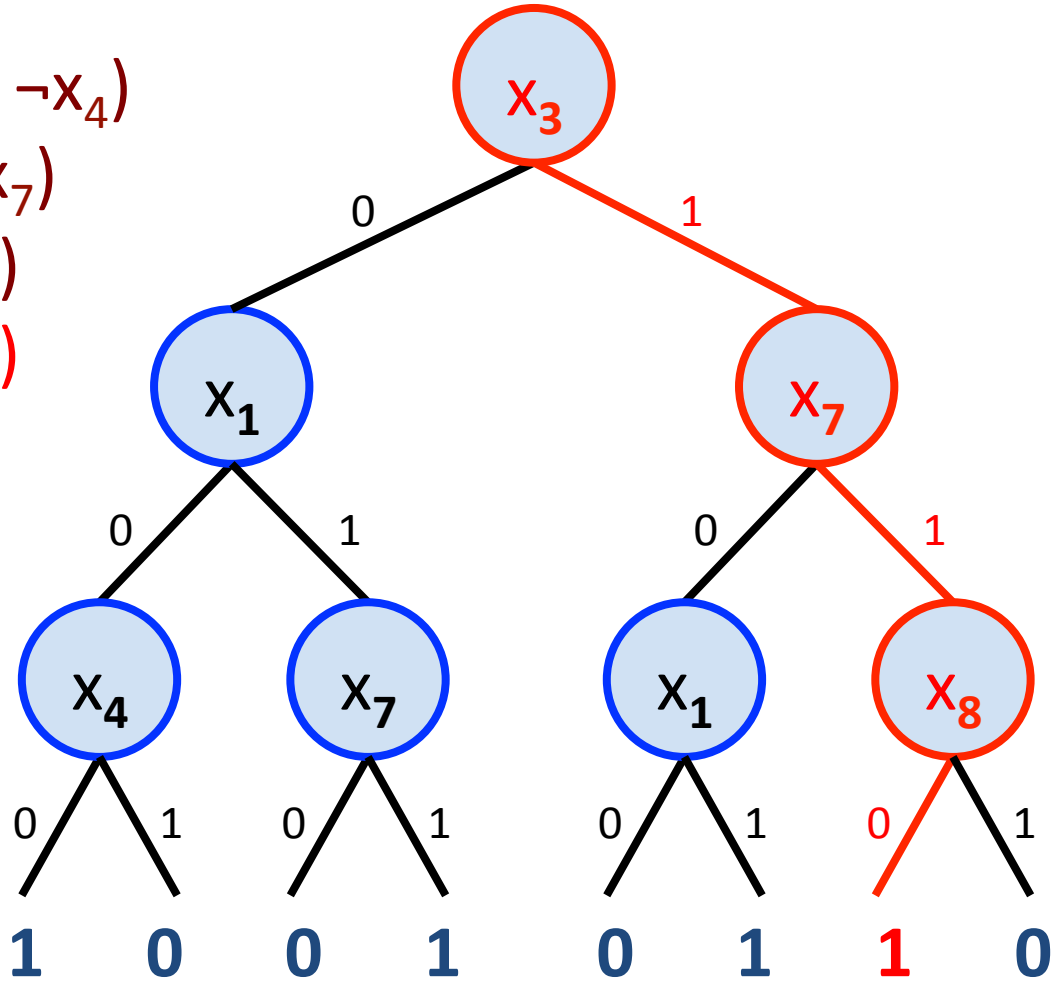
Decision Tree to DNF

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



Decision Tree to DNF

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



Canonical DT of a DNF

$$(x_1 \wedge x_2 \wedge x_3)$$
$$\vee\ (\neg x_2 \wedge x_4)$$
$$\vee\ (x_1 \wedge \neg x_3 \wedge \neg x_7)$$

Canonical DT of a DNF

$(x_1\ x_2\ x_3)$

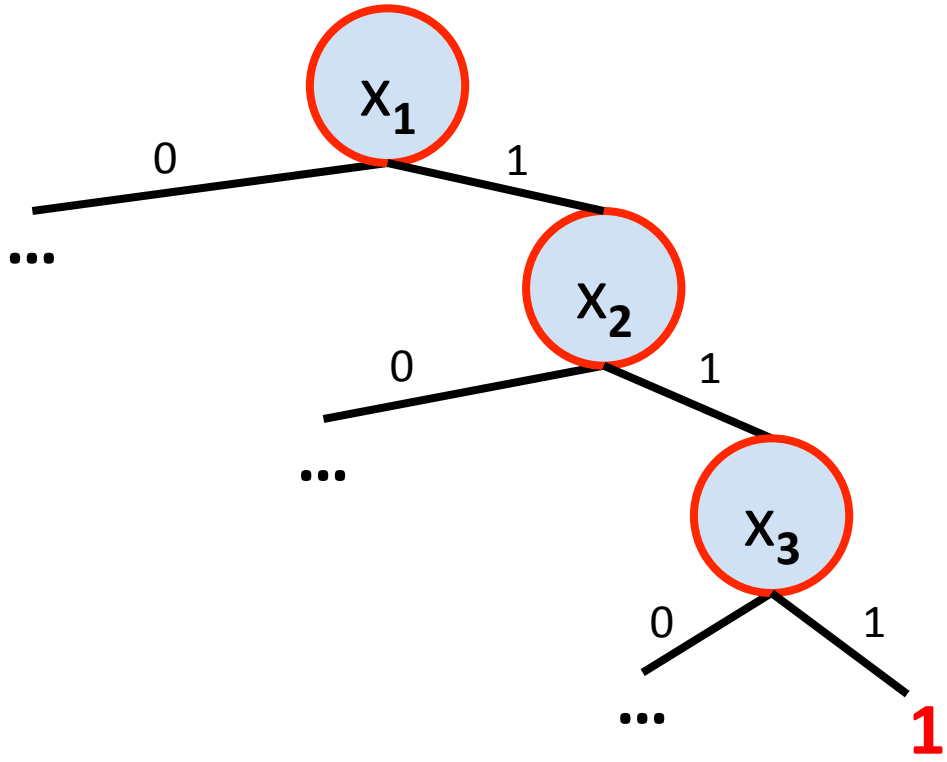
$\vee\ (\neg x_2\ x_4)$

$\vee\ (x_1\ \neg x_3\ \neg x_7)$

Canonical DT of a DNF

$(x_1\ x_2\ x_3)$

...

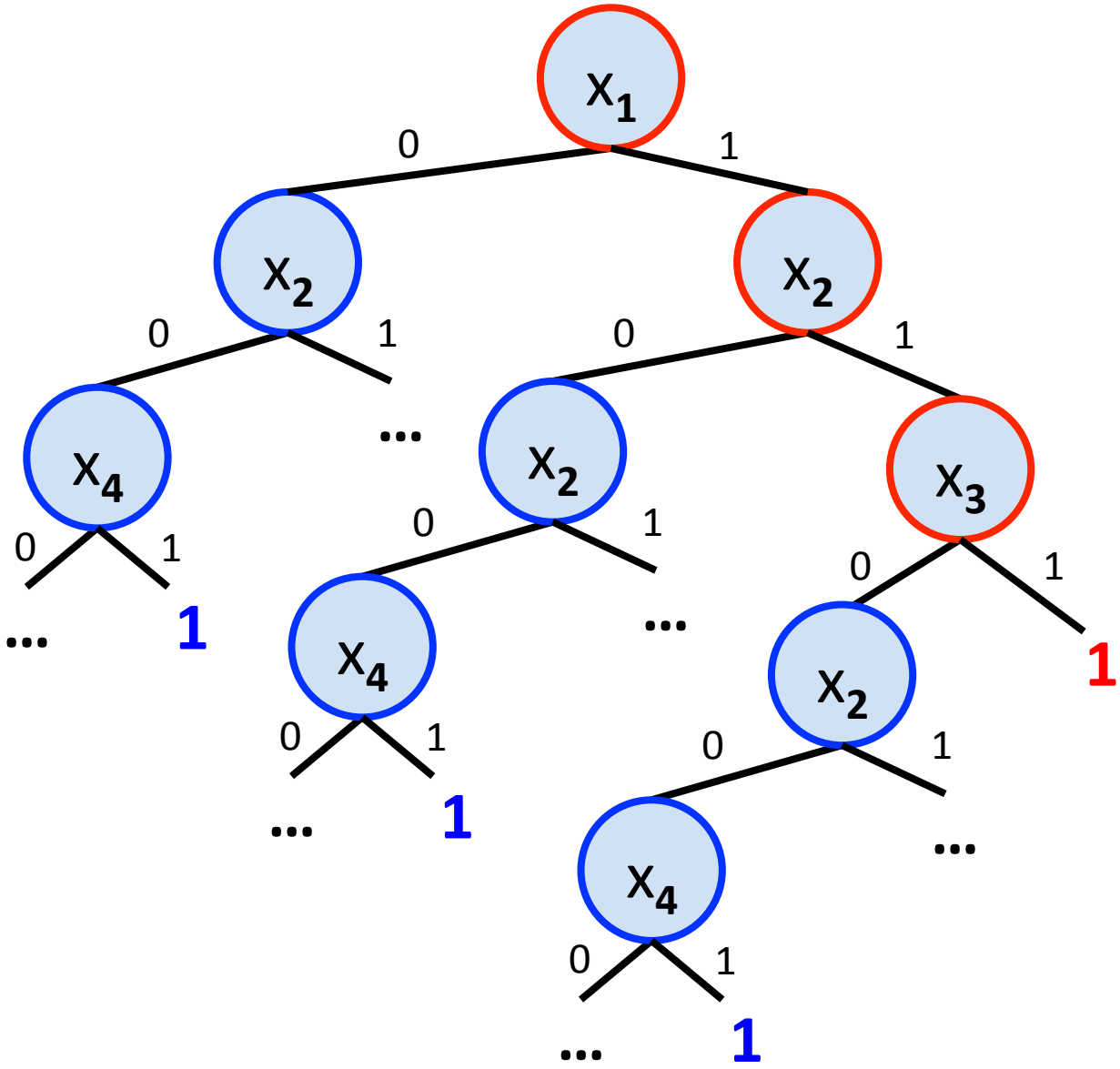


Canonical DT of a DNF

$(x_1\ x_2\ x_3)$

$\vee\ (\neg x_2\ x_4)$

...

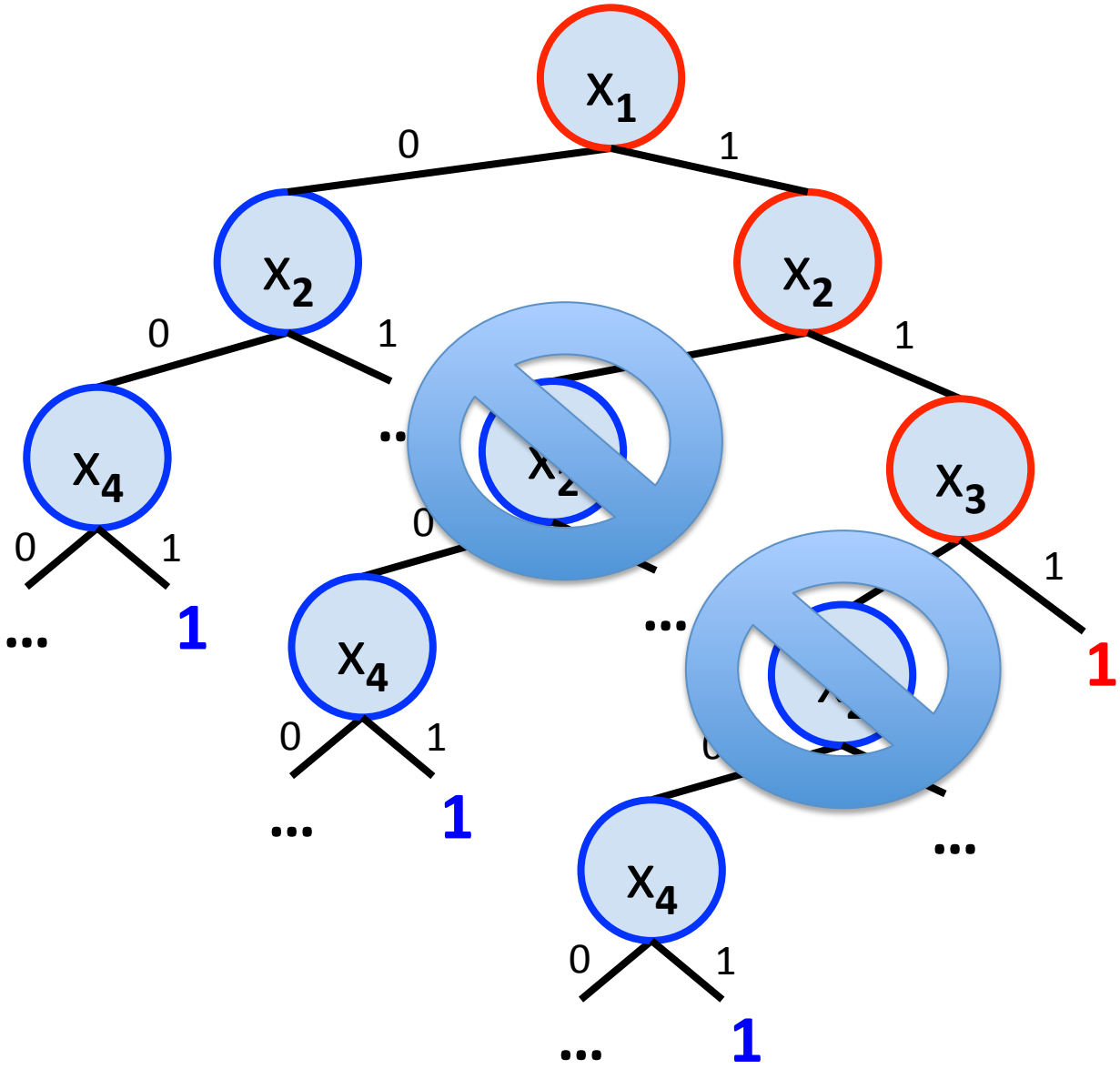


Canonical DT of a DNF

$(x_1\ x_2\ x_3)$

$\vee\ (\neg x_2\ x_4)$

...

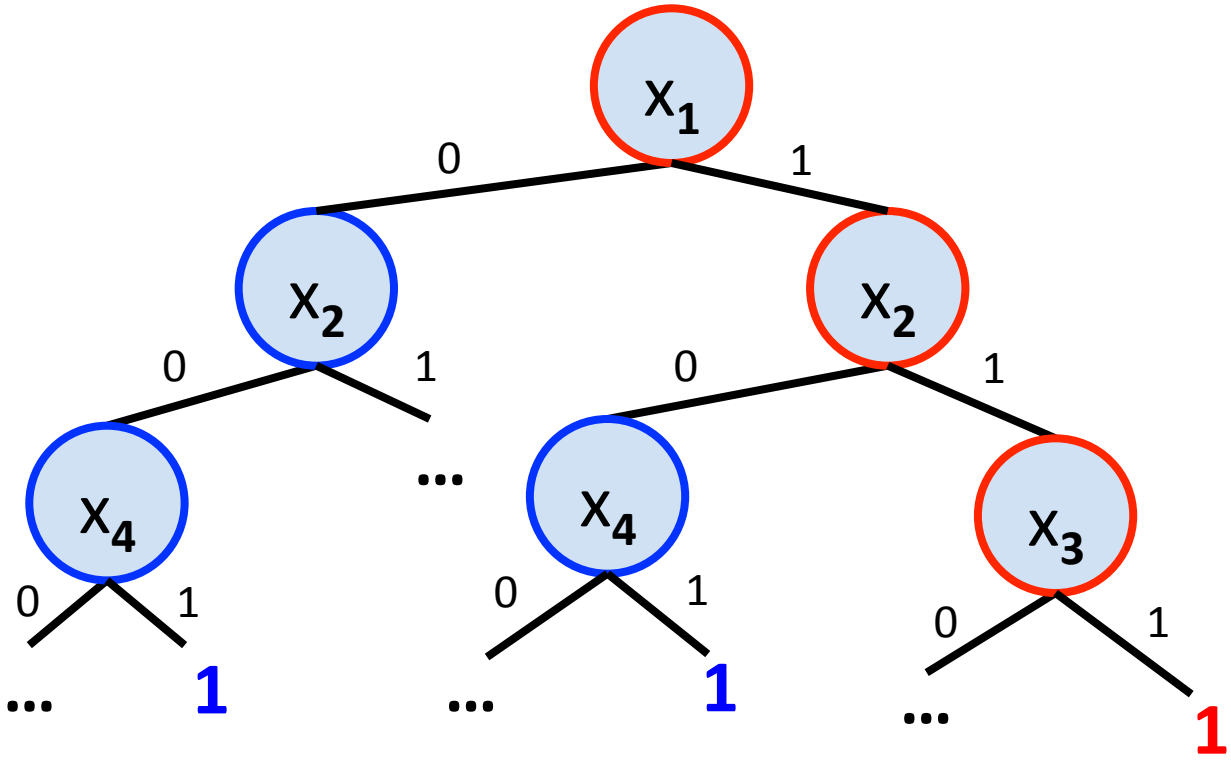


Canonical DT of a DNF

$(x_1\ x_2\ x_3)$

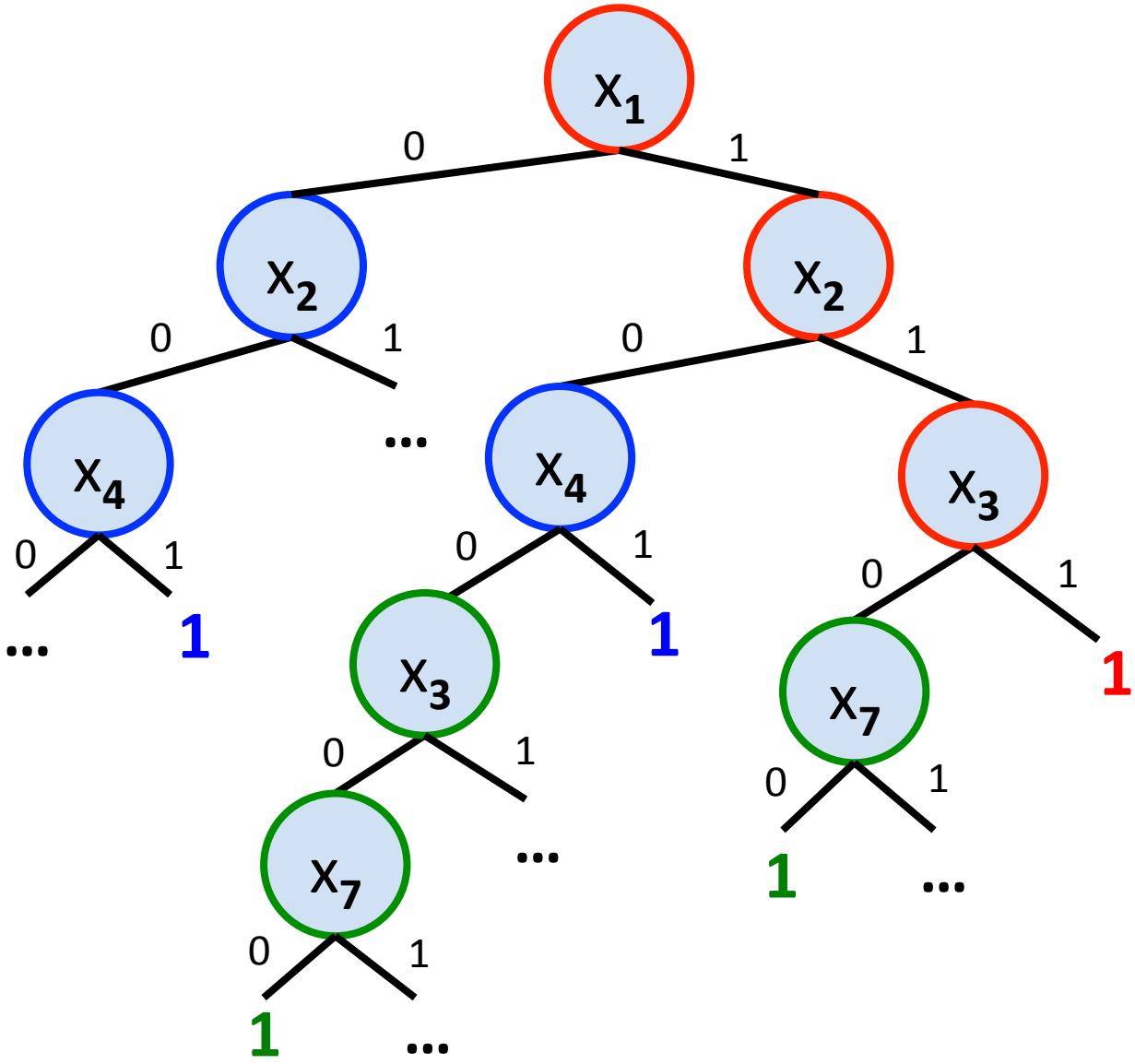
$\vee\ (\neg x_2\ x_4)$

...



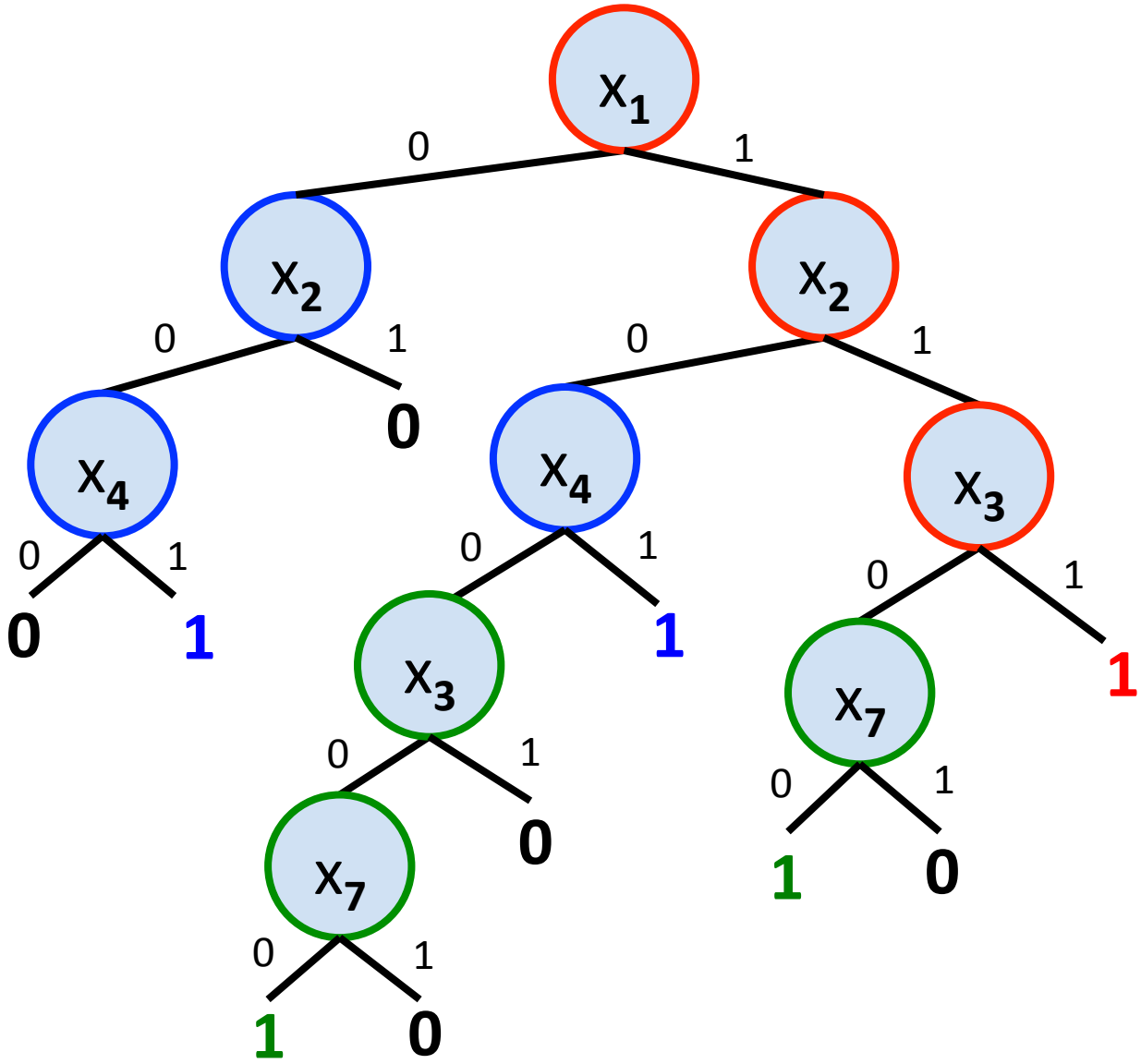
Canonical DT of a DNF

$(x_1\ x_2\ x_3)$
$\vee\ (\neg x_2\ x_4)$
$\vee\ (x_1\ \neg x_3\ \neg x_7)$



Canonical DT of a DNF

$(x_1\ x_2\ x_3)$
$\vee\ (\neg x_2\ x_4)$
$\vee\ (x_1\ \neg x_3\ \neg x_7)$



Restrictions

a.k.a. functions $[n] \to \{0,1,\star\}$

a.k.a. subcubes of $\{0,1\}^n$

Restrictions

- Consider a Boolean function

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

- A *restriction* (w.r.t. the variables of f) is a function

$$R : [n] \to \{0,1,\star\}$$

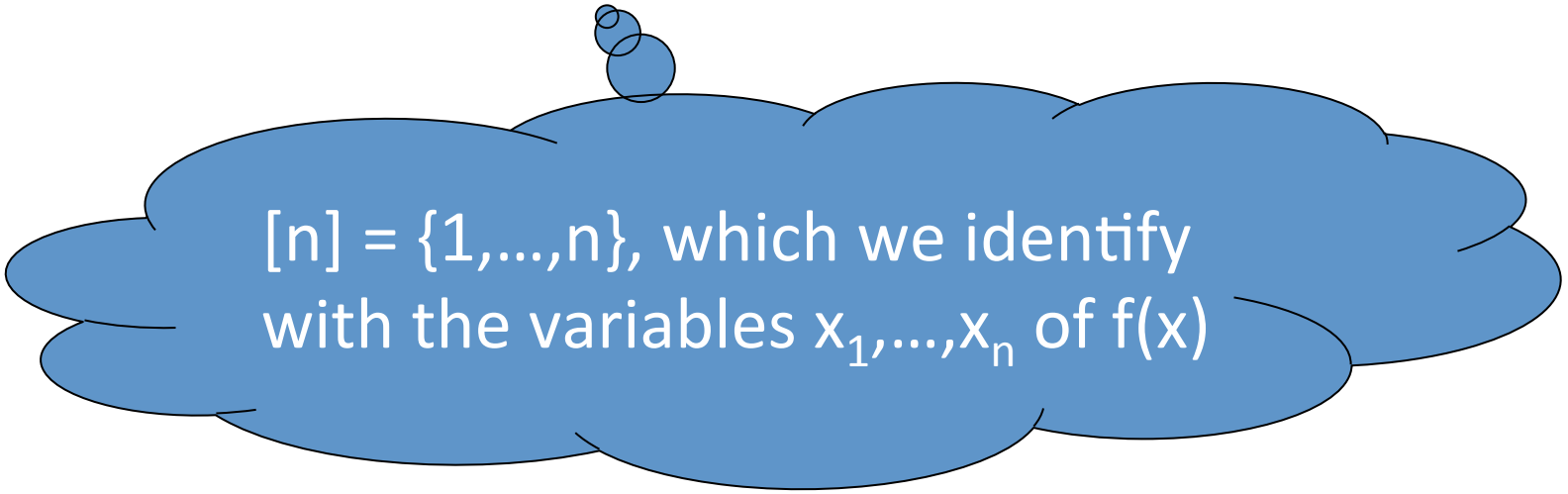
Restrictions

- Consider a Boolean function

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

- A *restriction* (w.r.t. the variables of f) is a function

$$R : [n] \to \{0,1,\star\}$$



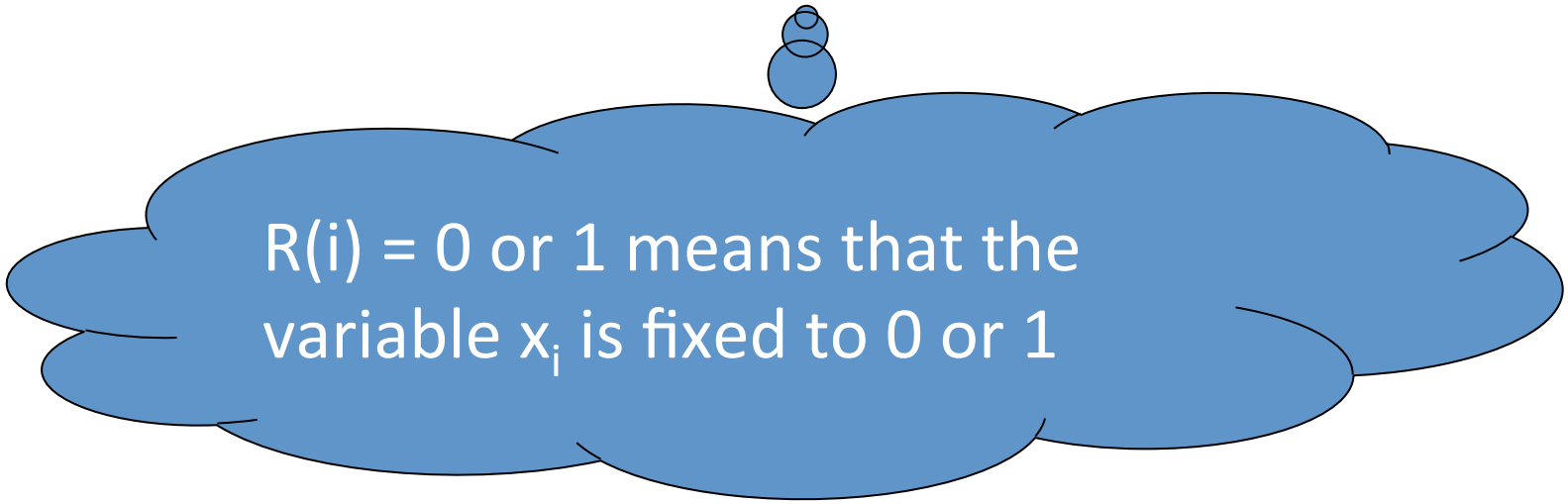
Restrictions

- Consider a Boolean function

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

- A *restriction* (w.r.t. the variables of f) is a function

$$R : [n] \rightarrow \{0,1,\star\}$$



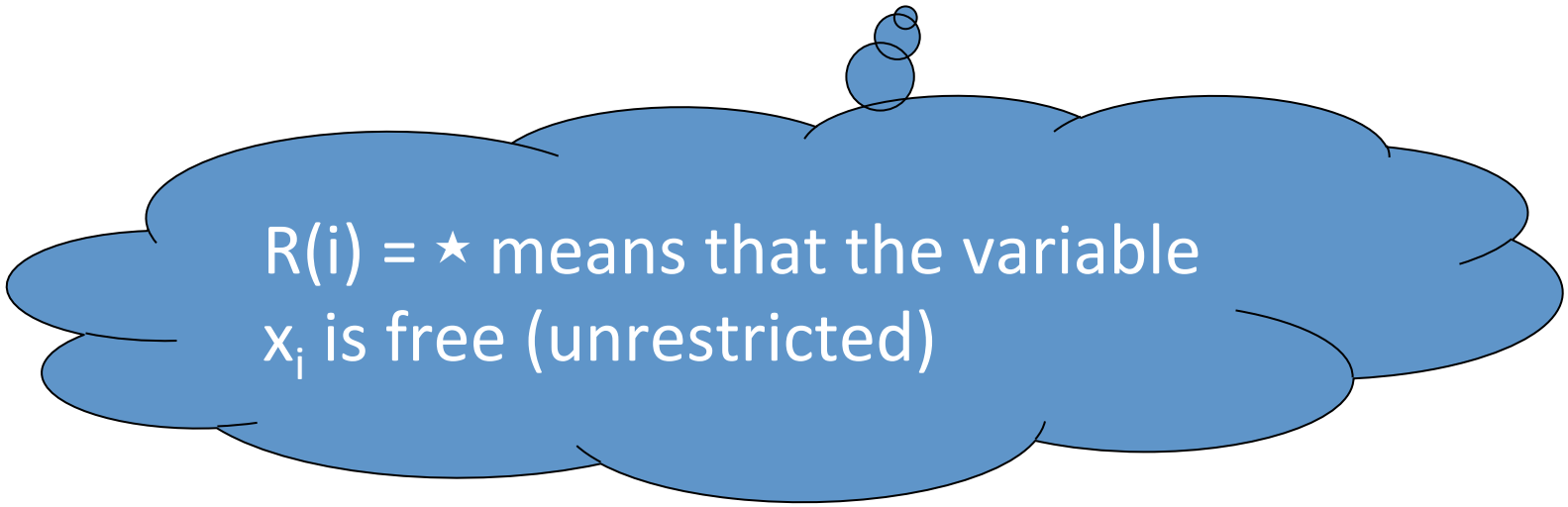
Restrictions

- Consider a Boolean function

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

- A *restriction* (w.r.t. the variables of f) is a function

$$R : [n] \rightarrow \{0,1,\star\}$$



Restrictions

- $f : \{0,1\}^n \to \{0,1\}$
- $R : [n] \to \{0,1,\star\}$
- Applying R to f, we get a Boolean function

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

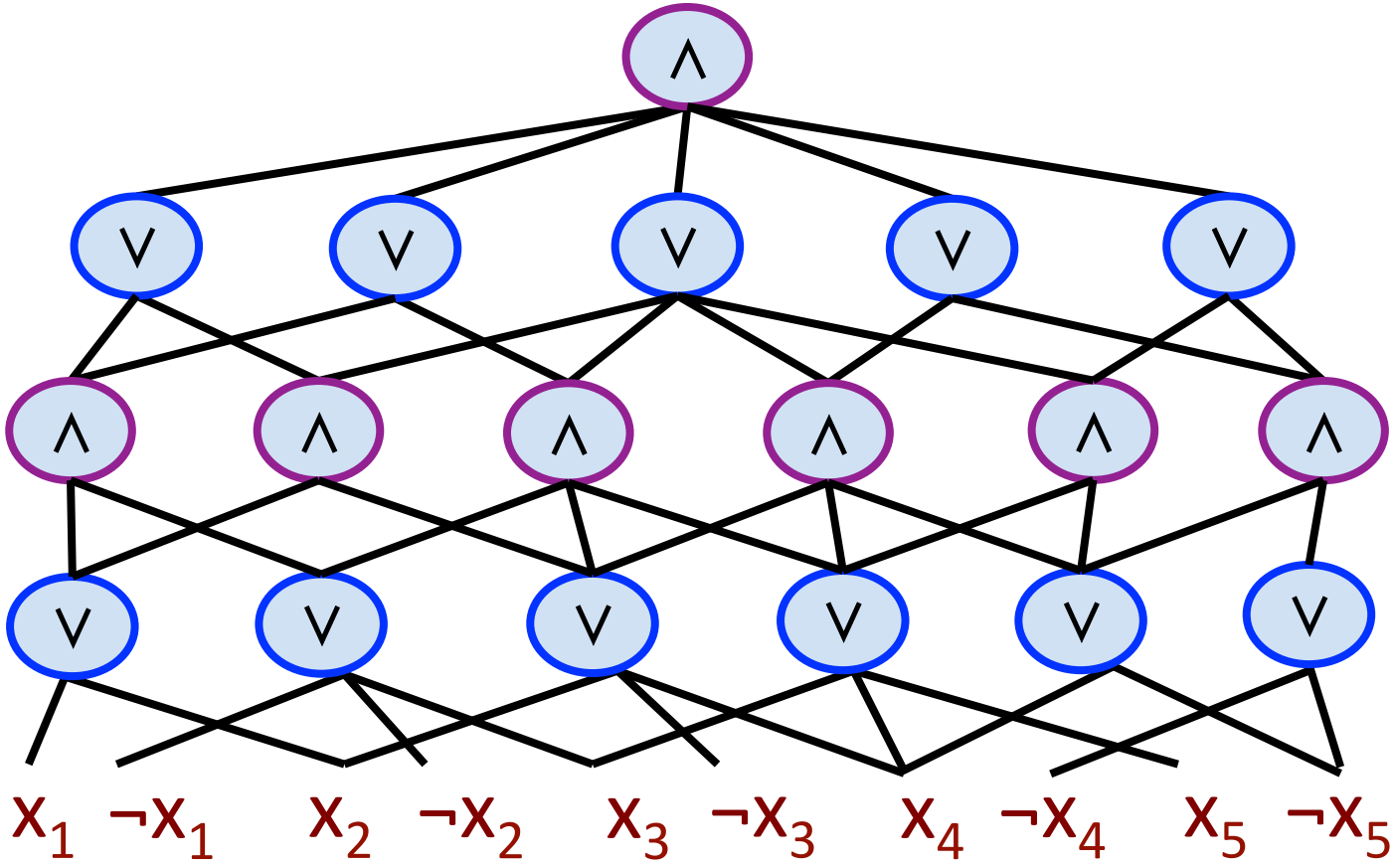
$$\begin{array}{l} R \quad \star 1 \star \star 1\,0 \star 1 \star 1\,0\,0 \star \star 0 \star 0 \star \star \star 0 \star 0 \\ f \restriction R\,(0 \quad 1\,0 \quad\quad 0 \quad 0 \quad\quad\quad 1\,1 \quad 1 \quad 1\,0\,1 \quad 1 \quad) \\ f\,(0\,1\,1\,0\,1\,0\,0\,1\,0\,1\,0\,0\,1\,1\,0\,1\,0\,1\,0\,1\,0) \end{array}$$

Restrictions

- Restrictions are applied *syntactically* to DNFs / CNFs / decision trees / AC^0 circuits, etc.

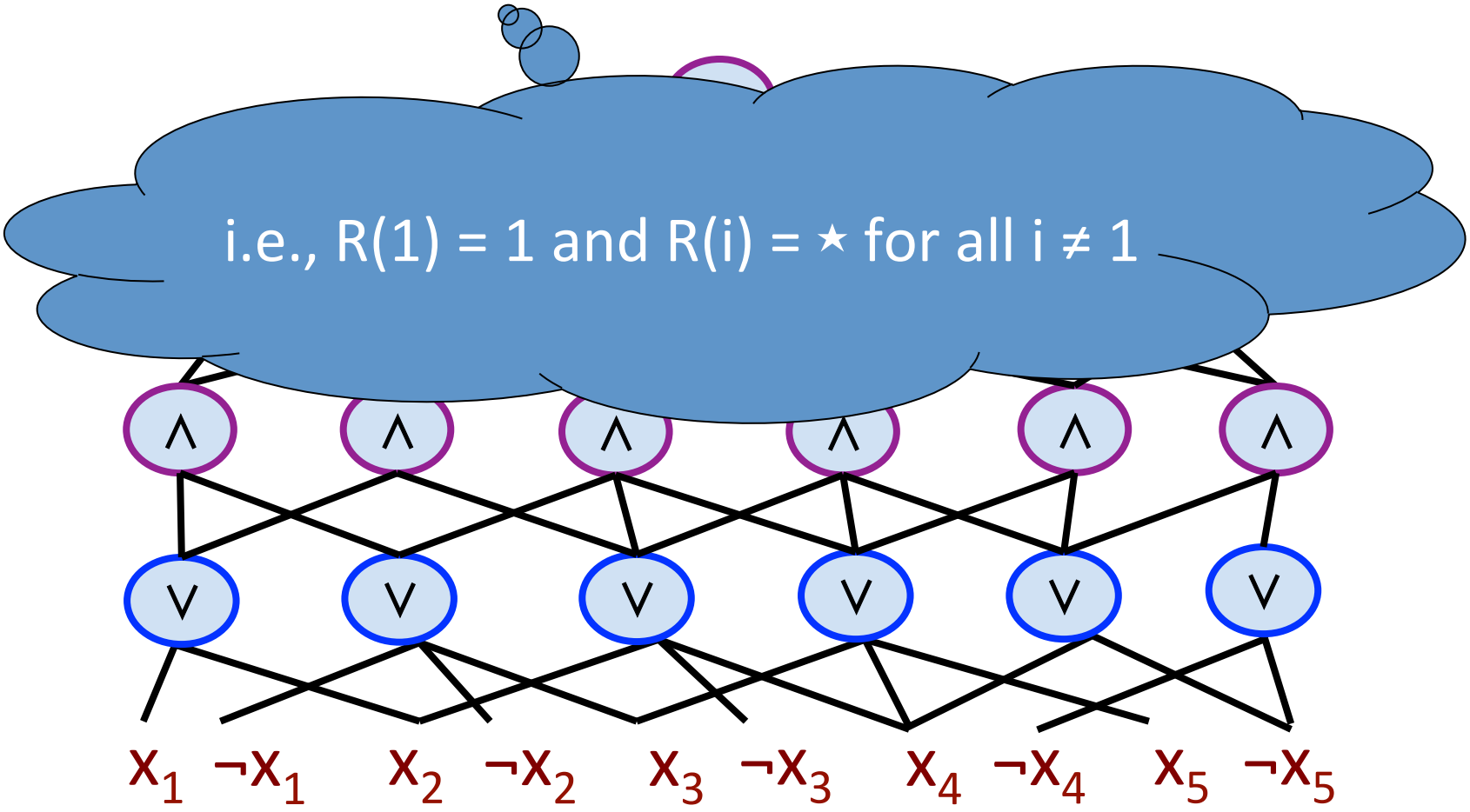
Restricting an AC^0 Circuit

- Consider $R = \{ x_1 \mapsto 1 \}$



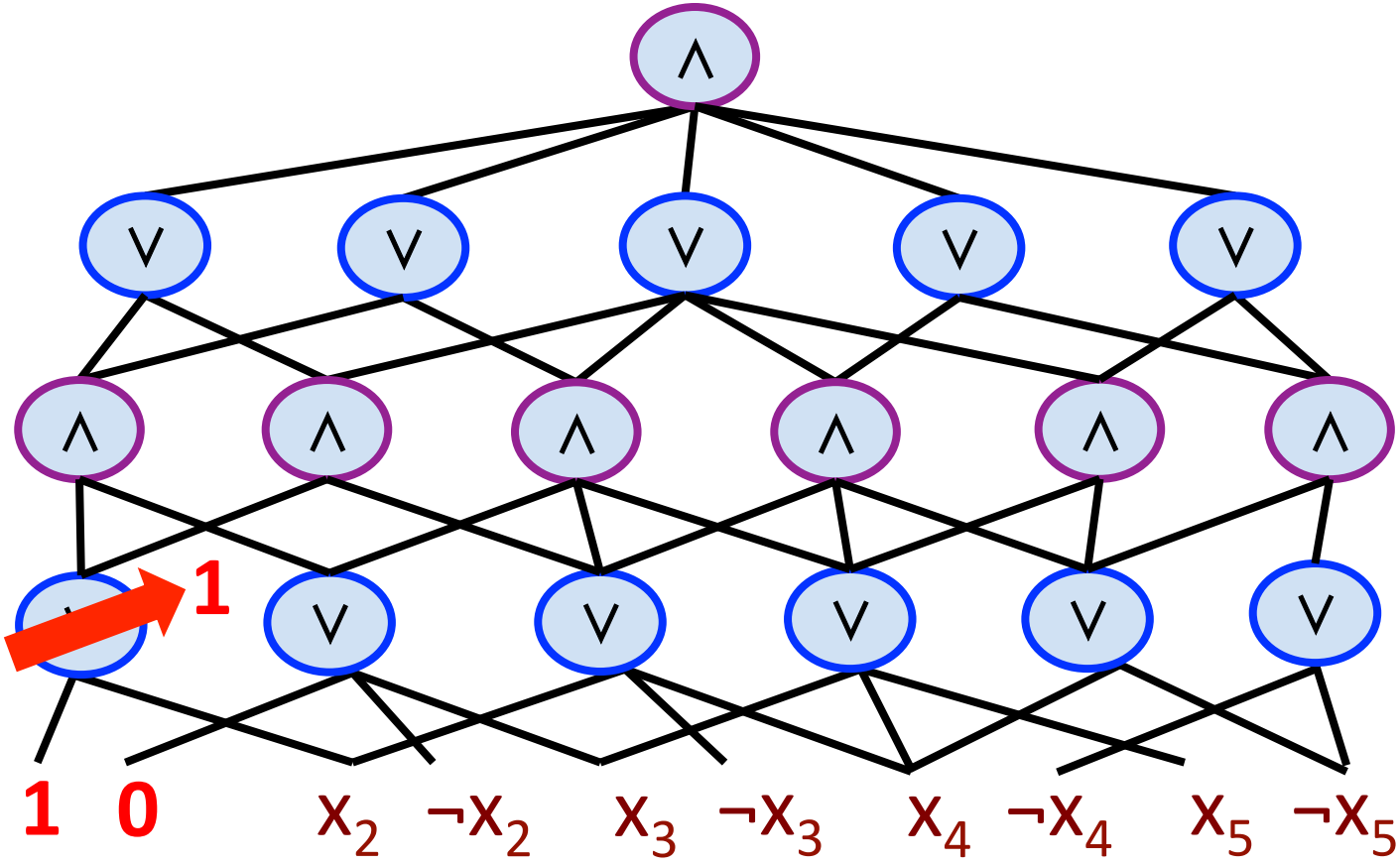
Restricting an AC^0 Circuit

- Consider $R = \{ x_1 \mapsto 1 \}$



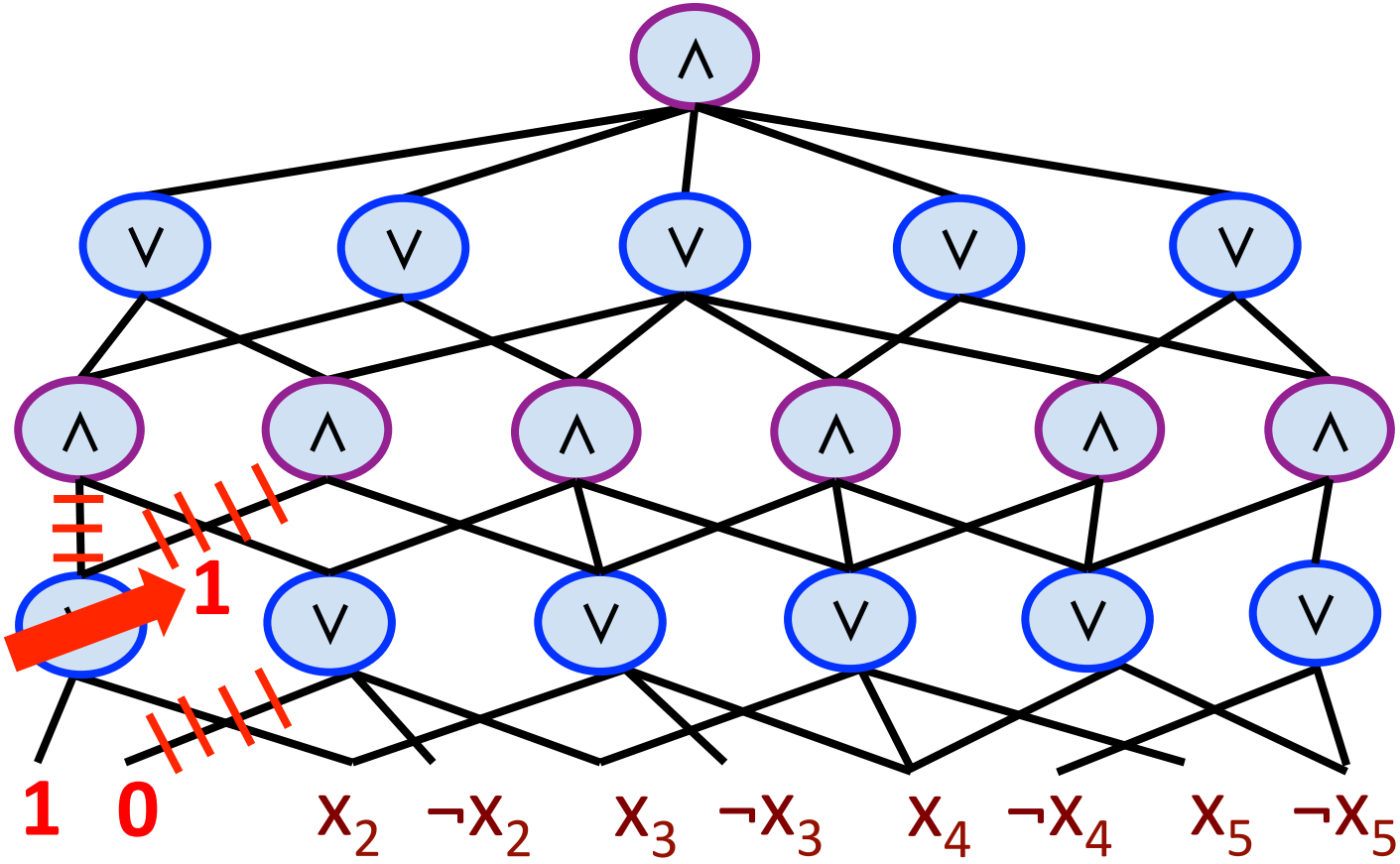
Restricting an AC^0 Circuit

- Consider $R = \{ x_1 \mapsto 1 \}$



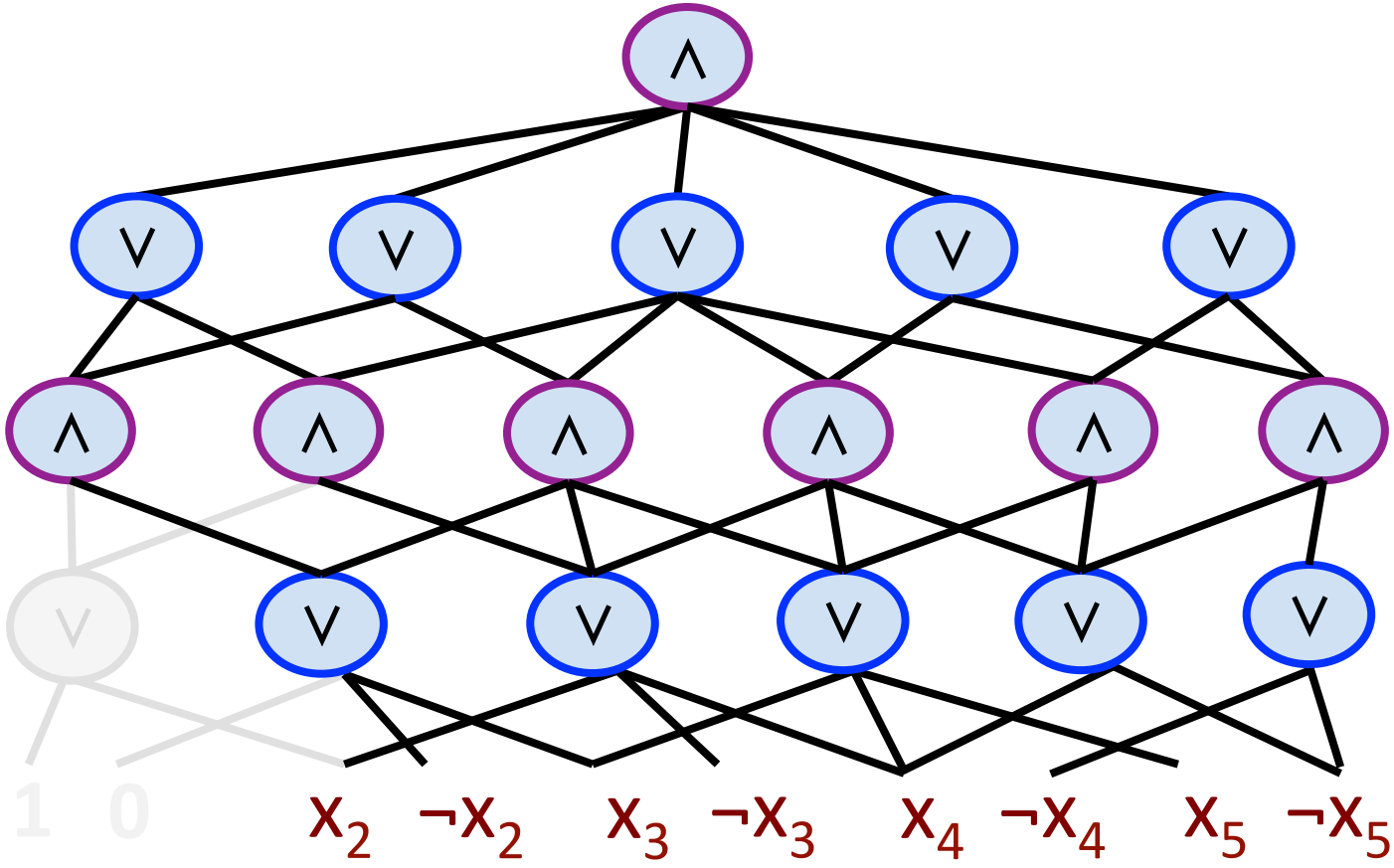
Restricting an AC^0 Circuit

- Consider $R = \{ x_1 \mapsto 1 \}$



Restricting an AC^0 Circuit

- Consider $R = \{ x_1 \mapsto 1 \}$

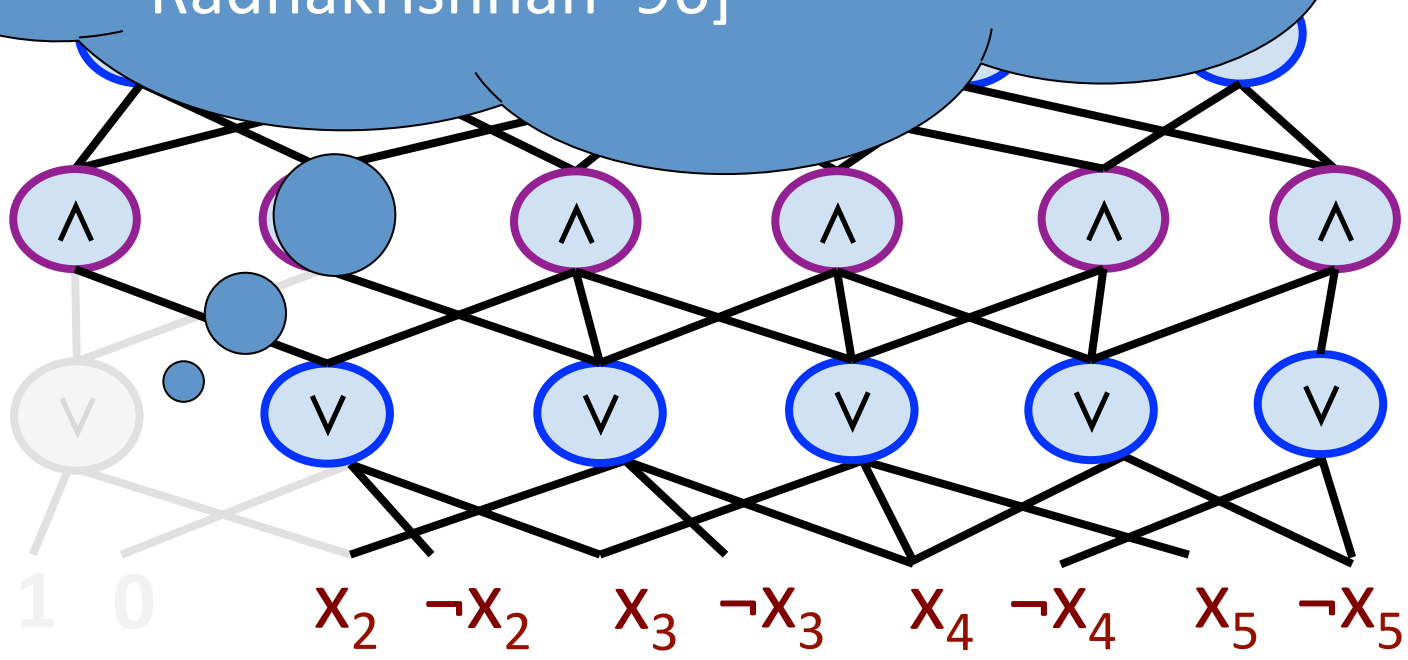


Restricting an AC^0 Circuit

- Co

Gate Elimination Method

$N^{1+1/\exp(d)}$ lower bound against depth-d circuits via *deterministic restrictions* [Chaudhuri & Radhakrishnan '96]



Restricting a DNF

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

$$x_1\, x_2\, \neg x_3 \vee \neg x_1\, x_3\, x_5 \vee x_2\, \neg x_4\, x_5 \vee x_3\, x_4\, \neg x_6 \vee x_7\, x_8\, x_9 \vee \neg x_4\, \neg x_7\, x_9$$

Restricting a DNF

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

$$\underset{1}{x_1}\, x_2\, \neg x_3 \vee \underset{0}{\neg x_1}\, x_3\, x_5 \vee \underset{1}{x_2}\, \neg \underset{0}{x_4}\, x_5 \vee x_3\, \underset{1}{x_4}\, \neg x_6 \vee x_7\, x_8\, x_9 \vee \neg \underset{1}{x_4}\, \neg x_7\, x_9$$

Restricting a DNF

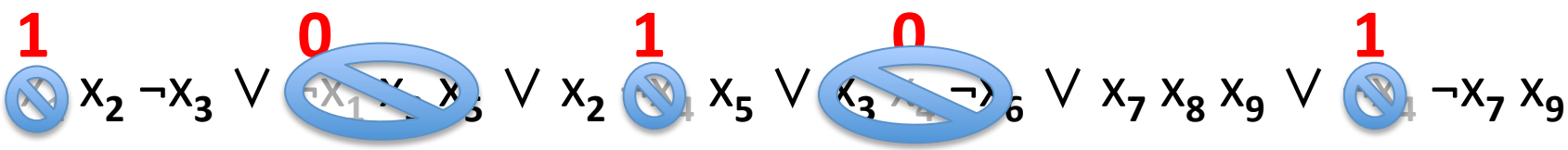
$$R = \{ x_1 \mapsto 1, x_4 \mapsto 0 \}$$

1 0 1 0 1

$x_1\ x_2\ \neg x_3 \vee \neg x_1\ x_3 \vee x_2\ \neg x_4\ x_5 \vee x_3\ x_4\ \neg x_6 \vee x_7\ x_8\ x_9 \vee \neg x_4\ \neg x_7\ x_9$

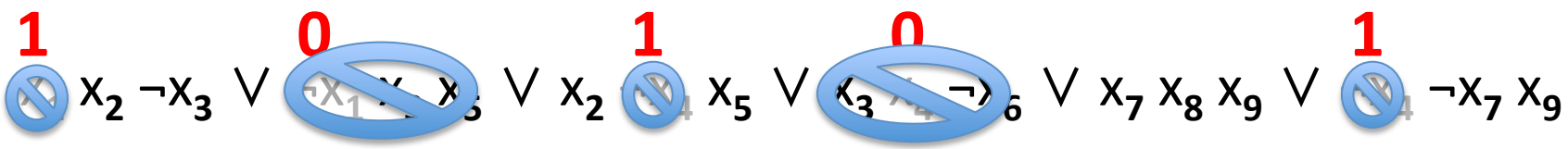
Restricting a DNF

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



Restricting a DNF

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

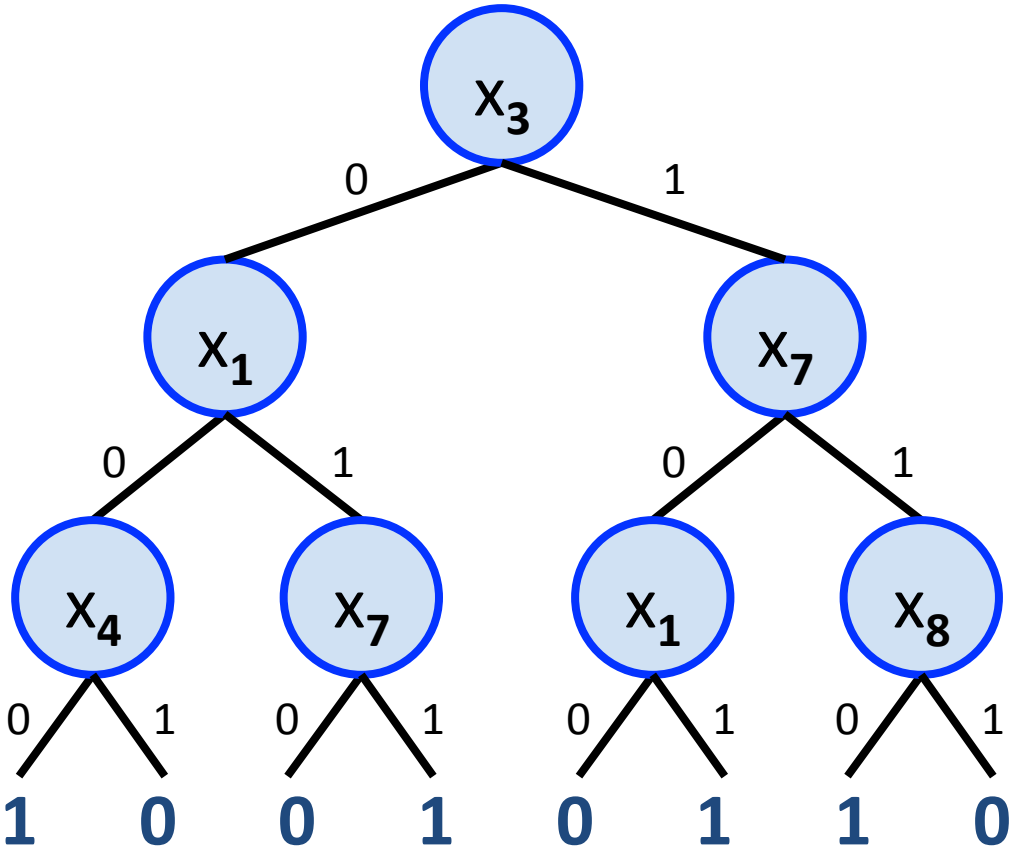


$\upharpoonright R$

$$x_2 \neg x_3 \vee x_2 x_5 \vee x_7 x_8 x_9 \vee \neg x_7 x_9$$

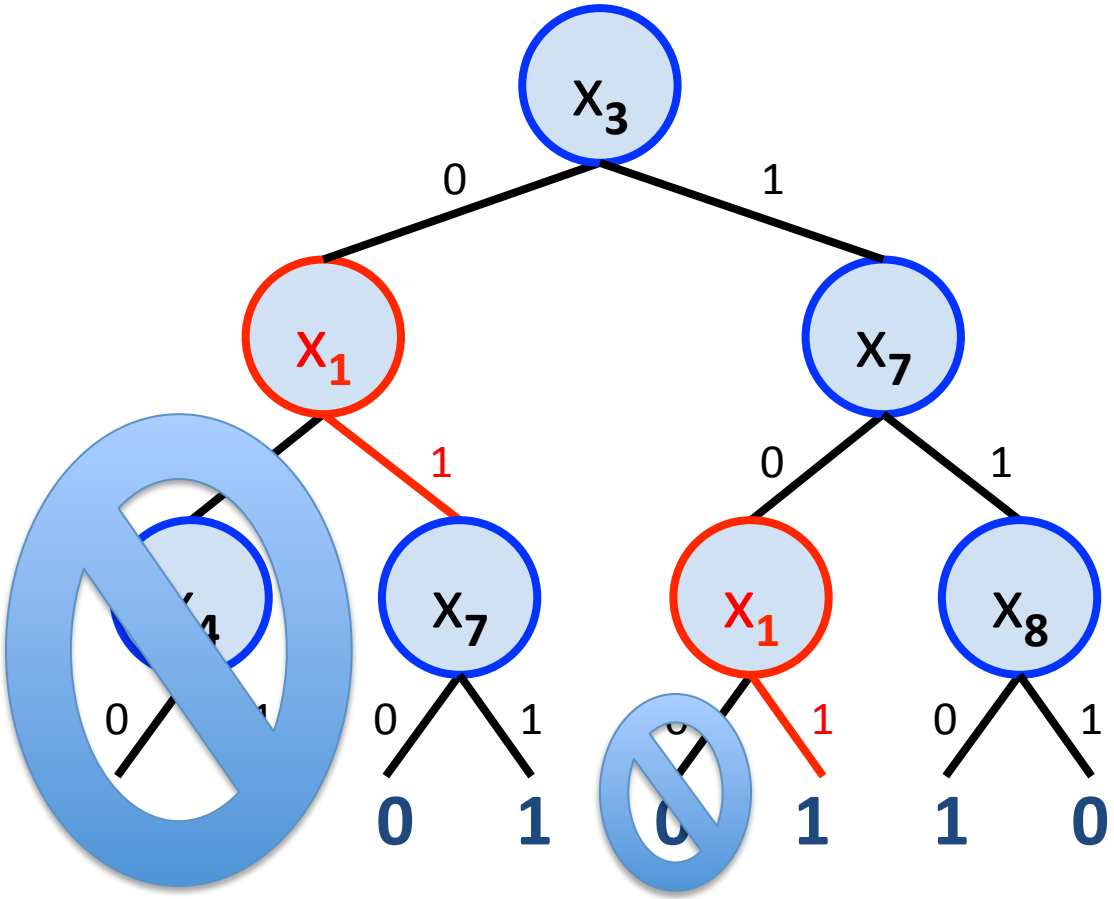
Restricting a Decision Tree

$R = \{ x_1 \mapsto 1 \}$



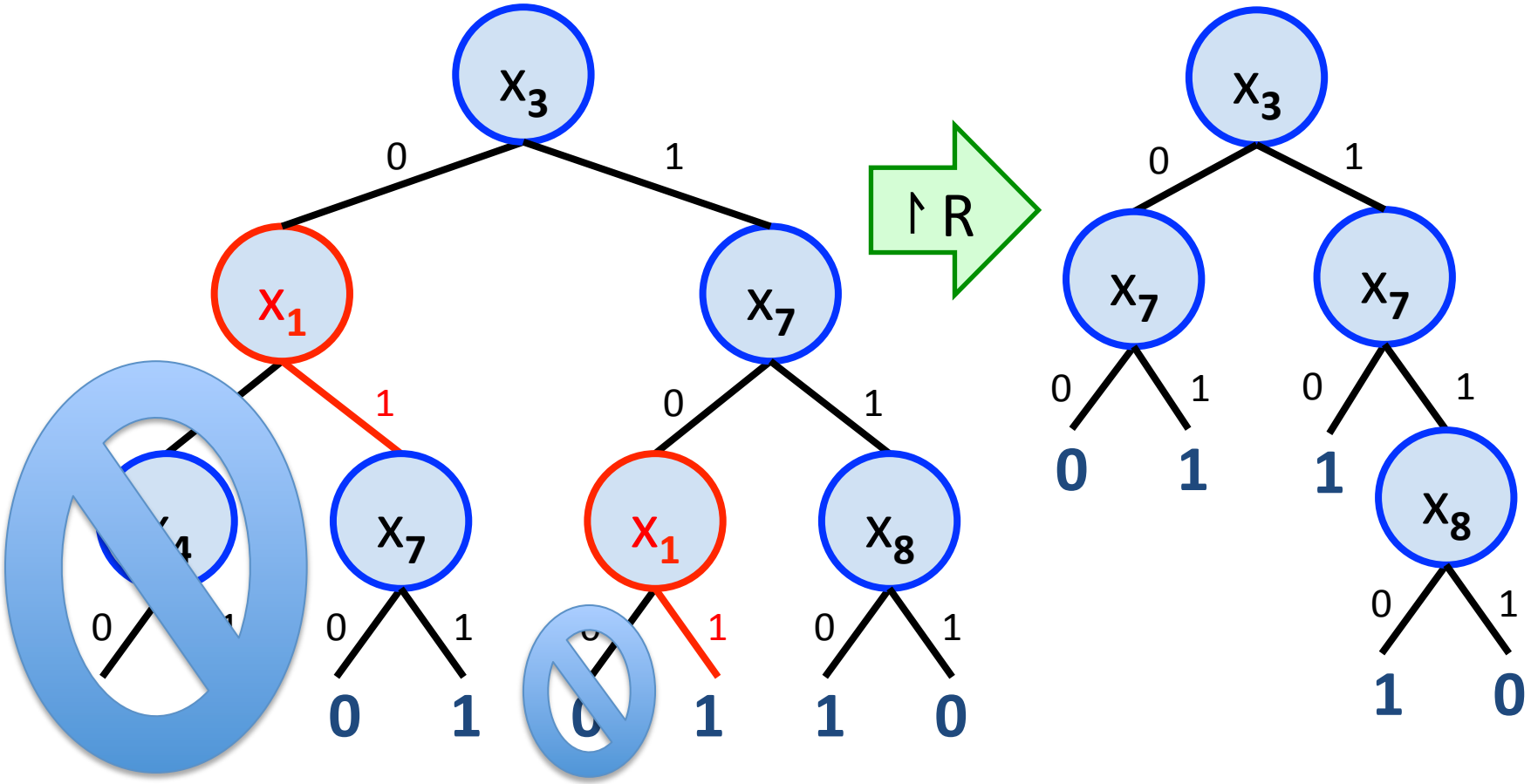
Restricting a Decision Tree

$R = \{ x_1 \mapsto 1 \}$

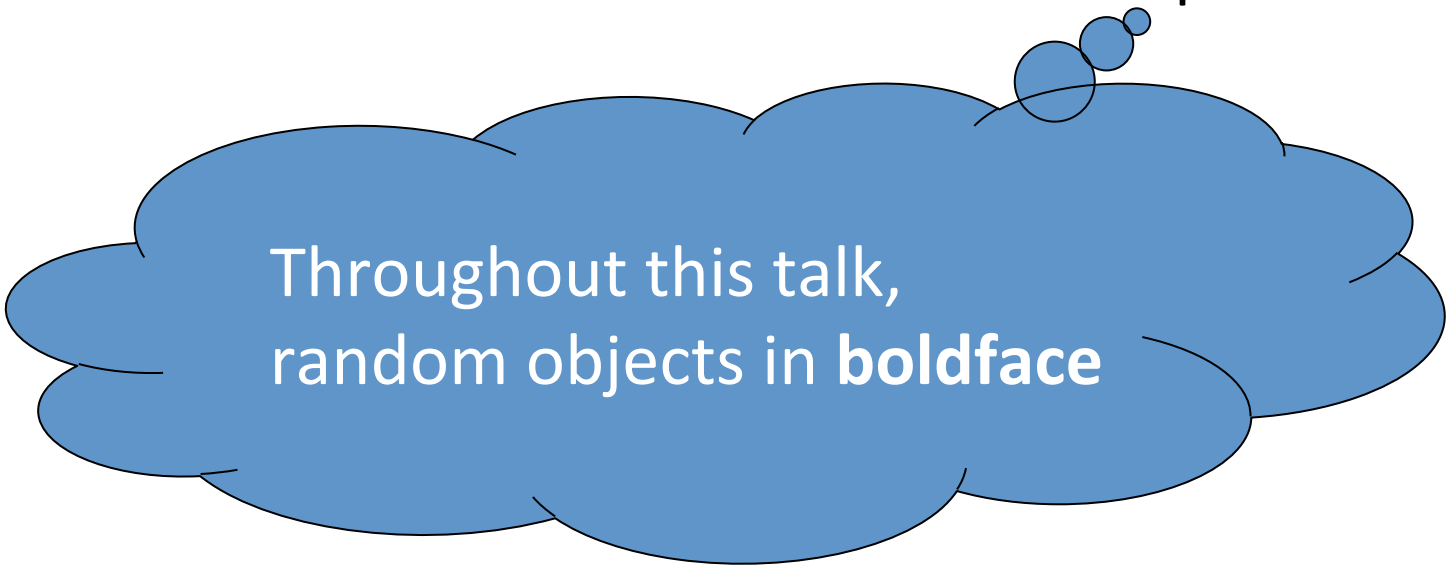


Restricting a Decision Tree

$R = \{ x_1 \mapsto 1 \}$



The Random Restriction $\mathbf{R}_p$



The Random Restriction $\mathbf{R}_p$

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

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

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

Effect of $\mathbf{R}_p$

- $\mathbf{R}_p$ simplifies Boolean functions represented by small decision trees / AC^0 circuits / deMorgan formulas, … [Subbotovskaya '61, …]
- Certain Boolean functions, like PARITY, maintain their complexity under $\mathbf{R}_p$
- => *lower bounds!*

Effect of $\mathbf{R}_p$ on Boolean Functions

- $\mathbf{R}_p$ kills AND_n with very high probability (for $p \leq 1/2$):

$$\Pr[\ \mathrm{AND}_n \restriction \mathbf{R}_p \equiv 0\ ] \geq 1 - (1/2)^{O(n)}$$

Effect of $\mathbf{R}_p$ on Boolean Functions

- $\mathbf{R}_p$ kills AND_n with very high probability (for $p \leq 1/2$):

$$\Pr[\ \mathrm{AND}_n \restriction \mathbf{R}_p \equiv 0\ ] \geq 1 - (1/2)^{O(n)}$$

- On the other hand, for any R with k stars,

$$\mathrm{PARITY}_n \restriction R \ \equiv\ \mathrm{PARITY}_k \text{ or } 1 - \mathrm{PARITY}_k$$

In particular, $\mathrm{DT}_{\mathrm{depth}}(\mathrm{PARITY}_n \restriction \mathbf{R}_p) \approx pn$ with high prob

Effect of $\mathbf{R}_p$ on Decision Trees

Decision Tree Switching Lemma

If T is a depth-k decision tree, then

$$\Pr[\ \text{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ] \leq (2pk)^{\ell}$$

Effect of $\mathbf{R}_p$ on Decision Trees

Decision Tree Switching Lemma

If T is a depth-k decision tree, then

$$\Pr[\ \text{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ] \leq (2pk)^{\ell}$$

$\leq 2^{-\ell}$ when $p \leq 1/4k$

Effect of $\mathbf{R}_p$ on DNFs

Decision Tree Switching Lemma

If T is a depth-k decision tree, then

$$\Pr[\ \mathrm{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ] \leq (2pk)^{\ell}$$

Hastad's Switching Lemma (1986)

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

$$\Pr[\ \mathrm{DT}_{\mathrm{depth}}(F \restriction \mathbf{R}_p) \geq \ell\ ] \leq (5pk)^{\ell}$$

Effect of $\mathbf{R}_p$ on DNFs

Decision Tree Switching Lemma

If T is a depth-k decision tree

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

Hastad's Switching Lemma (1986)

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

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

Effect of $\mathbf{R}_p$ on DNFs

Corollary (usual statement of the S.L.)

If F is a k-DNF, then

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

Hastad's Switching Lemma (1986)

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

$$\Pr[\ \mathrm{DT}_{\mathrm{depth}}(F \restriction \mathbf{R}_p) \geq \ell\ ] \leq (5pk)^{\ell}$$

Effect of $\mathbf{R}_p$ on ~~DNFs~~ CNFs

Corollary (usual statement of the S.L.)

If F is a k-CNF, then

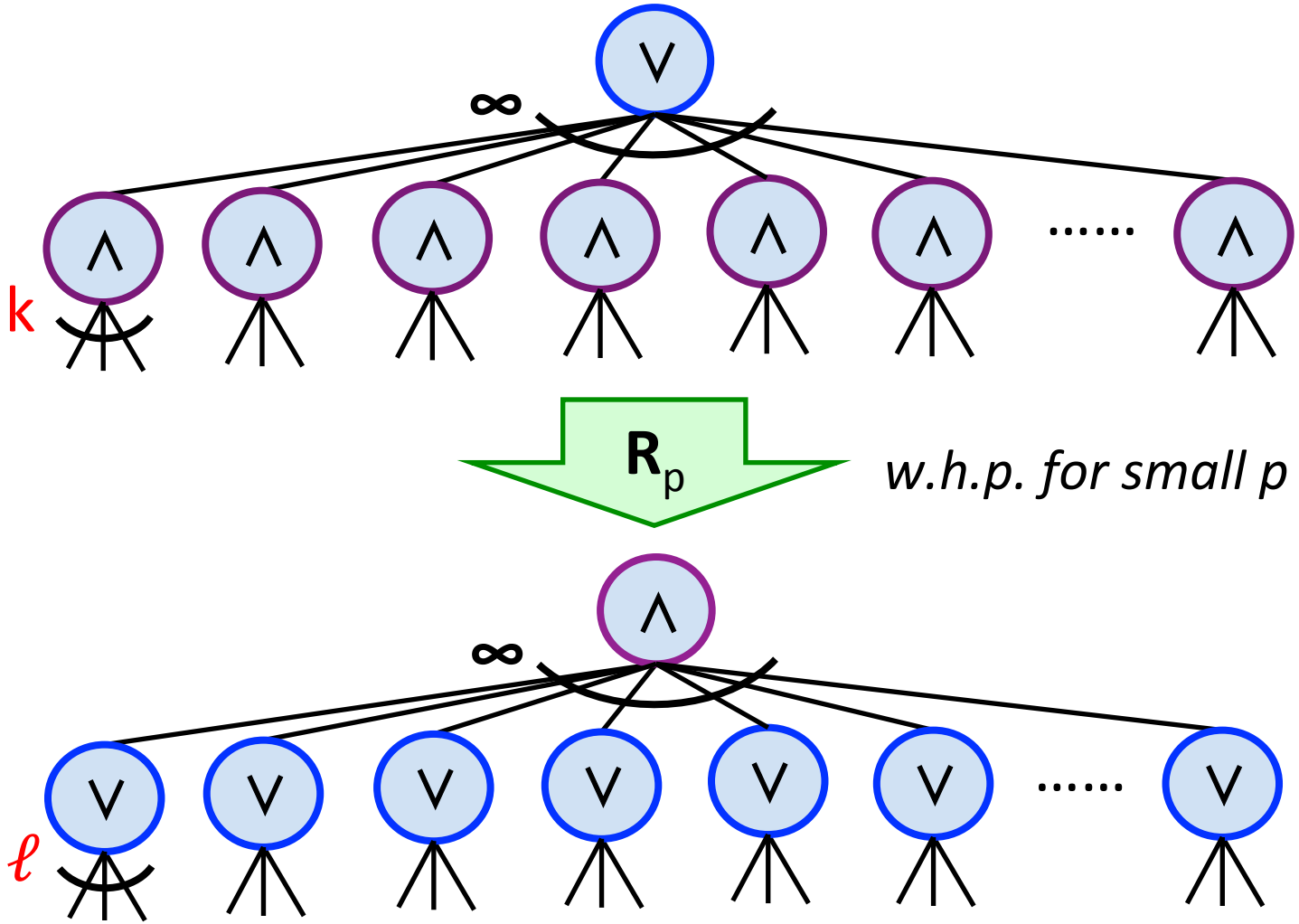
$$\Pr[F \restriction \mathbf{R}_p \text{ is not equivalent to an } \ell\text{-DNF }] \leq (5pk)^{\ell}$$

Hastad's Switching Lemma (1986)

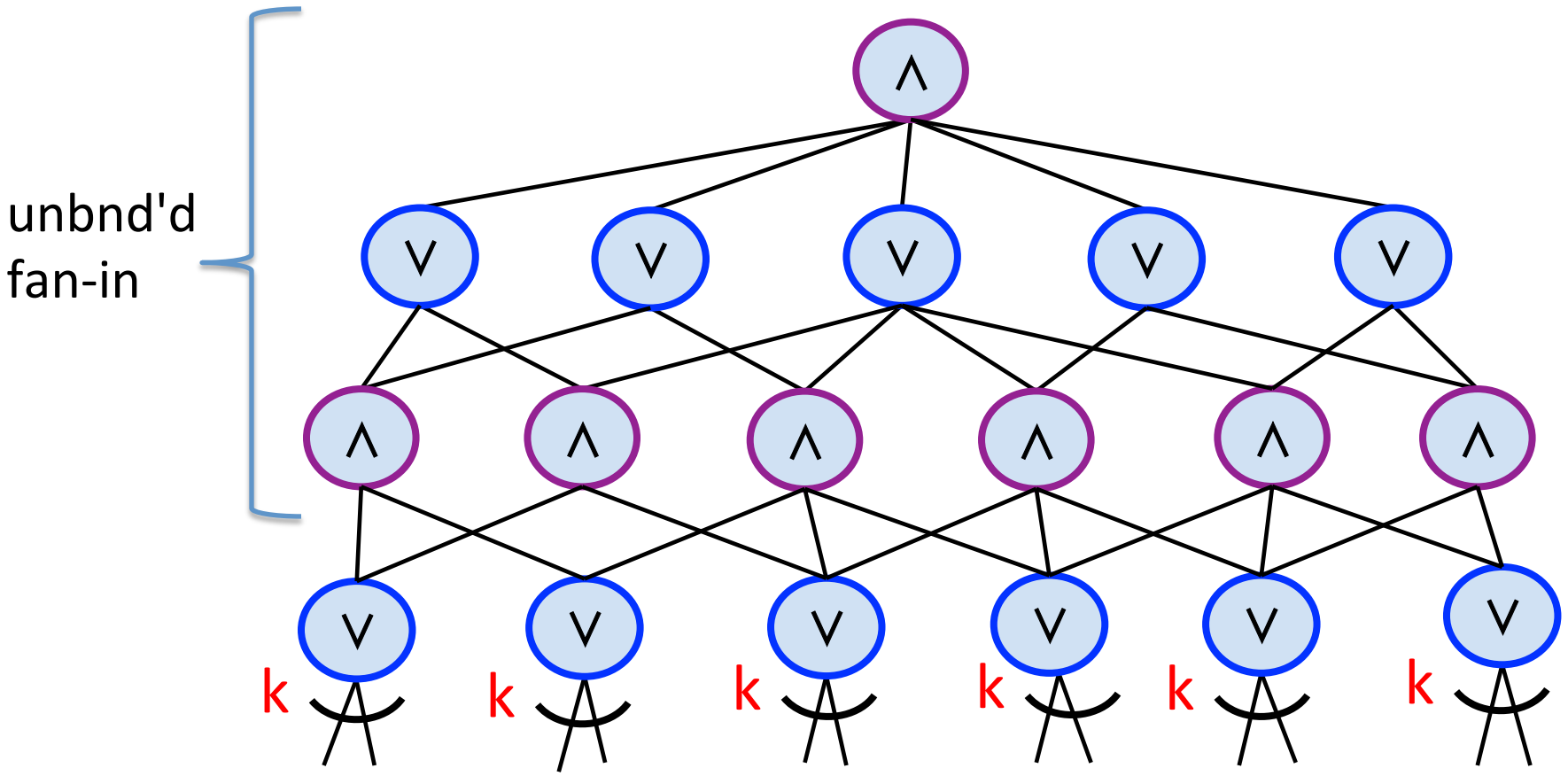
If F is a k-CNF (i.e. AND_∞ of depth-k decision trees), then

$$\Pr[\ \text{DT}_{\text{depth}}(F \restriction \mathbf{R}_p) \geq \ell\ ] \leq (5pk)^{\ell}$$

Effect of $\mathbf{R}_p$ on DNFs



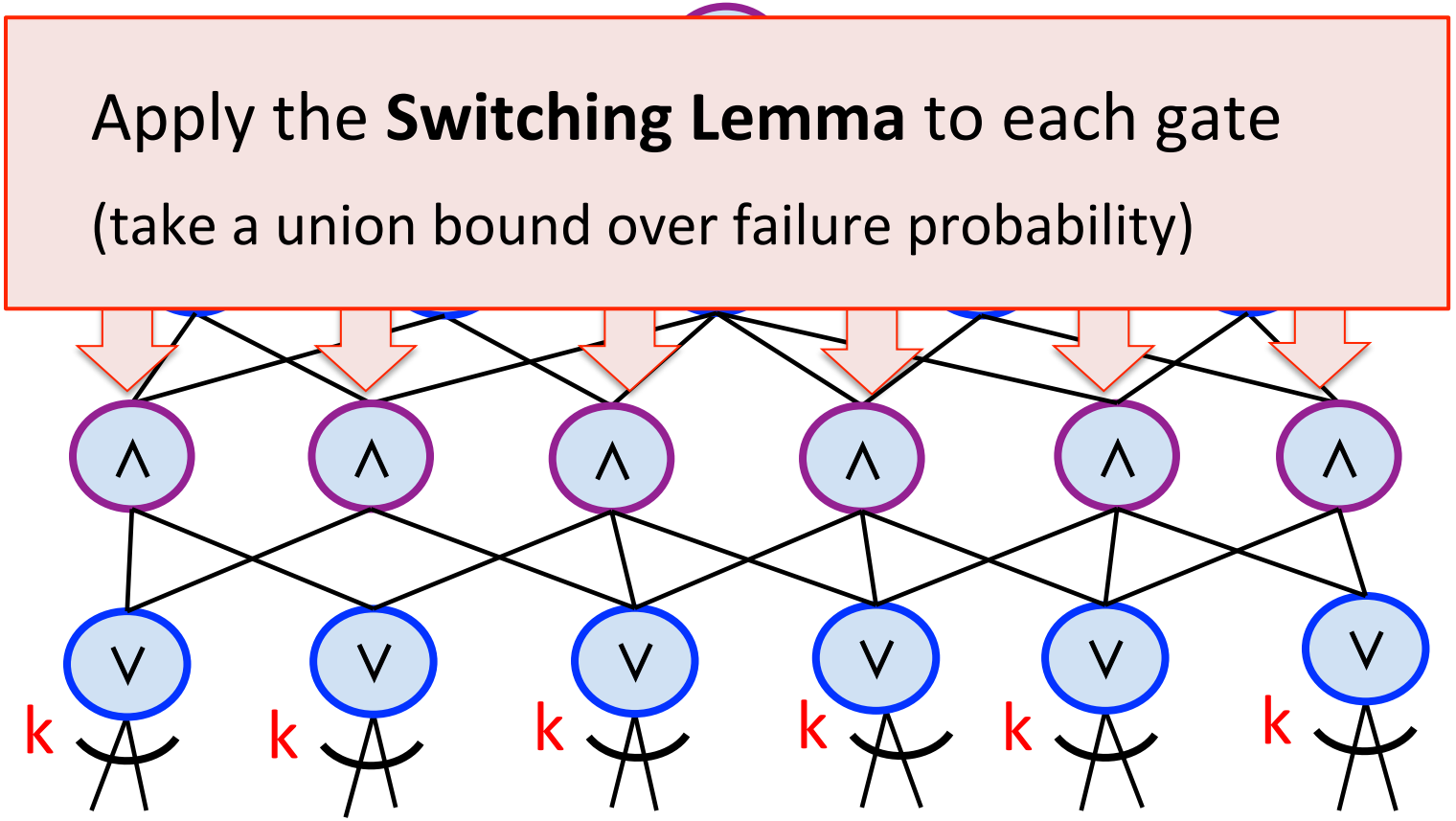
Depth Reduction



Depth Reduction

Apply the **Switching Lemma** to each gate

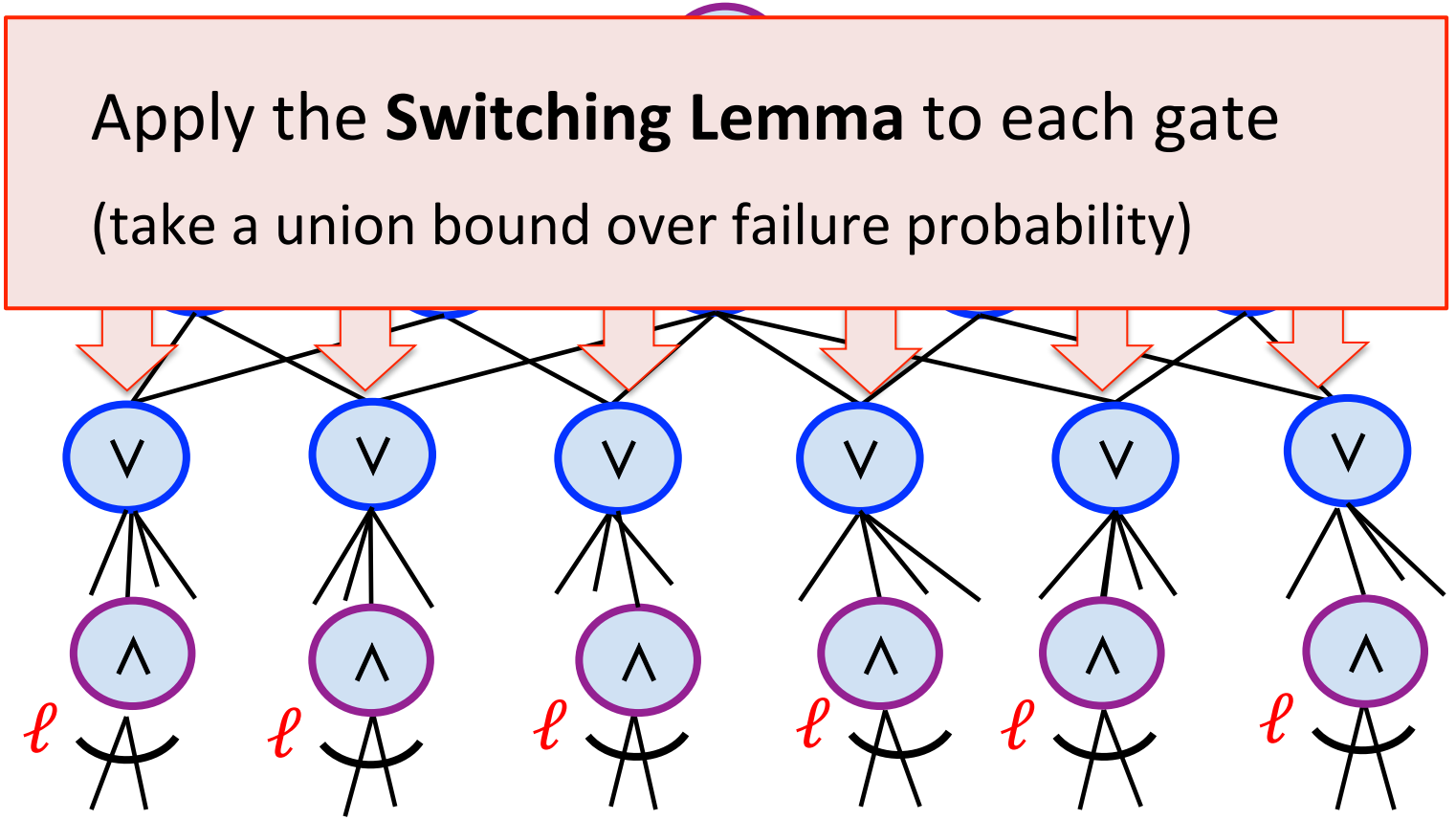
(take a union bound over failure probability)



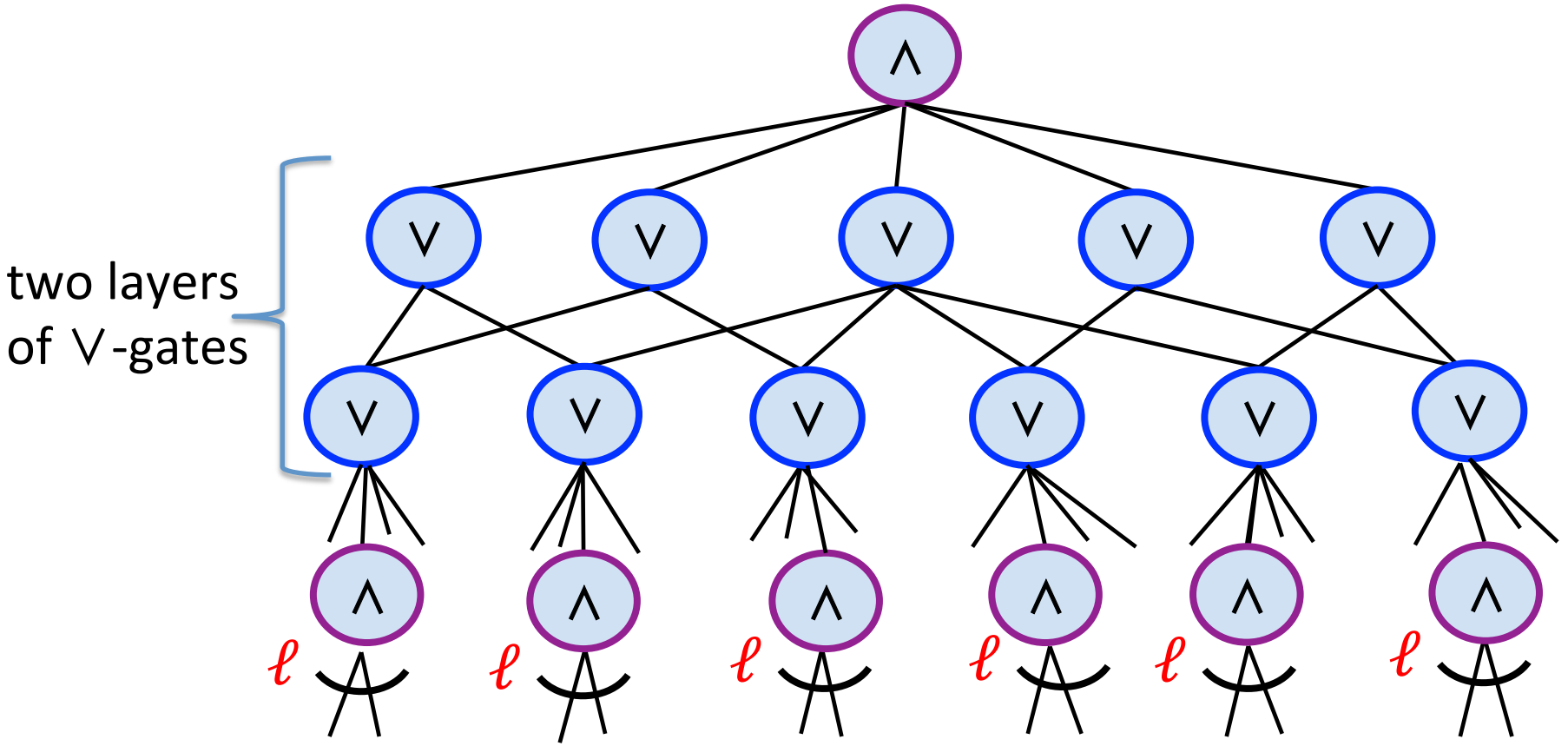
Depth Reduction

Apply the **Switching Lemma** to each gate

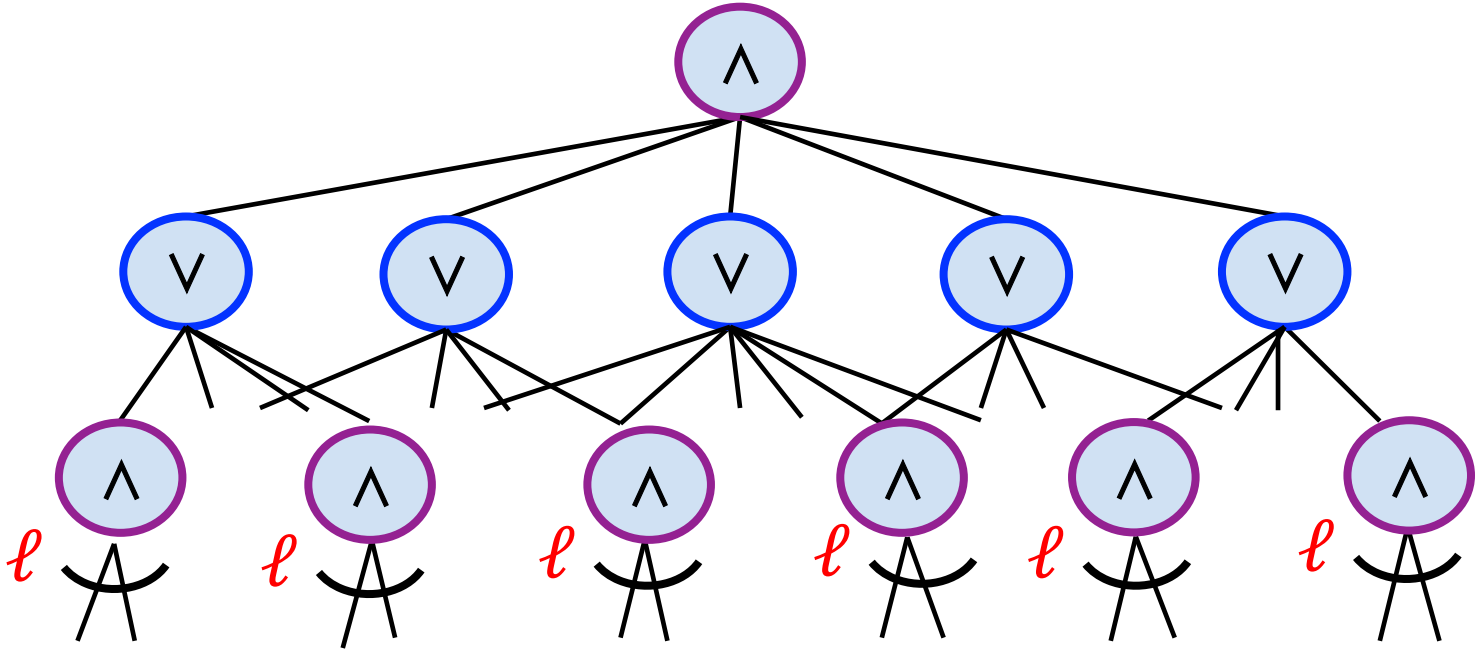
(take a union bound over failure probability)



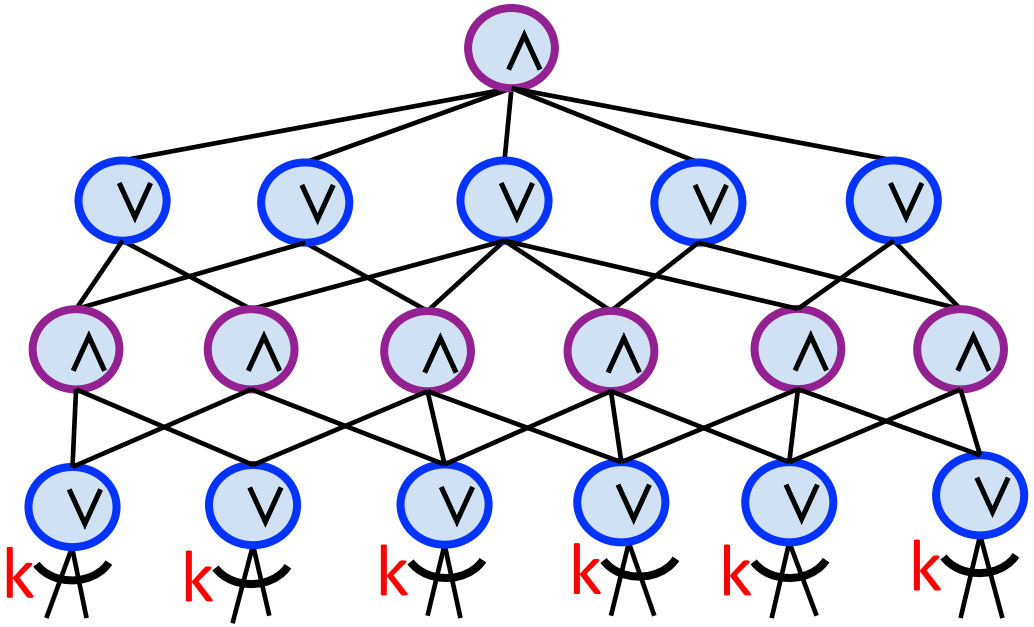
Depth Reduction



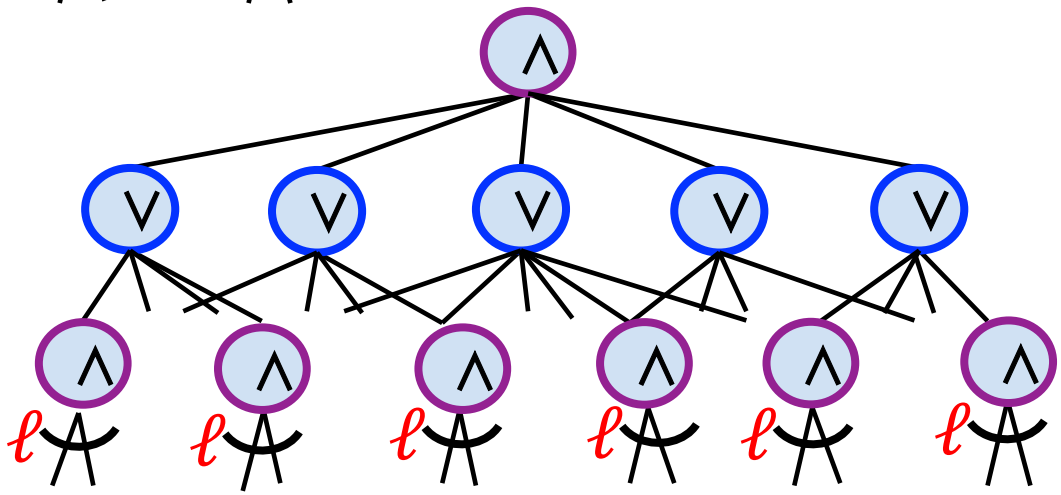
Depth Reduction



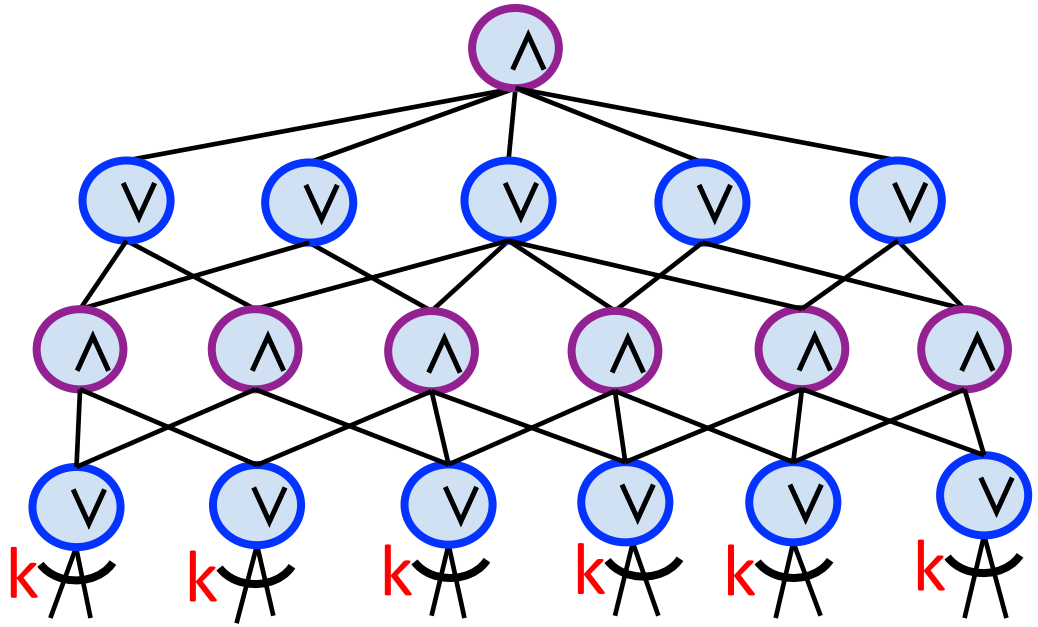
Depth Reduction



Applying the S.L. to the bottom-2 layers

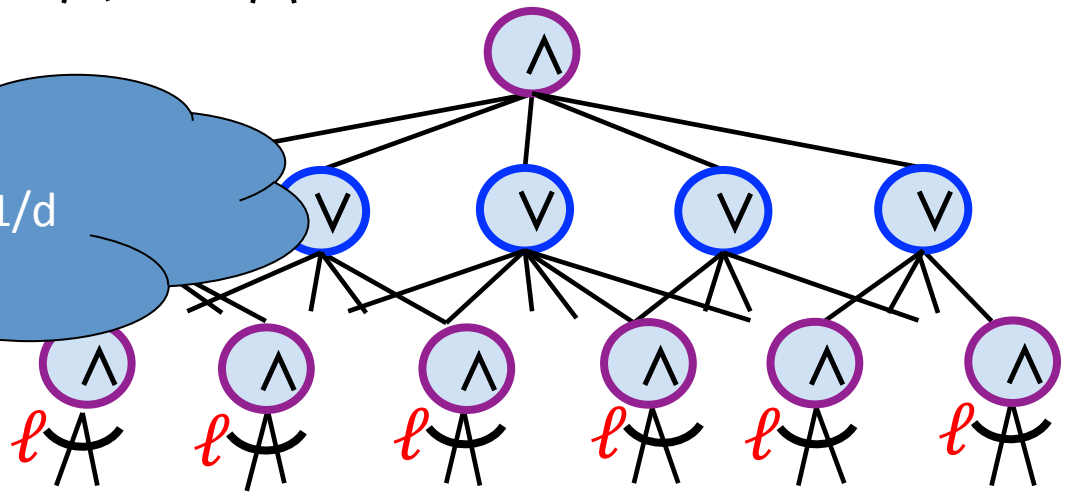


Depth Reduction

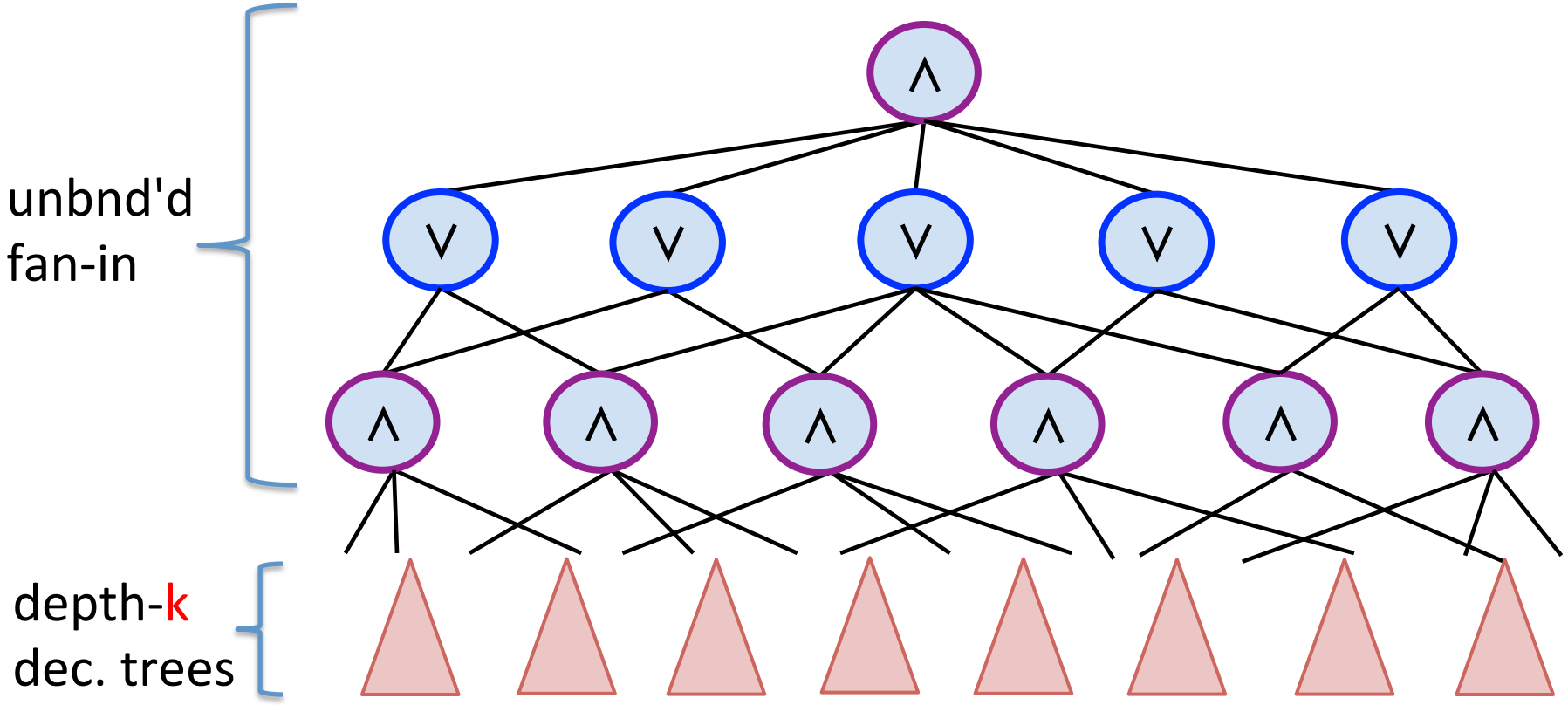


Applying the S.L. to the bottom-2 layers

typically, $k = \ell \approx n^{1/d}$



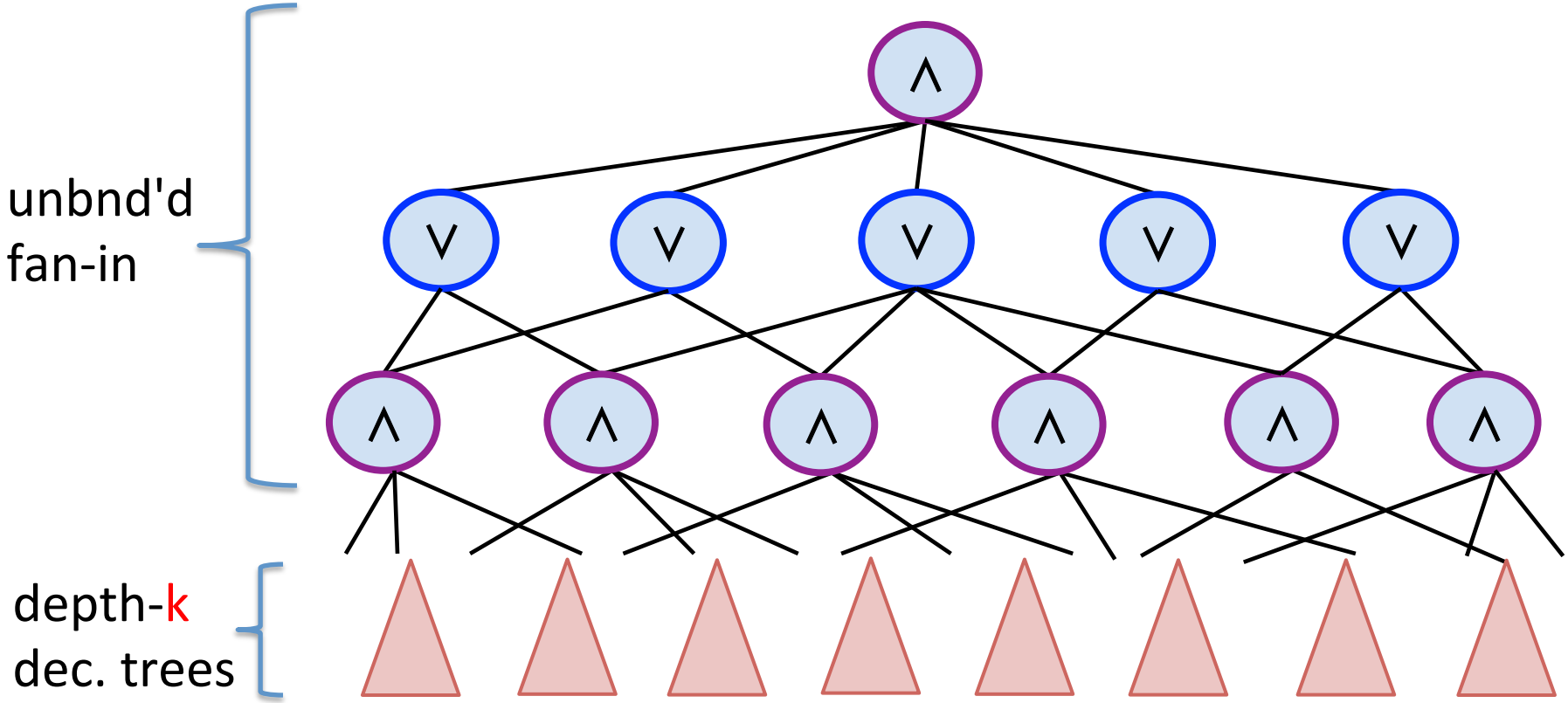
Depth Reduction



Hastad's Switching Lemma (decision tree version)

If $T_1, \ldots, T_m$ are depth-k decision trees, then

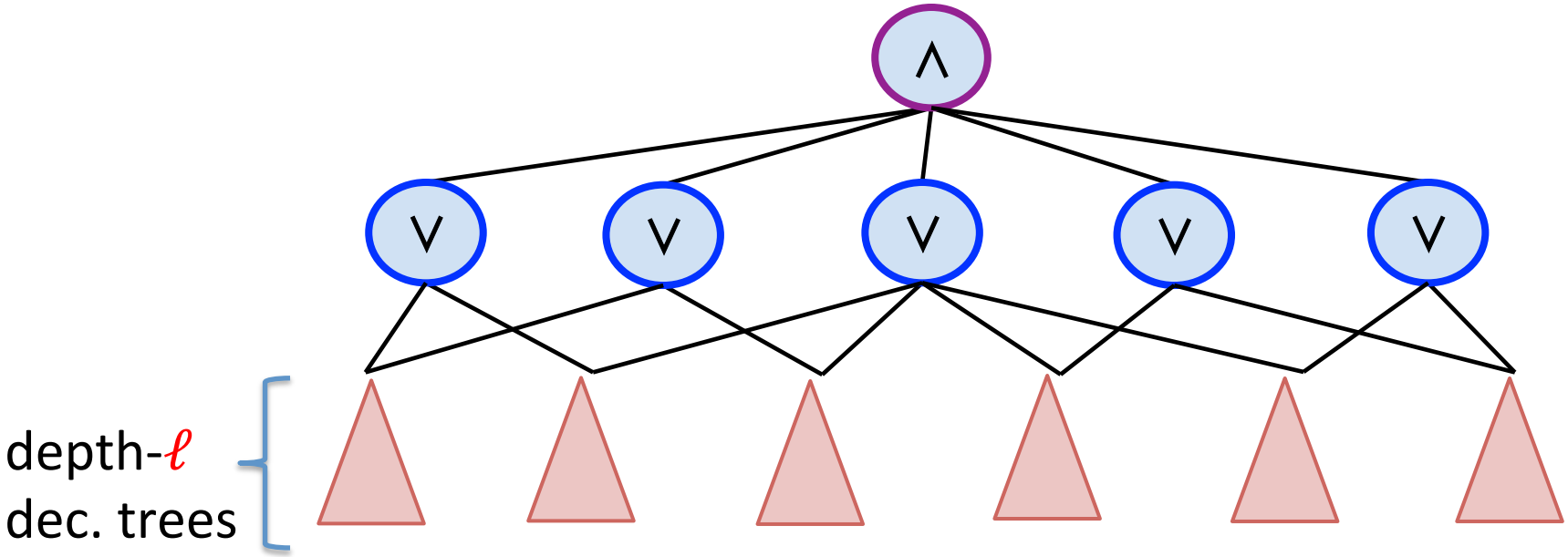
$$\Pr[\, DT_{depth}((T_1 \wedge \cdots \wedge T_m) \restriction \mathbf{R}_p) \geq \ell \,] \leq (5pk)^{\ell}$$



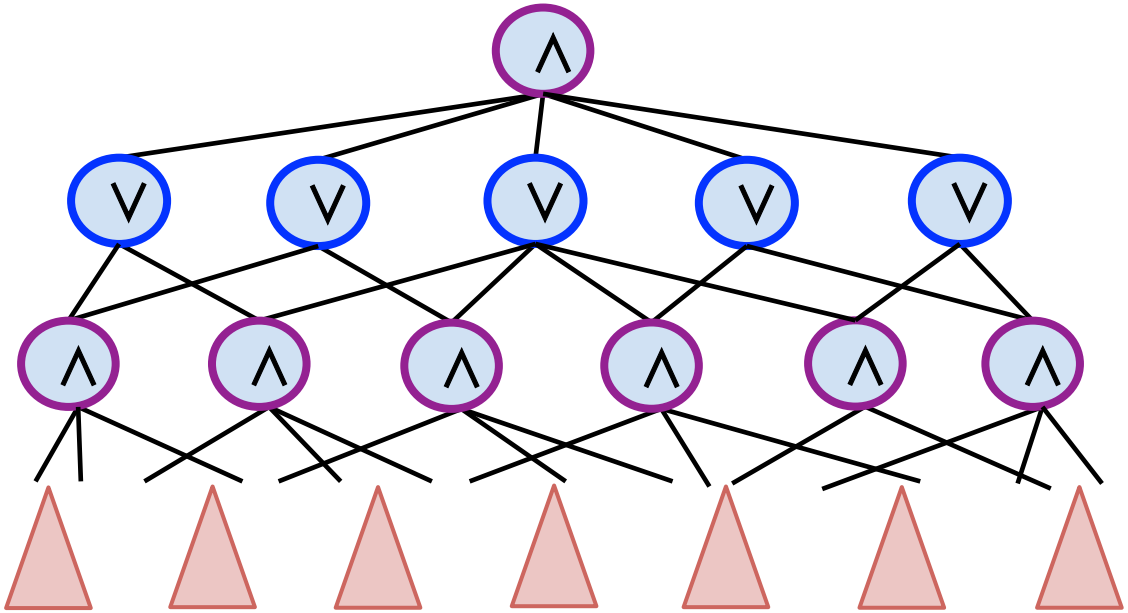
Hastad's Switching Lemma (decision tree version)

If $T_1, \ldots, T_m$ are depth-k decision trees, then

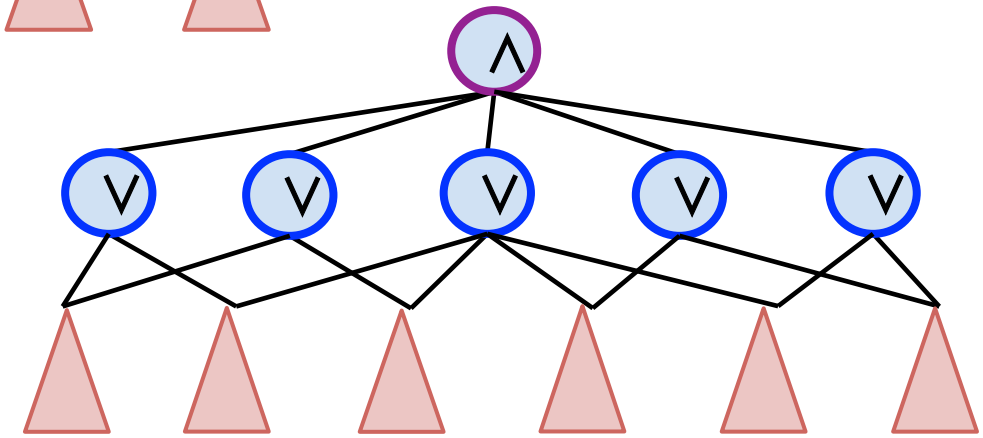
$$\Pr[\, DT_{depth}((T_1 \wedge \cdots \wedge T_m) \restriction \mathbf{R}_p) \geq \ell \,] \leq (5pk)^{\ell}$$



Depth Reduction



applying the S.L. to the bottom layer of gates



PARITY Lower Bound

Hastad ’86

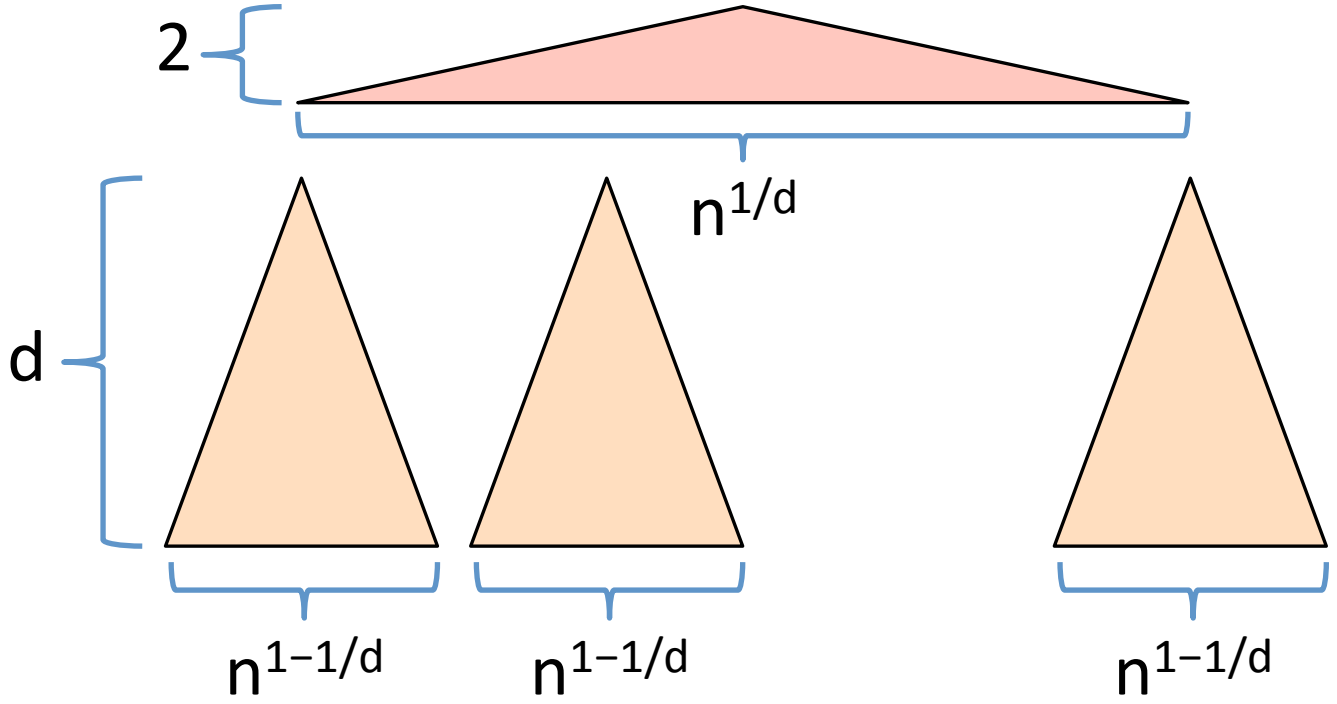
Depth d+1 **circuits** for PARITY require size $\exp(\Omega(n^{1/d}))$

Hastad ’86

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

(Trivial) Upper Bound

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

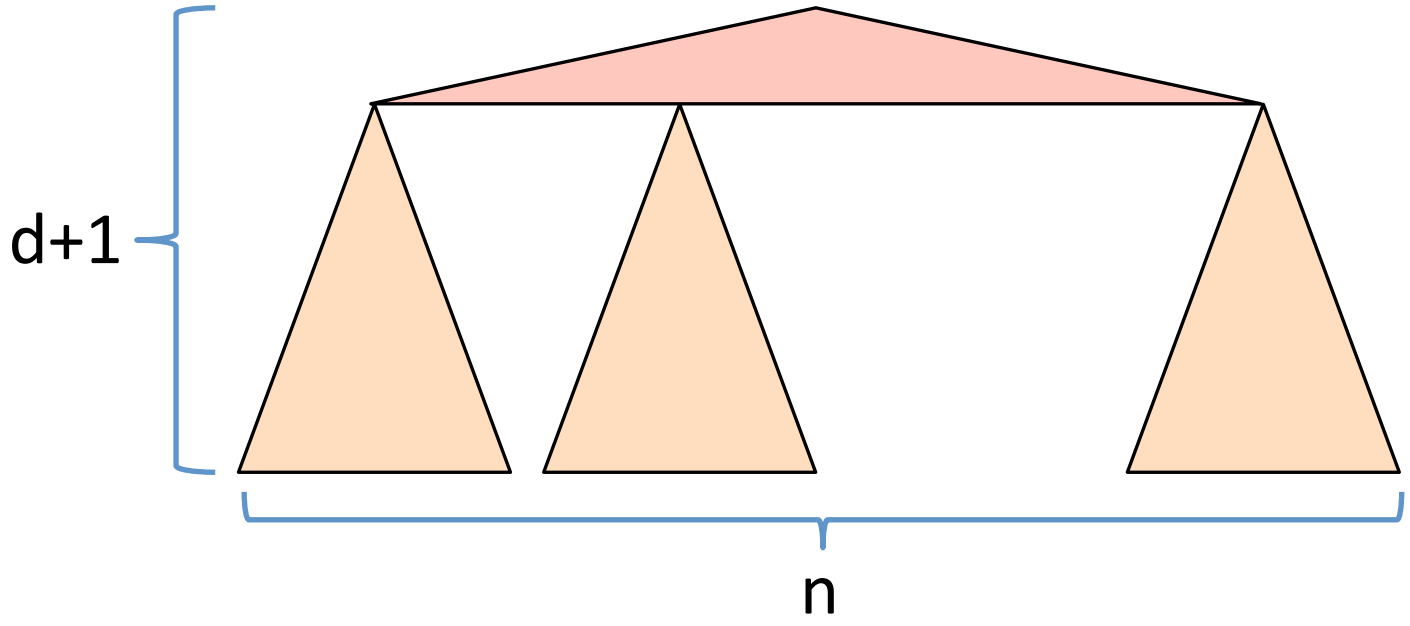


Hastad ’86

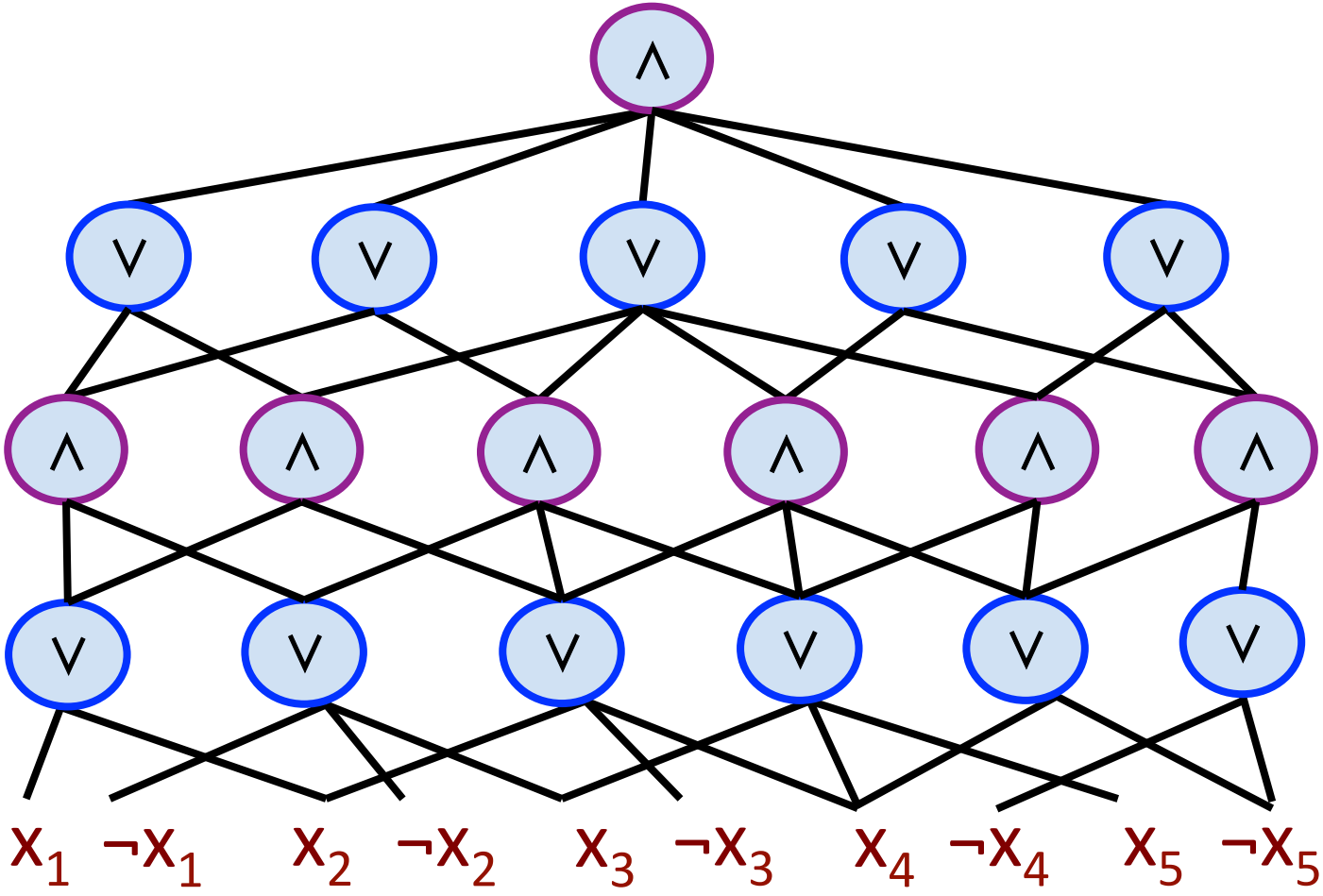
Depth d+1 **circuits** for PARITY require size $\exp(\Omega(n^{1/d}))$

(Trivial) Upper Bound

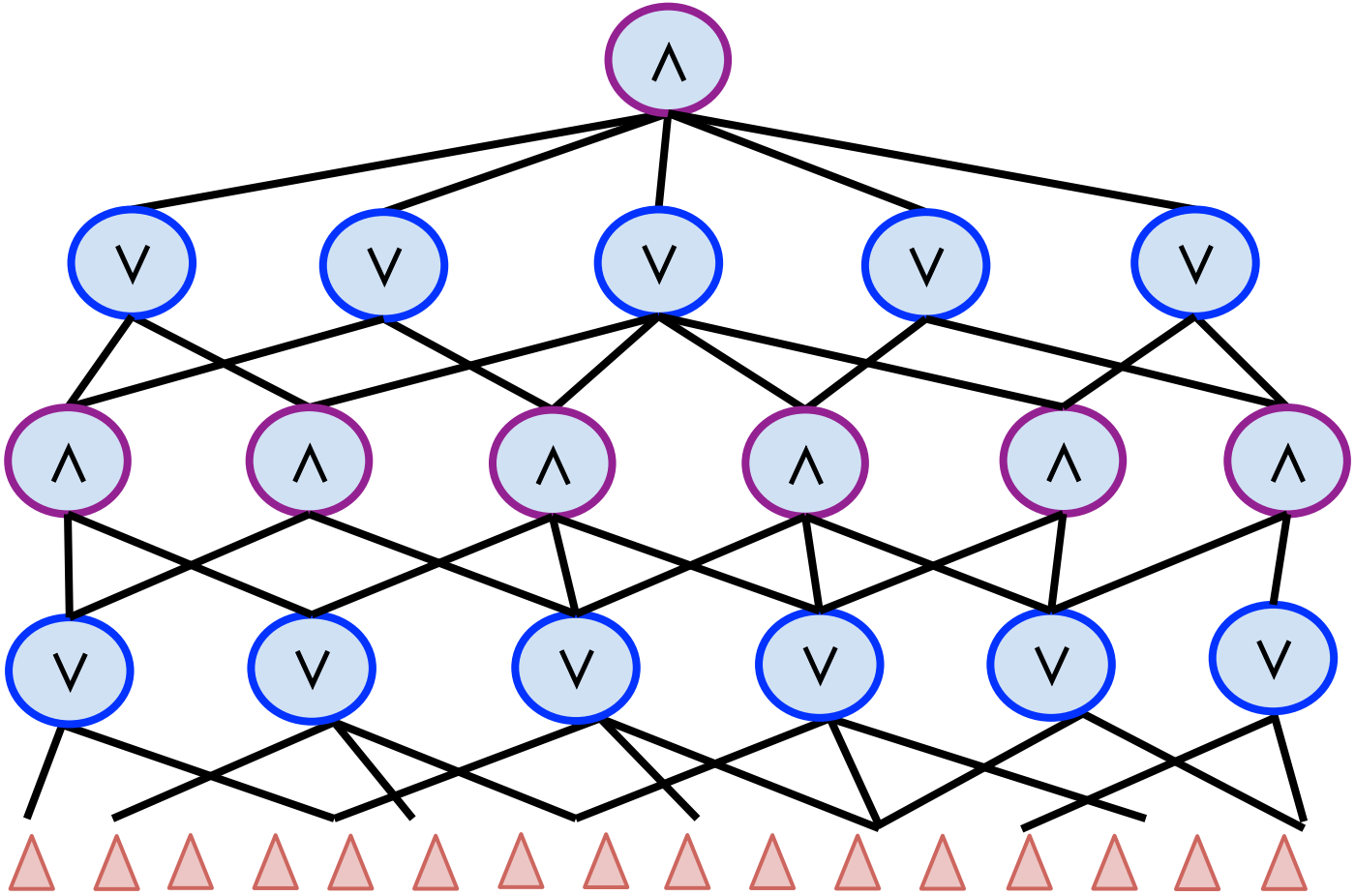
PARITY has depth d+1 **circuits** of size $\exp(O(n^{1/d}))$



PARITY Lower Bound

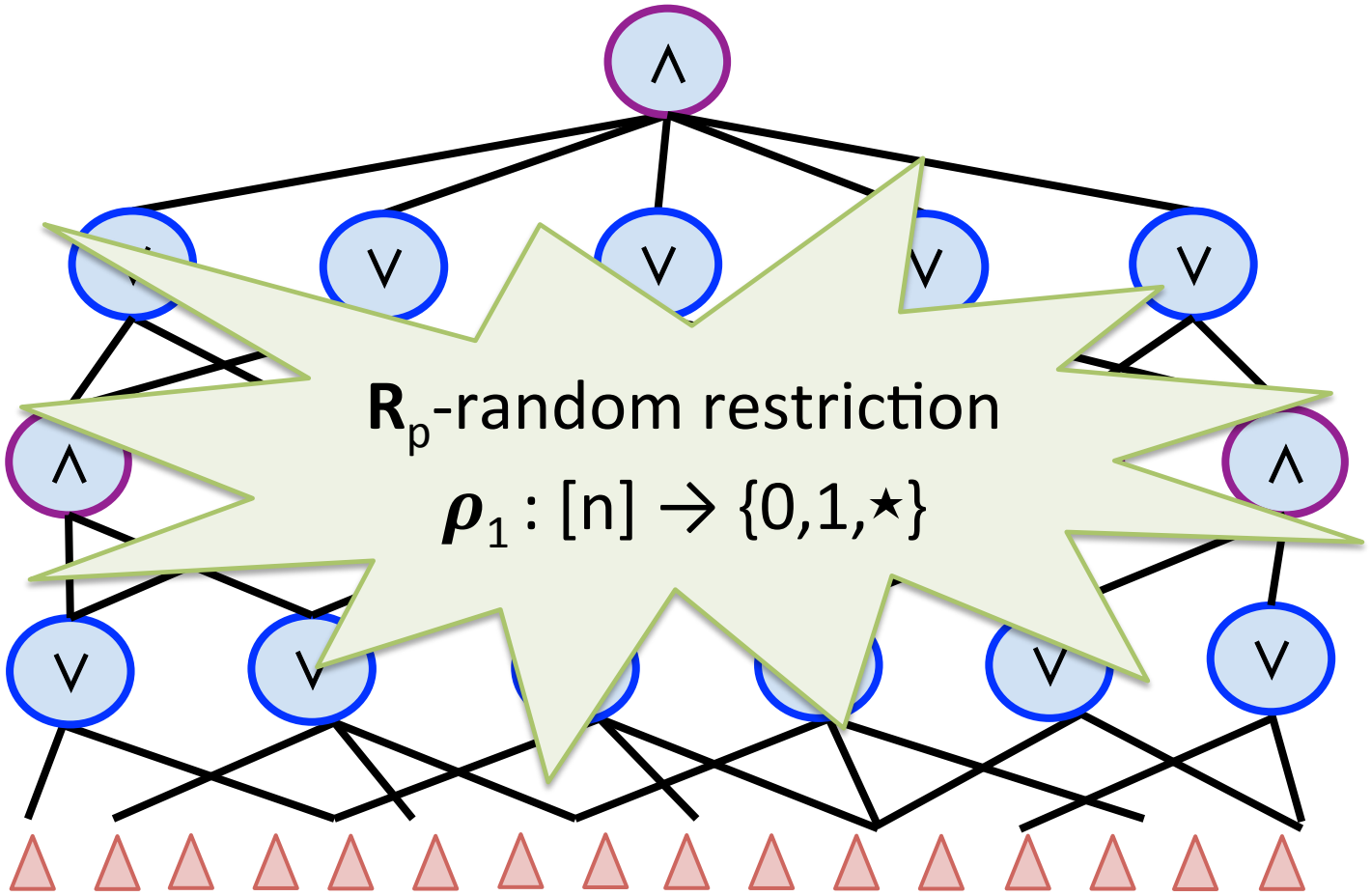


PARITY Lower Bound



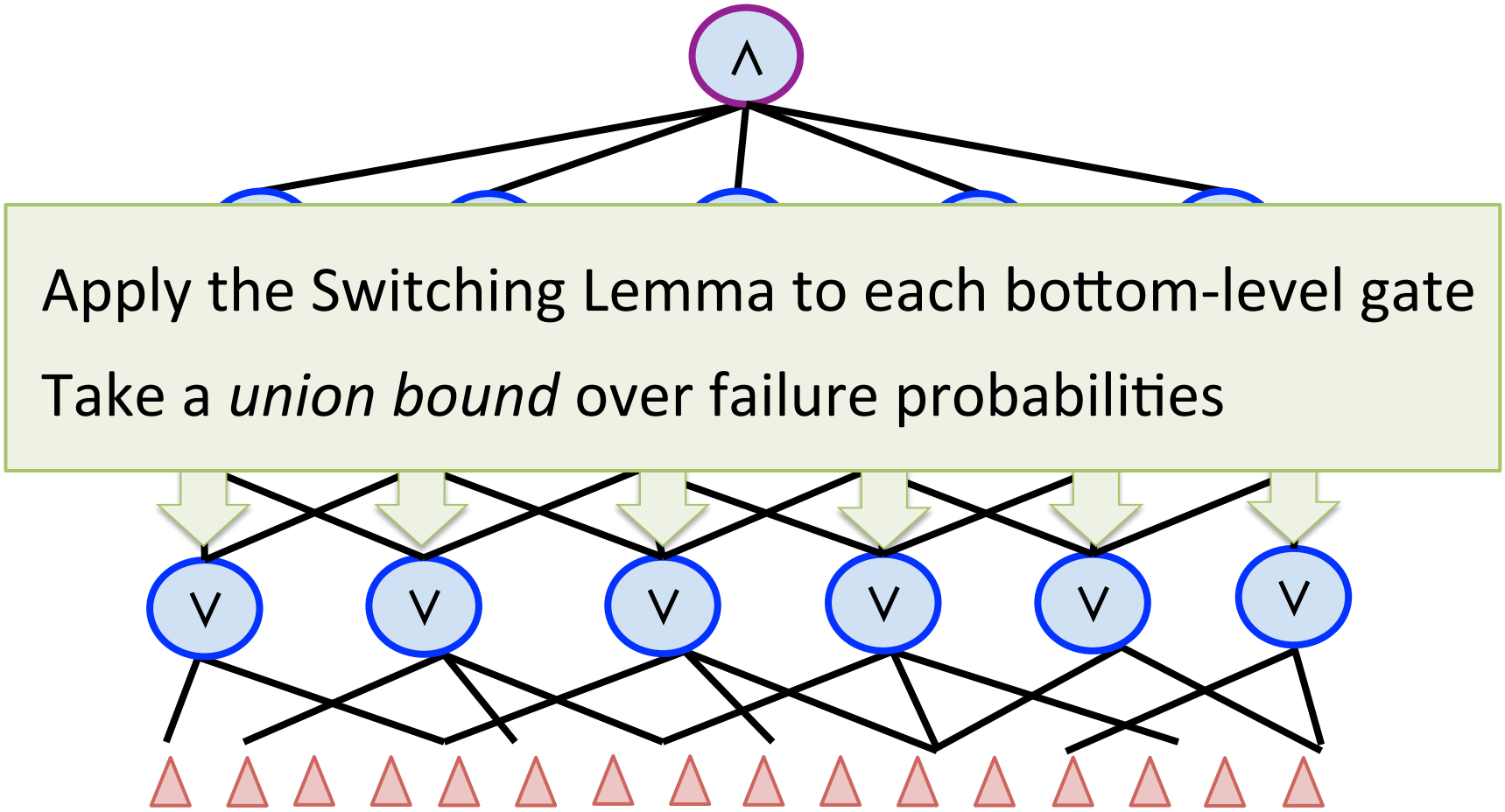
depth-1 decision trees on n variables

PARITY Lower Bound

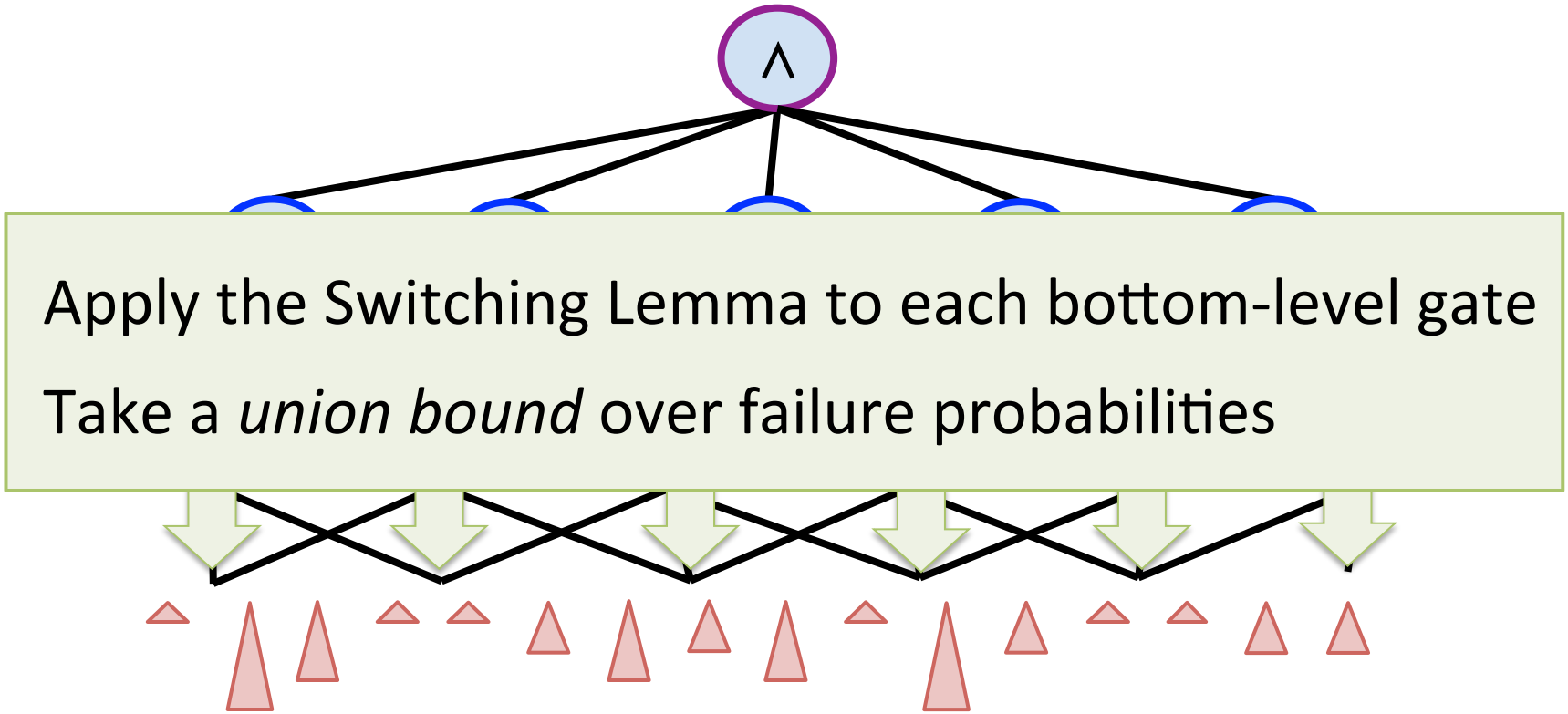


depth-1 decision trees on n variables

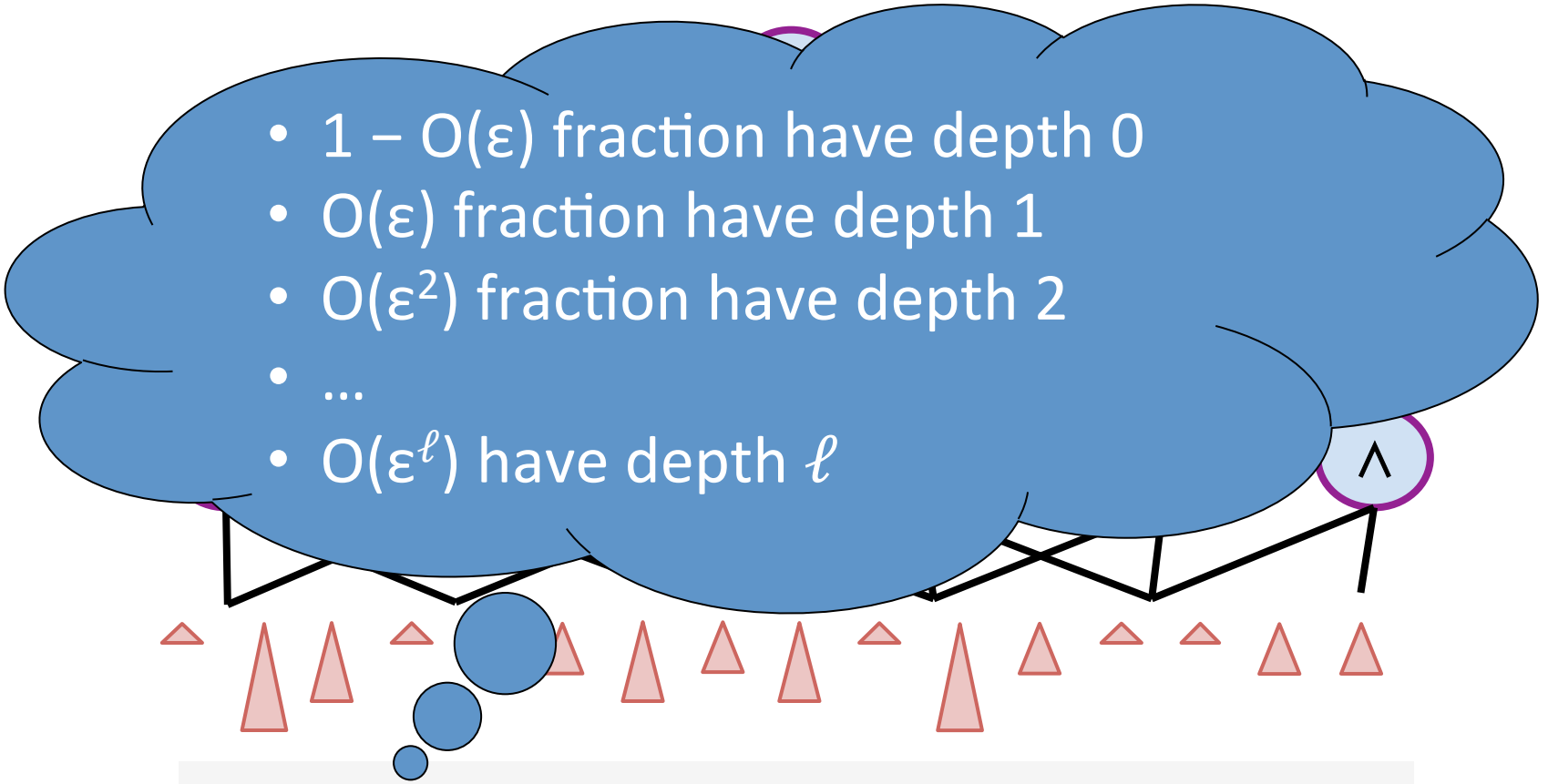
PARITY Lower Bound



PARITY Lower Bound

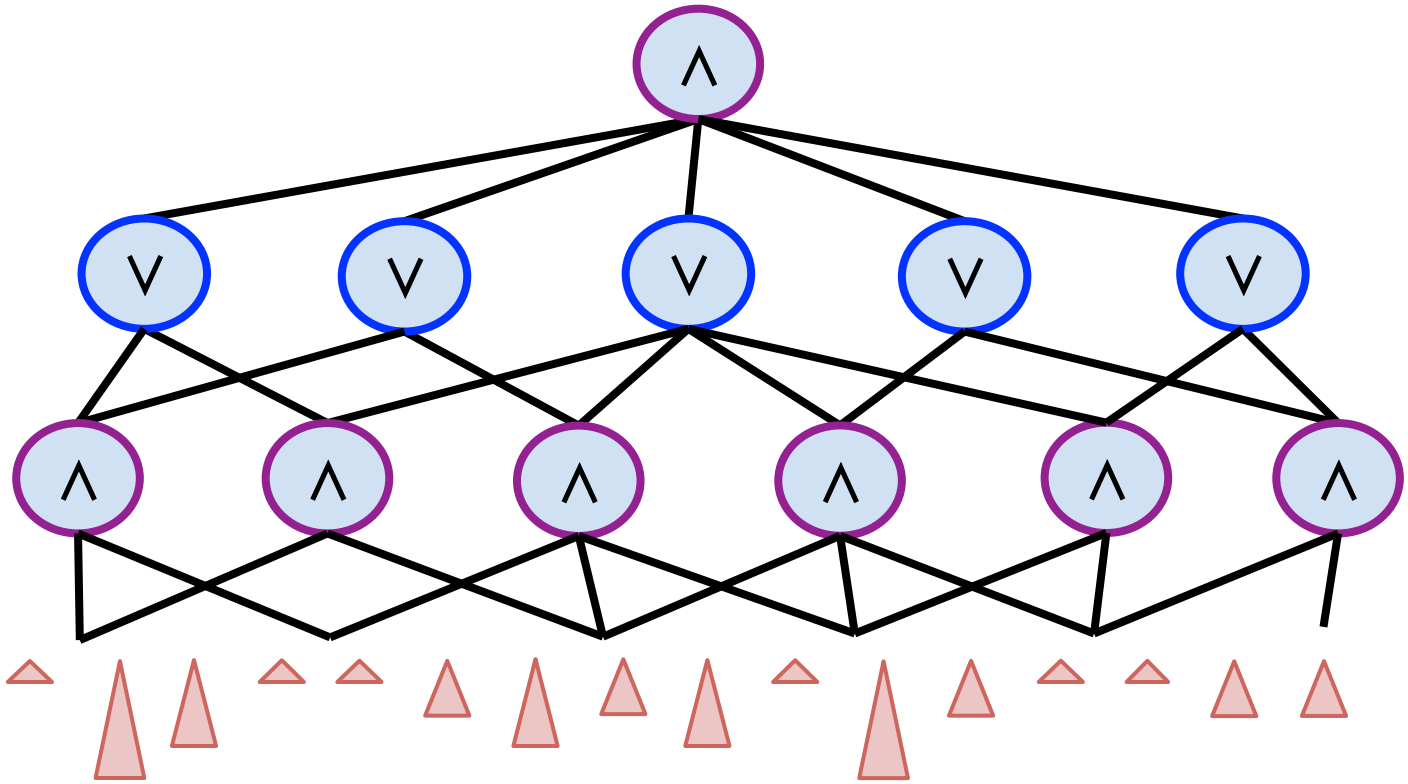


PARITY Lower Bound



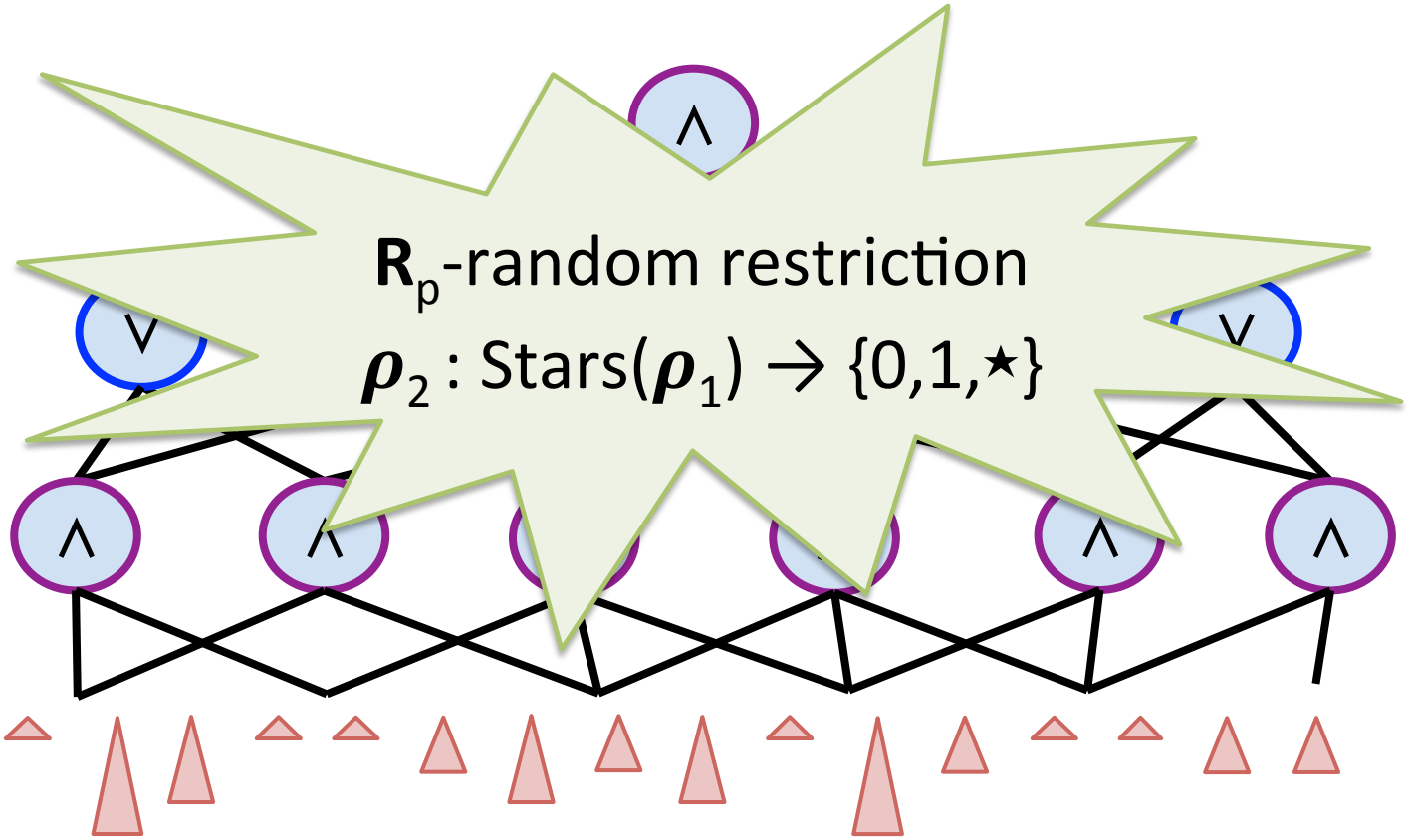
low-depth decision trees on pn variables

PARITY Lower Bound



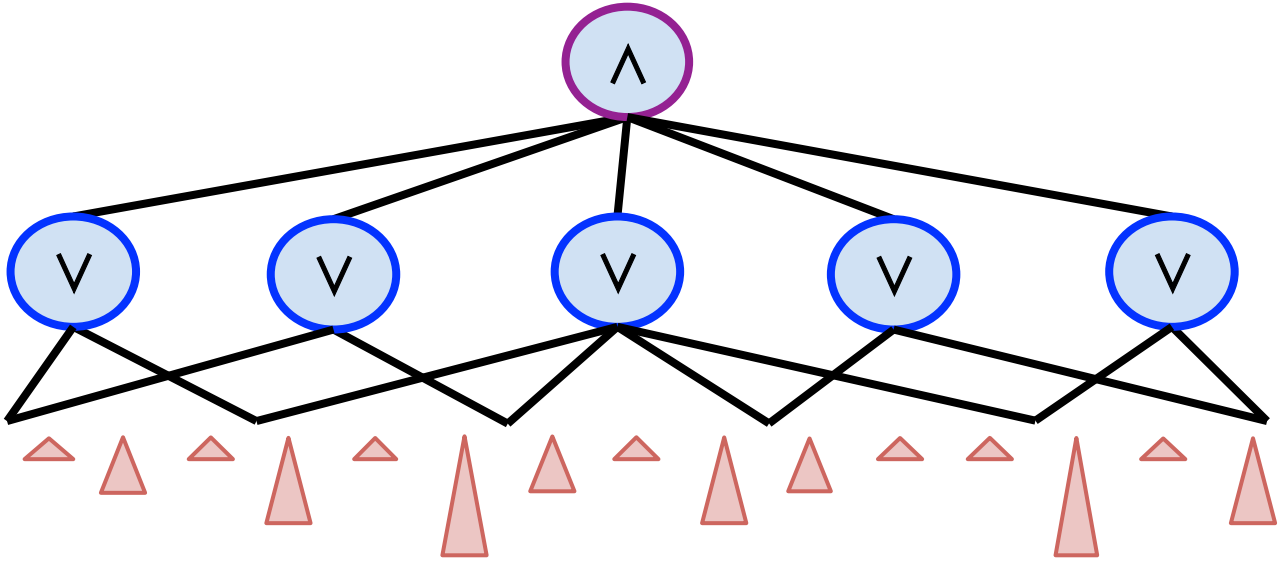
low-depth decision trees on pn variables

PARITY Lower Bound



low-depth decision trees on pn variables

PARITY Lower Bound

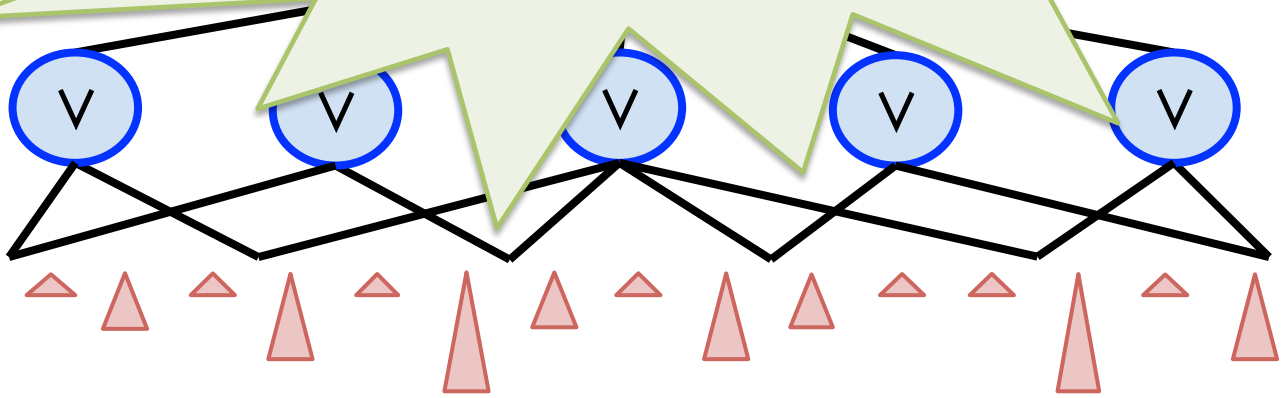


low-depth decision trees on p^2n variables

PARITY Lower Bound

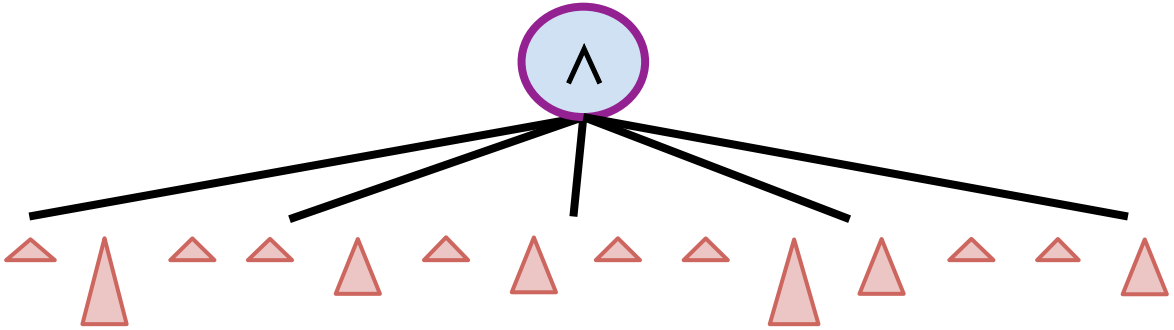
$\mathbf{R}_p$-random restriction

$\boldsymbol{\rho}_3 : \text{Stars}(\boldsymbol{\rho}_2) \to \{0,1,\star\}$

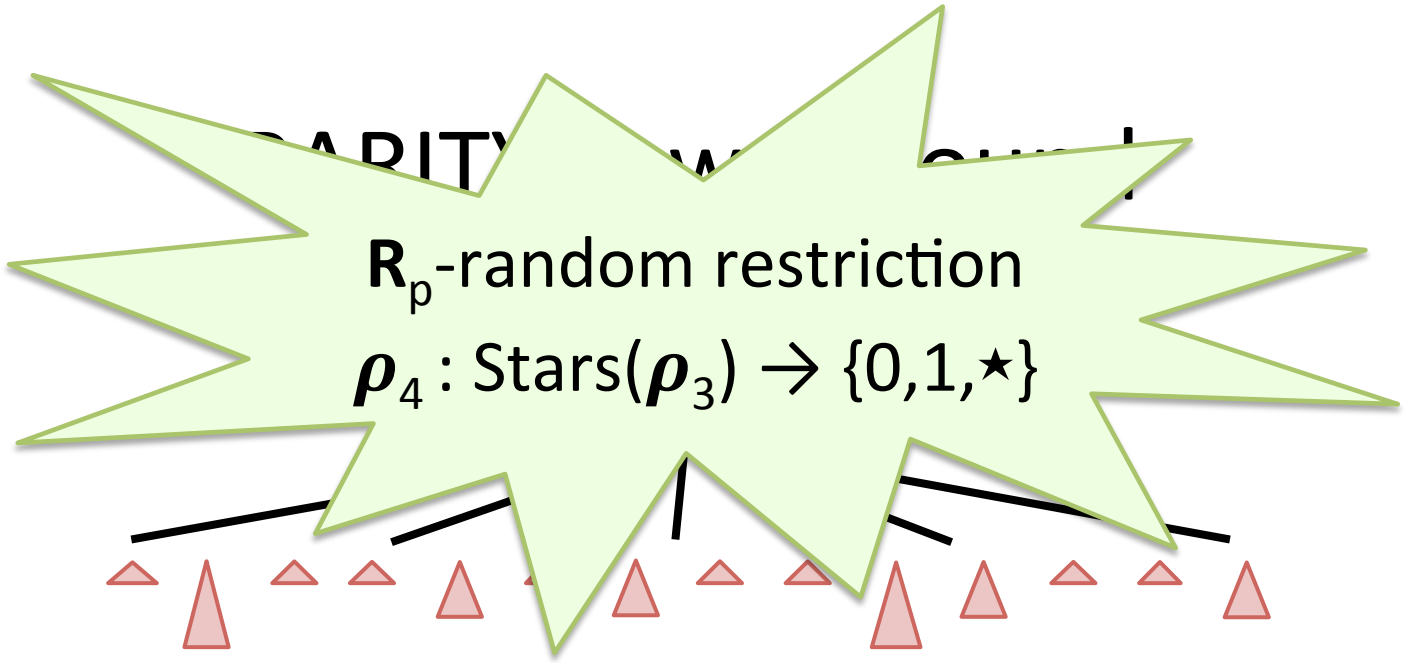


low-depth decision trees on p^2n variables

PARITY Lower Bound



low-depth decision trees on p^3n variables



low-depth decision trees on p^3n variables

PARITY Lower Bound

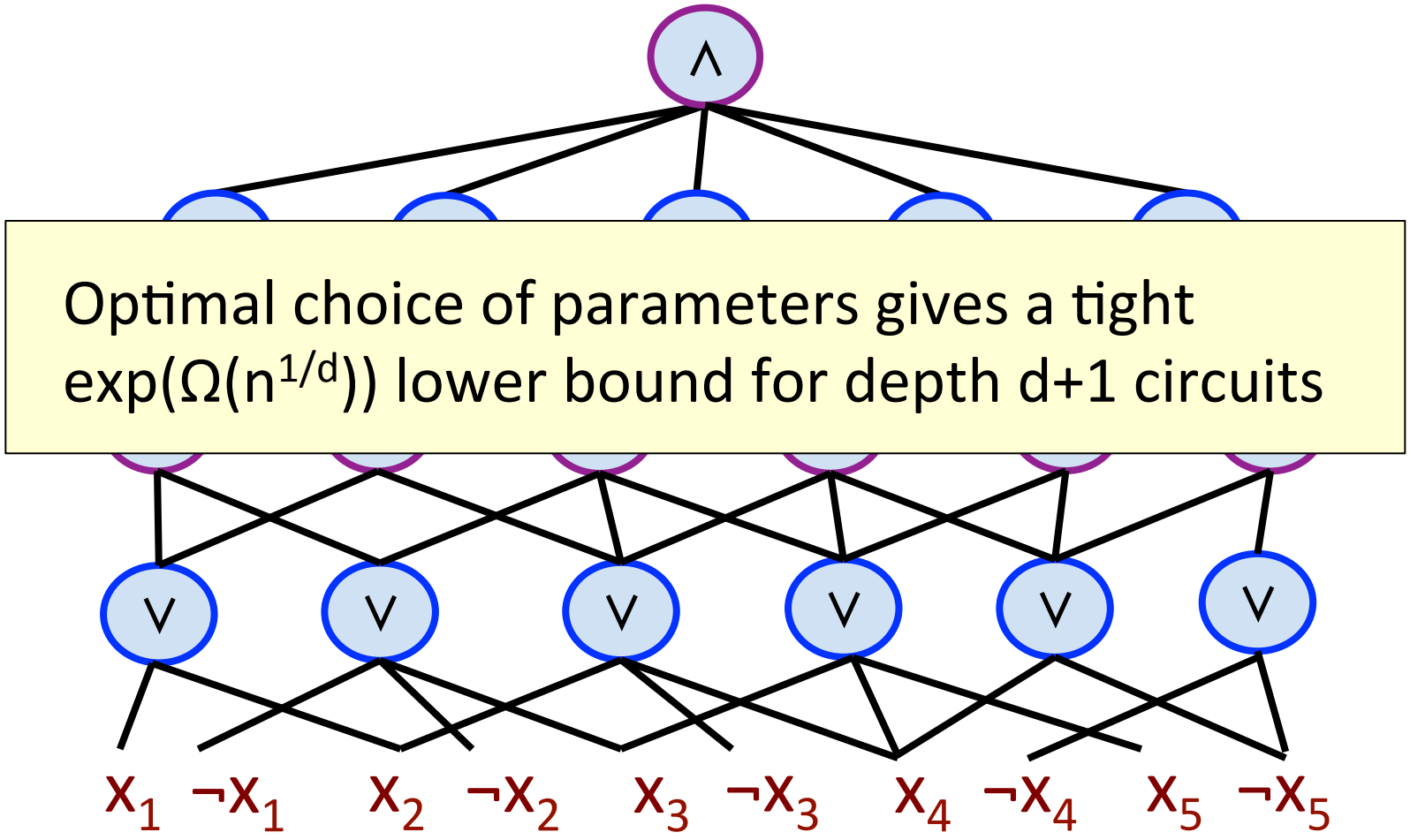
depth-0 decision tree
(i.e. **constant function**)
on p^4n variables

PARITY Lower Bound

depth-0 decision tree
(i.e. **constant function**)
on p^4n variables

- w.h.p., output is fixed to 0 or 1 after restrictions $\boldsymbol{\rho}_1 \boldsymbol{\rho}_2 \boldsymbol{\rho}_3 \boldsymbol{\rho}_4$ (equivalent to $\mathbf{R}_{p^4}$)
- If $p^4n \gg 1$, this shows the original circuit does not compute PARITY_n

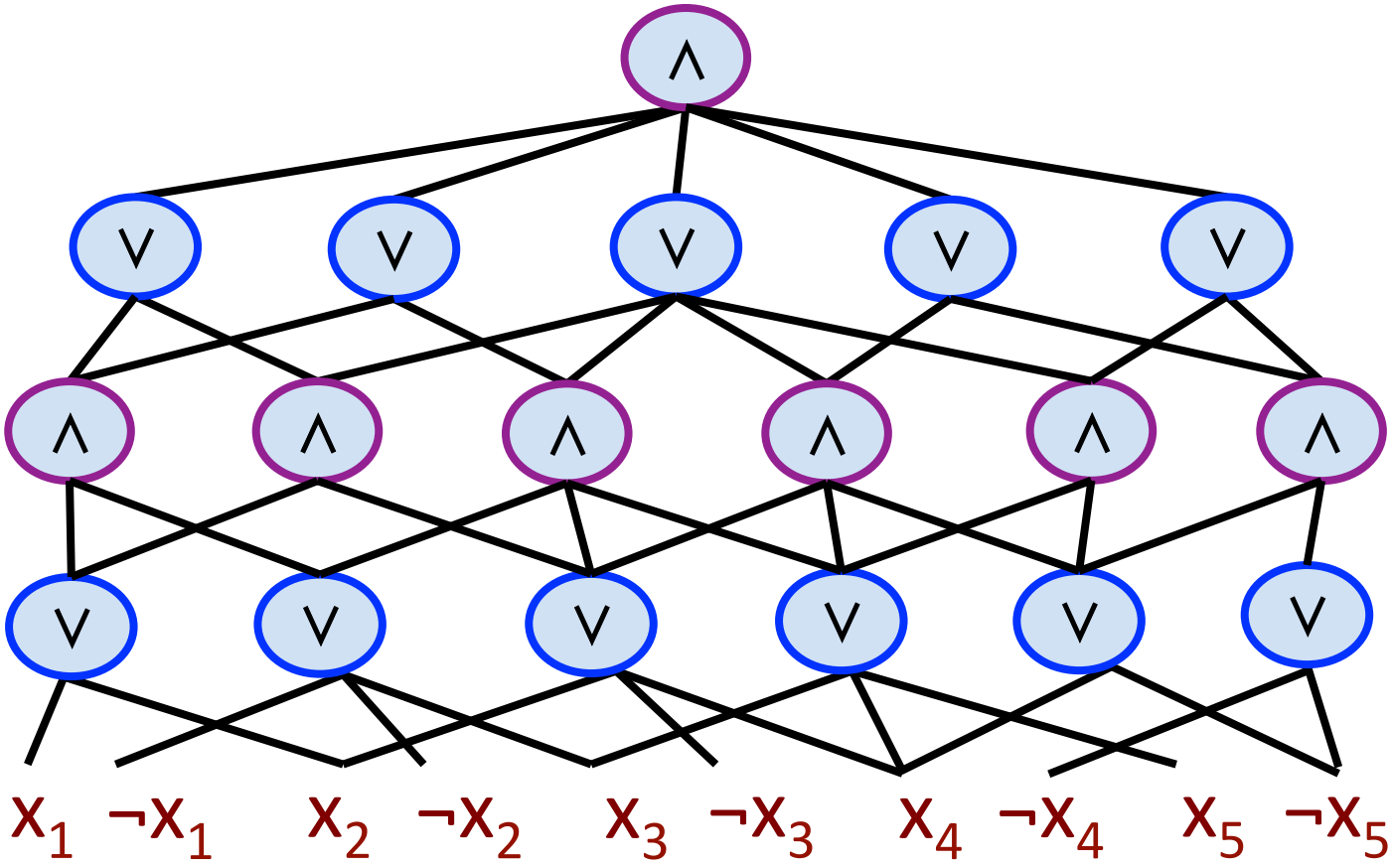
PARITY Lower Bound



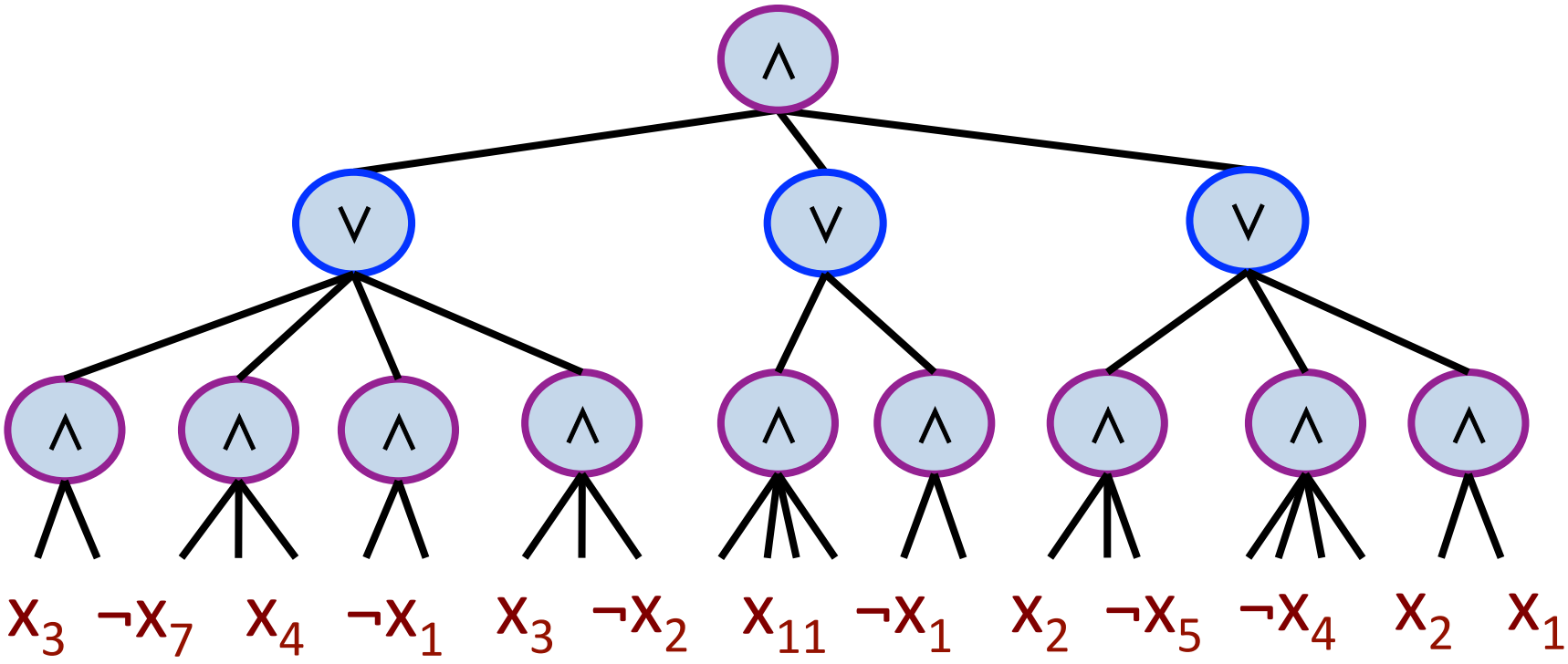
Optimal choice of parameters gives a tight $\exp(\Omega(n^{1/d}))$ lower bound for depth d+1 circuits

Formulas vs. Circuits

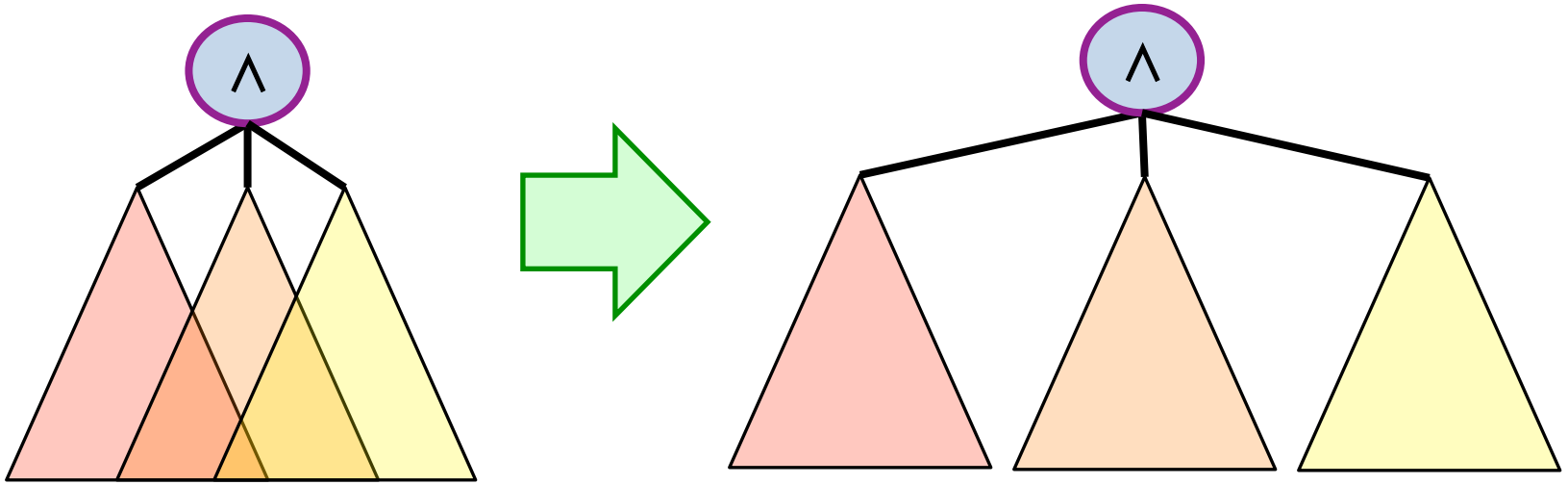
AC^0 Circuits



AC^0 Formulas



Fact: Every depth d+1 **circuit** of size S is equivalent to a depth d+1 **formula** of size at most S^d



PARITY Lower Bound

Hastad ’86

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

R. ‘15

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

PARITY Lower Bound

Hastad ’86

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

Poly-size **circuits** for PARITY have depth $\frac{\log n}{\log\log n + O(1)}$

R. ‘15

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

Poly-size **formulas** for PARITY have depth $\Omega(\log n)$

Two Views of $\mathbf{R}_p : [n] \to \{0,1,\star\}$

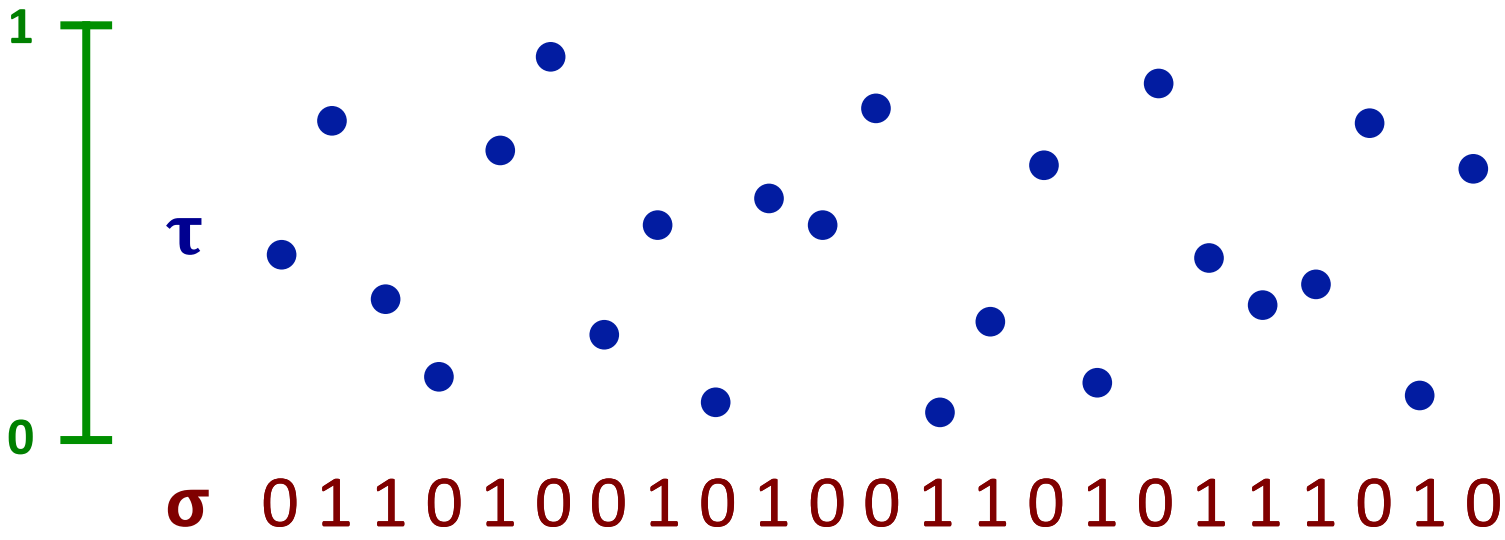
(1) Independently, for each coordinate $i \in [n]$, set

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

(2) $\boldsymbol{\sigma} \leftarrow \{0,1\}^n$ uniform random "assignment"

$\boldsymbol{\tau} \leftarrow [0,1]^n$ uniform random "time-stamp"

$$\mathbf{R}_p(i) = \begin{cases} \star & \text{if } \boldsymbol{\tau}_i \le p \\ \boldsymbol{\sigma}_i & \text{if } \boldsymbol{\tau}_i > p \end{cases}$$



$\boldsymbol{\sigma} \leftarrow \{0,1\}^n$ uniform random "assignment"

$\boldsymbol{\tau} \leftarrow [0,1]^n$ uniform random "time-stamp"

$$\mathbf{R}_p(i) = \begin{cases} \star & \text{if } \boldsymbol{\tau}_i \le p \\ \boldsymbol{\sigma}_i & \text{if } \boldsymbol{\tau}_i > p \end{cases}$$

1

0

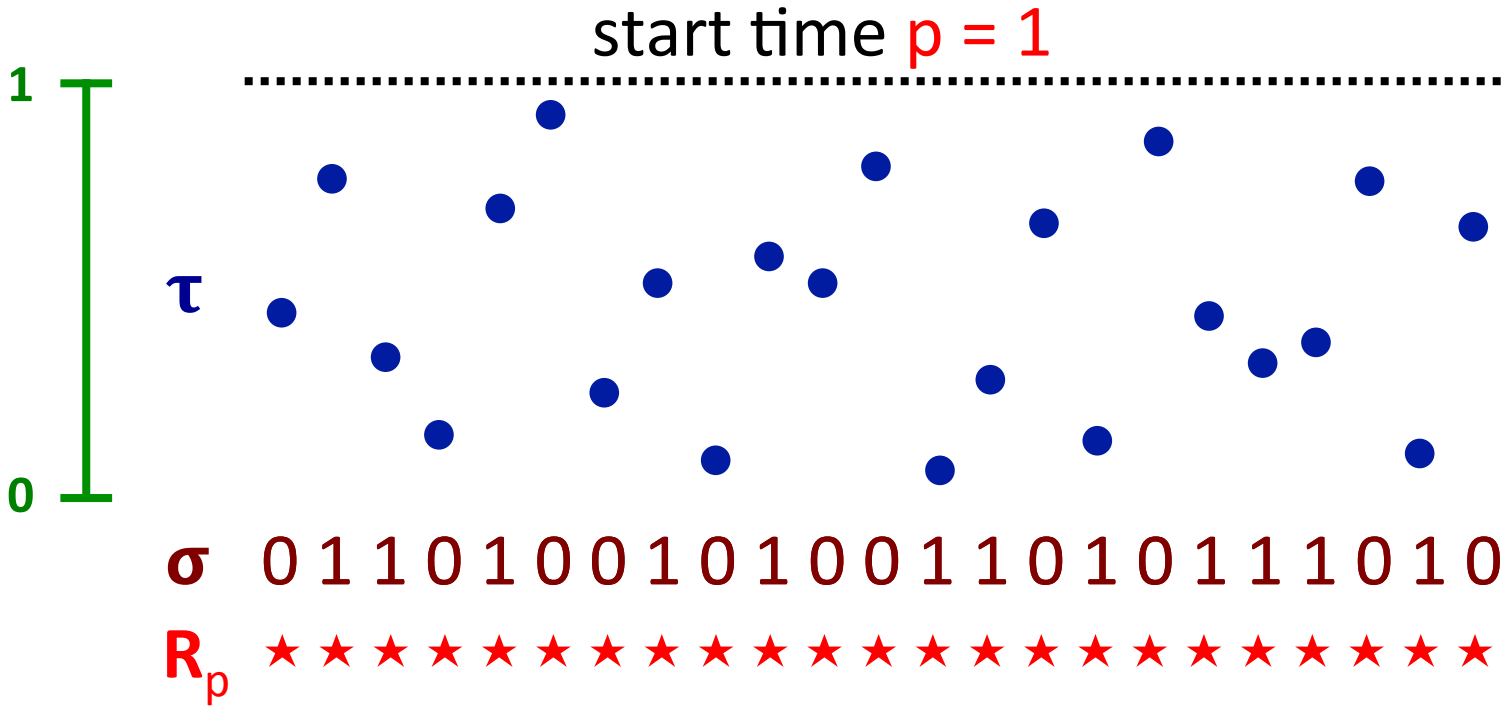
"time" p runs from 1 to 0

σ 0 1 1 0 1 0 0 1 0 1 0 0 1 1 0 1 0 1 1 1 0 1 0

$\sigma \leftarrow \{0,1\}^n$ uniform random "assignment"

$\tau \leftarrow [0,1]^n$ uniform random "time-stamp"

$$\mathbf{R}_p(i) = \begin{cases} \star & \text{if } \tau_i \le p \\ \sigma_i & \text{if } \tau_i > p \end{cases}$$



$\boldsymbol{\sigma} \leftarrow \{0,1\}^n$ uniform random "assignment"

$\boldsymbol{\tau} \leftarrow [0,1]^n$ uniform random "time-stamp"

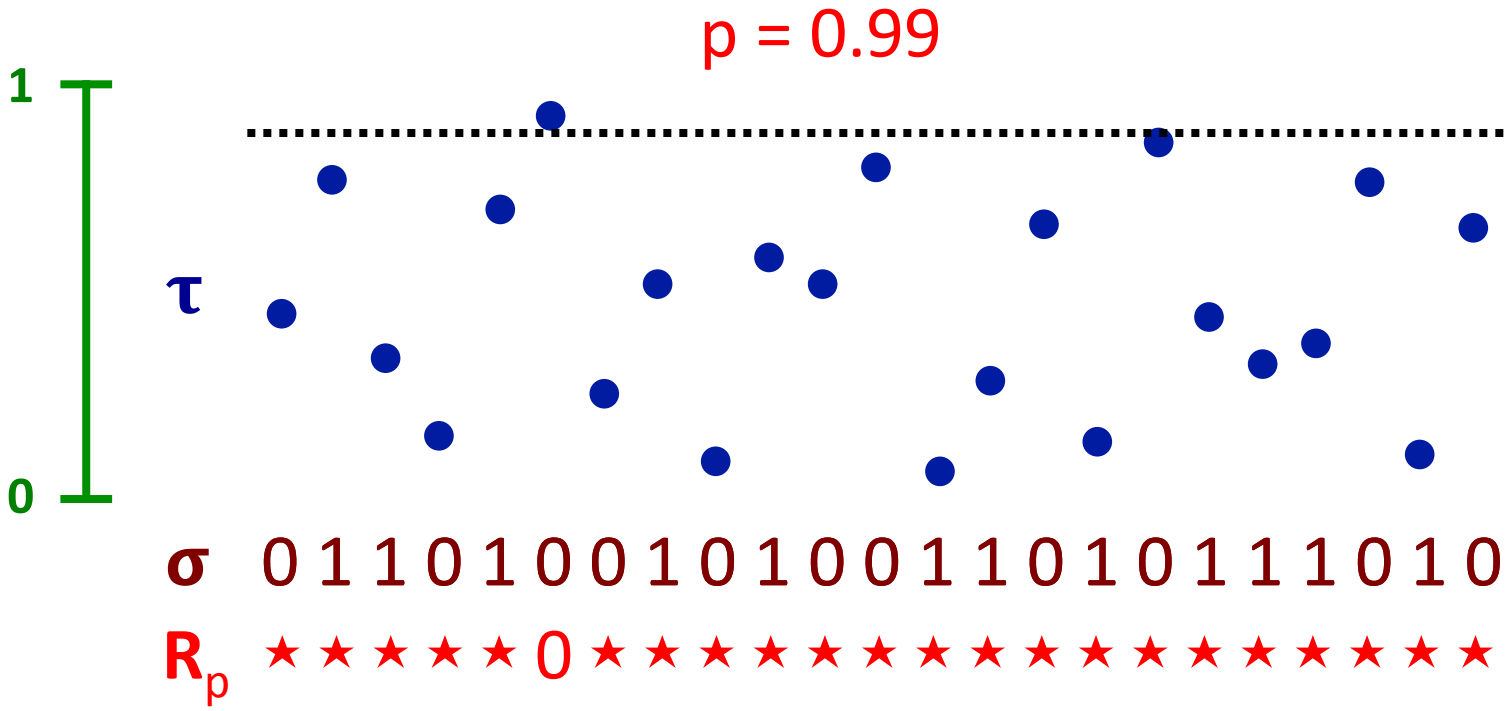
$$\mathbf{R}_p(i) = \begin{cases} \star & \text{if } \boldsymbol{\tau}_i \le p \\ \boldsymbol{\sigma}_i & \text{if } \boldsymbol{\tau}_i > p \end{cases}$$

start time p = 1

$\boldsymbol{\sigma} \leftarrow \{0,1\}^n$ uniform random "assignment"

$\boldsymbol{\tau} \leftarrow [0,1]^n$ uniform random "time-stamp"

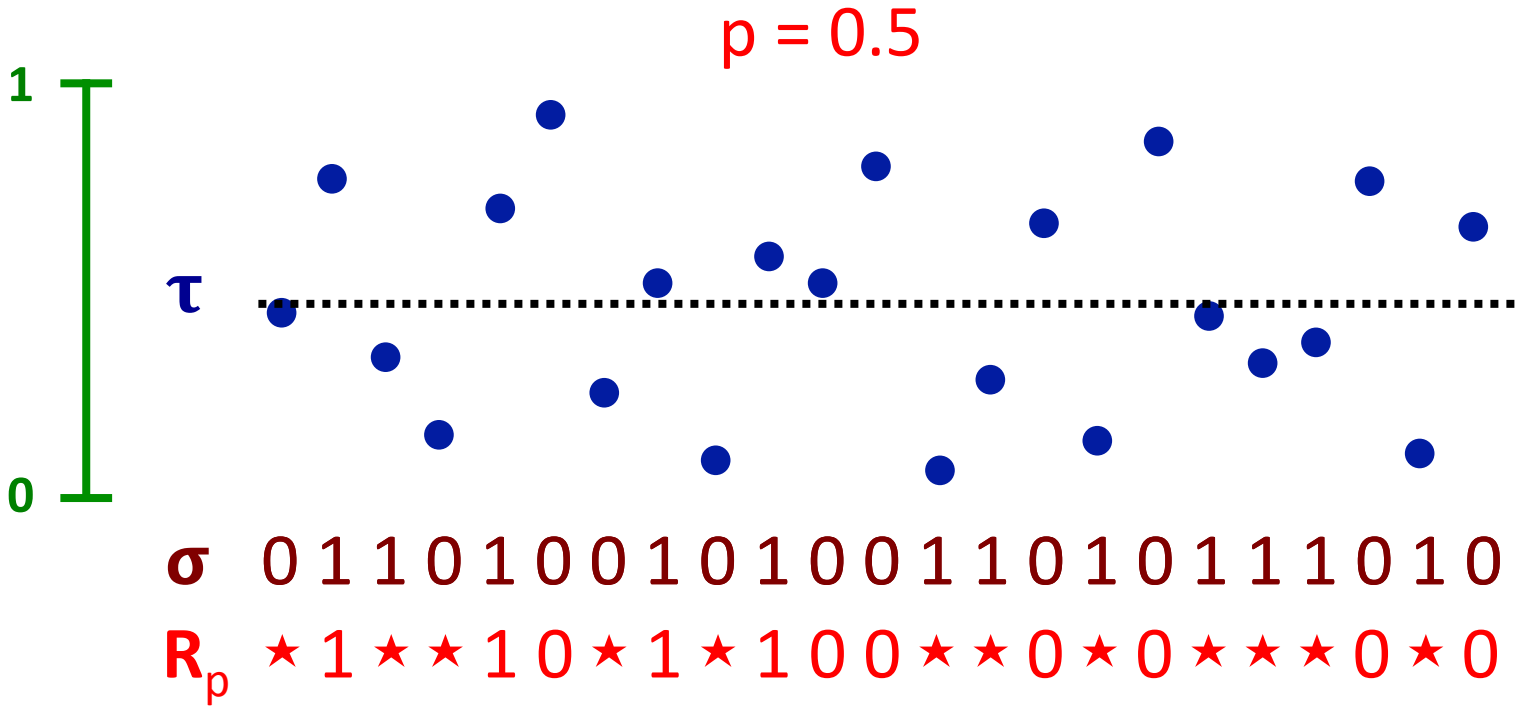
$$\mathbf{R}_p(i) = \begin{cases} \star & \text{if } \boldsymbol{\tau}_i \le p \\ \boldsymbol{\sigma}_i & \text{if } \boldsymbol{\tau}_i > p \end{cases}$$



$\boldsymbol{\sigma} \leftarrow \{0,1\}^n$ uniform random "assignment"

$\boldsymbol{\tau} \leftarrow [0,1]^n$ uniform random "time-stamp"

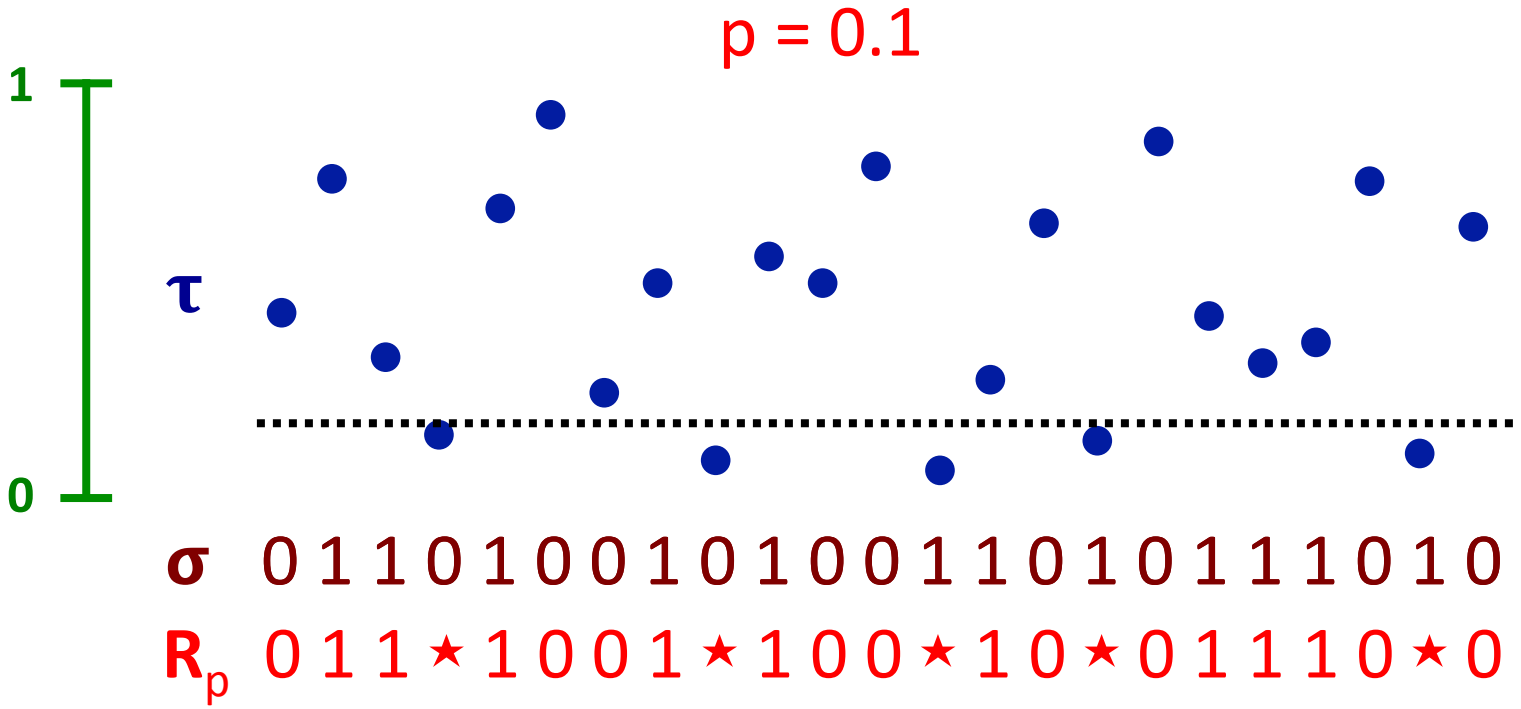
$$\mathbf{R}_p(i) = \begin{cases} \star & \text{if } \boldsymbol{\tau}_i \le p \\ \boldsymbol{\sigma}_i & \text{if } \boldsymbol{\tau}_i > p \end{cases}$$



$\boldsymbol{\sigma} \leftarrow \{0,1\}^n$ uniform random "assignment"

$\boldsymbol{\tau} \leftarrow [0,1]^n$ uniform random "time-stamp"

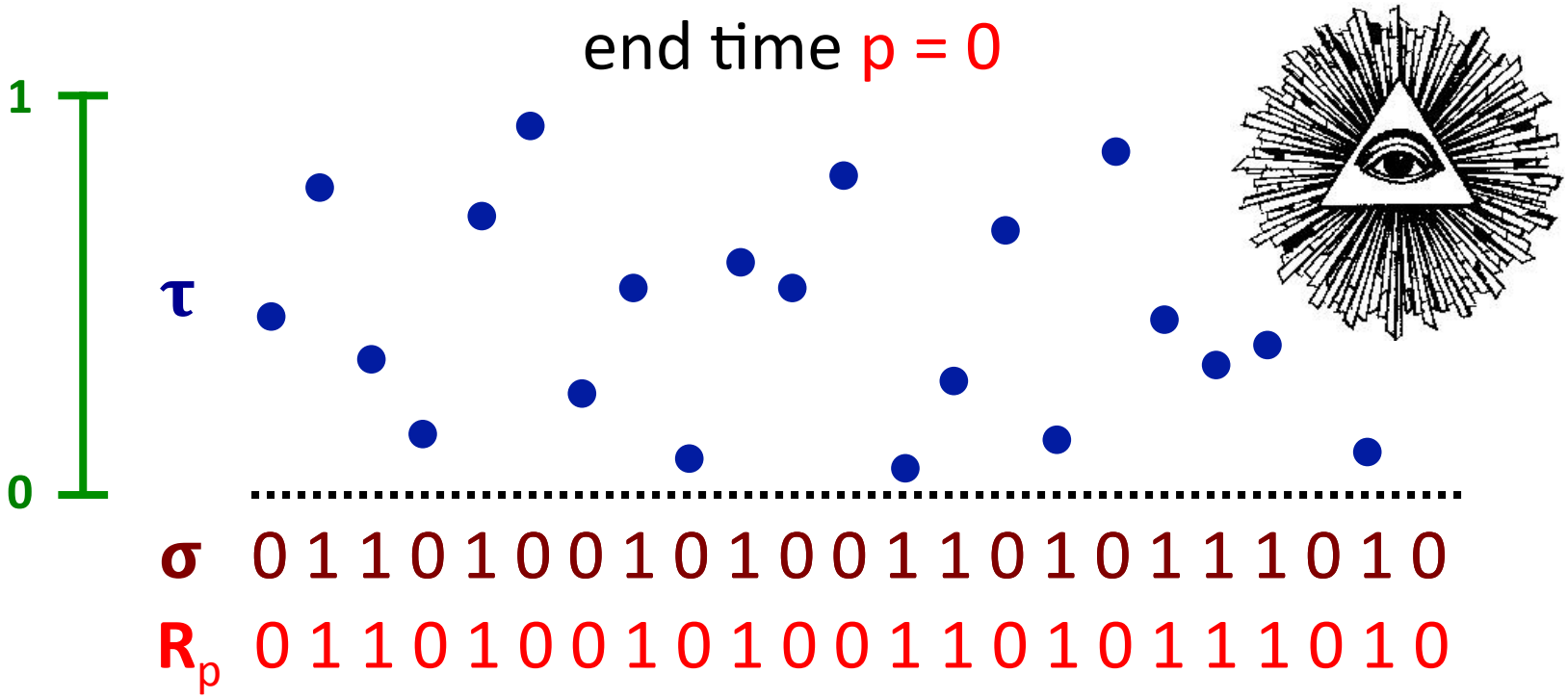
$$\mathbf{R}_p(i) = \begin{cases} \star & \text{if } \boldsymbol{\tau}_i \le p \\ \boldsymbol{\sigma}_i & \text{if } \boldsymbol{\tau}_i > p \end{cases}$$



$\boldsymbol{\sigma} \leftarrow \{0,1\}^n$ uniform random "assignment"

$\boldsymbol{\tau} \leftarrow [0,1]^n$ uniform random "time-stamp"

$$\mathbf{R}_p(i) = \begin{cases} \star & \text{if } \boldsymbol{\tau}_i \le p \\ \boldsymbol{\sigma}_i & \text{if } \boldsymbol{\tau}_i > p \end{cases}$$

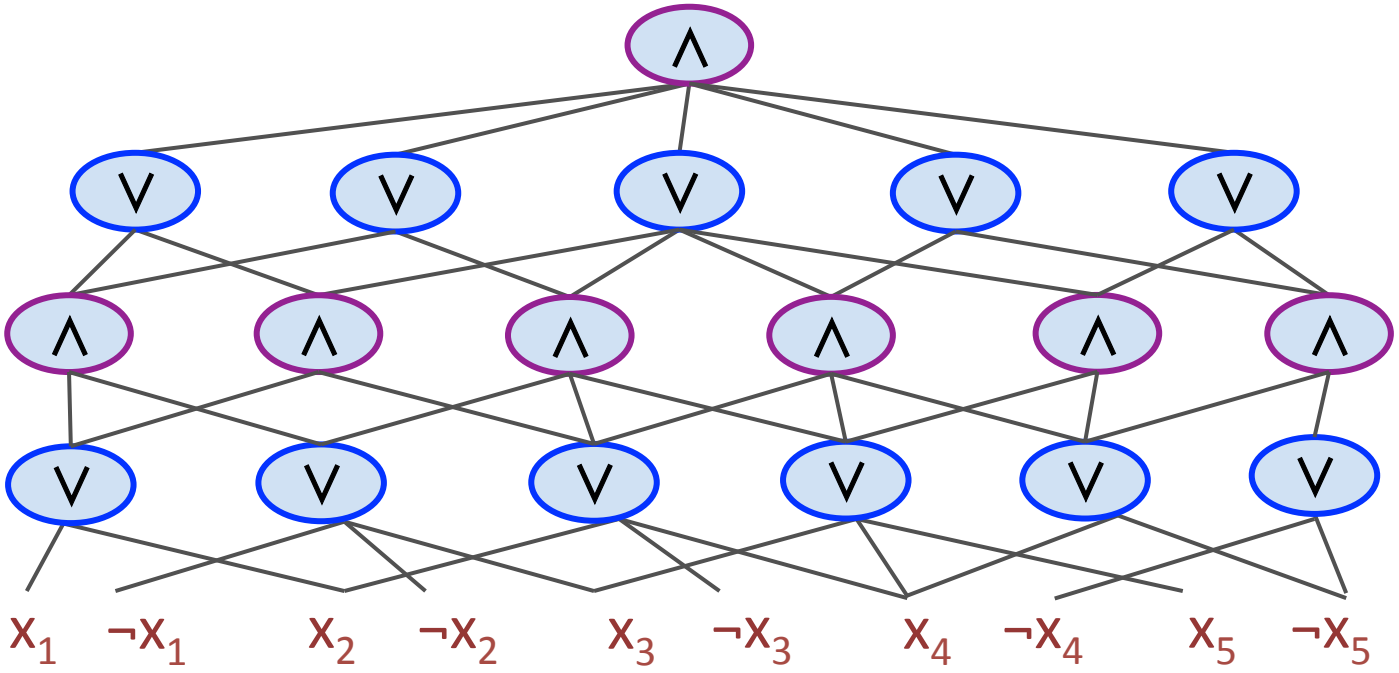


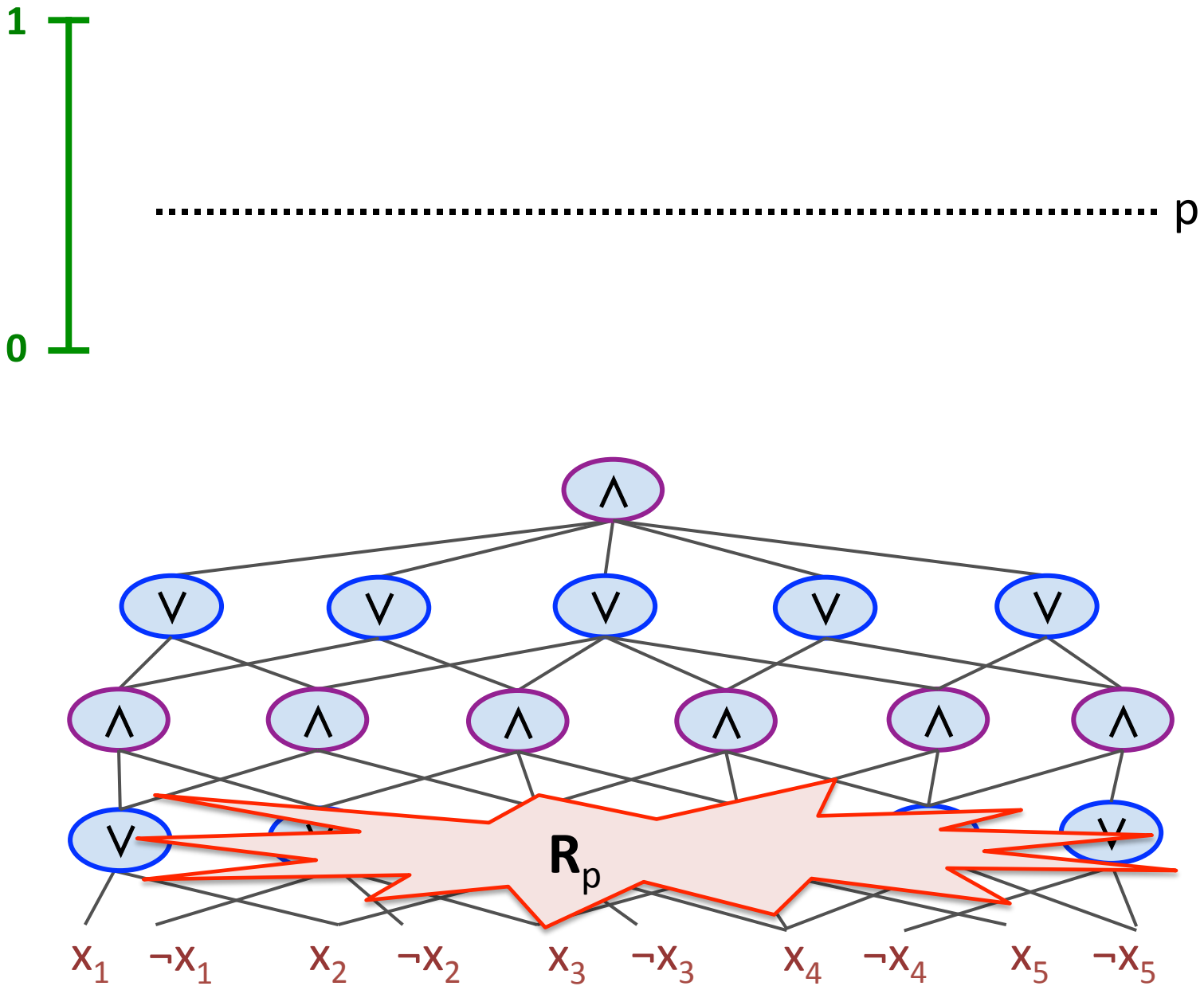
$\boldsymbol{\sigma} \leftarrow \{0,1\}^n$ uniform random "assignment"

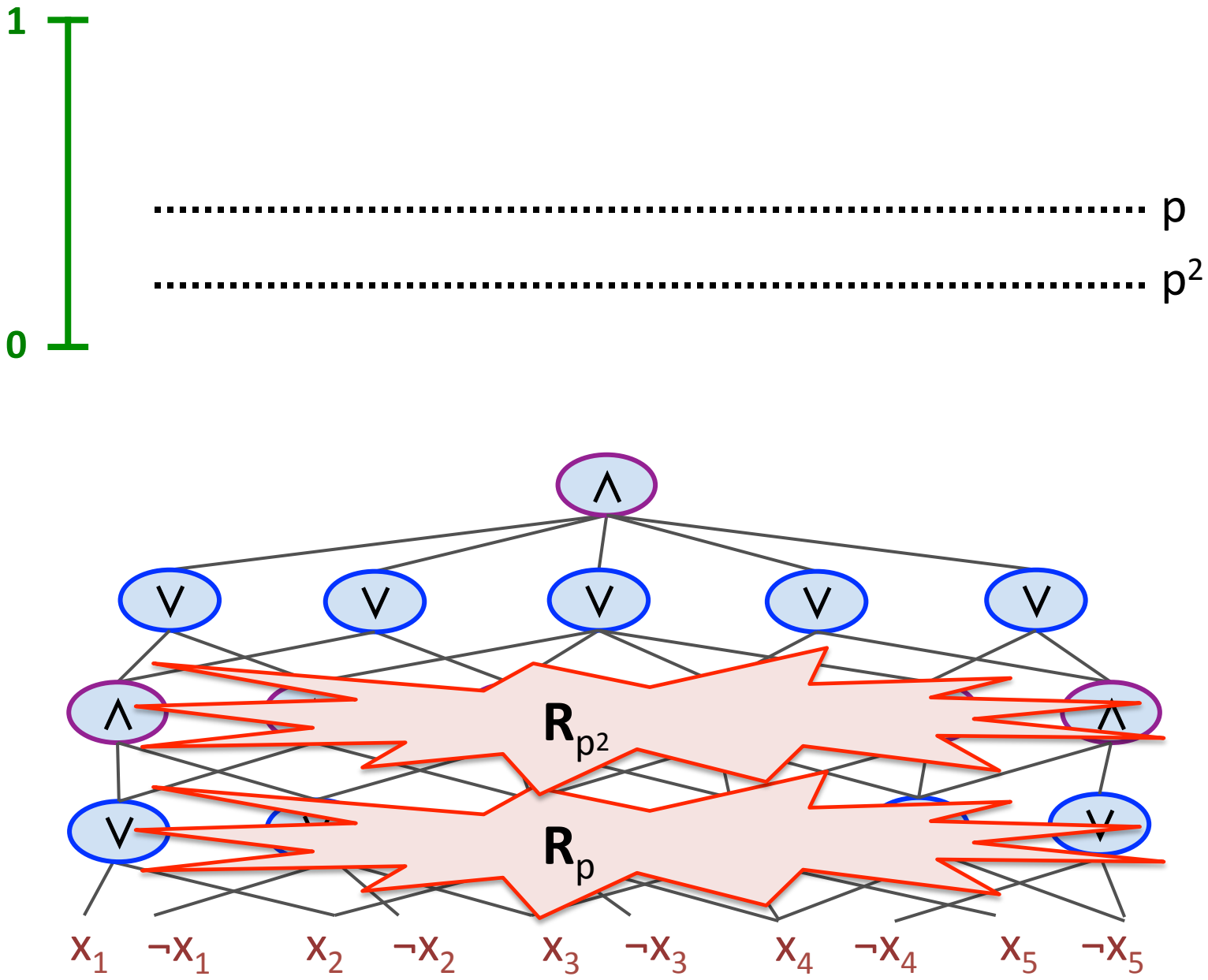
$\boldsymbol{\tau} \leftarrow [0,1]^n$ uniform random "time-stamp"

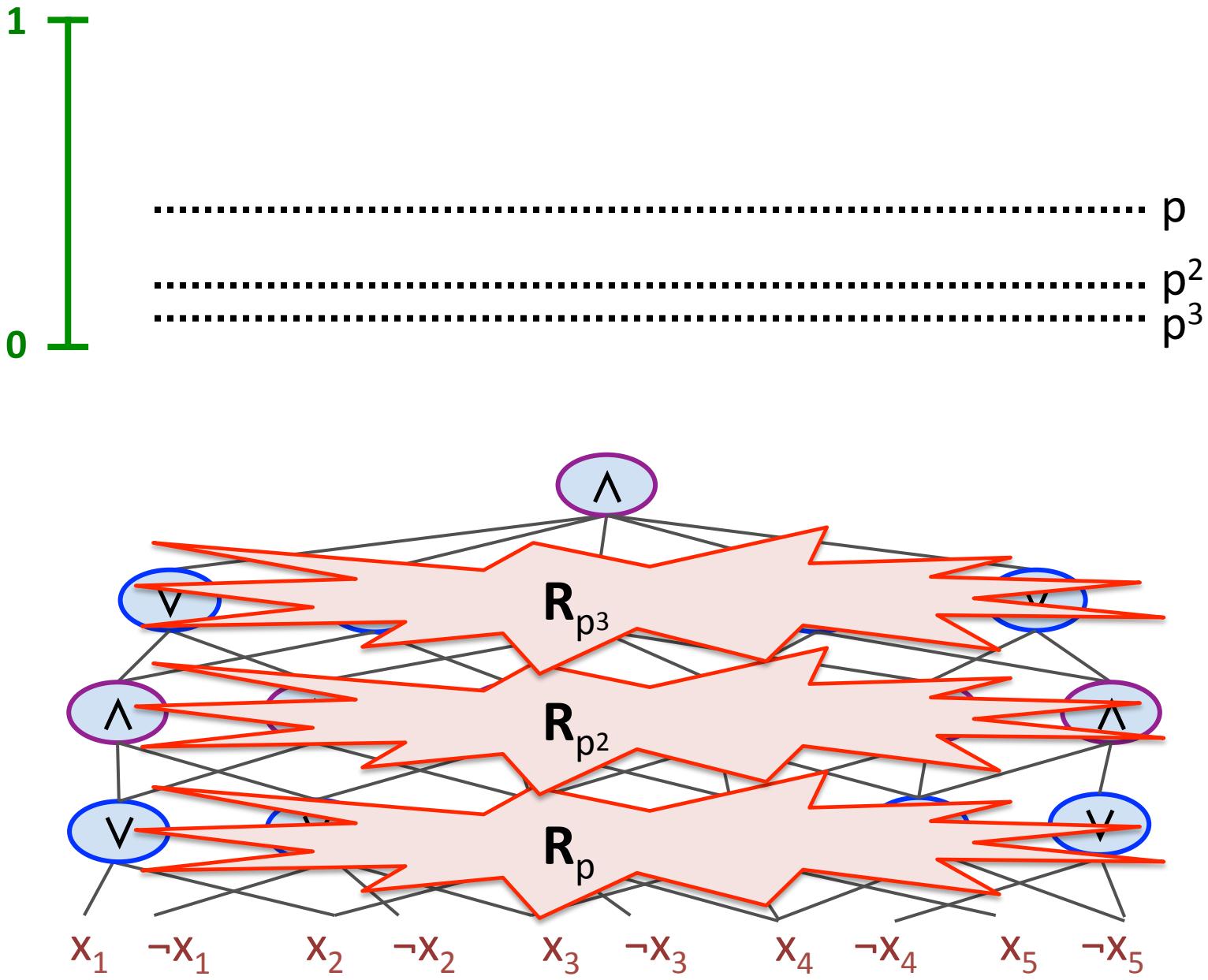
$$\mathbf{R}_p(i) = \begin{cases} \star & \text{if } \boldsymbol{\tau}_i \le p \\ \boldsymbol{\sigma}_i & \text{if } \boldsymbol{\tau}_i > p \end{cases}$$

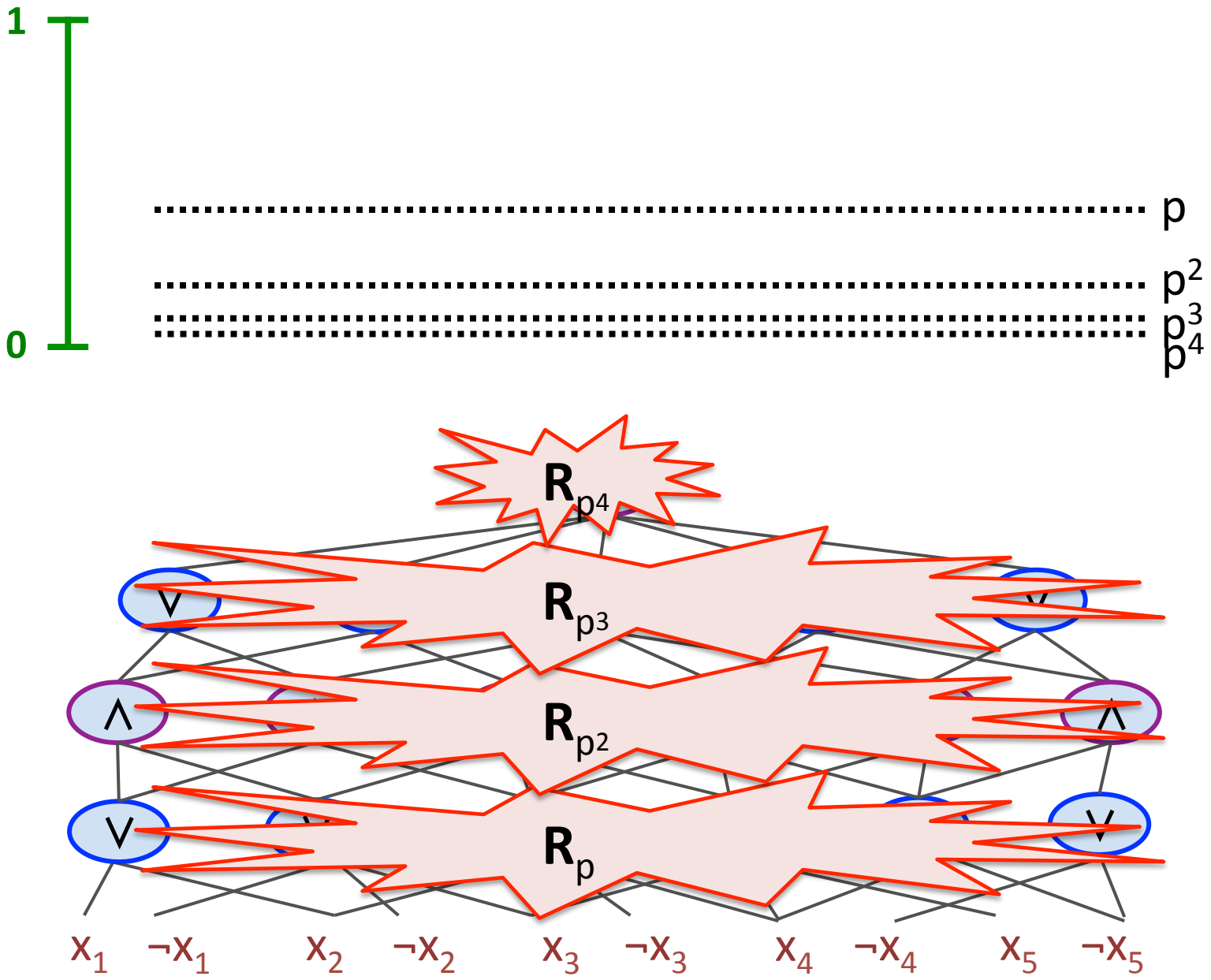

1
0

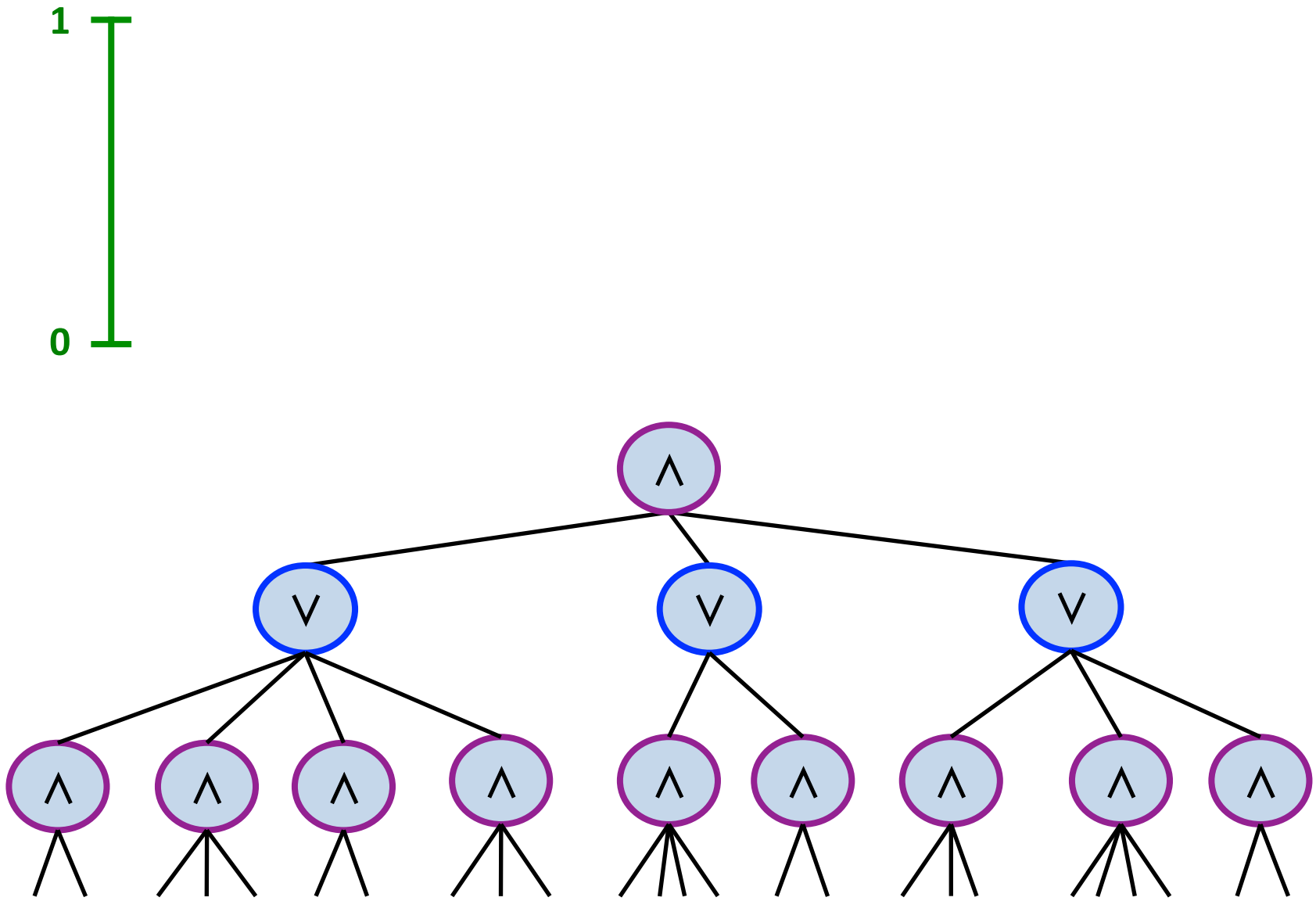

∧
∨ ∨ ∨ ∨ ∨
∧ ∧ ∧ ∧ ∧ ∧
∨ ∨ ∨ ∨ ∨ ∨
x1 ¬x1 x2 ¬x2 x3 ¬x3 x4 ¬x4 x5 ¬x5


1
0
p
∧
∨
∨
∨
∨
∨
∧
∧
∧
∧
∧
∧
∨
∨
R_p
x_1
$\neg x_1$
x_2
$\neg x_2$
x_3
$\neg x_3$
x_4
$\neg x_4$
x_5
$\neg x_5$

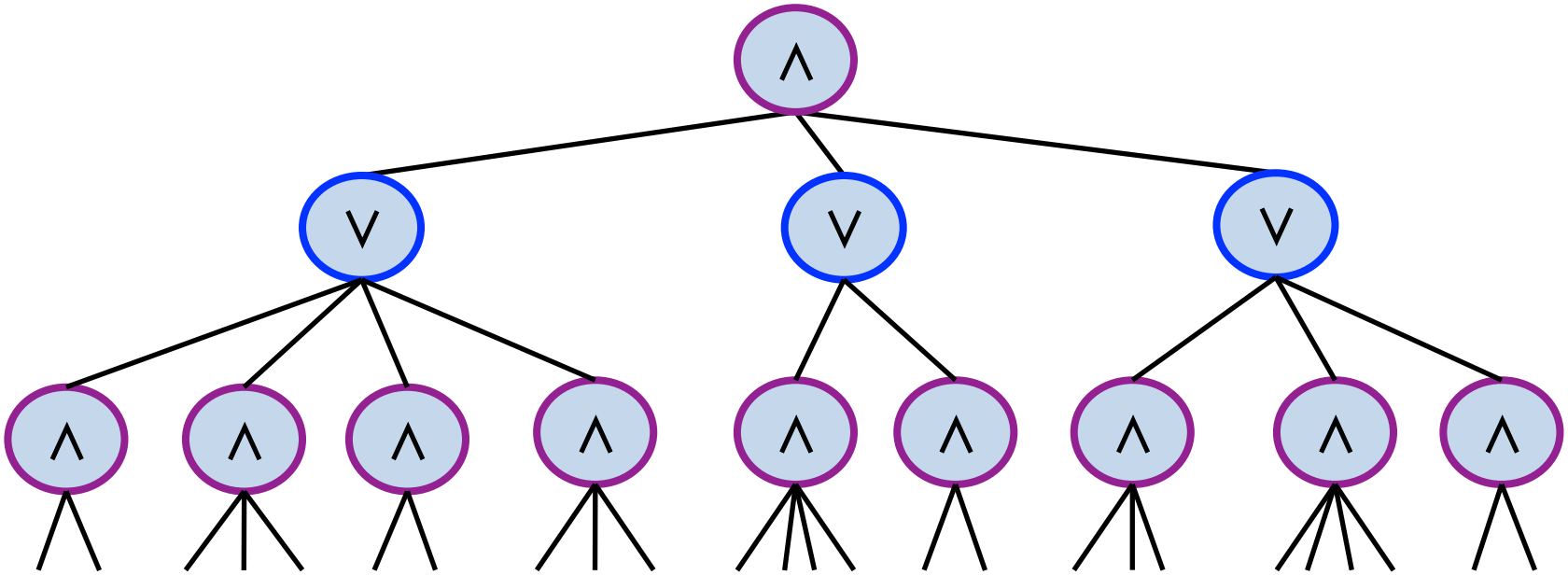

1
0
p
p²
∧
∨
∨
∨
∨
∨
∧
∧
∨
∨
R_p²
R_p
x₁
¬x₁
x₂
¬x₂
x₃
¬x₃
x₄
¬x₄
x₅
¬x₅

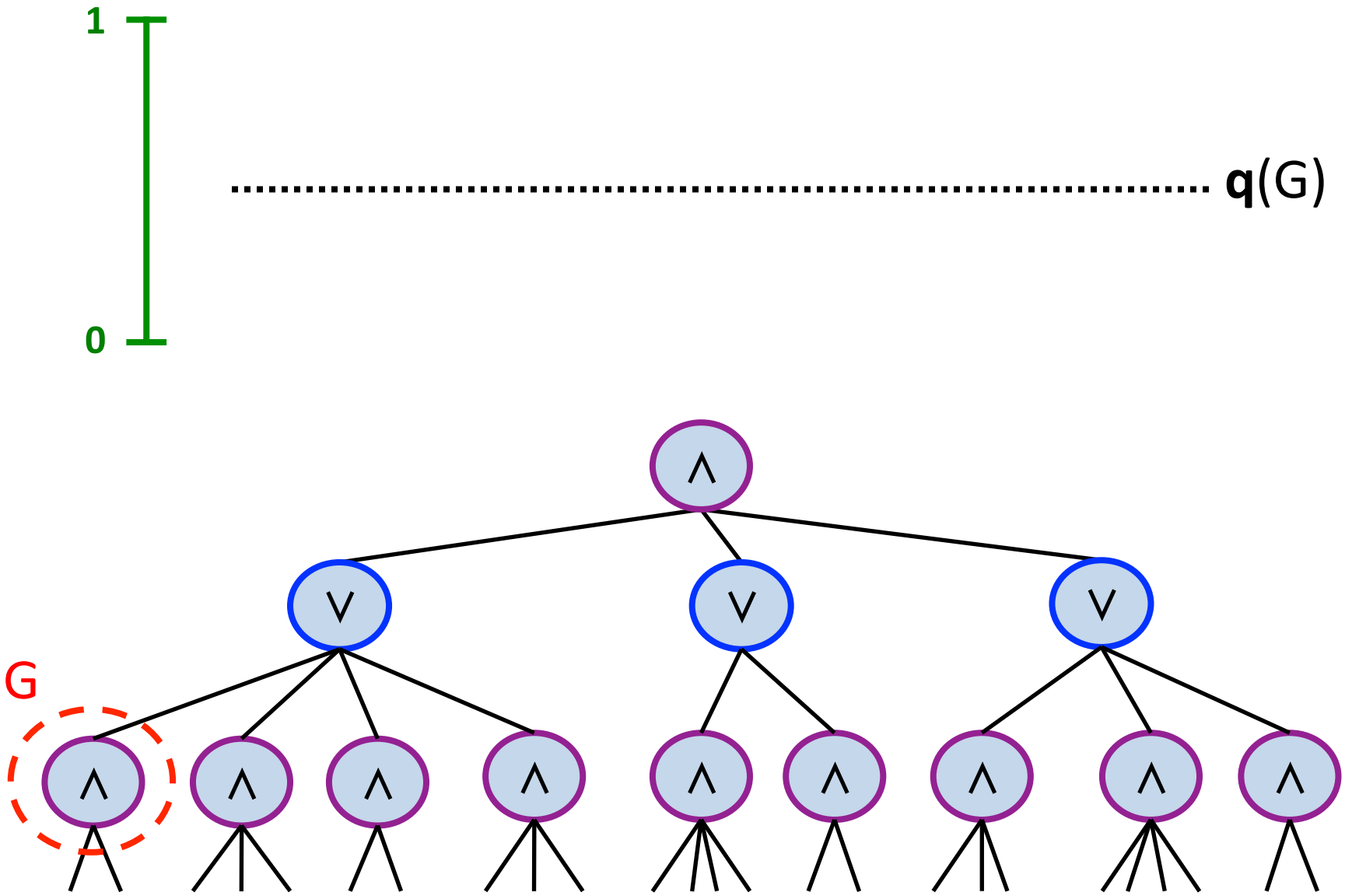

1
0
p
p2
p3
∧
∨
∧
∨
∨
∧
Rp3
Rp2
Rp
x1
¬x1
x2
¬x2
x3
¬x3
x4
¬x4
x5
¬x5

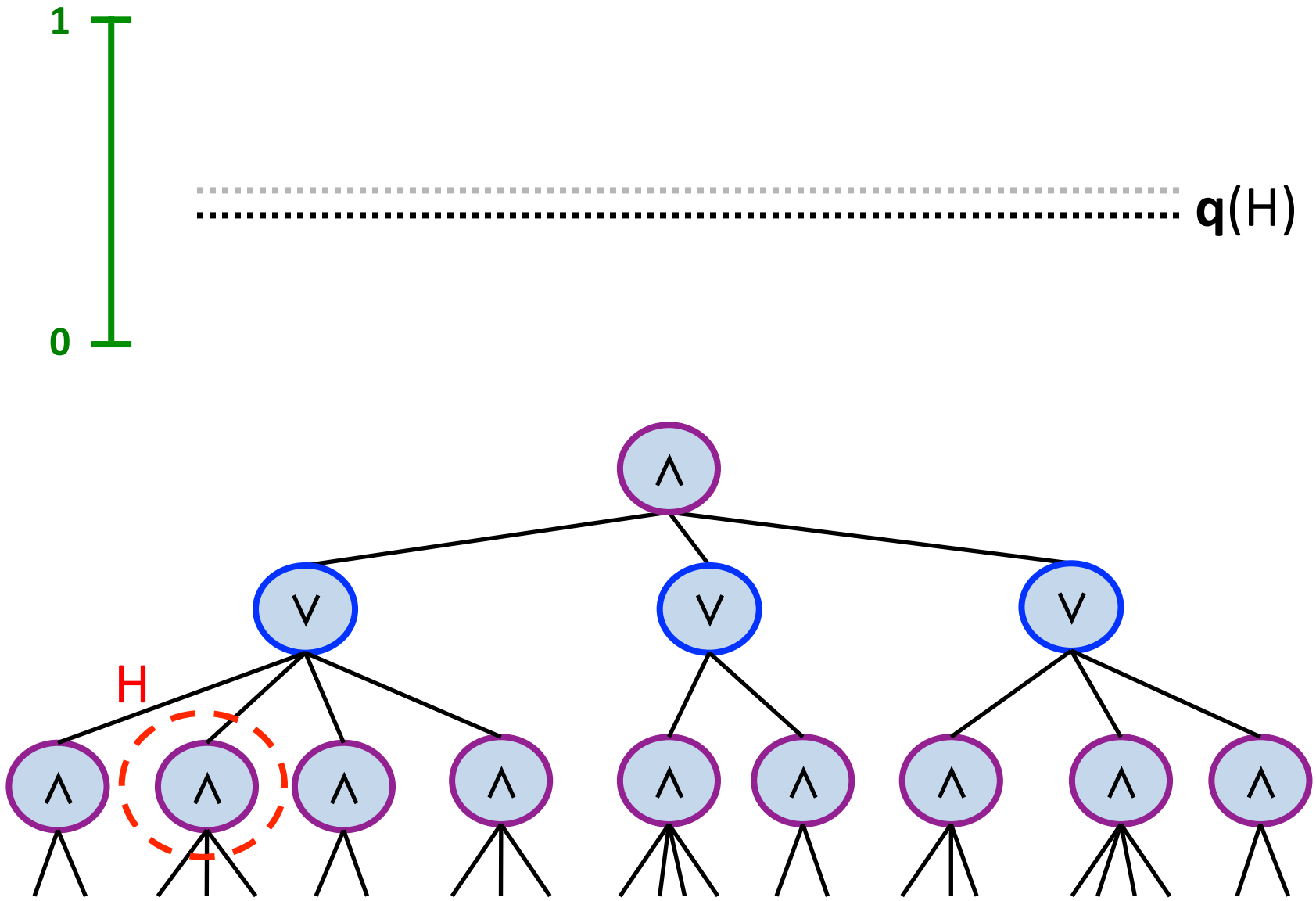

1
0
p
p2
p3
p4
Rp4
Rp3
Rp2
Rp
∨
∧
x1
¬x1
x2
¬x2
x3
¬x3
x4
¬x4
x5
¬x5

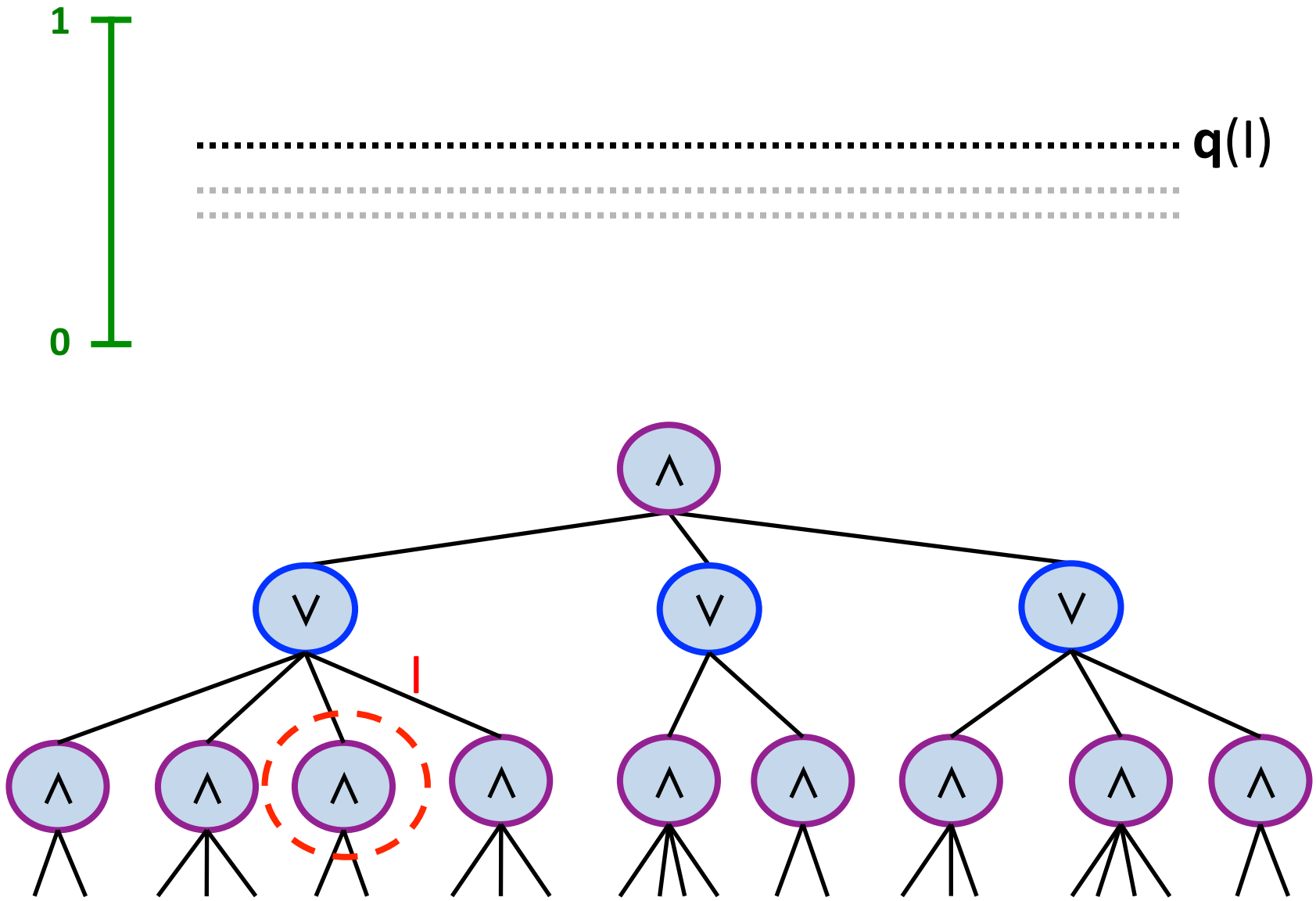

1
0
∧
∨
∨
∨
∧
∧
∧
∧
∧
∧
∧
∧
∧

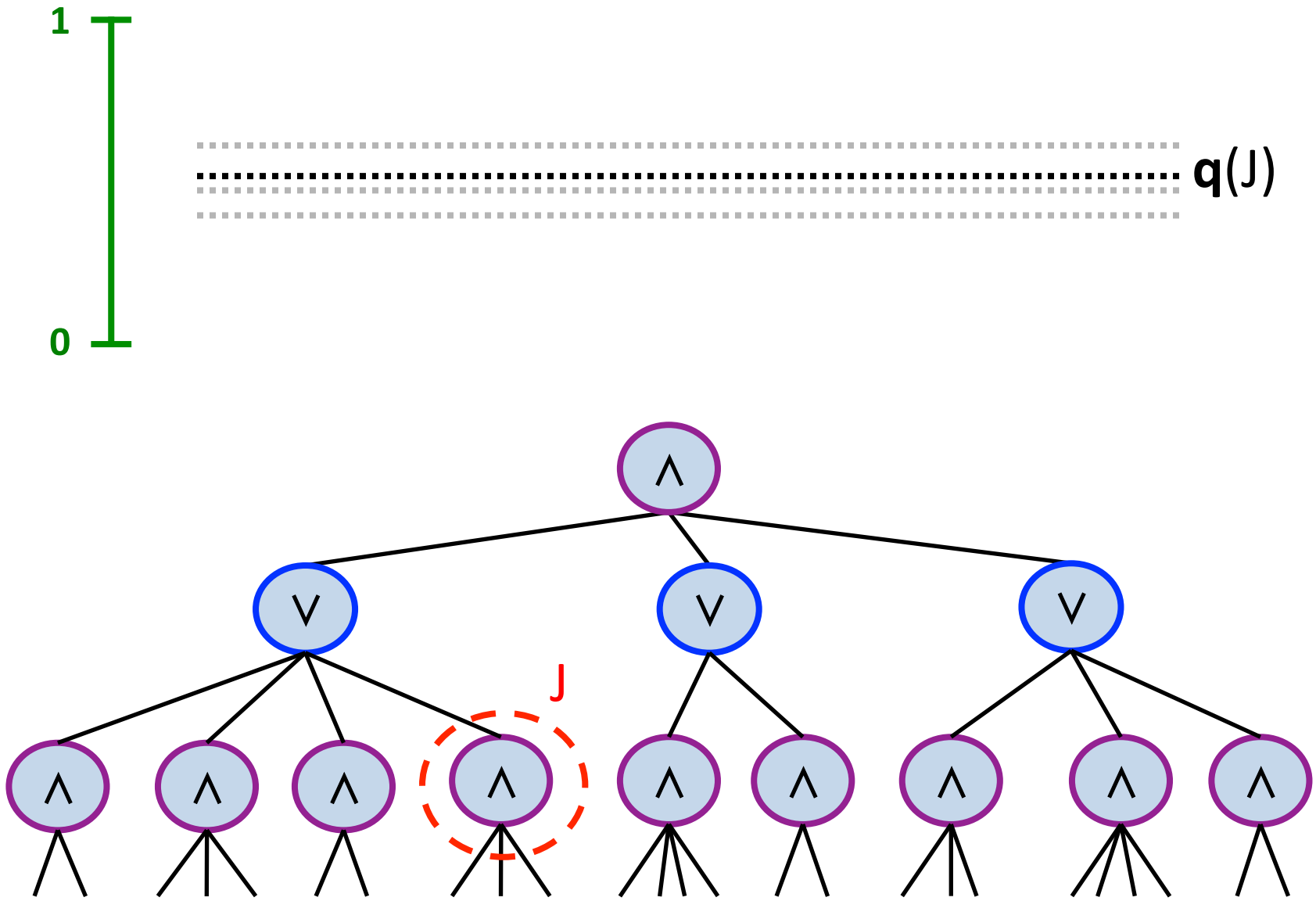
- Each sub-formula F will have its own “stopping time” **q**(F)
- **q**(F) is a random variable in [0,1], which is determined by **σ** and **τ**

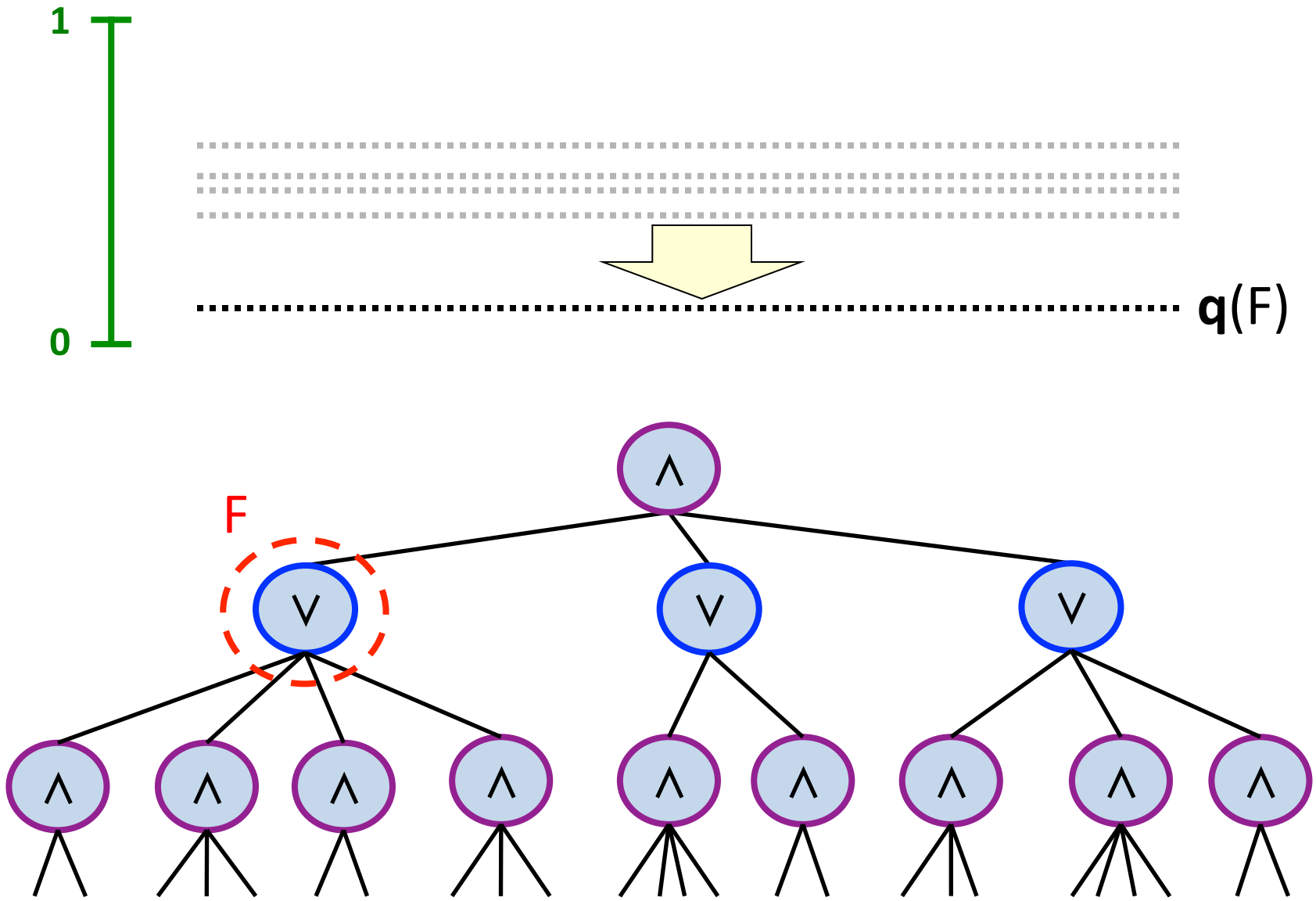


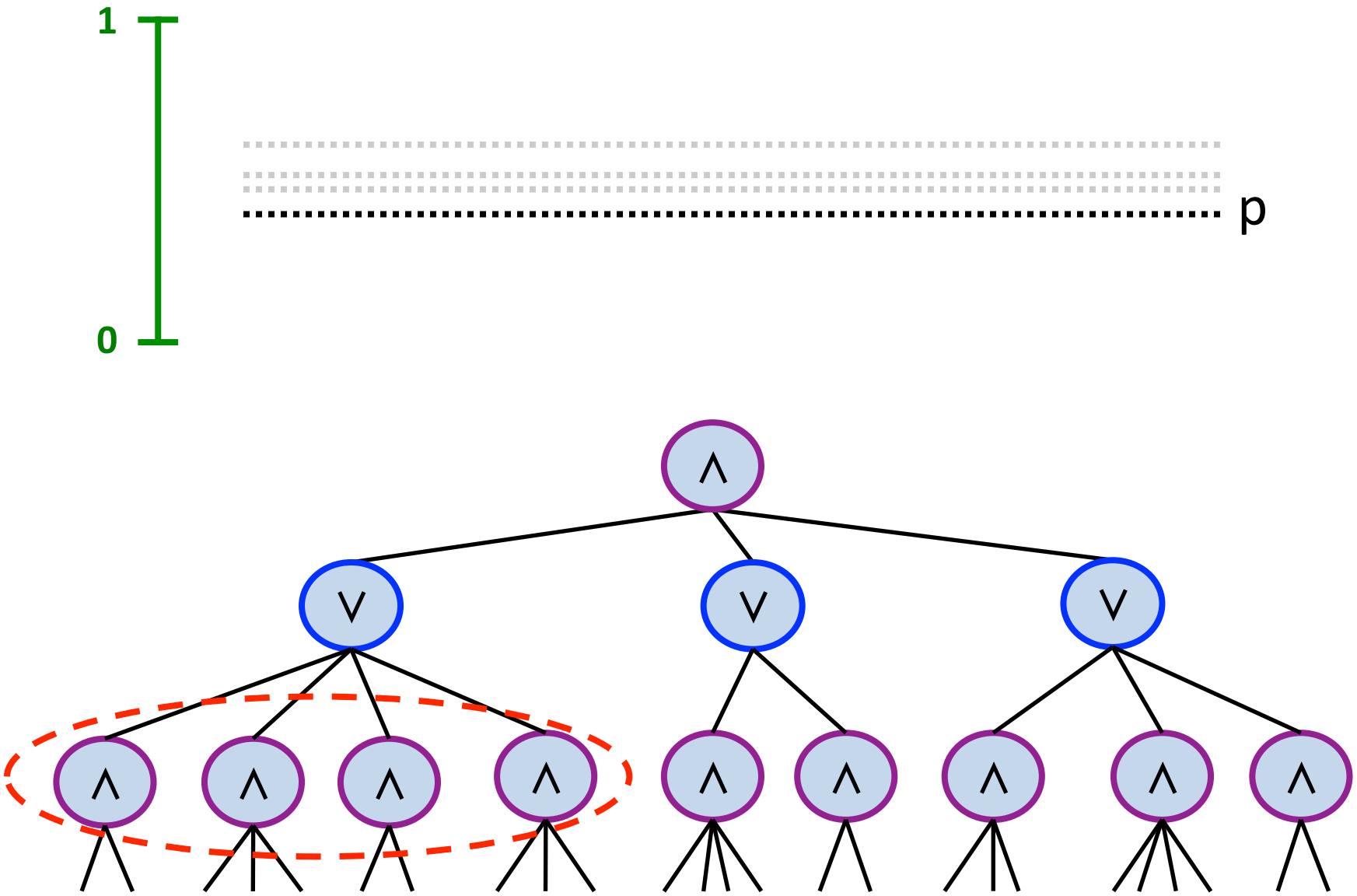

1
0
q(G)
G
∧
∨
∨
∨
∧
∧
∧
∧
∧
∧
∧
∧
∧

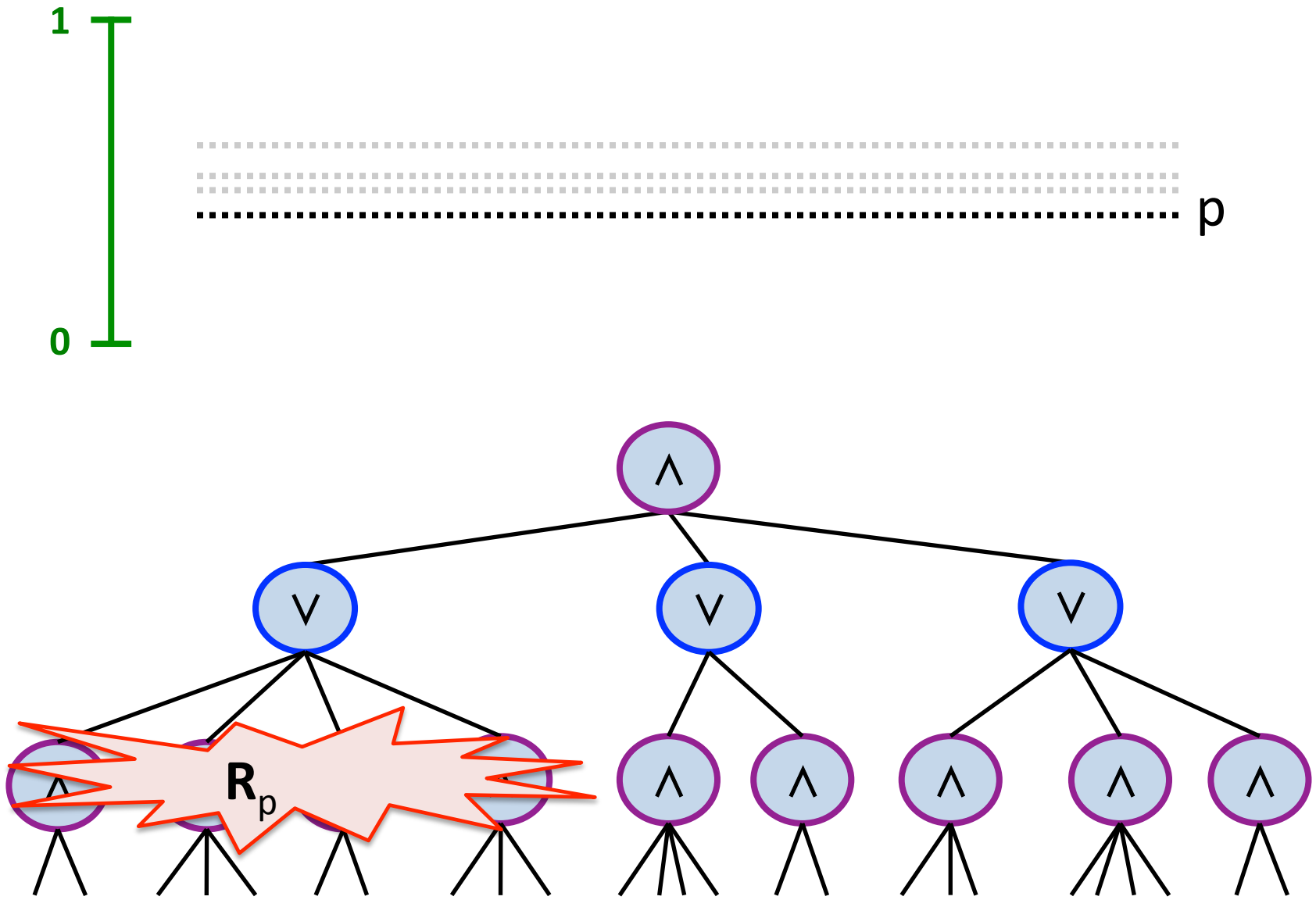

1
0
q(H)
∧
∨
∨
∨
H
∧
∧
∧
∧
∧
∧
∧
∧
∧

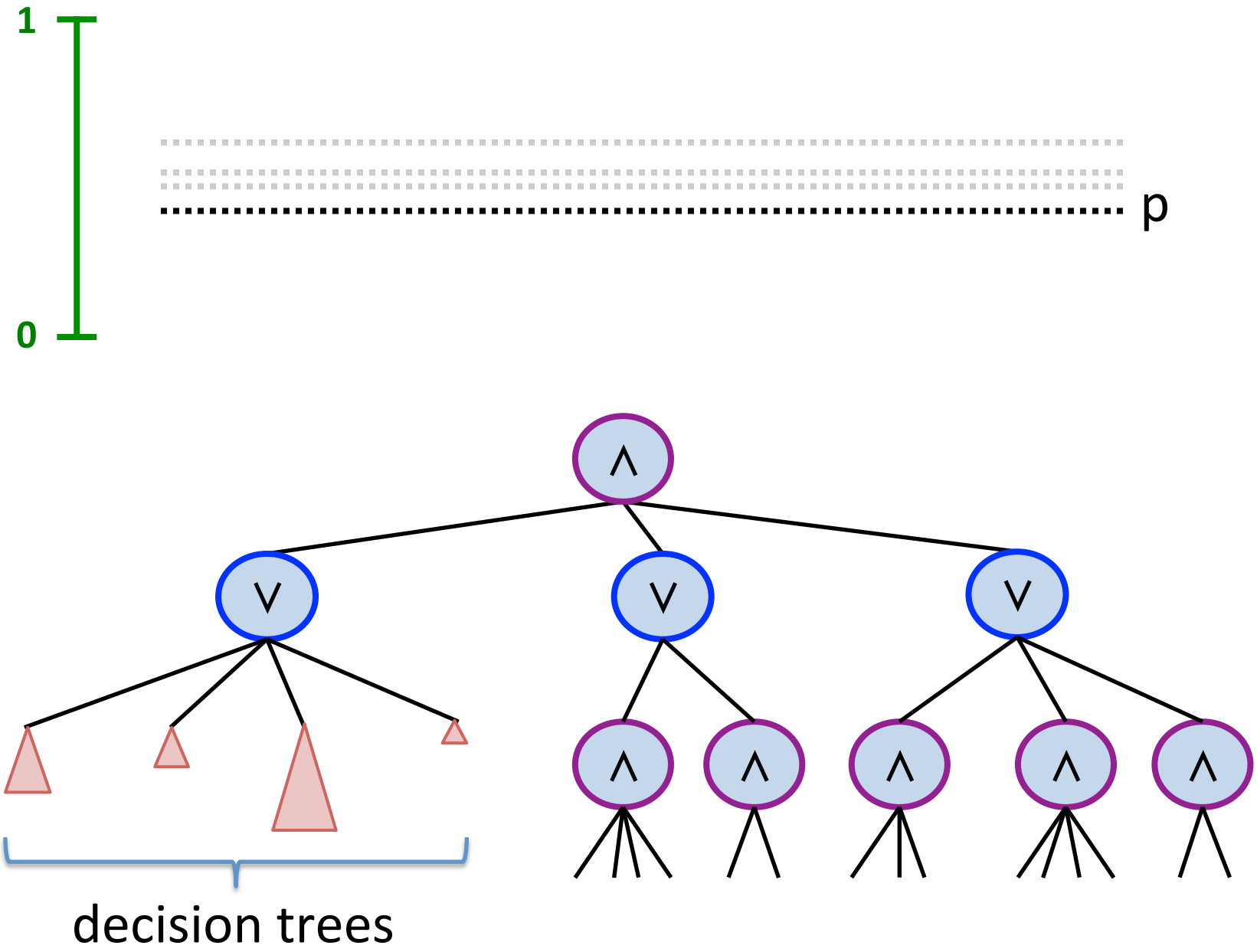

1
0
q(l)
∧
∨
∨
∨
l
∧
∧
∧
∧
∧
∧
∧
∧
∧

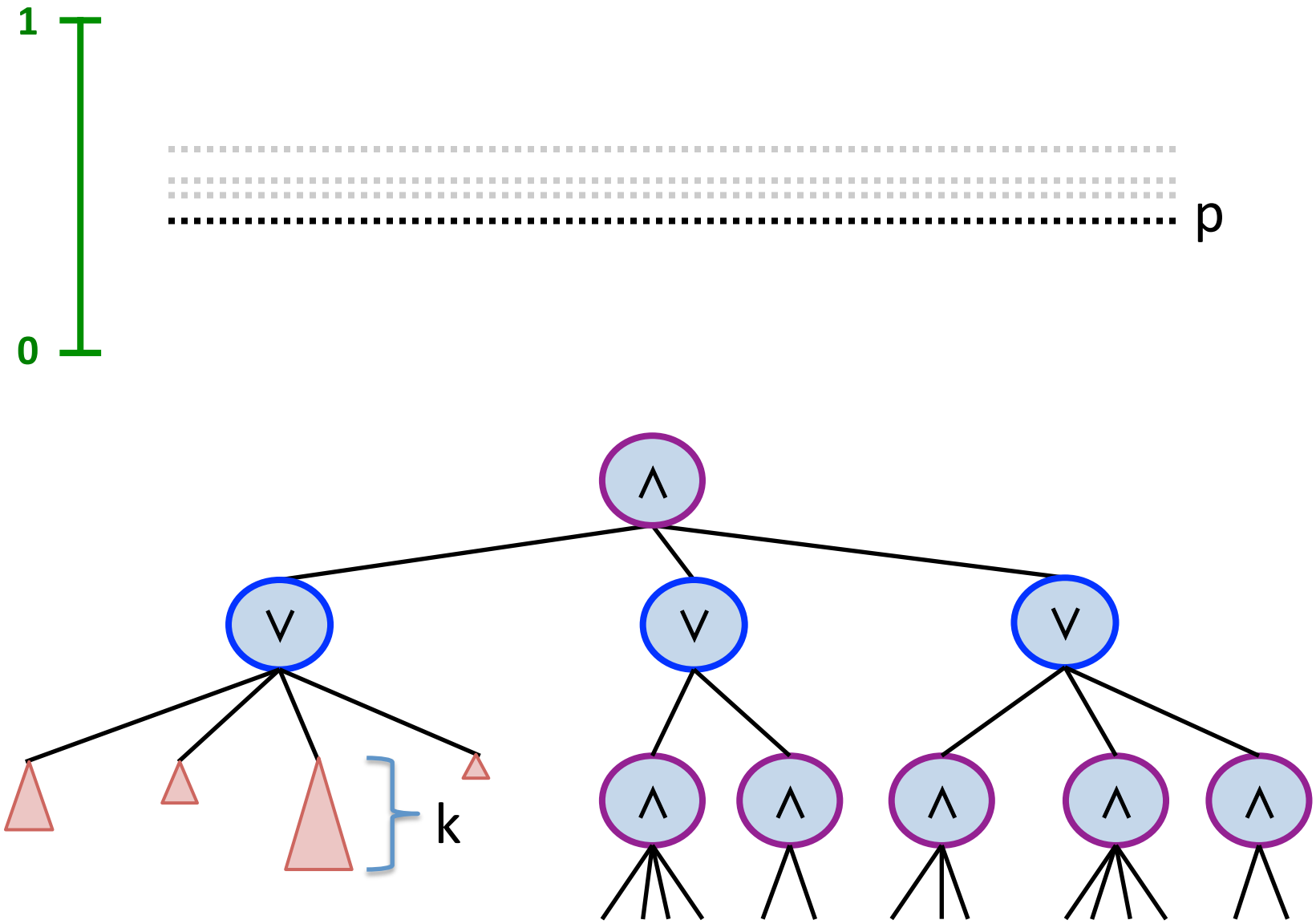

1
0
q(J)
∧
∨
∨
∨
J
∧
∧
∧
∧
∧
∧
∧
∧
∧

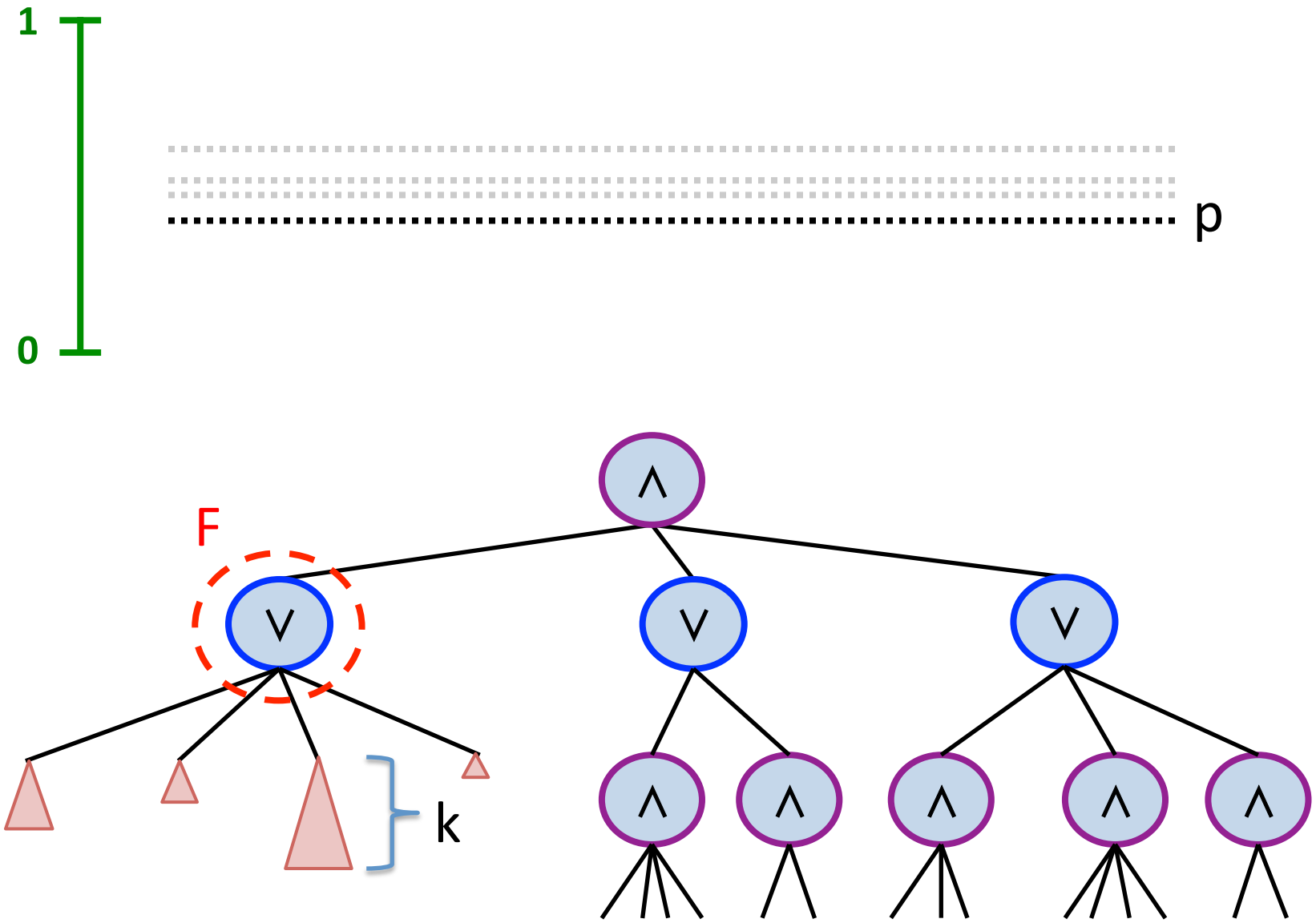

1
0
q(F)
F
∧
∨
∨
∨
∧
∧
∧
∧
∧
∧
∧
∧
∧

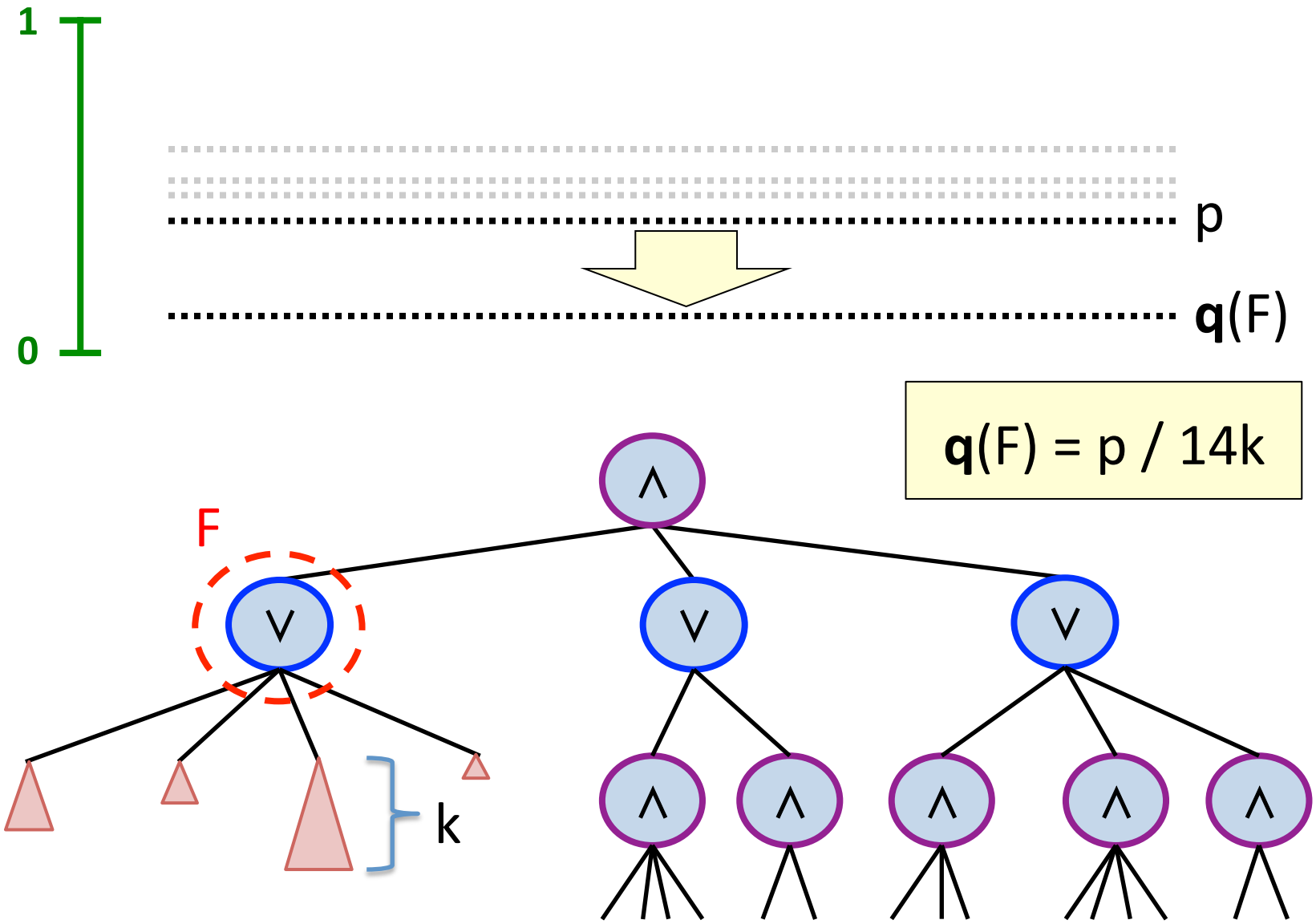

1
0
p
∧
∨
∨
∨
∧
∧
∧
∧
∧
∧
∧
∧
∧


1
0
p
∧
∨
∨
∨
∧
∧
∧
∧
∧
R_p


1
0
p
∧
∨
∨
∨
∧
∧
∧
∧
∧
decision trees


1
0
p
∧
∨
∨
∨
∧
∧
∧
∧
∧
k


1
0
p
F
∧
∨
∨
∨
∧
∧
∧
∧
∧
k


1
0
p
q(F)
q(F) = p / 14k
F
∧
∨
∨
∨
∧
∧
∧
∧
∧
k

Hastad's Switching Lemma

If F is k-DNF or k-CNF, then

$$\Pr[\, DT_{depth}(f \restriction \mathbf{R}_{1/14k}) \geq \ell \,] \leq e^{-\ell}$$

"Stopping Time Version"

For every Boolean formula F,

$$\Pr[\, DT_{depth}(F \restriction \mathbf{R}_{\mathbf{q}(F)}) \geq \ell \,] \leq e^{-\ell}$$

Technical Main Lemma (tail bound for **q**(F))

If F has depth d+1, then for all $0 \le \lambda \le 1$,

$$\Pr[\ \mathbf{q}(F) \le \lambda\ ] \ \le\ \text{size}(F) \times \frac{C^d}{\exp(\Omega(d\lambda^{-1/d}))}$$

- The constant $C < 8$ is defined by

$$1 + \sum_{i=0}^{\infty} \frac{1}{\exp(e^{i-1} - (i+1)e^{-2})} + \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} \frac{1}{\exp((j+1)e^{i-1} - (i+j+2)e^{-2})}$$

Technical Main Lemma (tail bound for **q**(F))

If F has depth d+1, then for all $0 \le \lambda \le 1$,

$$\Pr[\, \mathbf{q}(F) \le \lambda \,] \;\le\; \mathrm{size}(F) \times \frac{C^d}{\exp(\Omega(d\lambda^{-1/d}))}$$

Corollary

Depth d+1 formulas for PARITY have size

$$\exp(\Omega(dn^{1/d}) - O(d))$$

Proof of Hastad's Switching Lemma

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

Switching Lemma:

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

- 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 $\restriction$ R)) $\geq \ell$ }
- <u>Goal</u>. Pr[$\mathbf{R}_p \in$ BAD] = $O(pk)^{\ell}$

<u>Key idea</u>. We associate each R $\in$ 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 $\restriction$ R)) $\geq \ell$ }
- <u>Goal</u>. Pr[$\mathbf{R}_p \in$ BAD] = $O(pk)^\ell$

<u>Key idea</u>. We associate each R $\in$ 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($F \restriction R$)) $\geq \ell$ }
- <u>Goal</u>. Pr[$\mathbf{R}_p \in$ BAD] = $O(pk)^\ell$

<u>Key idea</u>. We associate each R $\in$ 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] = $((1-p)/2p)^\ell$

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 $R \in BAD$ with a restriction R^* such that

① $|Stars(R^*)| = |Stars(R)| - \ell$

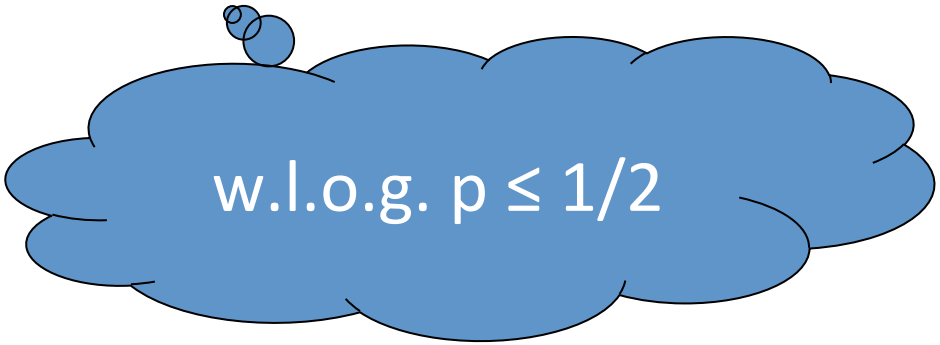
② the map $R \mapsto R^*$ is $(4k)^\ell$-to-1

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

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

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

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



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

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

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

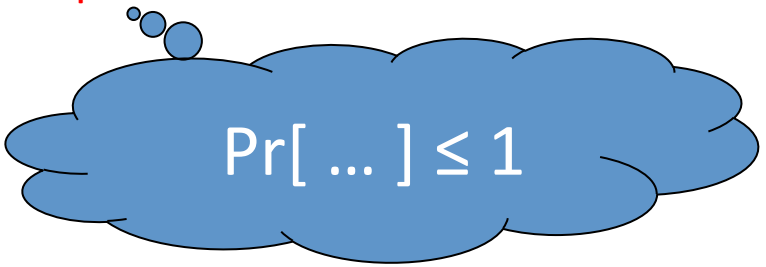
$$\Pr[\, \mathbf{R}_p \in BAD \,]$$

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

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

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

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



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

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

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:

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

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

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

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

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

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

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 $R \in \mathrm{BAD}$ with a pair (R*,Code(R)) such that

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

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 $|Stars(R^*)| = |Stars(R)| - \ell$

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

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

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

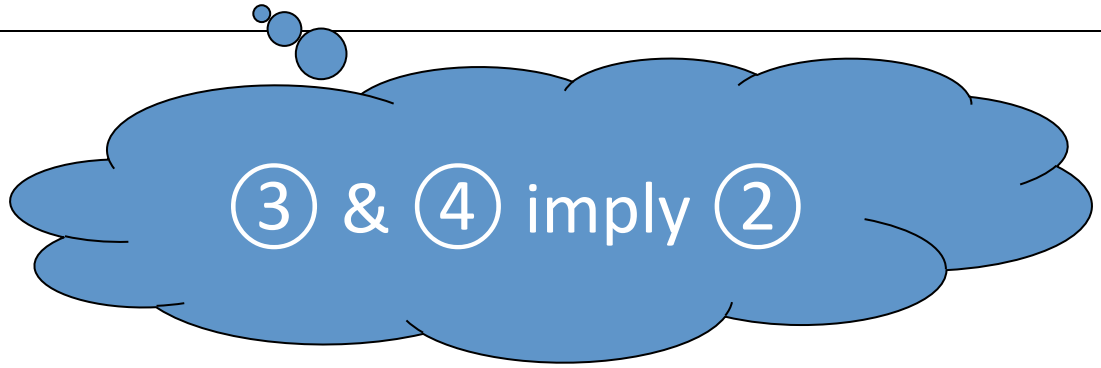
Key idea. We associate each $R \in \mathrm{BAD}$ with a pair $(R^*, \mathrm{Code}(R))$ such that

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 $R \in \text{BAD}$ with a pair $(R^*, \text{Code}(R))$ 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

intuitively, Code(R) is a "recipe" for inverting $R \mapsto (R^*, \text{Code}(R))$ 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, $\ell = 4$

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

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

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

$k = 3,\ \ell = 4$

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

$$F \restriction R = \underset{1}{x_1}\, x_2\, \neg x_3 \vee \underset{0}{\neg x_1}\, x_3\, x_5 \vee \underset{1}{x_2}\, \neg x_4\, x_5 \vee \underset{0}{x_3}\, x_4\, \neg x_6 \vee \underset{1}{x_1}\, \underset{1}{\neg x_4}\, \neg x_7$$

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

$k = 3,\ \ell = 4$

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

1 0 1 0 1 1

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

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

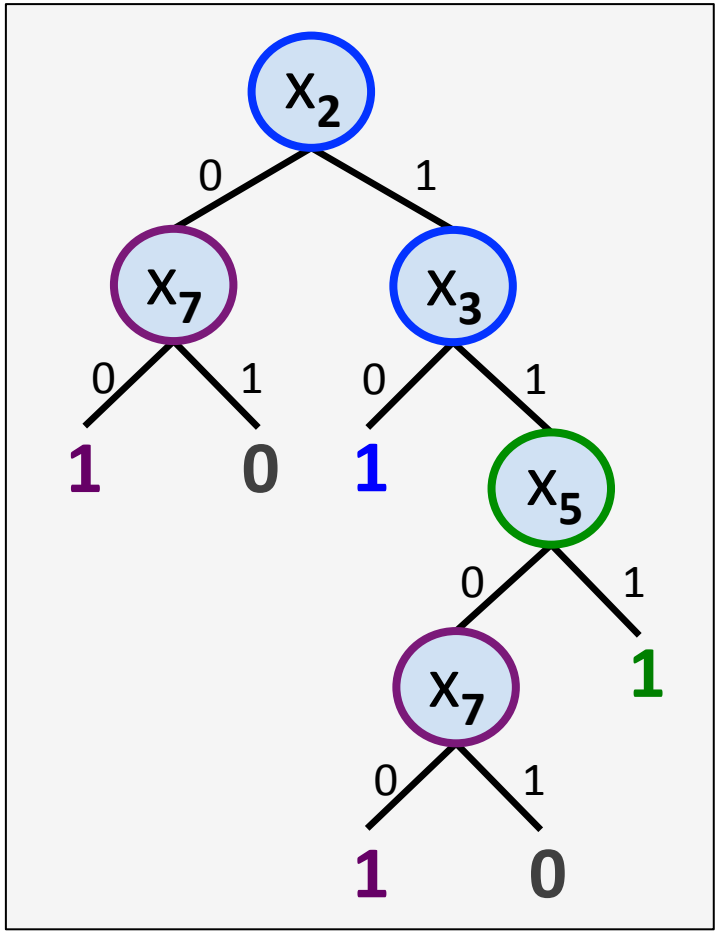
k = 3, $\ell = 4$

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

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

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

CanDT($F \restriction R$) =



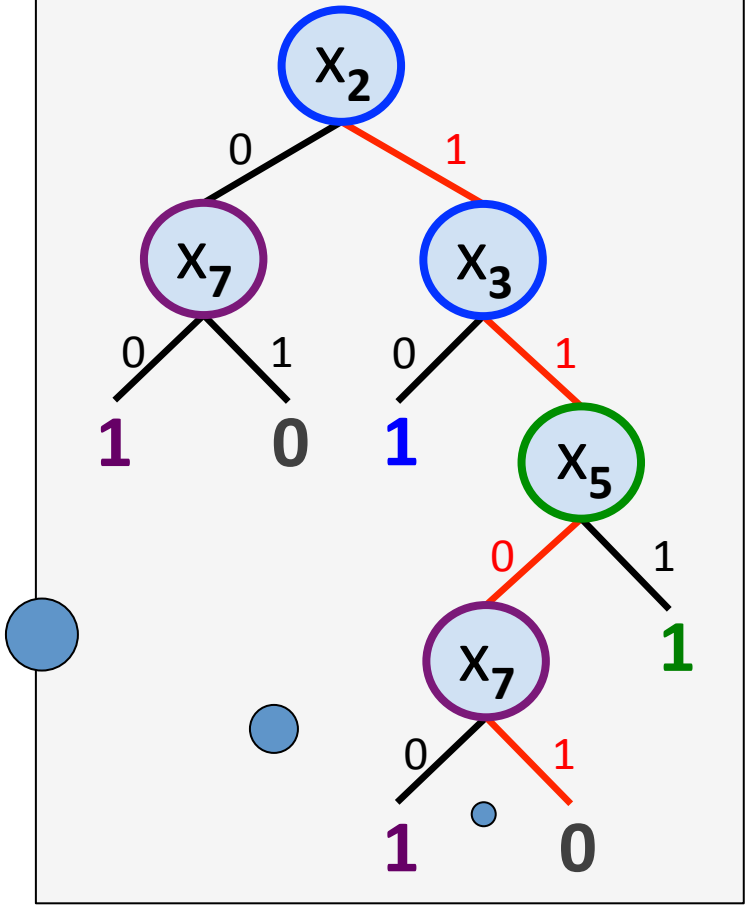
k = 3, $\ell = 4$

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

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

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

R ∈ BAD, since
CanDT(F ↾ R) ≥ ℓ



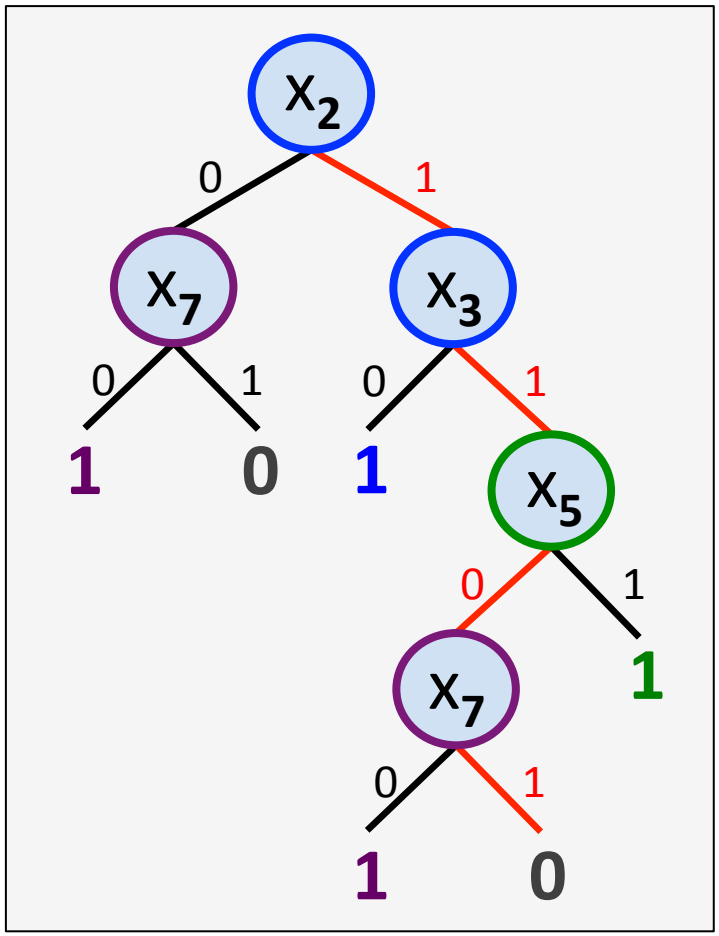
$k = 3,\ \ell = 4$

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

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

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

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



k = 3, $\ell = 4$

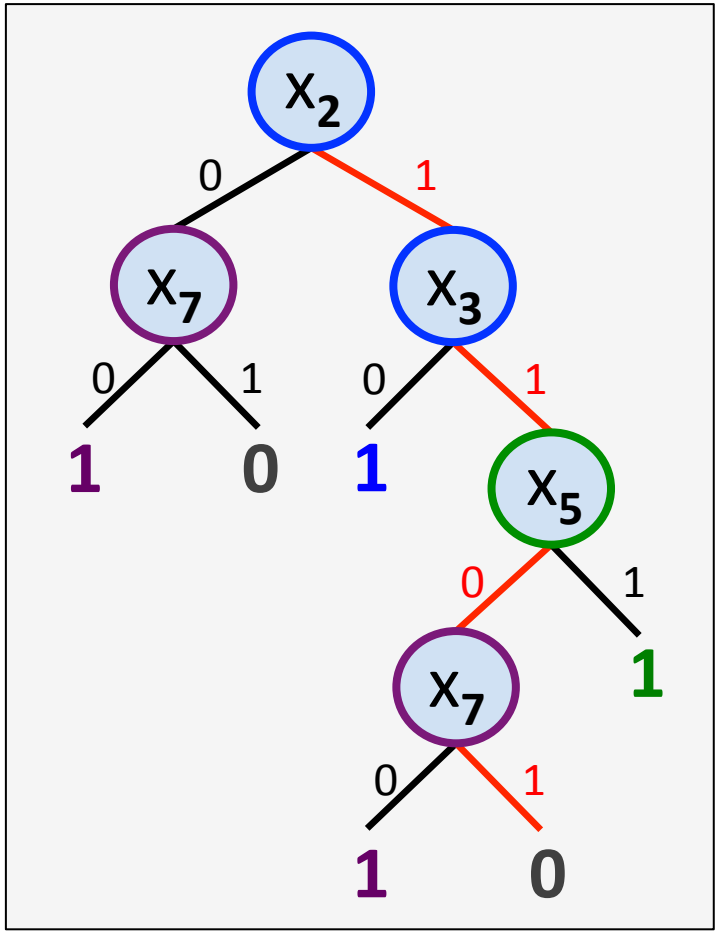
$R \mapsto (R^*, \mathrm{Code}(R))$

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

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

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

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



$k = 3,\ \ell = 4$

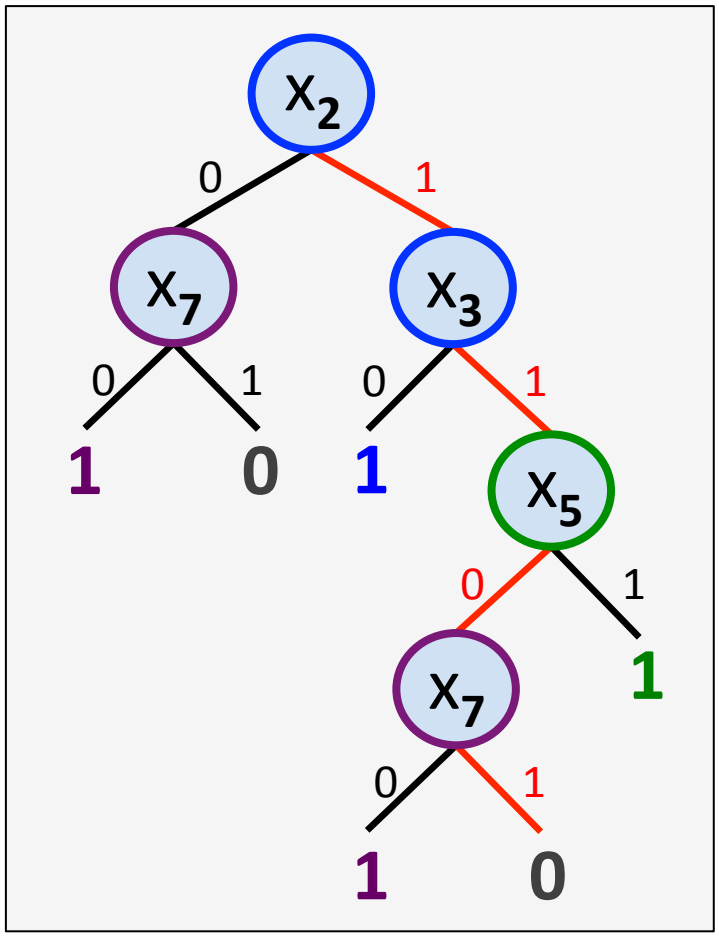
$R \mapsto (R^*, \mathrm{Code}(R))$

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

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

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

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



$k = 3,\ \ell = 4$

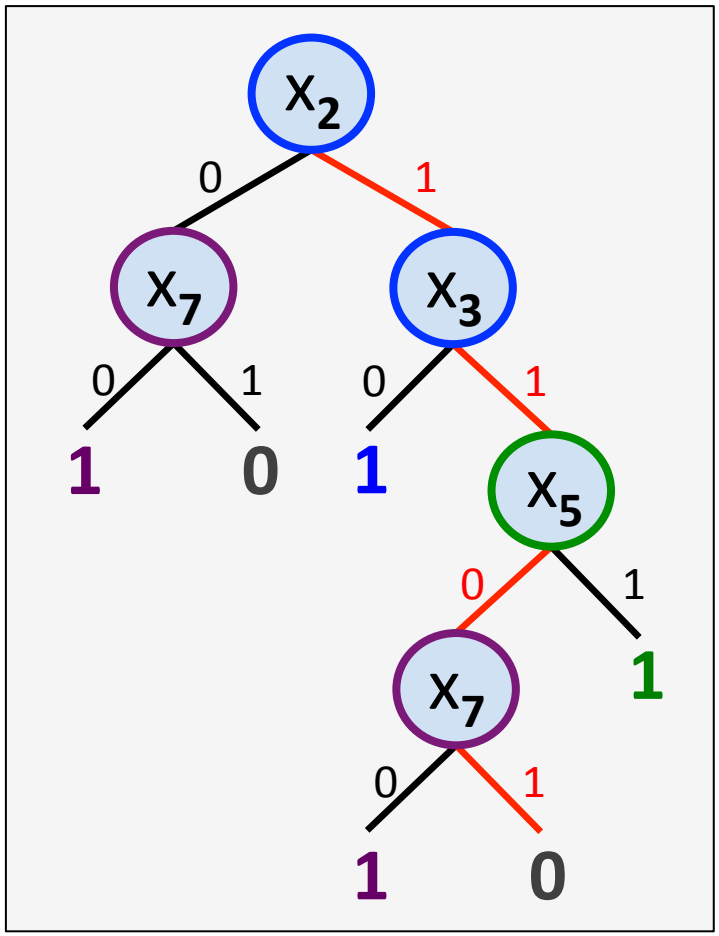
$R \mapsto (R^*, \mathrm{Code}(R))$

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

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

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

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



$k = 3,\ \ell = 4$

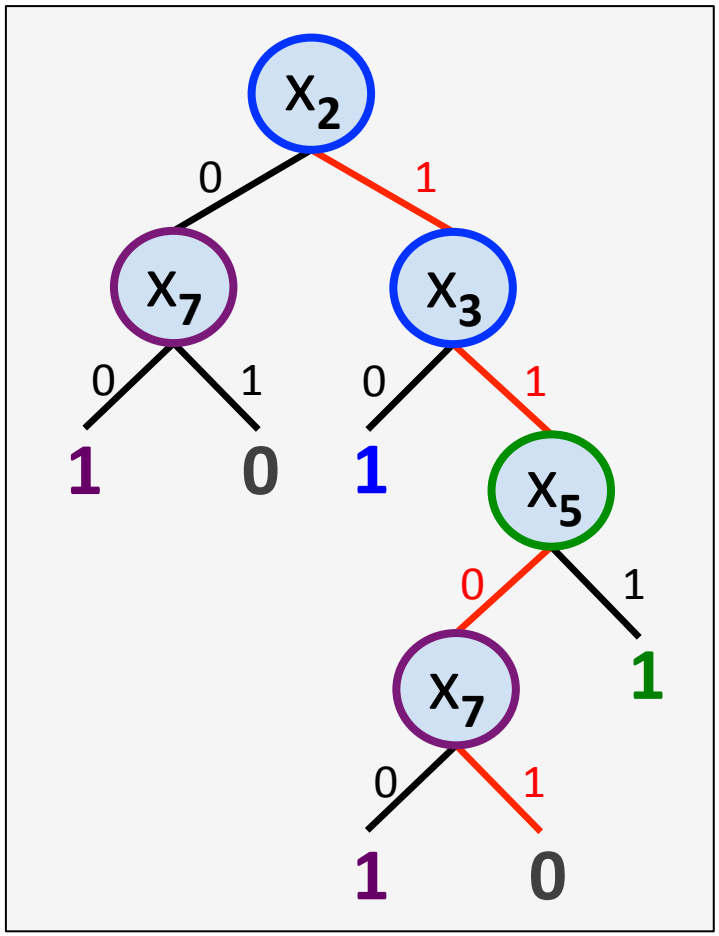
$R \mapsto (R^*, \mathrm{Code}(R))$

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

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

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

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



$k = 3,\ \ell = 4$

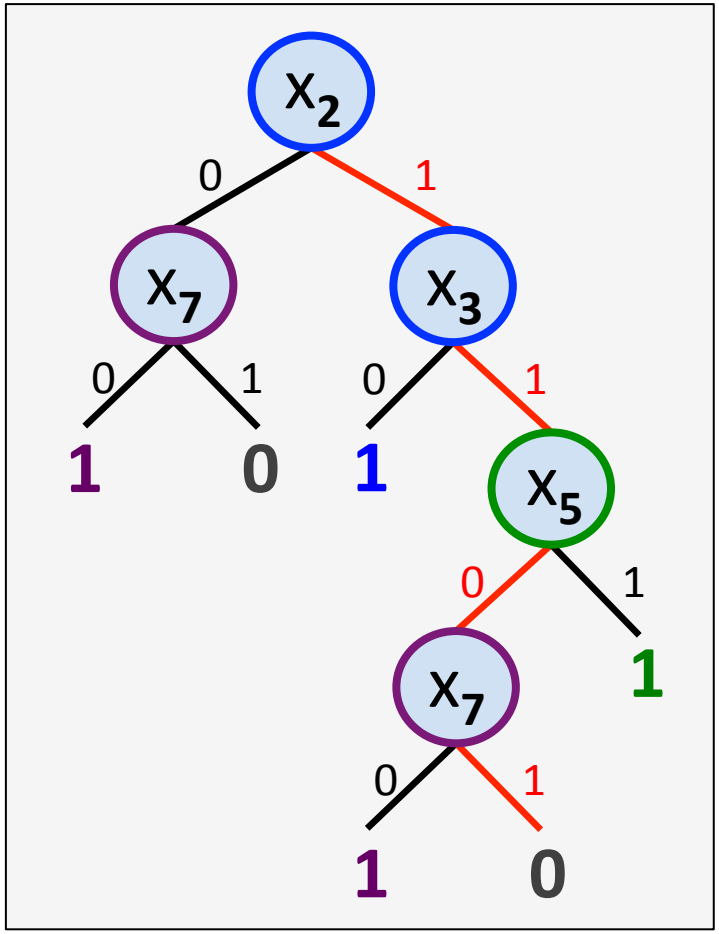
$R \mapsto (R^*, \mathrm{Code}(R))$

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

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

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

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



k = 3, $\ell = 4$

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

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

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

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

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

Code(R) says:

- find the first satisfied term of $F \restriction R^*$
- the "long path" begins with

  $x_2 \mapsto 1, x_3 \mapsto 1$

  (i.e. var_2 of term $\mapsto 1$ and var_3 of term $\mapsto 1$)
- …

$k = 3,\ \ell = 4$

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

1 0 1

$F_R = x_1 x_2 \neg x_3 \vee \neg x_1 \neg x_3 x_5 \vee x_2 \neg x_4 x_5 \vee x_3 \neg x_4 \neg x_5 \vee x_1 \neg x_4 \neg x_7$

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

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

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

Fix variables according to the beginning of the long path

$k = 3,\ \ell = 4$

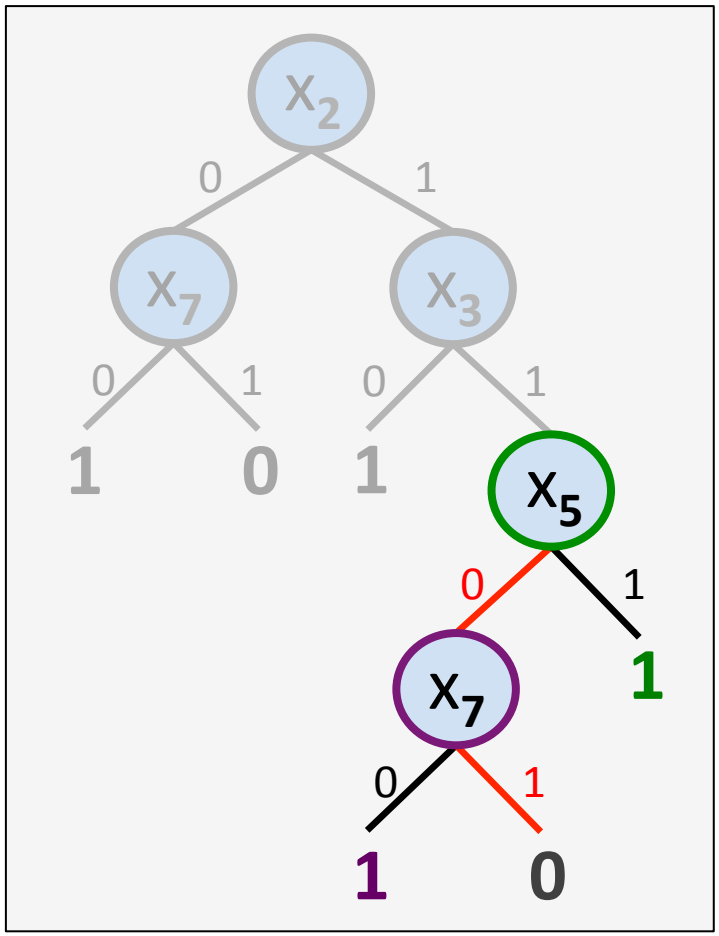
$R \mapsto (R^*, \mathrm{Code}(R))$

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

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

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

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



$k = 3,\ \ell = 4$

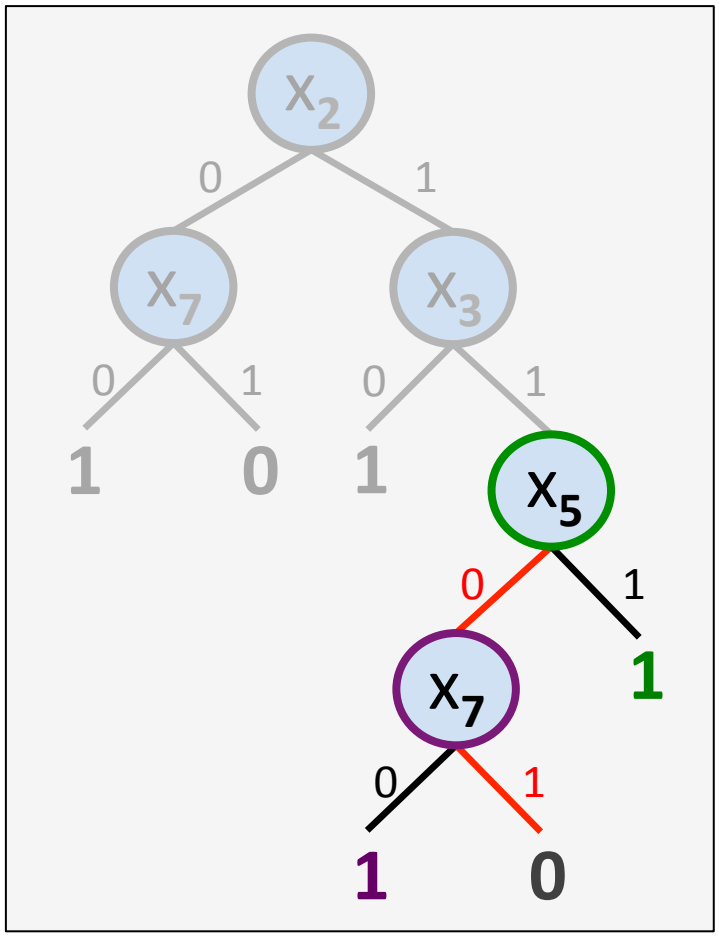
$R \mapsto (R^*, \mathrm{Code}(R))$

$F \upharpoonright R = [\ldots] \vee [\ldots] \vee x_2\, \neg x_4\, x_5 \vee [\ldots] \vee x_1\, \neg x_4\, \neg x_7$

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

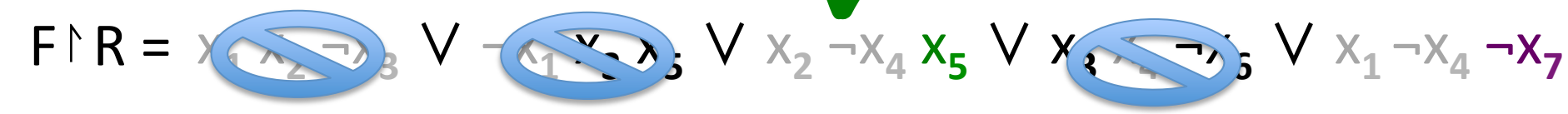
$R\sim = \{ x_1 \mapsto 1,\ x_4 \mapsto 0,$
$x_2 \mapsto 1,\ x_3 \mapsto 1,$
$x_5 \mapsto \quad x_7 \mapsto \quad \}$

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



$k = 3,\ \ell = 4$

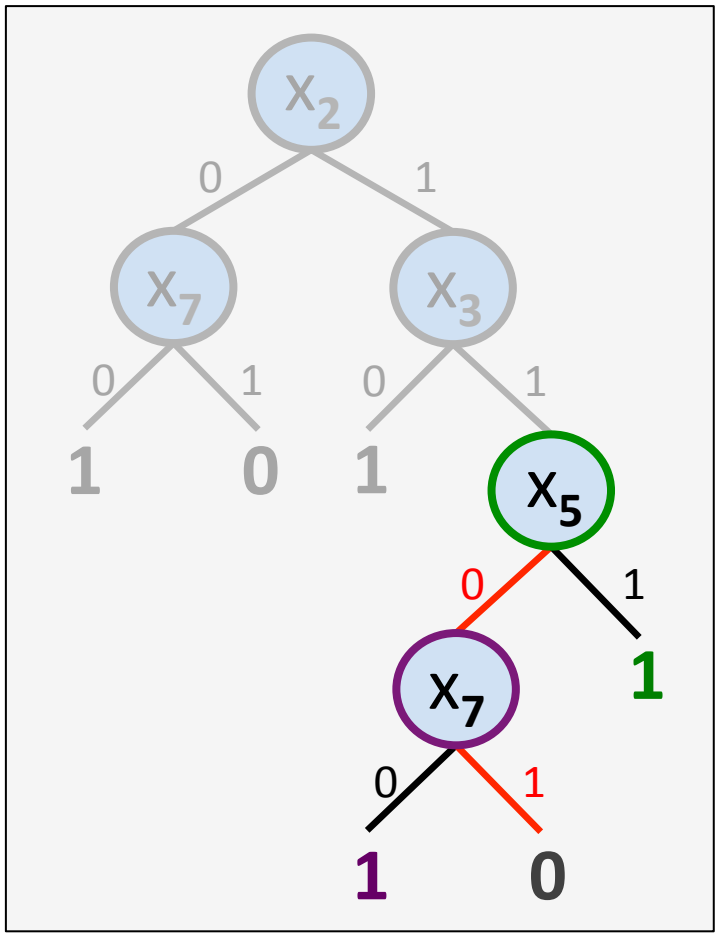
$R \mapsto (R^*, \mathrm{Code}(R))$



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

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

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



$k = 3,\ \ell = 4$

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

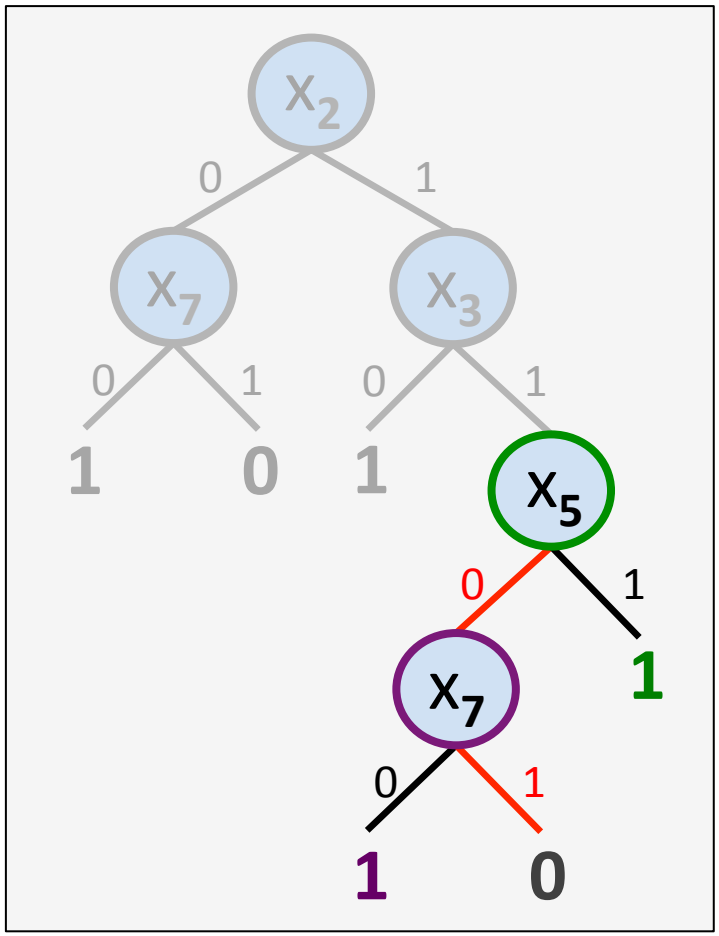
✓

$F \upharpoonright R = \cancel{X_1\ X_2\ \neg X_3} \vee \cancel{\neg X_1\ X_3\ X_5} \vee X_2\ \neg X_4\ X_5 \vee \cancel{X_3\ \neg X_4\ \neg X_6} \vee X_1\ \neg X_4\ \neg X_7$

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

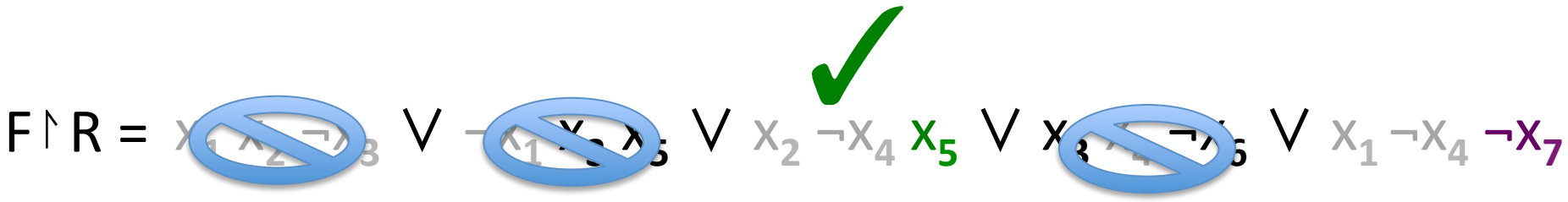
$R\sim = \{ x_1 \mapsto 1, x_4 \mapsto 0,$
$x_2 \mapsto 1, x_3 \mapsto 1,$
$x_5 \mapsto 0\ x_7 \mapsto \ \ \}$

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



$k = 3,\ \ell = 4$

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



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

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

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

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 $\mapsto 0$)
- …

$k = 3,\ \ell = 4$

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

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

0

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

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

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

Fix variables according to the long path

$k = 3,\ \ell = 4$

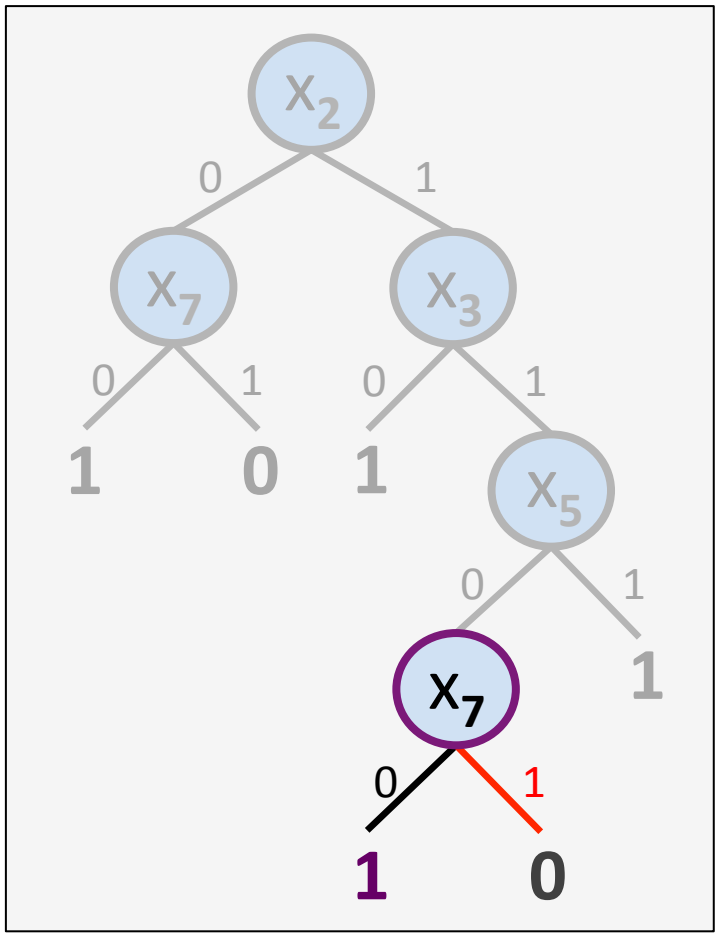
$R \mapsto (R^*, \mathrm{Code}(R))$

$F \upharpoonright R = \quad \vee \quad \vee \quad \vee \quad \vee\ x_1\, \neg x_4\, \neg x_7$

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

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

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



$k = 3,\ \ell = 4$

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

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

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

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

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

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

given knowledge of R^* (and F), follow these instructions to recover R (and along the way $R\sim$)

$k = 3,\ \ell = 4$

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

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

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

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

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

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

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

A Different Approach

A Different Approach

Hastad's Switching Lemma

If F is a k-DNF, then

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

Weak (but flexible) Switching Lemma

If F is a k-DNF, then

$$\Pr[\ \text{depth}(\text{CanDT}(F) \restriction \mathbf{R}_p) \geq \ell\ ] = O(pk2^k)^{\ell}$$

Shows that PARITY has depth-d circuit size

$$\exp\left(\Omega\left(\left(\frac{\log n}{d}\right)^2\right)\right)$$

Weak (but flexible) Switching Lemma

If F is a k-DNF, then

$$\Pr[\ \text{depth}(\text{CanDT}(F) \restriction \mathbf{R}_p) \geq \ell\ ] = O(pk2^k)^{\ell}$$

Proof generalizes to *affine restrictions!*

Weak (but flexible) Switching Lemma

If F is a k-DNF, then

$$\Pr[\ \mathrm{depth}(\mathrm{CanDT}(F) \restriction \mathbf{R}_p) \geq \ell\ ] = O(pk2^k)^{\ell}$$

A Different Approach

1. Decision Tree Switching Lemma
2. k-Clipped Decision Trees
3. Arbitrary Distribution of Stars
4. *Switching Lemma for Affine Restrictions*
5. Tseitin Expander Switching Lemma

A Different Approach

1. **Decision Tree Switching Lemma**
2. k-Clipped Decision Trees
3. Arbitrary Distribution of Stars
4. *Switching Lemma for Affine Restrictions*
5. Tseitin Expander Switching Lemma

Binomial Distribution

- For a finite set N, let

$$\mathbf{S} \subseteq_p N$$

  Denote "**S** is a p-biased random subset of N", i.e.,

$$\Pr[\ \mathbf{S} = S\ ] = p^{|S|}(1-p)^{|N|-|S|}$$

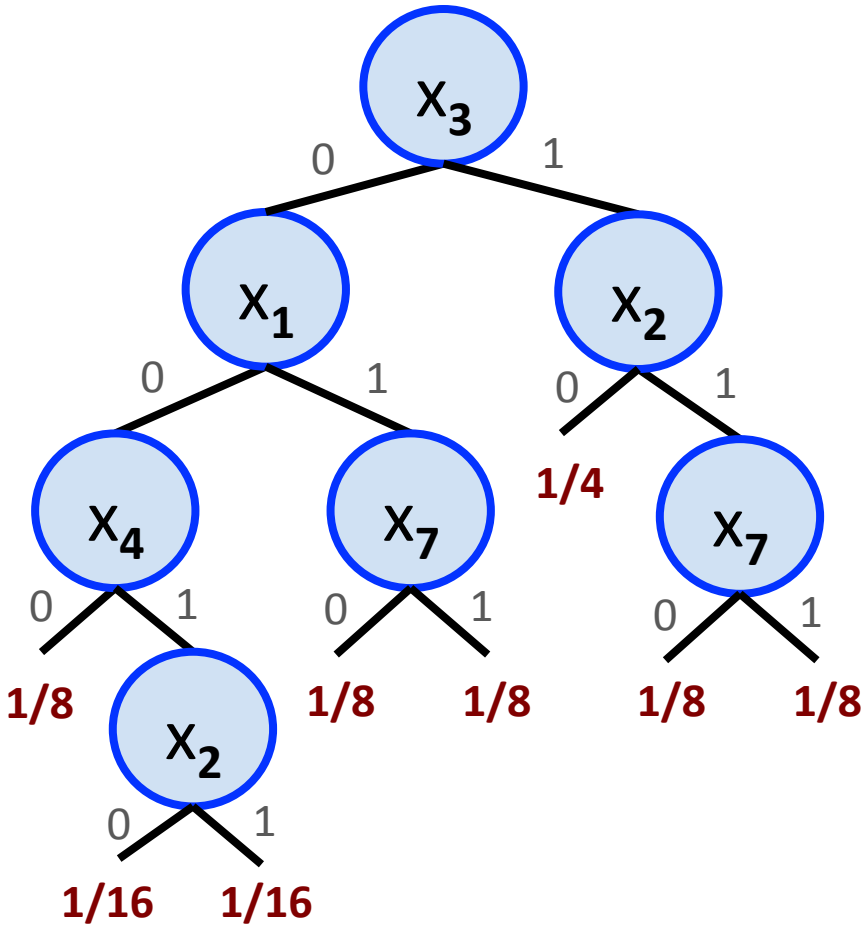
- For a natural number n and $0 \le p \le 1$, the *binomial random variable* **Bin**(n,p) is equivalent to $|\mathbf{S}|$ where $\mathbf{S} \subseteq_p [n]$

Decision Tree Switching Lemma

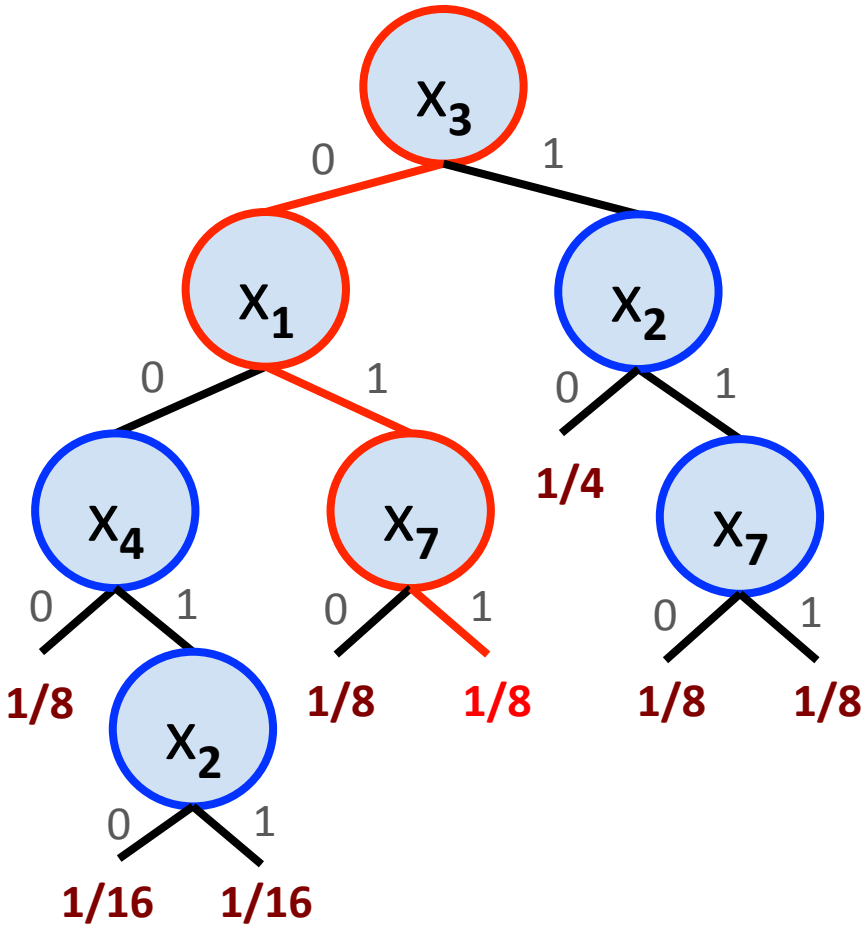
If T is a depth-k decision tree, then

$$\Pr[\ \mathrm{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ] \leq (2pk)^{\ell}$$

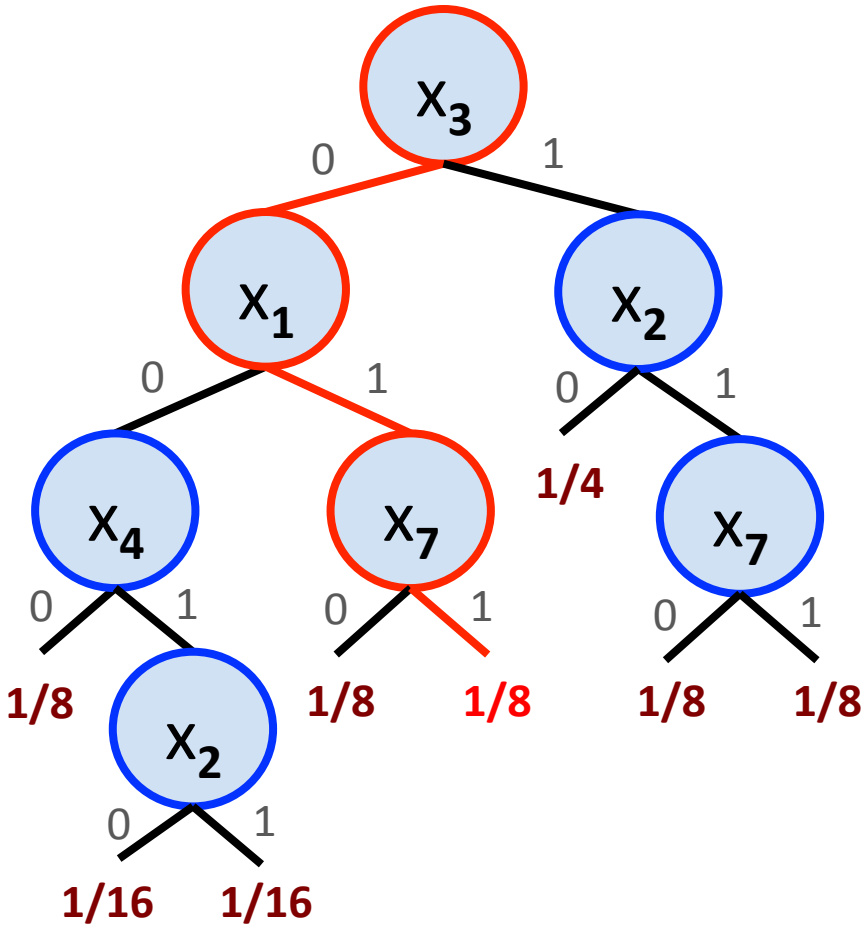
- Consider a **random branch** of T:



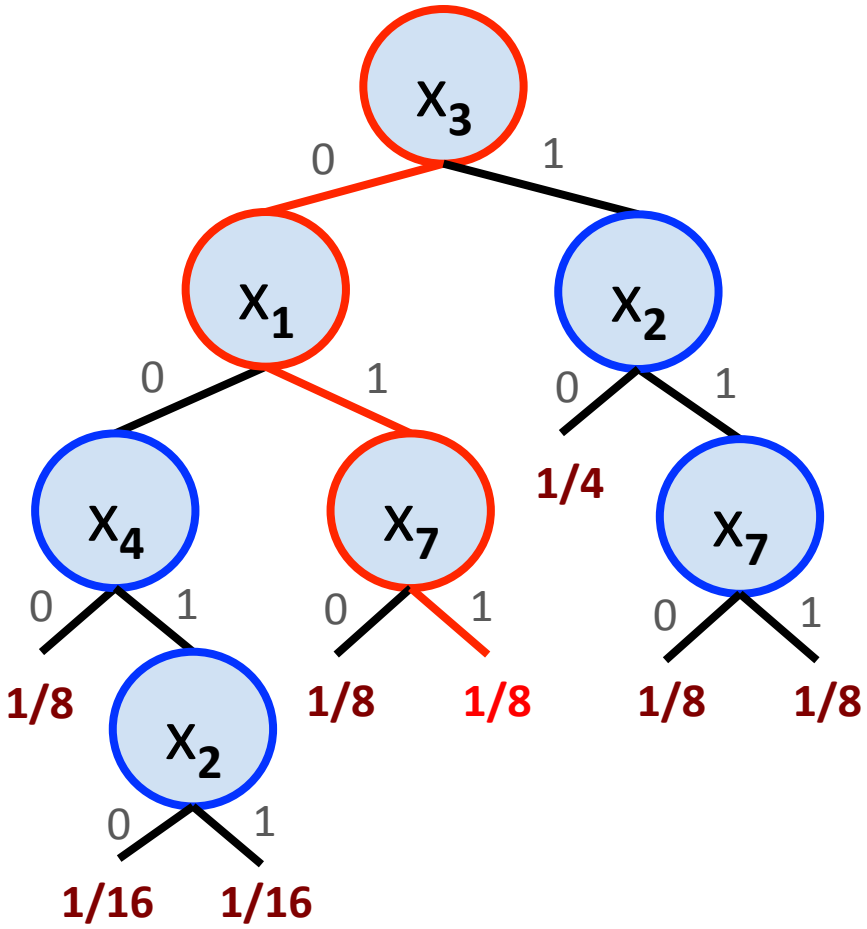
- Consider a **random branch** of T:



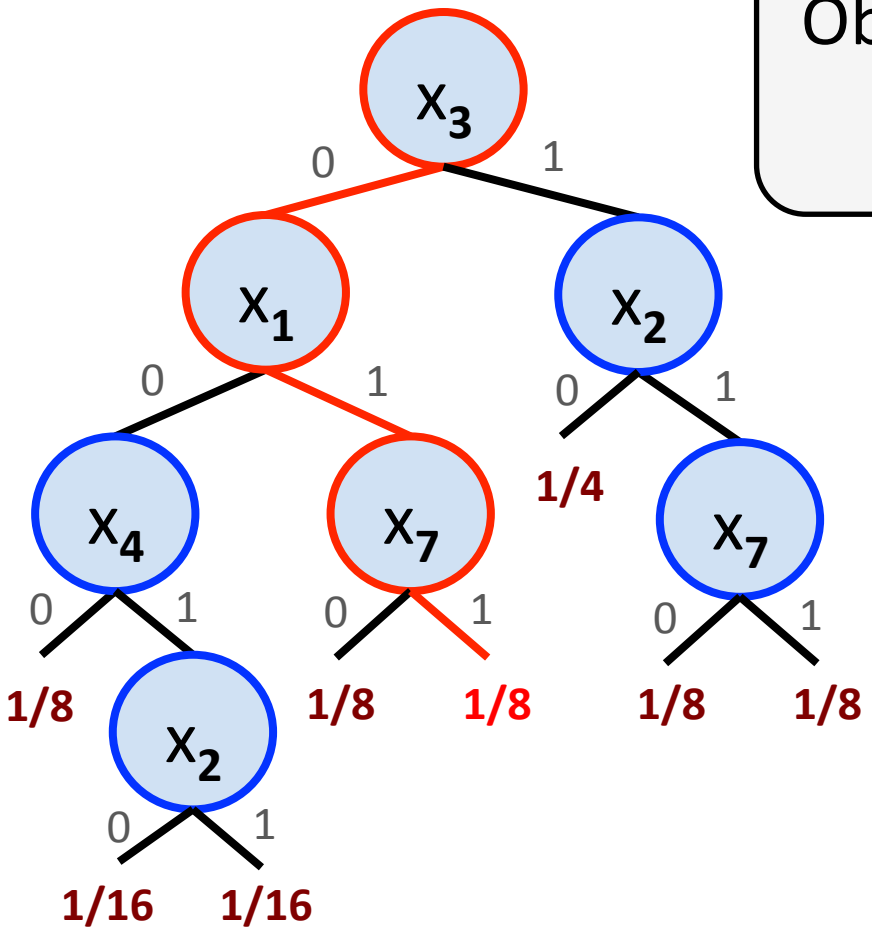
- Let $\boldsymbol{\beta}(T) \subseteq [n]$ be the <u>set</u> of variables queried on a random branch of T



- #$\boldsymbol{\beta}$(T) = the number of variables queried on a random branch of T



- #$\boldsymbol{\beta}$(T) = the number of variables queried on a random branch of T



Obs: If depth(T) ≥ k, then

$\Pr[\ \#\boldsymbol{\beta}(T) \geq k\ ] \geq 2^{-k}$

Claim. The following random variables have the same distribution:

1. $\boldsymbol{\beta}(T \upharpoonright \mathbf{R}_p)$

   the set of variables queried on a random branch of $T \upharpoonright \mathbf{R}_p$

2. $\mathbf{S} \subseteq_p \boldsymbol{\beta}(T)$

   a p-biased subset of the vars. on a random branch of T

Claim. The following random variables have the same distribution:

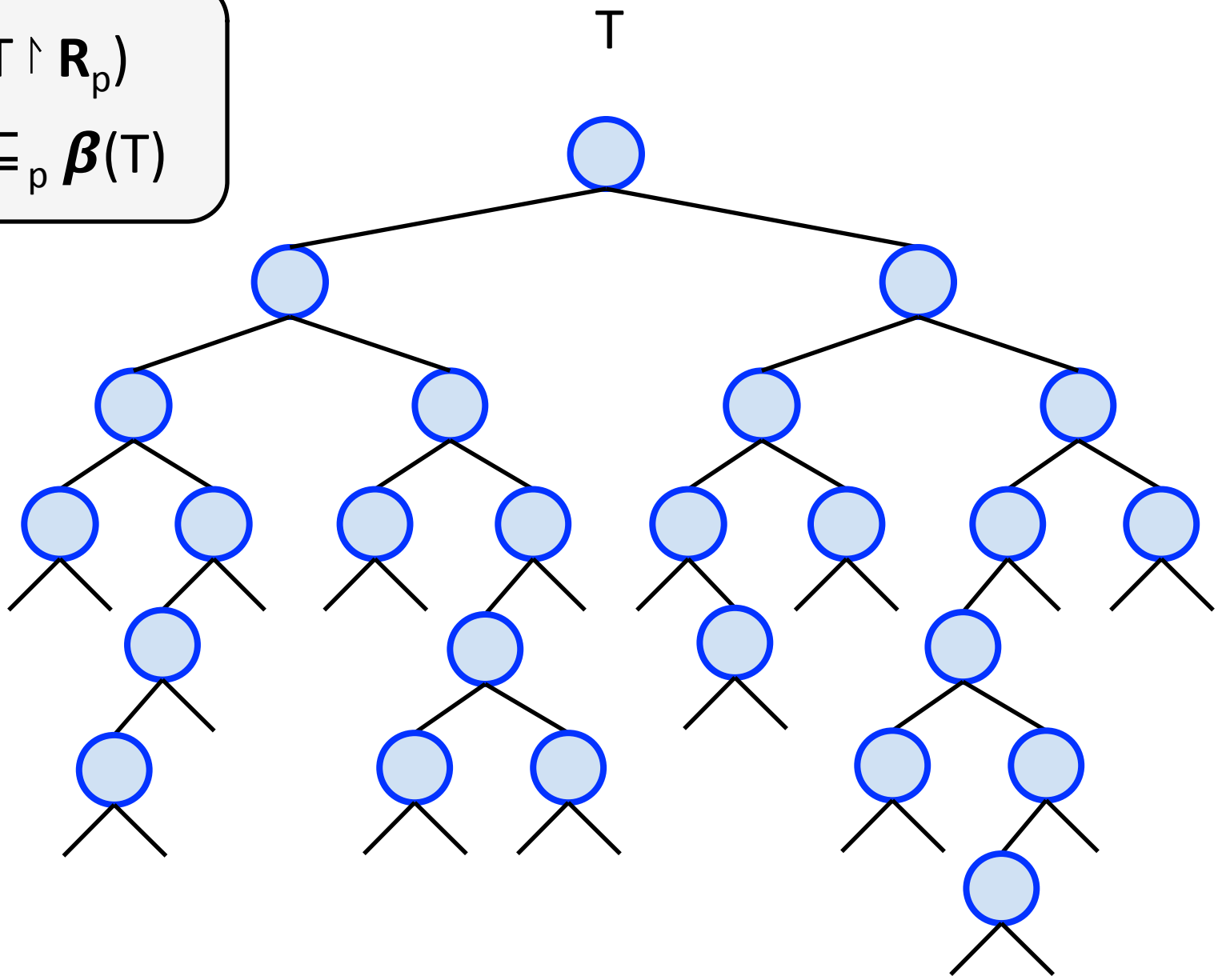
1. $\boldsymbol{\beta}(T \upharpoonright \mathbf{R}_p)$ $\quad$ $\#\boldsymbol{\beta}(T \upharpoonright \mathbf{R}_p)$

   the set of variables queried on a random branch of $T \upharpoonright \mathbf{R}_p$

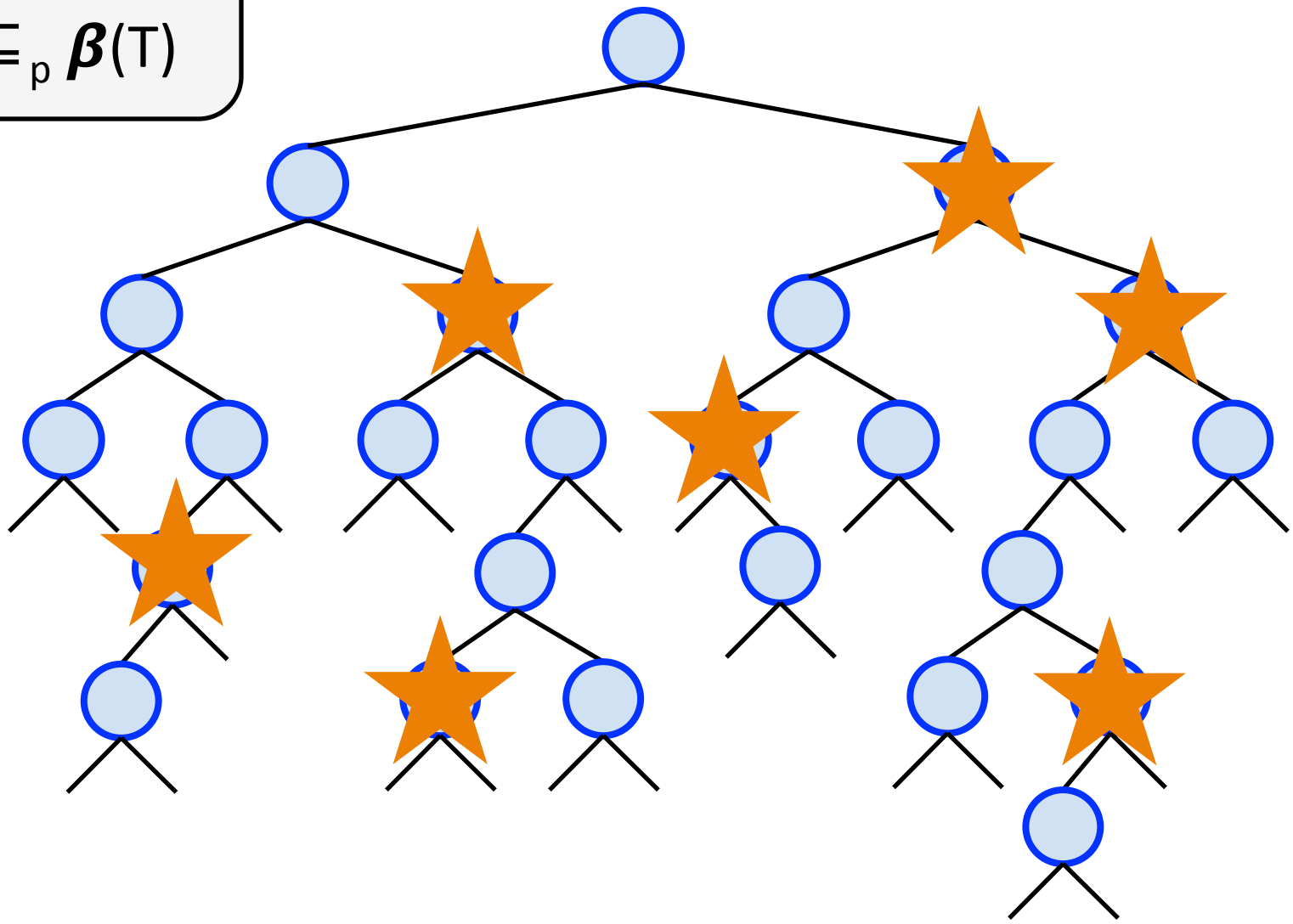
2. $\mathbf{S} \subseteq_p \boldsymbol{\beta}(T)$ $\quad$ $\mathbf{Bin}(\#\boldsymbol{\beta}(T), p)$

   a p-biased subset of the vars. on a random branch of T

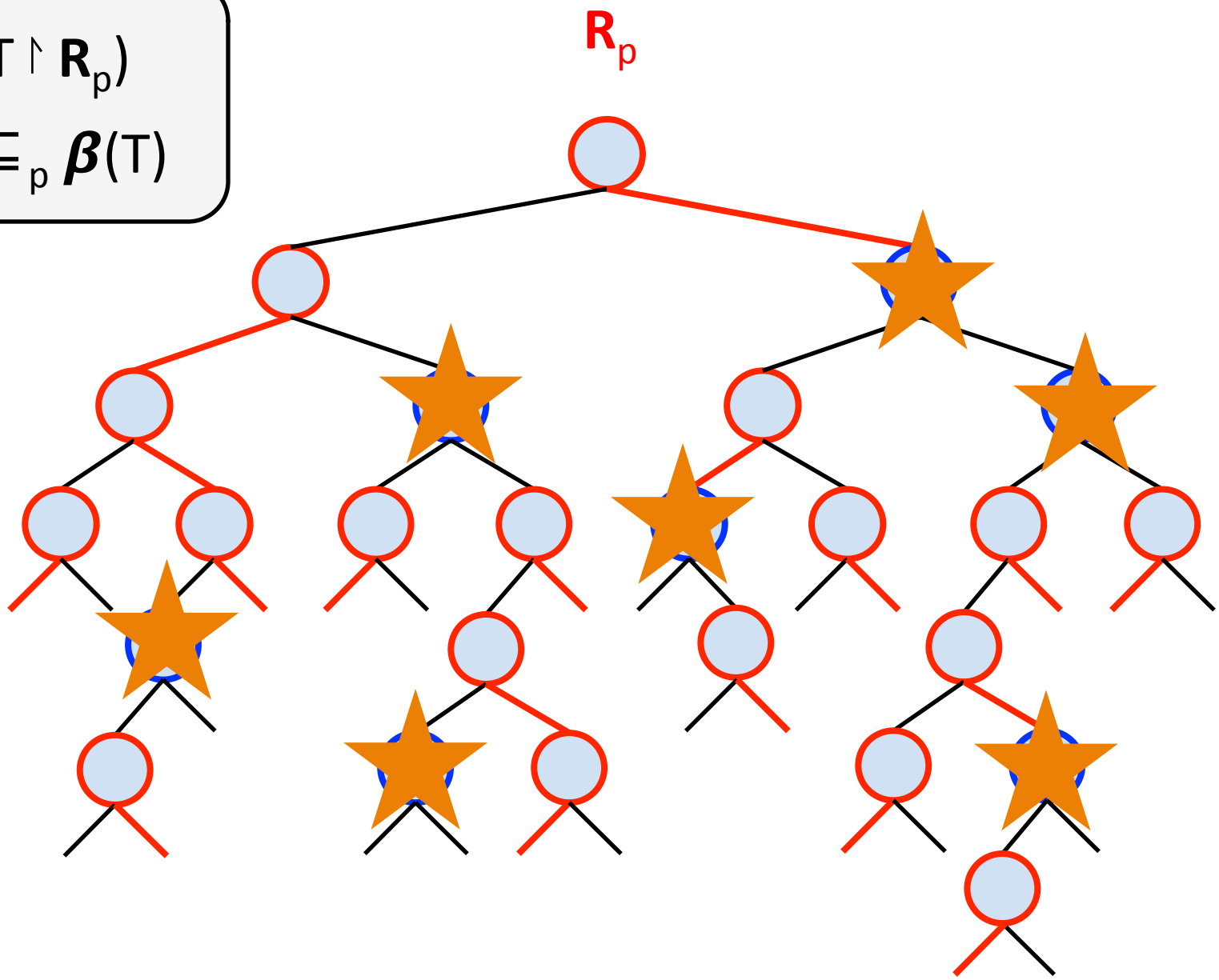
1. $\boldsymbol{\beta}(T \upharpoonright \mathbf{R}_p)$
2. $\mathbf{S} \subseteq_p \boldsymbol{\beta}(T)$



1. $\boldsymbol{\beta}(T \upharpoonright \mathbf{R}_p)$
2. $\mathbf{S} \subseteq_p \boldsymbol{\beta}(T)$

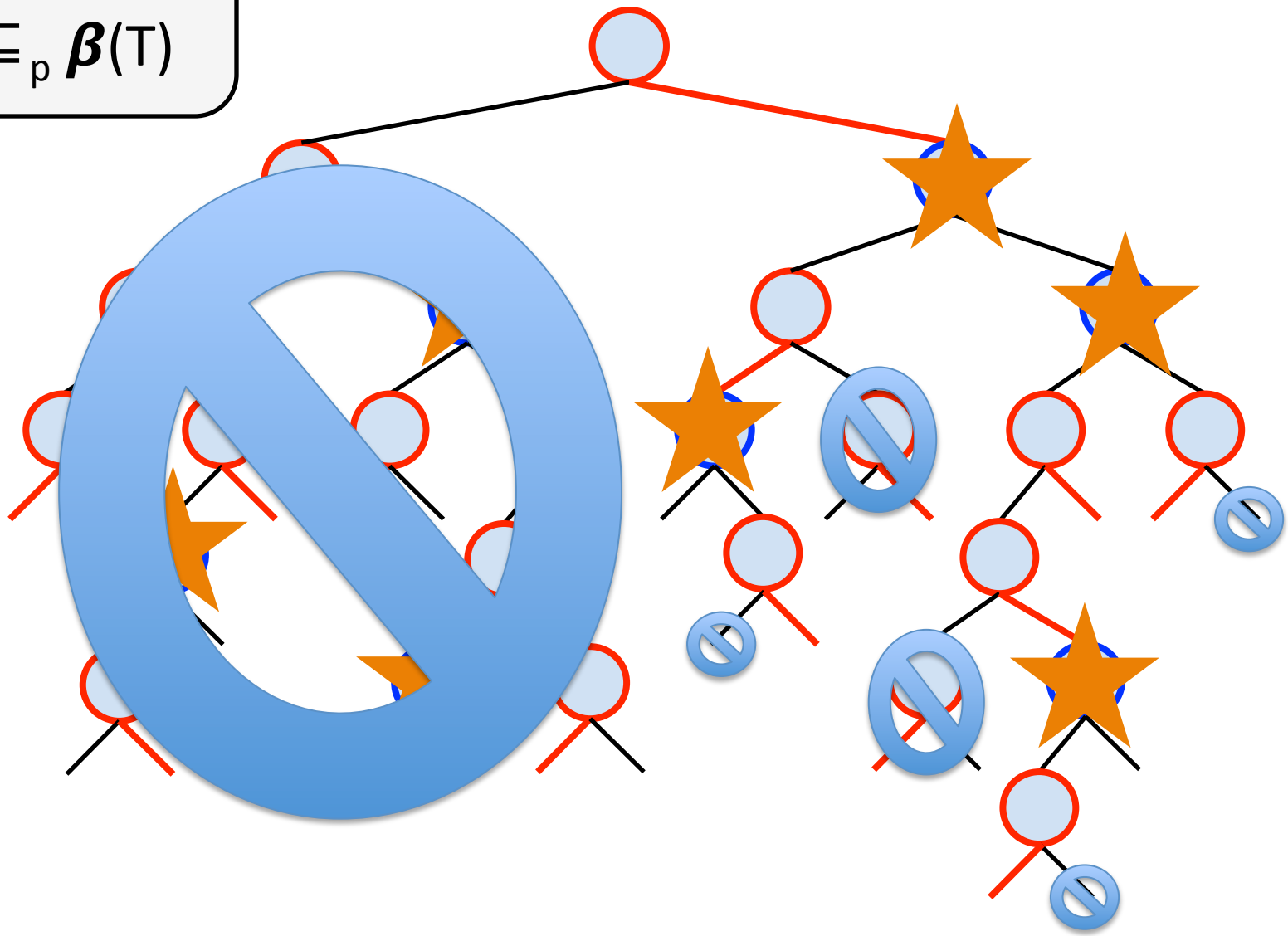


1. $\boldsymbol{\beta}(T \upharpoonright \mathbf{R}_p)$
2. $\mathbf{S} \subseteq_p \boldsymbol{\beta}(T)$



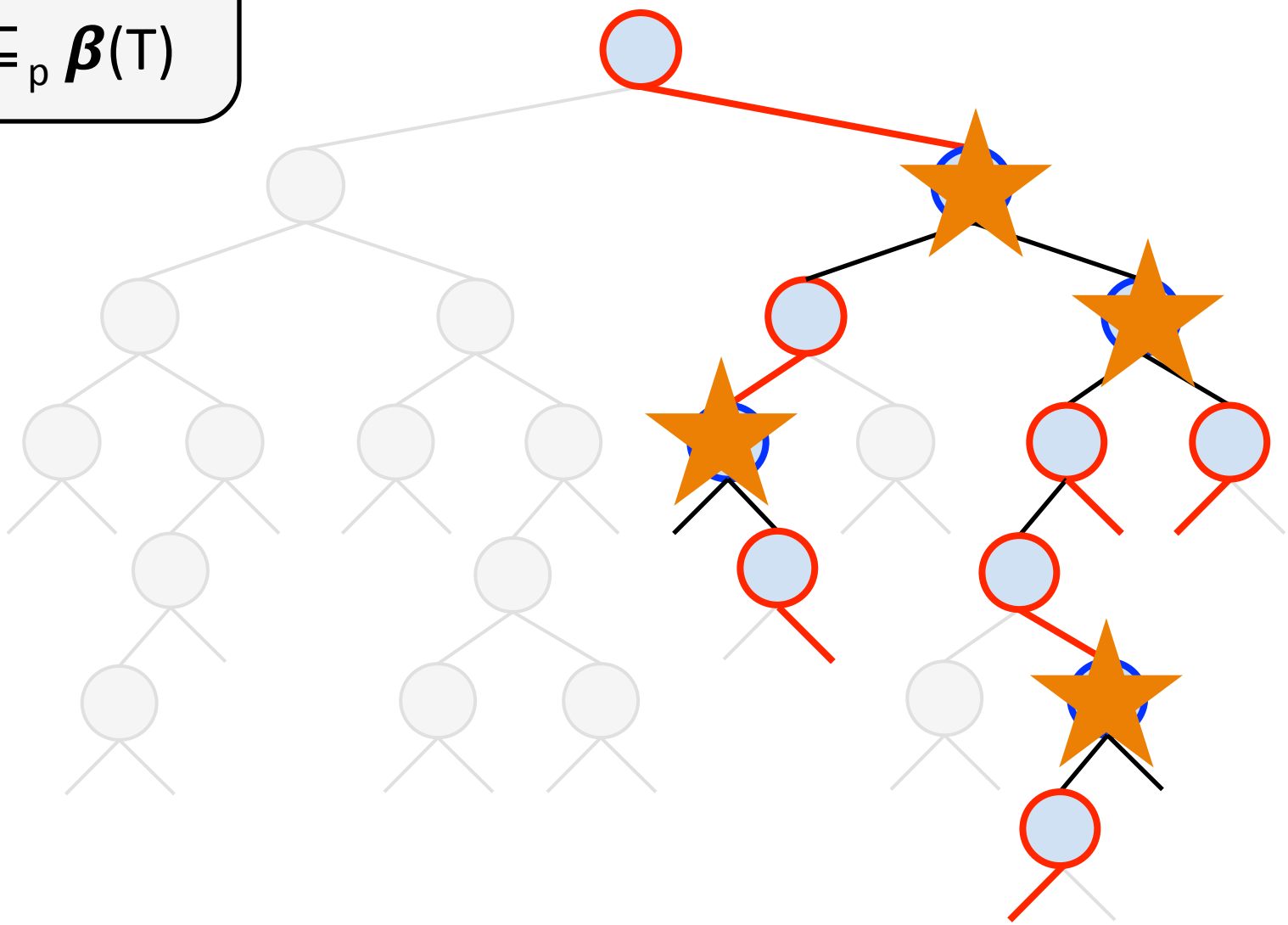
1. $\boldsymbol{\beta}(T \upharpoonright \mathbf{R}_p)$
2. $\mathbf{S} \subseteq_p \boldsymbol{\beta}(T)$

$T \upharpoonright \mathbf{R}_p$



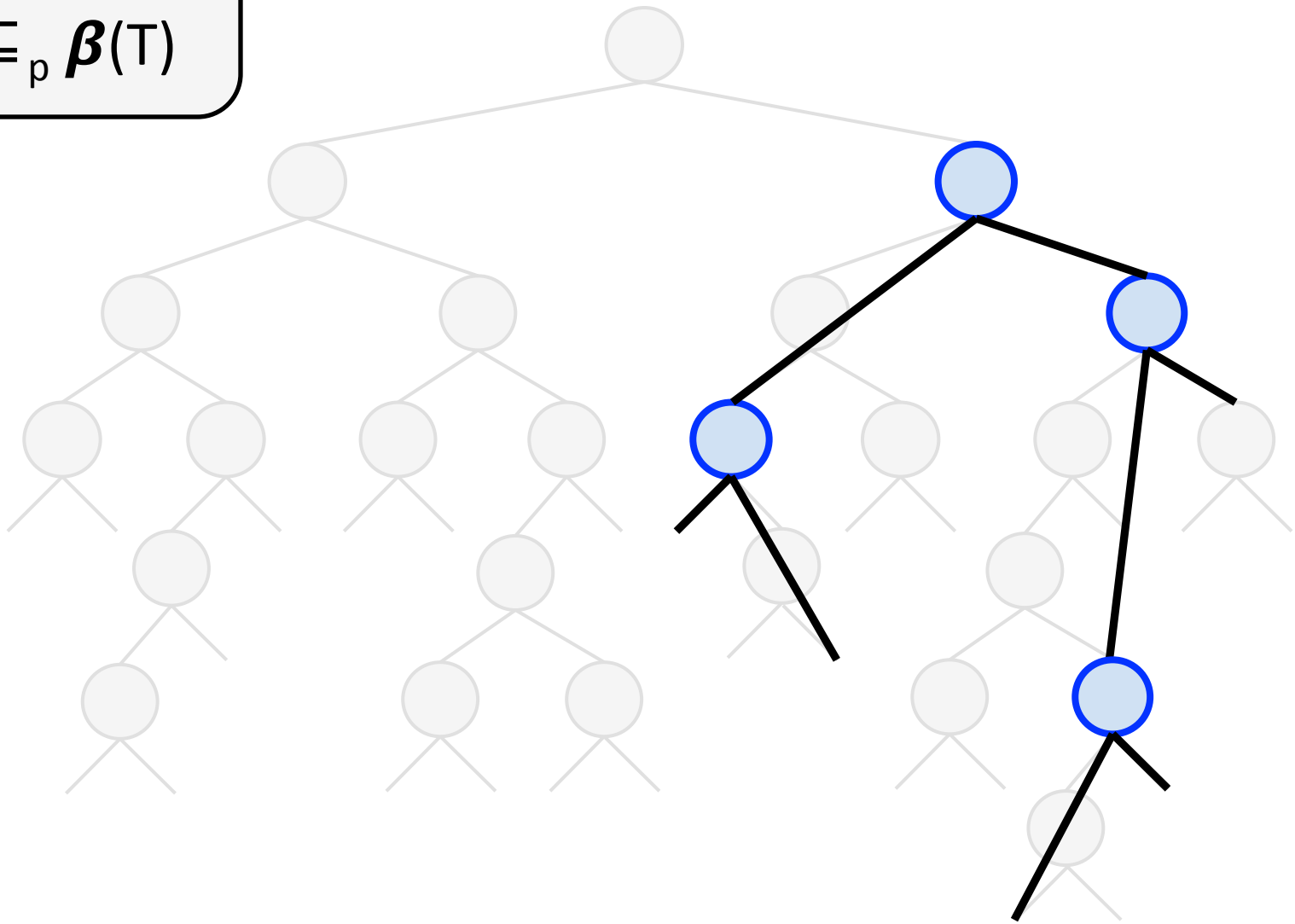
1. $\boldsymbol{\beta}(T \upharpoonright \mathbf{R}_p)$
2. $\mathbf{S} \subseteq_p \boldsymbol{\beta}(T)$

$T \upharpoonright \mathbf{R}_p$

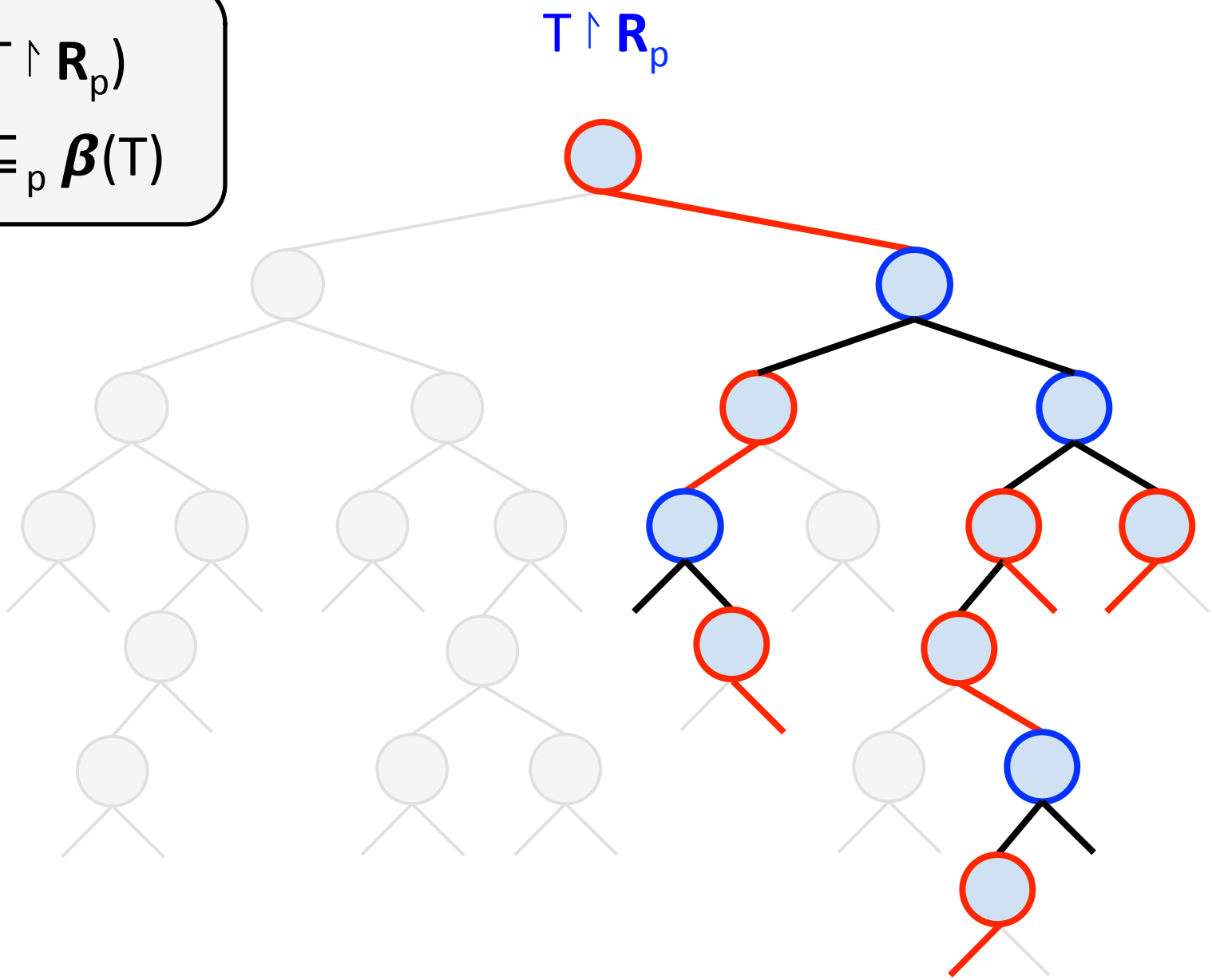


1. $\boldsymbol{\beta}(T \upharpoonright \mathbf{R}_p)$
2. $\mathbf{S} \subseteq_p \boldsymbol{\beta}(T)$

$T \upharpoonright \mathbf{R}_p$

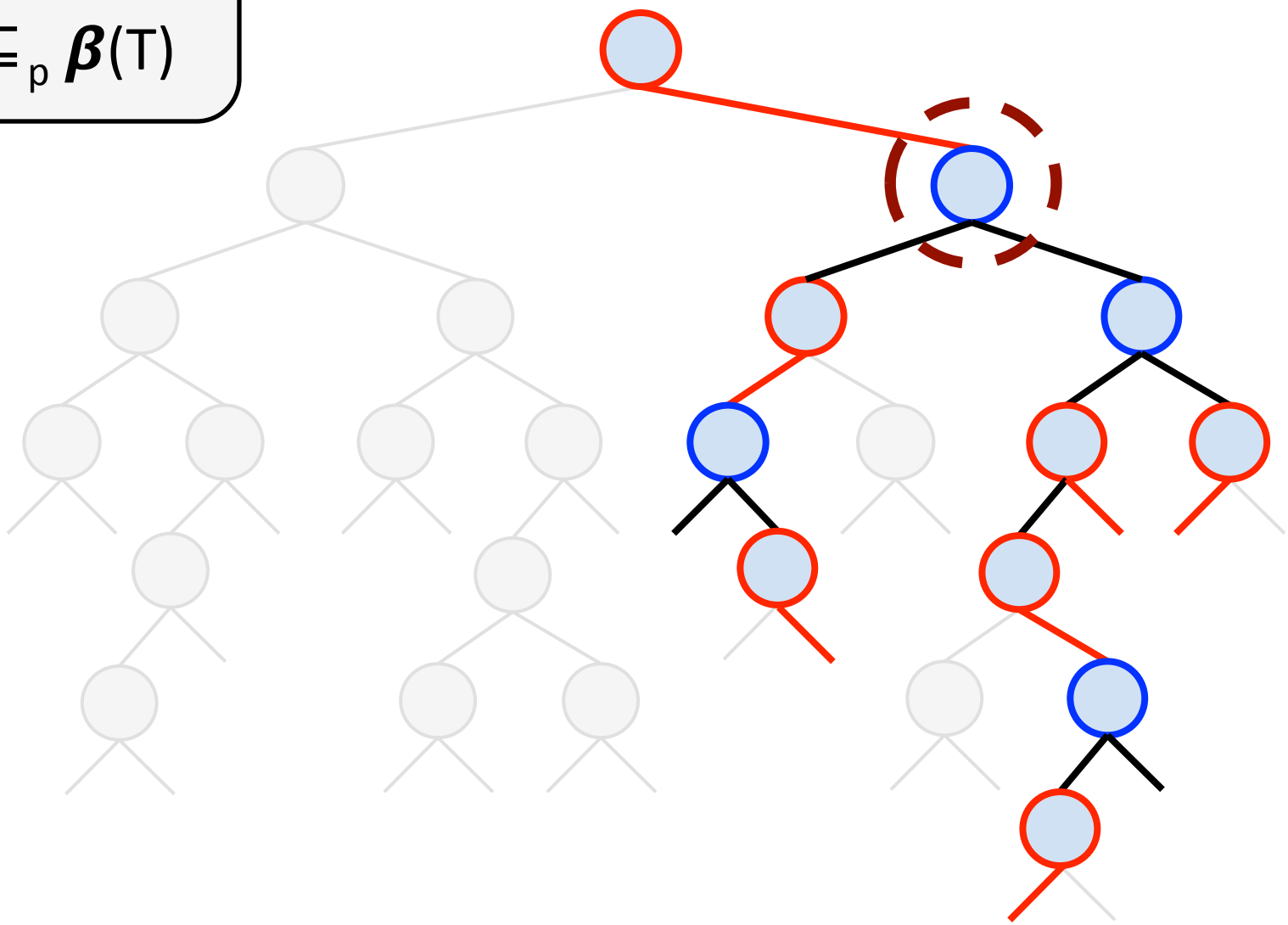


1. $\boldsymbol{\beta}(T \upharpoonright \mathbf{R}_p)$
2. $\mathbf{S} \subseteq_p \boldsymbol{\beta}(T)$



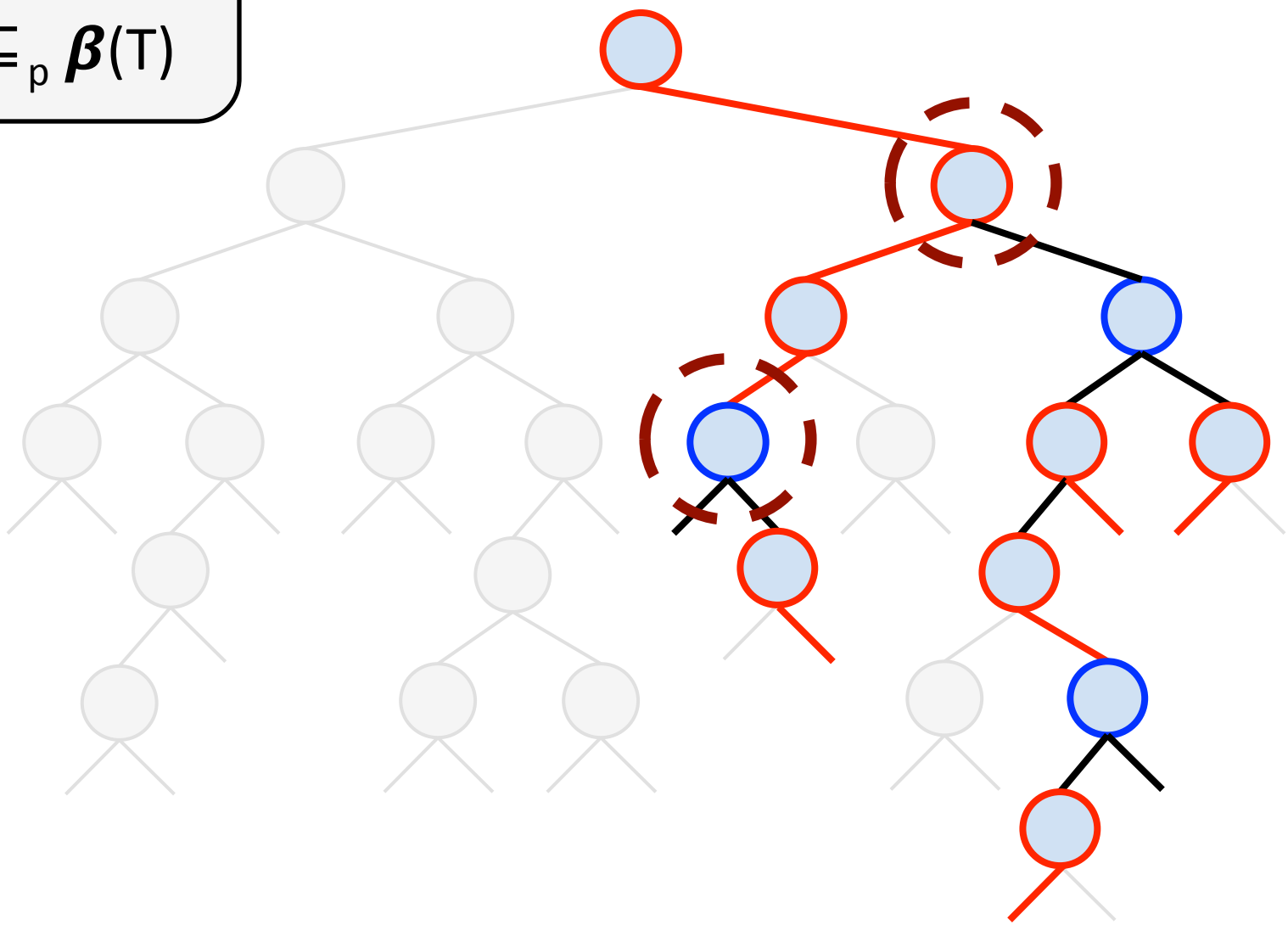
1. $\boldsymbol{\beta}(T \upharpoonright \mathbf{R}_p)$
2. $\mathbf{S} \subseteq_p \boldsymbol{\beta}(T)$

$\boldsymbol{\beta}(T \upharpoonright \mathbf{R}_p)$



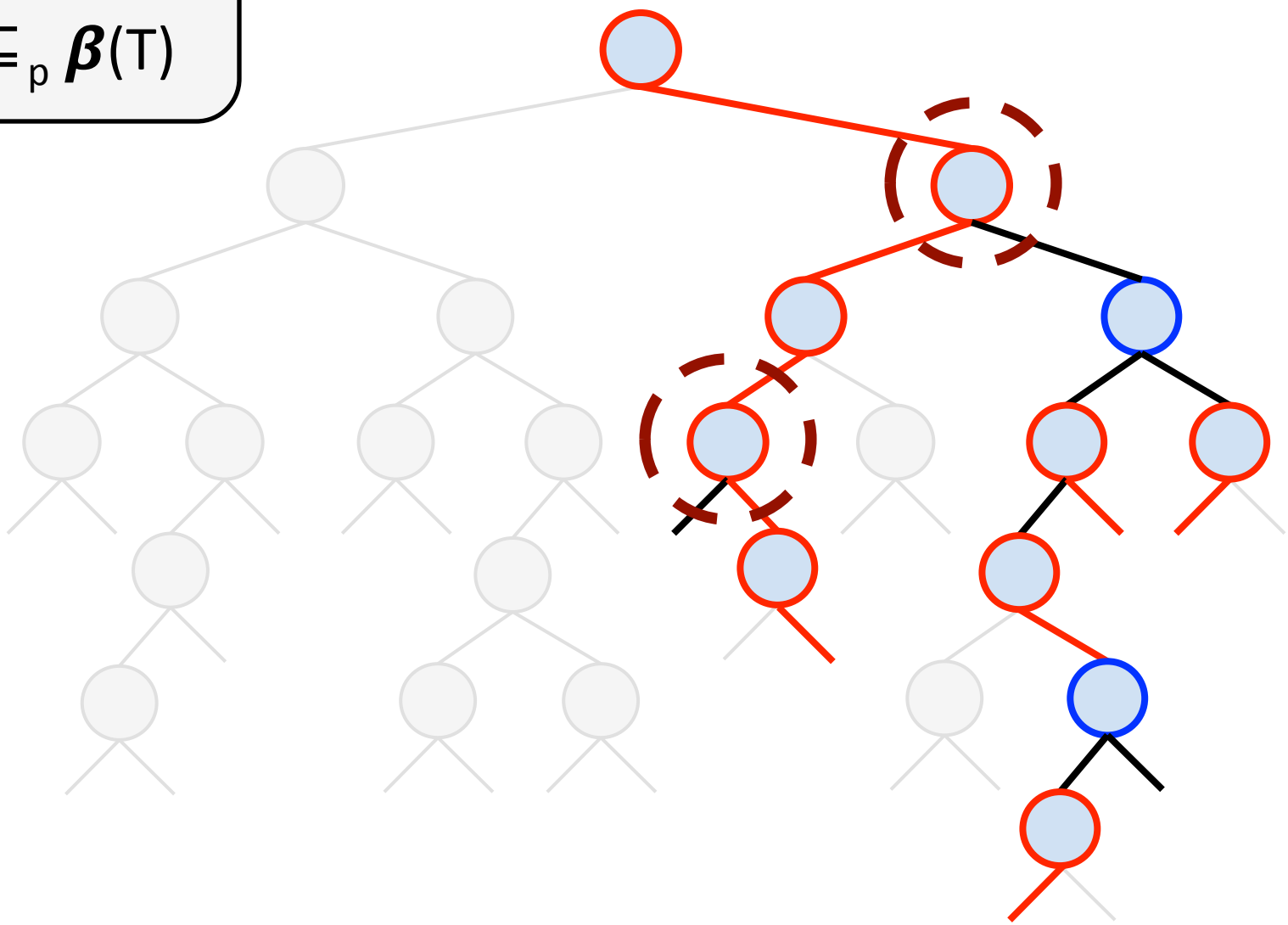
1. $\boldsymbol{\beta}(T \upharpoonright \mathbf{R}_p)$
2. $\mathbf{S} \subseteq_p \boldsymbol{\beta}(T)$

$\boldsymbol{\beta}(T \upharpoonright \mathbf{R}_p)$



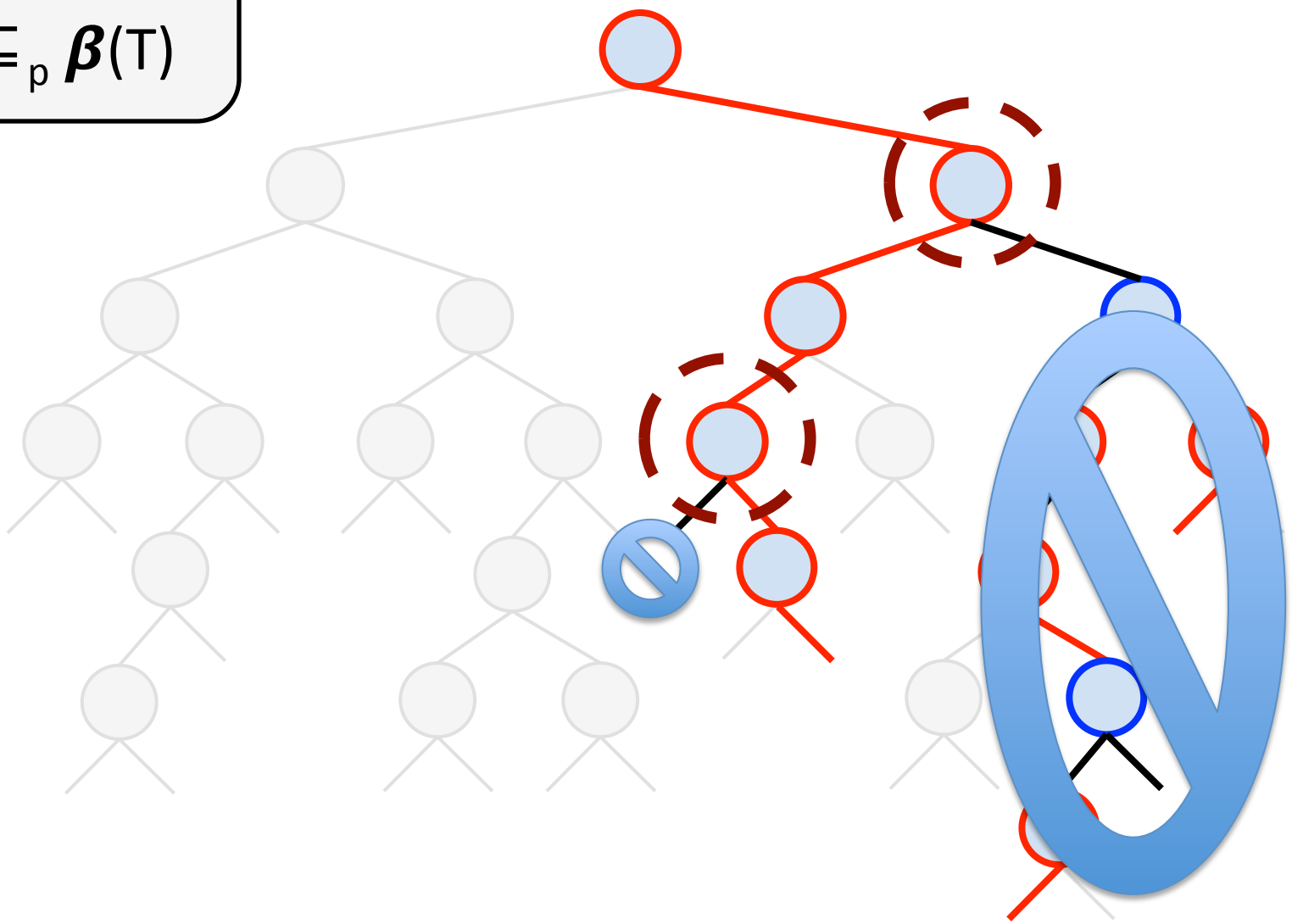
1. $\boldsymbol{\beta}(T \upharpoonright \mathbf{R}_p)$
2. $\mathbf{S} \subseteq_p \boldsymbol{\beta}(T)$

$\boldsymbol{\beta}(T \upharpoonright \mathbf{R}_p)$

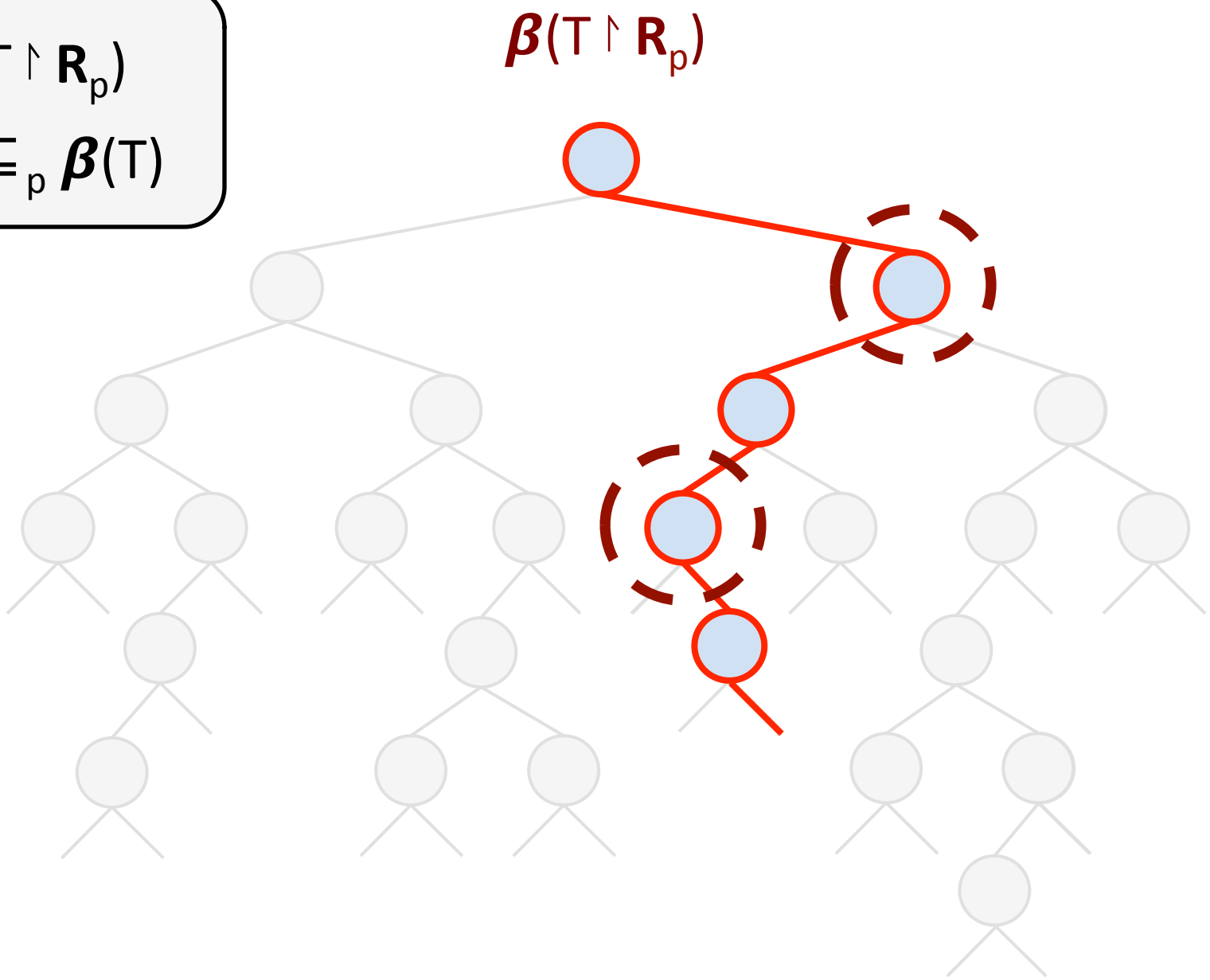


1. $\boldsymbol{\beta}(T \upharpoonright \mathbf{R}_p)$
2. $\mathbf{S} \subseteq_p \boldsymbol{\beta}(T)$

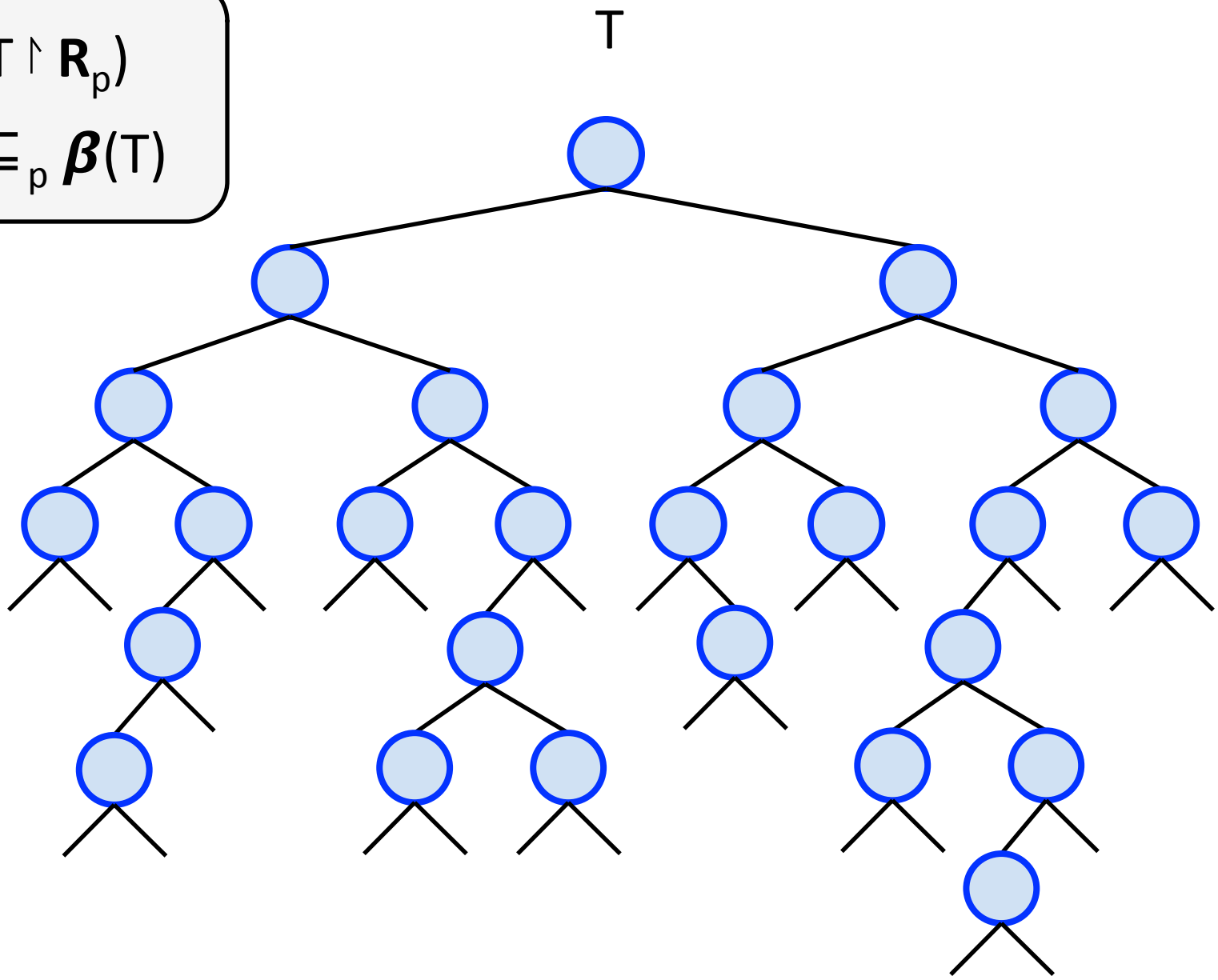
$\boldsymbol{\beta}(T \upharpoonright \mathbf{R}_p)$



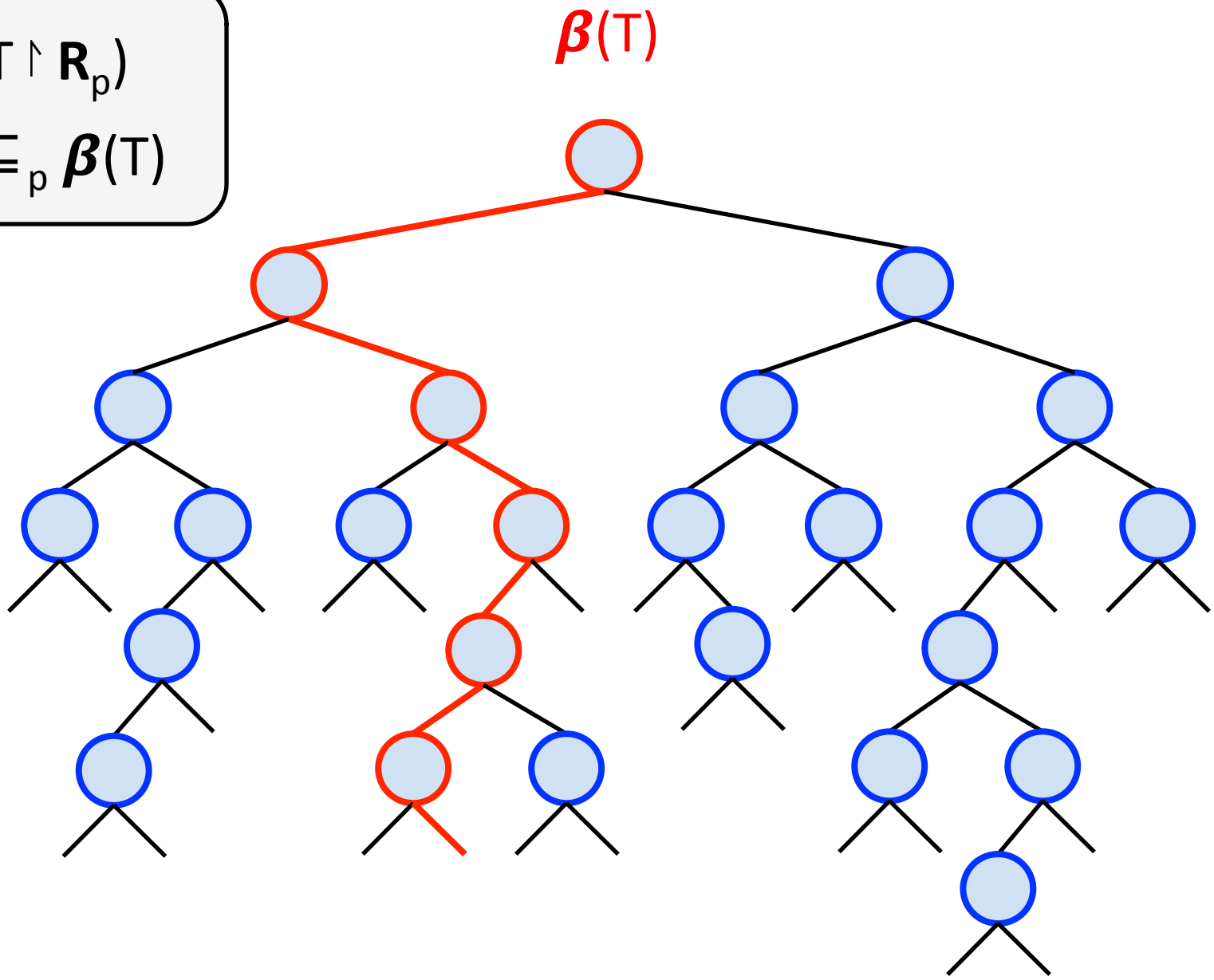
1. $\boldsymbol{\beta}(T \upharpoonright \mathbf{R}_p)$
2. $\mathbf{S} \subseteq_p \boldsymbol{\beta}(T)$



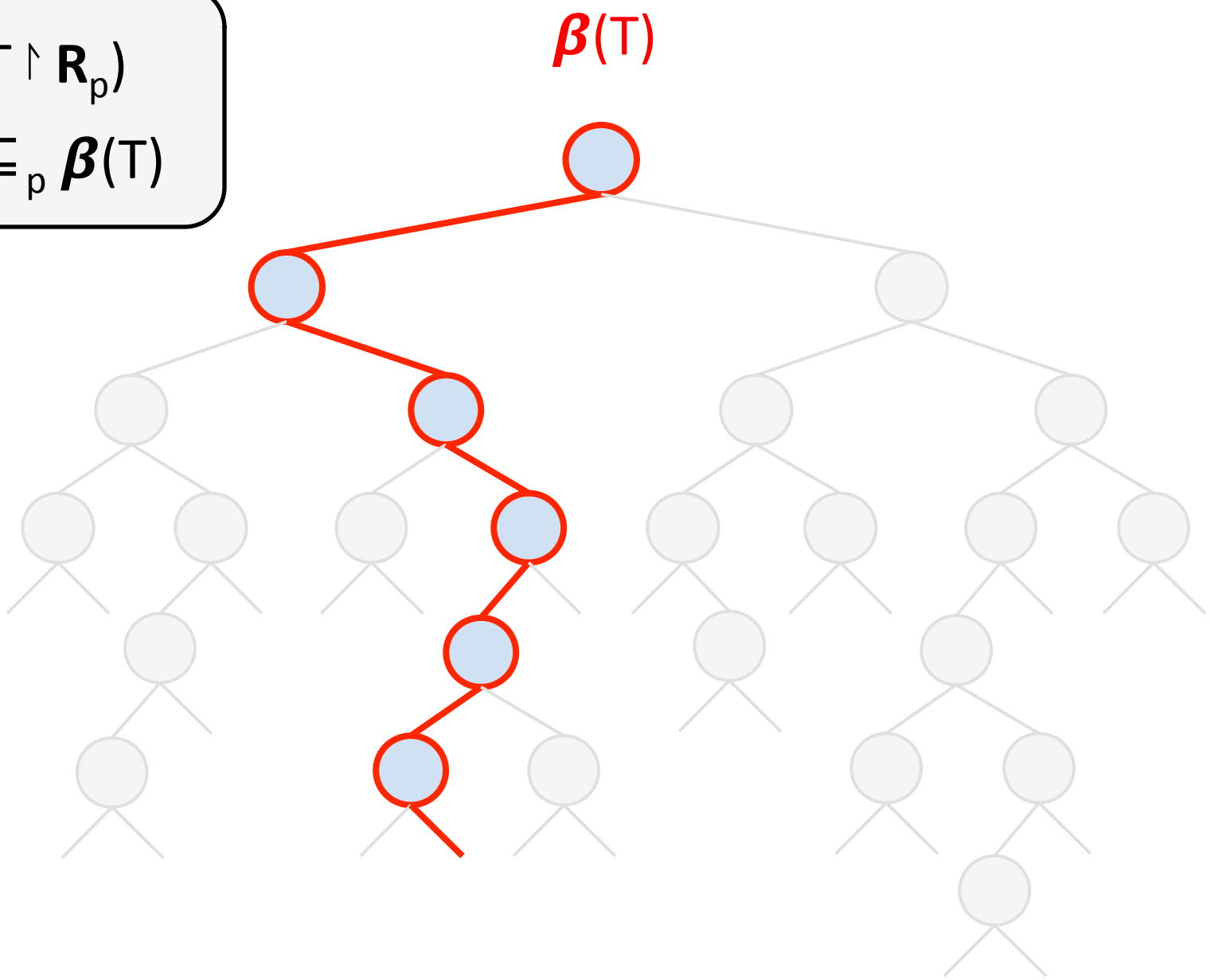
1. $\boldsymbol{\beta}(T \upharpoonright \mathbf{R}_p)$
2. $\mathbf{S} \subseteq_p \boldsymbol{\beta}(T)$



1. $\boldsymbol{\beta}(T \upharpoonright \mathbf{R}_p)$
2. $\mathbf{S} \subseteq_p \boldsymbol{\beta}(T)$

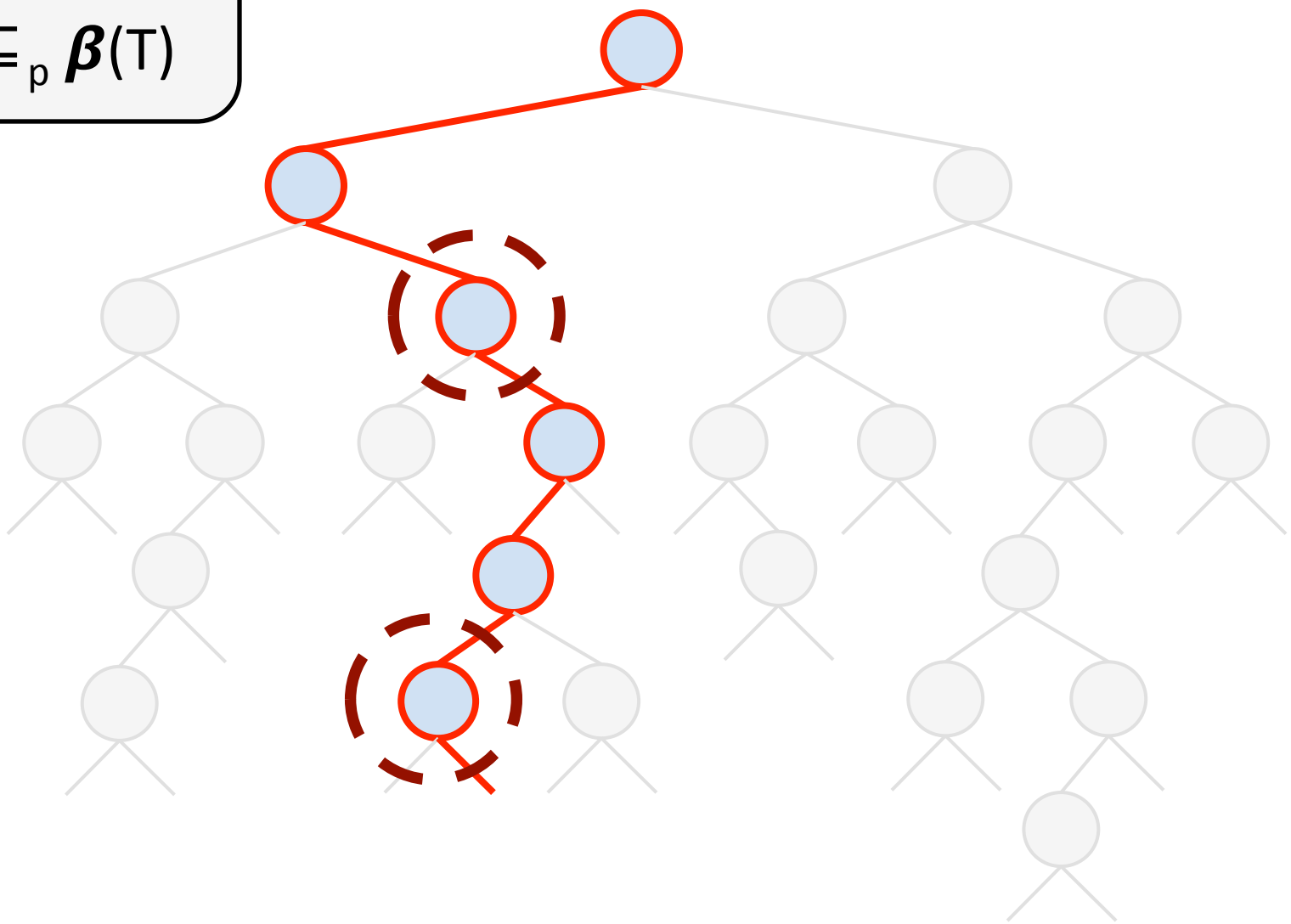


1. $\boldsymbol{\beta}(T \upharpoonright \mathbf{R}_p)$
2. $\mathbf{S} \subseteq_p \boldsymbol{\beta}(T)$



1. $\boldsymbol{\beta}(T \upharpoonright \mathbf{R}_p)$
2. $\mathbf{S} \subseteq_p \boldsymbol{\beta}(T)$

$\mathbf{S} \subseteq_p \boldsymbol{\beta}(T)$



1. $\boldsymbol{\beta}(T \upharpoonright \mathbf{R}_p)$
2. $\mathbf{S} \subseteq_p \boldsymbol{\beta}(T)$

$\Rightarrow$

1. $\#\boldsymbol{\beta}(T \upharpoonright \mathbf{R}_p)$
2. $\mathbf{Bin}(\boldsymbol{\beta}(T), p)$

Decision Tree Switching Lemma

If T is a depth-k decision tree, then

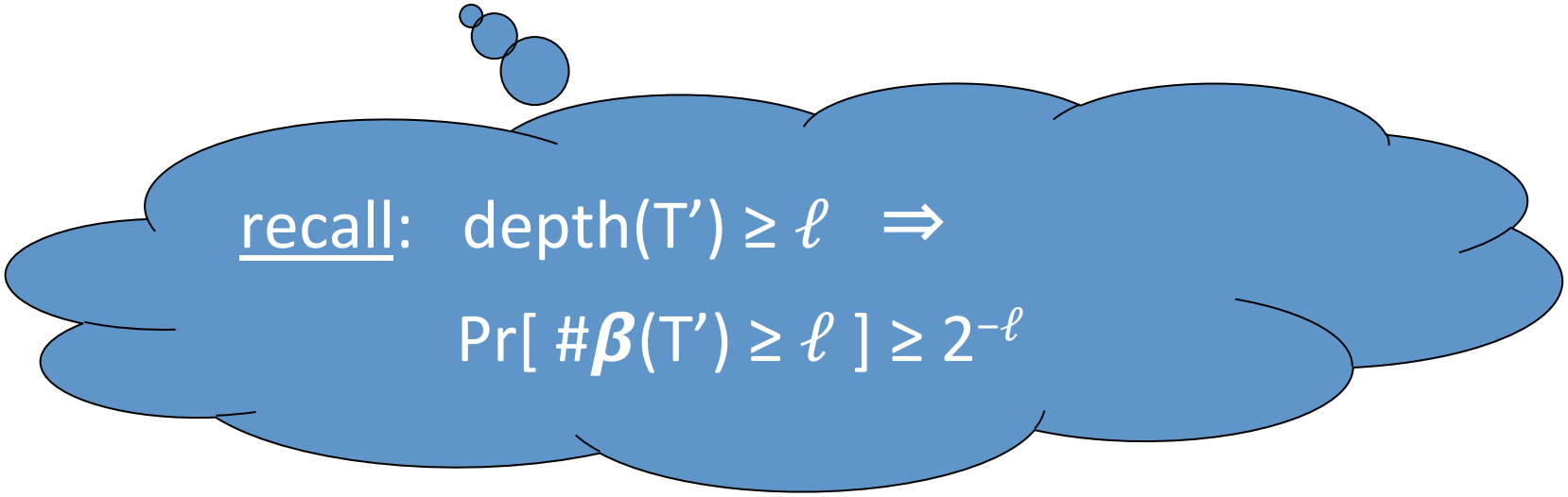
$$\Pr[\ \text{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ] \leq (2pk)^{\ell}$$

Decision Tree Switching Lemma

If T is a depth-k decision tree, then

$$\Pr[\ \mathrm{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ] \leq (2pk)^{\ell}$$

$\Pr[\ \mathrm{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ]$



Decision Tree Switching Lemma

If T is a depth-k decision tree, then

$$\Pr[\ \mathrm{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ] \leq (2pk)^{\ell}$$

$$\Pr[\ \mathrm{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ]$$

$$\leq \Pr_{\mathbf{R}_p}[\ \Pr_{\boldsymbol{\beta}(T \restriction \mathbf{R}_p)}[\ \#\boldsymbol{\beta}(T \restriction \mathbf{R}_p) \geq \ell\ ] \geq 2^{-\ell}\ ]$$

recall: $\mathrm{depth}(T') \geq \ell \Rightarrow$

$$\Pr[\ \#\boldsymbol{\beta}(T') \geq \ell\ ] \geq 2^{-\ell}$$

Decision Tree Switching Lemma

If T is a depth-k decision tree, then

$$\Pr[\ \mathrm{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ] \leq (2pk)^{\ell}$$

$$\Pr[\ \mathrm{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ]$$

$$\leq \Pr_{\mathbf{R}_p}[\ \Pr_{\boldsymbol{\beta}(T \restriction \mathbf{R}_p)}[\ \#\boldsymbol{\beta}(T \restriction \mathbf{R}_p) \geq \ell\ ] \geq 2^{-\ell}\ ]$$

Decision Tree Switching Lemma

If T is a depth-k decision tree, then

$$\Pr[\ \mathrm{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ] \leq (2pk)^{\ell}$$

$$\Pr[\ \mathrm{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ]$$

$$\leq \Pr_{\mathbf{R}_p}[\ \Pr_{\boldsymbol{\beta}(T \restriction \mathbf{R}_p)}[\ \#\boldsymbol{\beta}(T \restriction \mathbf{R}_p) \geq \ell\ ] \geq 2^{-\ell}\ ]$$

$$\leq 2^{\ell}\ \mathrm{Ex}_{\mathbf{R}_p}[\ \Pr_{\boldsymbol{\beta}(T \restriction \mathbf{R}_p)}[\ \#\boldsymbol{\beta}(T \restriction \mathbf{R}_p) \geq \ell\ ]\ ]$$

Markov's inequality

Decision Tree Switching Lemma

If T is a depth-k decision tree, then

$$\Pr[\ \mathrm{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ] \leq (2pk)^{\ell}$$

$$\Pr[\ \mathrm{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ]$$

$$\leq \Pr_{\mathbf{R}_p}[\ \Pr_{\boldsymbol{\beta}(T \restriction \mathbf{R}_p)}[\ \#\boldsymbol{\beta}(T \restriction \mathbf{R}_p) \geq \ell\ ] \geq 2^{-\ell}\ ]$$

$$\leq 2^{\ell}\ \mathrm{Ex}_{\mathbf{R}_p}[\ \Pr_{\boldsymbol{\beta}(T \restriction \mathbf{R}_p)}[\ \#\boldsymbol{\beta}(T \restriction \mathbf{R}_p) \geq \ell\ ]\ ]$$

Decision Tree Switching Lemma

If T is a depth-k decision tree, then

$$\Pr[\ \mathrm{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ] \leq (2pk)^{\ell}$$

$$\Pr[\ \mathrm{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ]$$

$$\leq \Pr_{\mathbf{R}_p}[\ \Pr_{\boldsymbol{\beta}(T \restriction \mathbf{R}_p)}[\ \#\boldsymbol{\beta}(T \restriction \mathbf{R}_p) \geq \ell\ ] \geq 2^{-\ell}\ ]$$

$$\leq 2^{\ell} \Pr[\ \#\boldsymbol{\beta}(T \restriction \mathbf{R}_p) \geq \ell\ ]$$

Decision Tree Switching Lemma

If T is a depth-k decision tree, then

$$\Pr[\ \mathrm{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ] \leq (2pk)^{\ell}$$

$$\Pr[\ \mathrm{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ]$$

$$\leq \Pr_{\mathbf{R}_p}[\ \Pr_{\boldsymbol{\beta}(T \restriction \mathbf{R}_p)}[\ \#\boldsymbol{\beta}(T \restriction \mathbf{R}_p) \geq \ell\ ] \geq 2^{-\ell}\ ]$$

$$\leq 2^{\ell} \Pr[\ \#\boldsymbol{\beta}(T \restriction \mathbf{R}_p) \geq \ell\ ]$$

$$= 2^{\ell} \Pr[\ \mathbf{Bin}(\#\boldsymbol{\beta}(T), p) \geq \ell\ ]$$

$\#\boldsymbol{\beta}(T \restriction \mathbf{R}_p)$ and $\mathbf{Bin}(\#\boldsymbol{\beta}(T), p)$ have the same distribution

Decision Tree Switching Lemma

If T is a depth-k decision tree, then

$$\Pr[\ \mathrm{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ] \leq (2pk)^{\ell}$$

$$\begin{aligned}
&\Pr[\ \mathrm{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ] \\
&\quad \leq \Pr_{\mathbf{R}_p}[\ \Pr_{\boldsymbol{\beta}(T \restriction \mathbf{R}_p)}[\ \#\boldsymbol{\beta}(T \restriction \mathbf{R}_p) \geq \ell\ ] \geq 2^{-\ell}\ ] \\
&\quad \leq 2^{\ell} \Pr[\ \#\boldsymbol{\beta}(T \restriction \mathbf{R}_p) \geq \ell\ ] \\
&\quad = 2^{\ell} \Pr[\ \mathbf{Bin}(\#\boldsymbol{\beta}(T), p) \geq \ell\ ] \\
&\quad \leq 2^{\ell} \Pr[\ \mathbf{Bin}(k, p) \geq \ell\ ]
\end{aligned}$$

$\#\boldsymbol{\beta}(T) \leq \mathrm{depth}(T) \leq k$

Decision Tree Switching Lemma

If T is a depth-k decision tree, then

$$\Pr[\ \mathrm{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ] \leq (2pk)^{\ell}$$

$$\begin{aligned}
&\Pr[\ \mathrm{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ] \\
&\quad \leq \Pr_{\mathbf{R}_p}[\ \Pr_{\boldsymbol{\beta}(T \restriction \mathbf{R}_p)}[\ \#\boldsymbol{\beta}(T \restriction \mathbf{R}_p) \geq \ell\ ] \geq 2^{-\ell}\ ] \\
&\quad \leq 2^{\ell} \Pr[\ \#\boldsymbol{\beta}(T \restriction \mathbf{R}_p) \geq \ell\ ] \\
&\quad = 2^{\ell} \Pr[\ \mathbf{Bin}(\#\boldsymbol{\beta}(T), p) \geq \ell\ ] \\
&\quad \leq 2^{\ell} \Pr[\ \mathbf{Bin}(k, p) \geq \ell\ ] \\
&\quad \leq 2^{\ell} (pk)^{\ell}
\end{aligned}$$

union bound

Decision Tree Switching Lemma

If T is a depth-k decision tree, then

$$\Pr[\ \mathrm{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ] \leq (2pk)^{\ell}$$

$$\begin{aligned}
&\Pr[\ \mathrm{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ] \\
&\quad \leq \Pr_{\mathbf{R}_p}[\ \Pr_{\boldsymbol{\beta}(T \restriction \mathbf{R}_p)}[\ \#\boldsymbol{\beta}(T \restriction \mathbf{R}_p) \geq \ell\ ] \geq 2^{-\ell}\ ] \\
&\quad \leq 2^{\ell}\ \Pr[\ \#\boldsymbol{\beta}(T \restriction \mathbf{R}_p) \geq \ell\ ] \\
&\quad = 2^{\ell}\ \Pr[\ \mathbf{Bin}(\#\boldsymbol{\beta}(T), p) \geq \ell\ ] \\
&\quad \leq 2^{\ell}\ \Pr[\ \mathbf{Bin}(k, p) \geq \ell\ ] \\
&\quad \leq 2^{\ell}\ (pk)^{\ell}
\end{aligned}$$

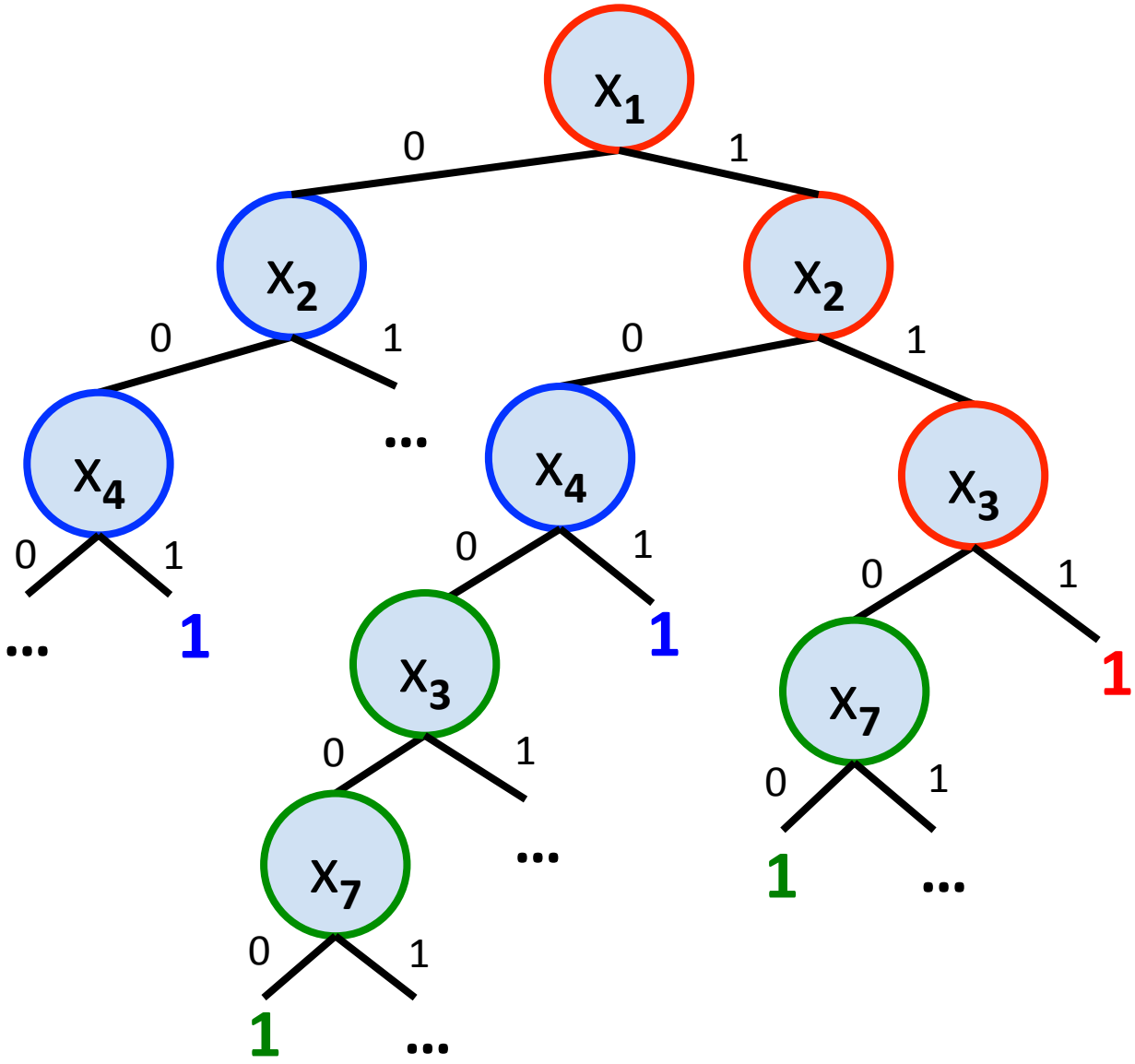
Q.E.D.

A Different Approach

1. Decision Tree Switching Lemma
2. **k-Clipped Decision Trees**
3. Arbitrary Distribution of Stars
4. *Switching Lemma for Affine Restrictions*
5. Tseitin Expander Switching Lemma

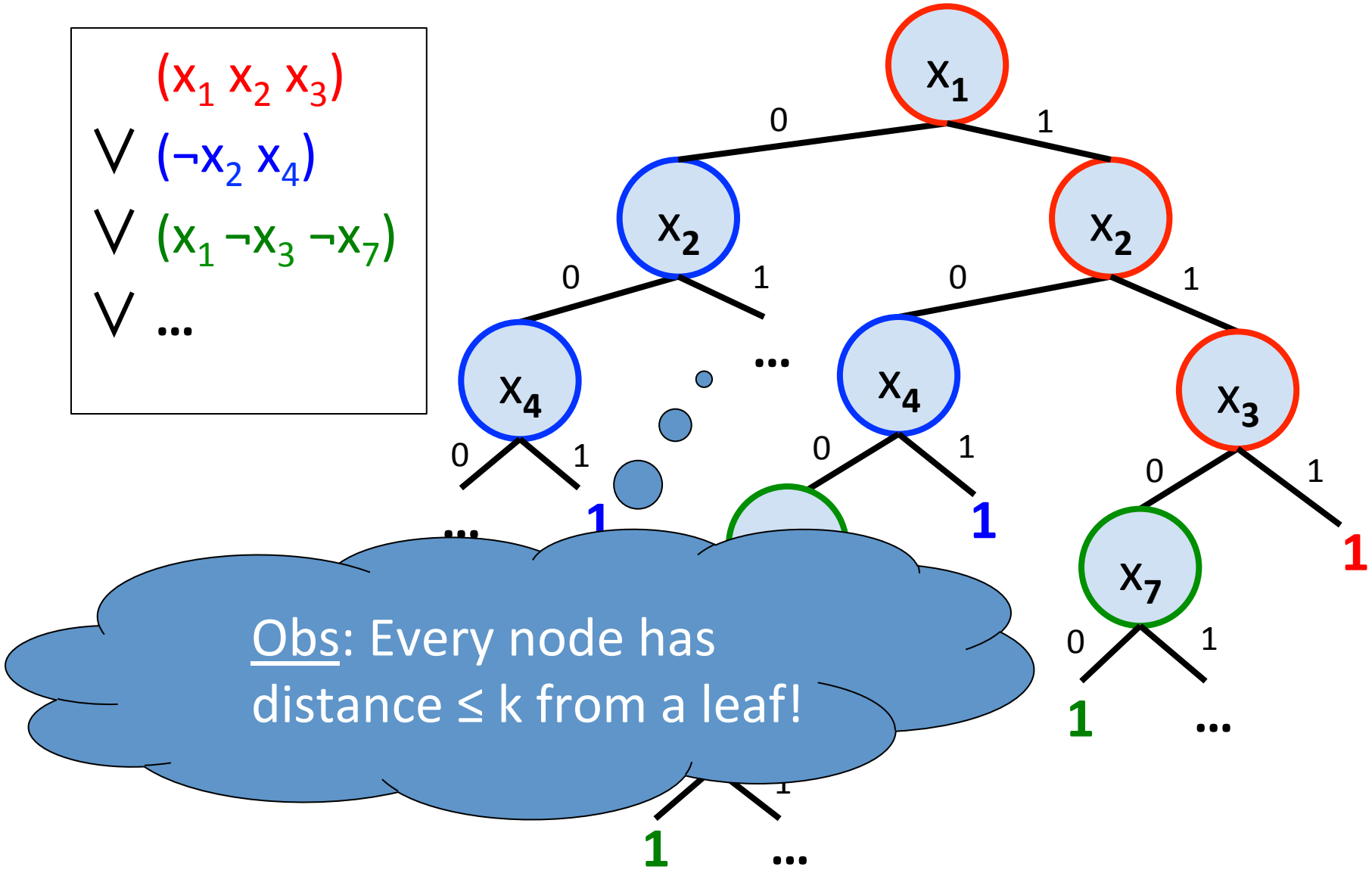
Recall: Canonical DT of a k-DNF

$(x_1\ x_2\ x_3)$
$\vee\ (\neg x_2\ x_4)$
$\vee\ (x_1\ \neg x_3\ \neg x_7)$
$\vee\ \ldots$



Recall: Canonical DT of a k-DNF

$(x_1\ x_2\ x_3)$
$\vee\ (\neg x_2\ x_4)$
$\vee\ (x_1\ \neg x_3\ \neg x_7)$
$\vee\ \ldots$



Definition: A decision tree is **k-clipped** if every node has distance ≤ k from a leaf

Definition: A decision tree is **k-clipped** if every node has distance ≤ k from a leaf

Lemma: If F is a k-DNF (or k-CNF), then CanDT(F) is k-clipped

Definition: A decision tree is **k-clipped** if every node has distance ≤ k from a leaf

Lemma: If F is a k-DNF (or k-CNF), then CanDT(F) is k-clipped

Lemma: If T is k-clipped, then

$$\mathrm{Ex}\left(\begin{matrix}\#\boldsymbol{\beta}(T)\\ \ell\end{matrix}\right) \le O(k2^k)^{\ell}$$

Definition: A decision tree is **k-clipped** if every node has distance ≤ k from a leaf

#β(T) stochastically dominated by the number of unbiased coin flips until seeing k consecutive heads

Lemma: If T is k-clipped, then

$$\mathrm{Ex}\left(\begin{matrix}\#\beta(T)\\ \ell\end{matrix}\right) \le O(k2^k)^{\ell}$$

<u>k-Clipped Decision Tree Switching Lemma</u>

If T is a k-clipped decision tree, then

$$\Pr[\ \mathrm{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ] = O(pk2^k)^{\ell}$$

k-Clipped Decision Tree Switching Lemma

If T is a k-clipped decision tree, then

$$\Pr[\ \mathrm{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ] = O(pk2^k)^{\ell}$$

$$\Pr[\ \mathrm{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ]$$

$$\leq \Pr_{\mathbf{R}_p}[\ \Pr_{\boldsymbol{\beta}(T \restriction \mathbf{R}_p)}[\ \#\boldsymbol{\beta}(T \restriction \mathbf{R}_p) \geq \ell\ ] \geq 2^{-\ell}\ ]$$

$$\leq 2^{\ell} \Pr[\ \#\boldsymbol{\beta}(T \restriction \mathbf{R}_p) \geq \ell\ ]$$

$$= 2^{\ell} \Pr[\ \mathbf{Bin}(\#\boldsymbol{\beta}(T), p) \geq \ell\ ]$$

same as before

k-Clipped Decision Tree Switching Lemma

If T is a k-clipped decision tree, then

$$\Pr[\ \mathrm{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ] = O(pk2^k)^{\ell}$$

$$\Pr[\ \mathrm{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ]$$

$$\leq \Pr_{\mathbf{R}_p}[\ \Pr_{\boldsymbol{\beta}(T \restriction \mathbf{R}_p)}[\ \#\boldsymbol{\beta}(T \restriction \mathbf{R}_p) \geq \ell\ ] \geq 2^{-\ell}\ ]$$

$$\leq 2^{\ell} \Pr[\ \#\boldsymbol{\beta}(T \restriction \mathbf{R}_p) \geq \ell\ ]$$

$$= 2^{\ell} \Pr[\ \mathbf{Bin}(\#\boldsymbol{\beta}(T), p) \geq \ell\ ]$$

$$\leq 2^{\ell}\, \mathrm{Ex}\left[\binom{\#\boldsymbol{\beta}(T)}{\ell} p^{\ell}\right]$$

union bound

k-Clipped Decision Tree Switching Lemma

If T is a k-clipped decision tree, then

Pr[depth(T ∧ **R**$_\ell$) > ℓ] ≤ O(pk2^k)$^\ell$

Lemma: If T is k-clipped, then

$$\mathrm{Ex}\left[\binom{\#\boldsymbol{\beta}(T)}{\ell}\right] \le O(k2^k)^\ell$$

≤ 2$^\ell$ Pr [**B**in(#$\boldsymbol{\beta}$(T), p) ≥ ℓ]

≤ 2$^\ell$ Ex[$\binom{\#\boldsymbol{\beta}(T)}{\ell}$ p$^\ell$]

≤ 2$^\ell$ p$^\ell$ O(k2^k)$^\ell$

k-Clipped Decision Tree Switching Lemma

If T is a k-clipped decision tree, then

$$\Pr[\ \mathrm{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ] = O(pk2^k)^{\ell}$$

$$\Pr[\ \mathrm{depth}(T \restriction \mathbf{R}_p) \geq \ell\ ]$$

$$\leq \Pr_{\mathbf{R}_p}[\ \Pr_{\boldsymbol{\beta}(T \restriction \mathbf{R}_p)}[\ \#\boldsymbol{\beta}(T \restriction \mathbf{R}_p) \geq \ell\ ] \geq 2^{-\ell}\ ]$$

$$\leq 2^{\ell} \Pr[\ \#\boldsymbol{\beta}(T \restriction \mathbf{R}_p) \geq \ell\ ]$$

$$= 2^{\ell} \Pr[\ \mathbf{Bin}(\#\boldsymbol{\beta}(T), p) \geq \ell\ ]$$

$$\leq 2^{\ell}\ \mathrm{Ex}\left[\ \binom{\#\boldsymbol{\beta}(T)}{\ell} p^{\ell}\ \right]$$

$$\leq 2^{\ell}\ p^{\ell}\ O(k2^k)^{\ell}$$

Q.E.D.

A Different Approach

1. Decision Tree Switching Lemma
2. k-Clipped Decision Trees
3. **Arbitrary Distribution of Stars**
4. *Switching Lemma for Affine Restrictions*
5. Tseitin Expander Switching Lemma

- Let **S** $\subseteq$ [n] be an *arbitrary* distribution of “stars”

- Let $\mathbf{S} \subseteq [n]$ be an *arbitrary* distribution of "stars"
- Let $\mathbf{u} \in_{unif} \{0,1\}^n$

- Let $\mathbf{S} \subseteq [n]$ be an *arbitrary* distribution of "stars"
- Let $\mathbf{u} \in_{unif} \{0,1\}^n$
- Define random restriction $\rho_{\mathbf{S},\mathbf{u}} : [n] \to \{0,1,\star\}$ by

$$\rho_{\mathbf{S},\mathbf{u}}(i) = \begin{cases} \star & \text{if } i \in \mathbf{S}, \\ \mathbf{u}_i & \text{otherwise.} \end{cases}$$

- Let $\mathbf{S} \subseteq [n]$ be an *arbitrary* distribution of "stars"
- Let $\mathbf{u} \in_{unif} \{0,1\}^n$
- Define random restriction $\rho_{\mathbf{S},\mathbf{u}} : [n] \to \{0,1,\star\}$ by

$$\rho_{\mathbf{S},\mathbf{u}}(i) = \begin{cases} \star & \text{if } i \in \mathbf{S}, \\ \mathbf{u}_i & \text{otherwise.} \end{cases}$$

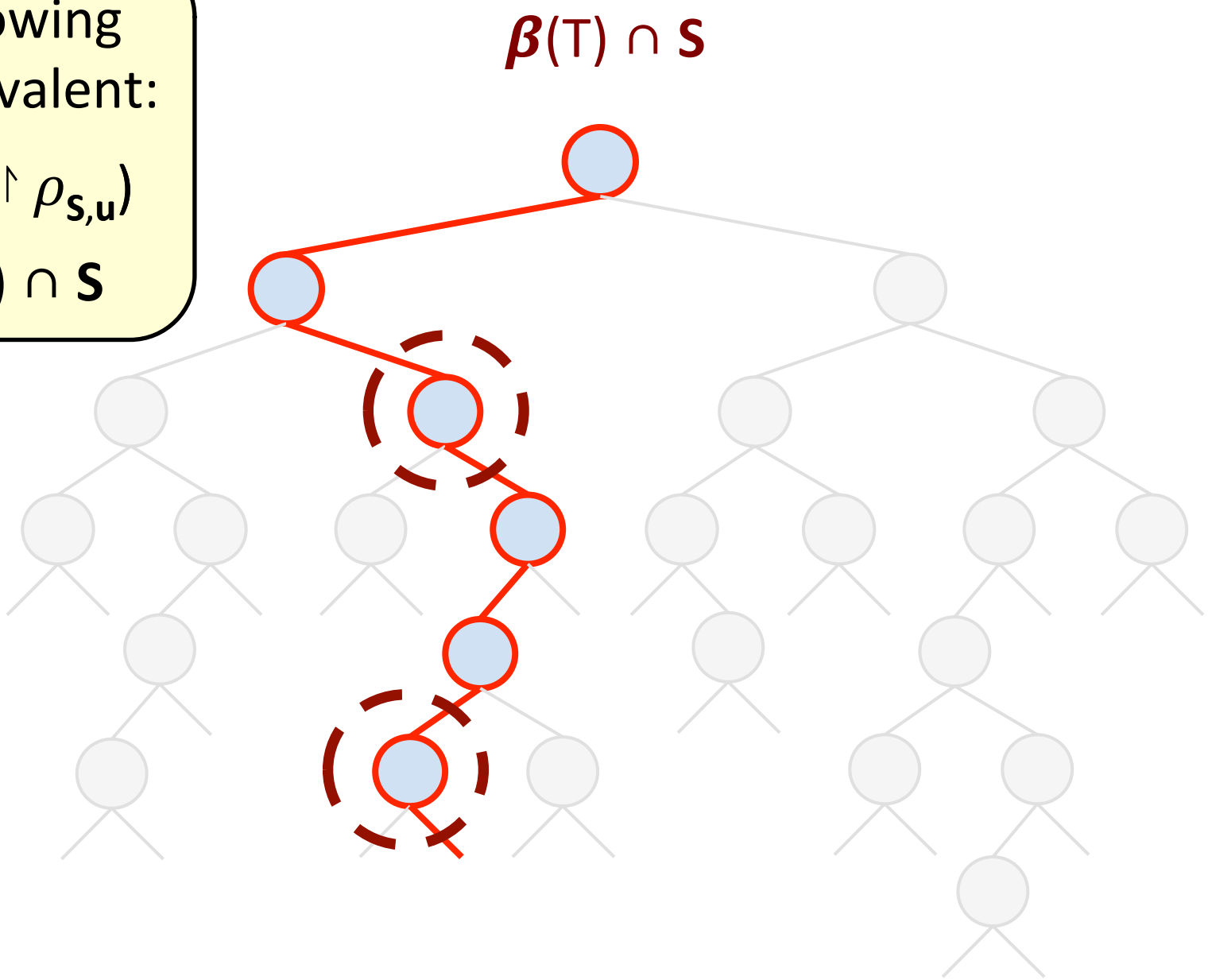
If $\mathbf{S} \subseteq_p [n]$, then $\rho_{\mathbf{S},\mathbf{u}}$ has the same distribution as $\mathbf{R}_p$

- Let $\mathbf{S} \subseteq [n]$ be an *arbitrary* distribution of "stars"

Definition: For $p \in [0,1]$, we say that $\mathbf{S}$ is p-*bounded* if $\Pr[\, J \subseteq \mathbf{S} \,] \leq p^{|J|}$ for every $J \subseteq [n]$

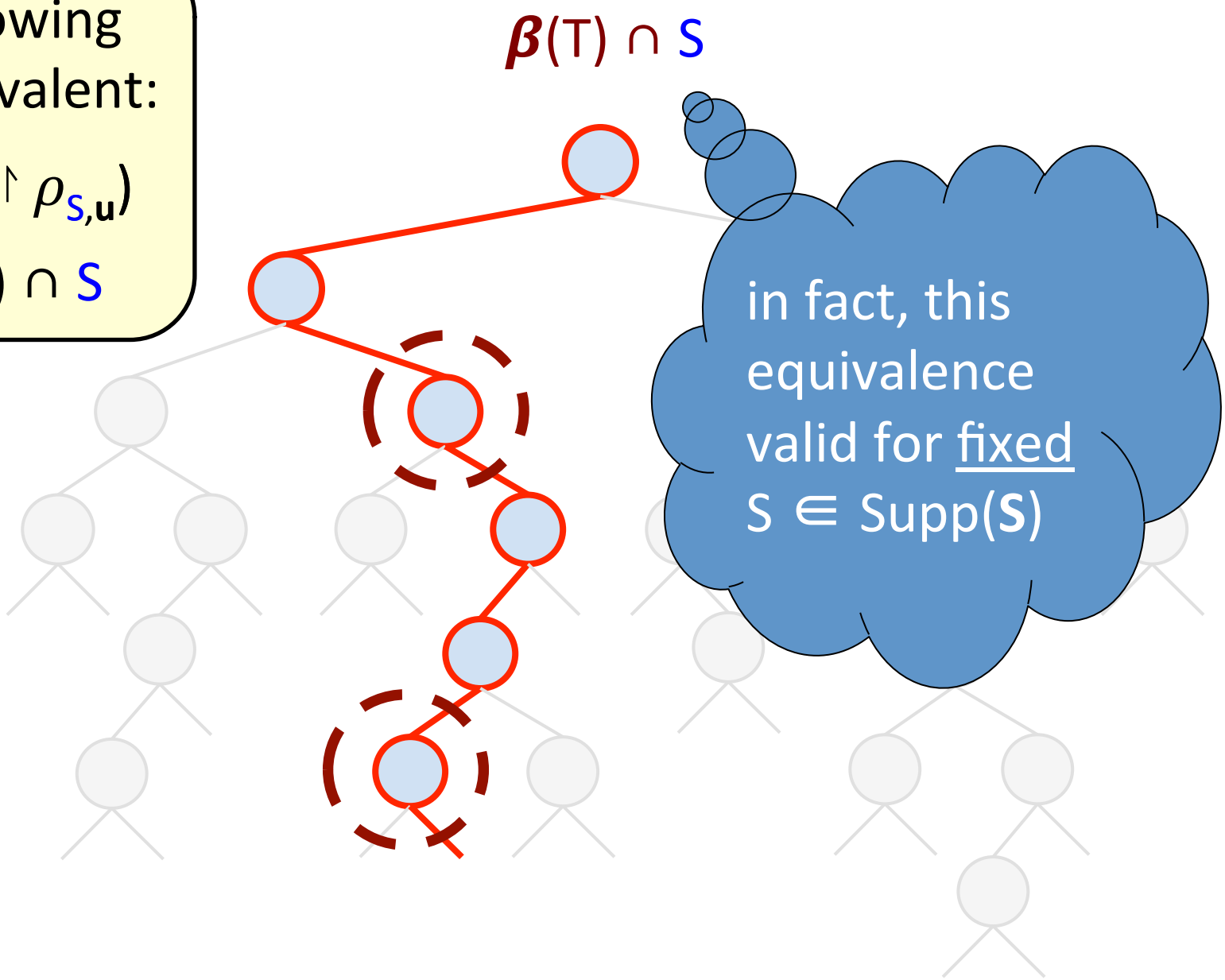
The following are equivalent:

1. $\boldsymbol{\beta}(T \restriction \rho_{\mathbf{S,u}})$
2. $\boldsymbol{\beta}(T) \cap \mathbf{S}$



The following are equivalent:

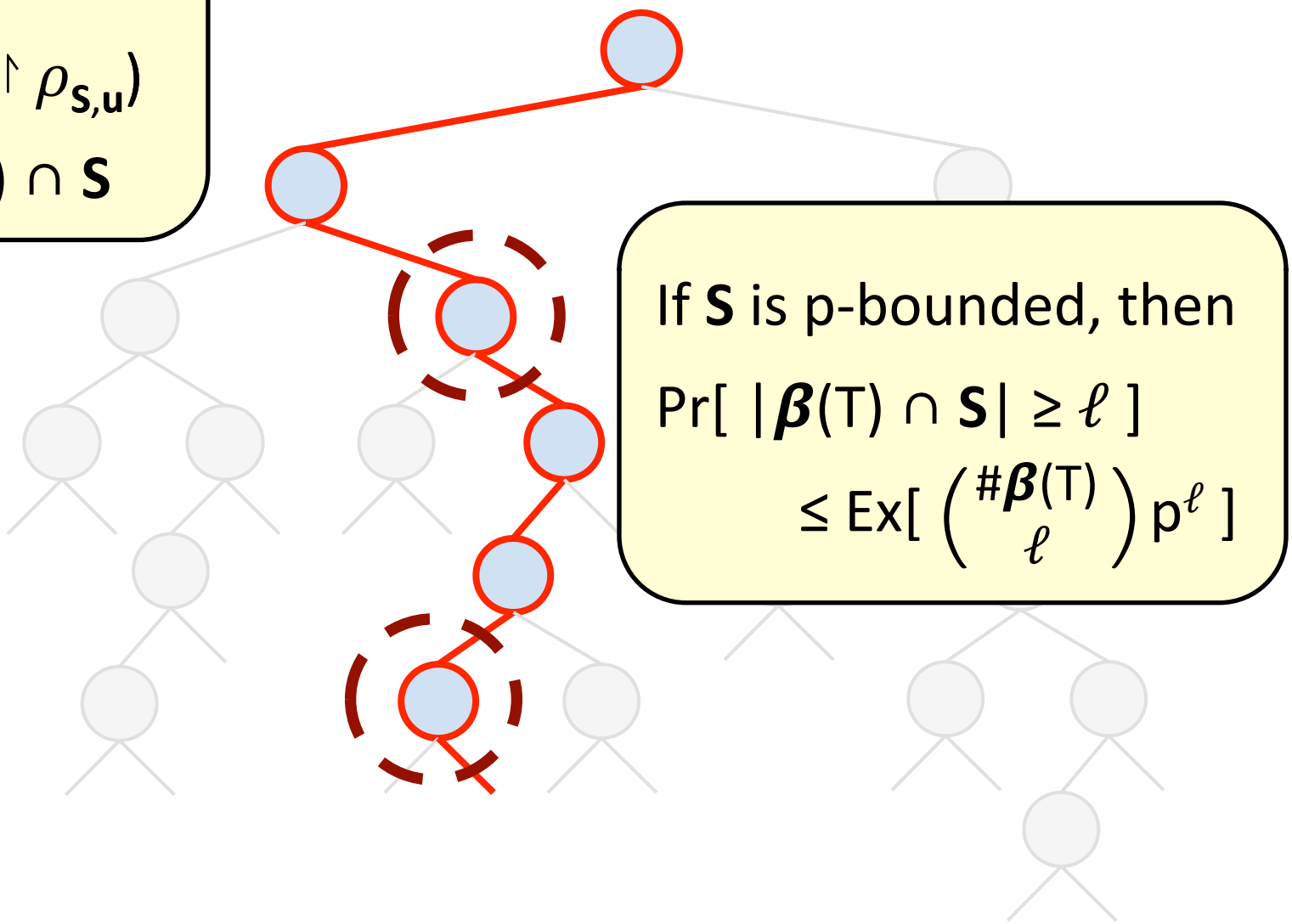
1. $\boldsymbol{\beta}(T \upharpoonright \rho_{S,\mathbf{u}})$
2. $\boldsymbol{\beta}(T) \cap S$



The following are equivalent:

1. $\boldsymbol{\beta}(T \restriction \rho_{\mathbf{S},\mathbf{u}})$
2. $\boldsymbol{\beta}(T) \cap \mathbf{S}$

$\boldsymbol{\beta}(T) \cap \mathbf{S}$



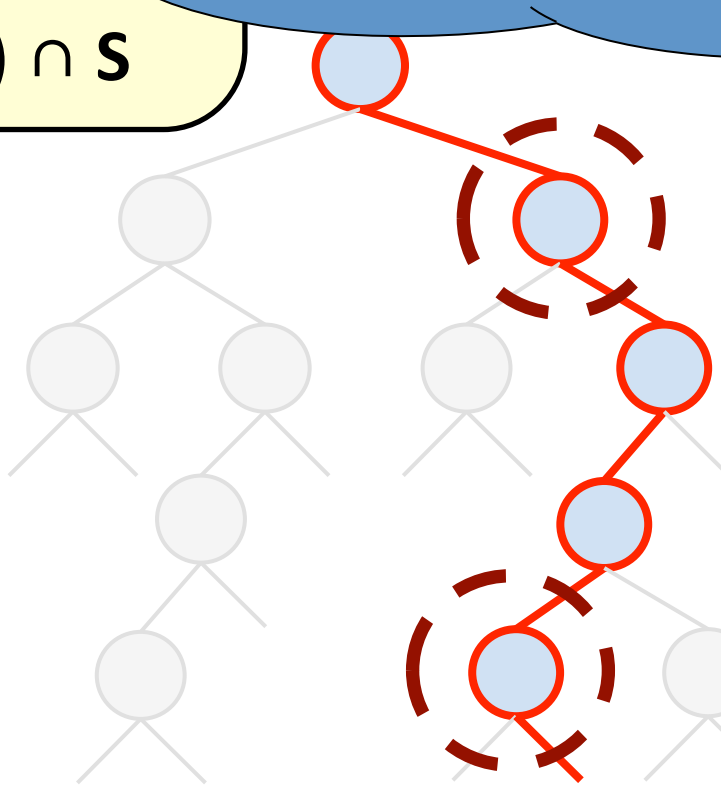
If **S** is p-bounded, then

$$\Pr[\ |\boldsymbol{\beta}(T) \cap \mathbf{S}| \geq \ell\ ] \leq \mathrm{Ex}\left[\ \binom{\#\boldsymbol{\beta}(T)}{\ell} p^{\ell}\ \right]$$

The following
are equiva

1. $\boldsymbol{\beta}$(T
2. $\boldsymbol{\beta}$(T) ∩ **S**

$\Pr[\, J \subseteq \mathbf{S} \,] \le p^{\ell}$
for every $J \subseteq [n]$ of size $|J| = \ell$



If **S** is p-bounded, then

$$\Pr[\, |\boldsymbol{\beta}(T) \cap \mathbf{S}| \ge \ell \,] \le \mathrm{Ex}\left[\binom{\#\boldsymbol{\beta}(T)}{\ell} p^{\ell} \right]$$

Theorem (Switching Lemma for $\rho_{\mathbf{S},\mathbf{u}}$)

If **S** is p-bounded and T is a k-clipped DT, then

$$\Pr[\ \mathrm{depth}(T \upharpoonright \rho_{\mathbf{S},\mathbf{u}}) \geq \ell\ ] = O(pk2^k)^{\ell}$$

Theorem (Switching Lemma for $\rho_{\mathbf{S},\mathbf{u}}$)

If **S** is p-bounded and T is a k-clipped DT, then

$$\Pr[\ \mathrm{depth}(T \restriction \rho_{\mathbf{S},\mathbf{u}}) \geq \ell\ ] = O(pk2^k)^{\ell}$$

$$\Pr[\ \mathrm{depth}(T \restriction \rho_{\mathbf{S},\mathbf{u}}) \geq \ell\ ]$$

$$\leq \Pr_{\mathbf{S},\mathbf{u}}[\ \Pr_{\mathbf{V}(T \restriction \rho_{\mathbf{S},\mathbf{u}})}[\ \#\boldsymbol{\beta}(T \restriction \rho_{\mathbf{S},\mathbf{u}}) \geq \ell\ ] \geq 2^{-\ell}\ ]$$

$$\leq 2^{\ell} \Pr[\ \#\boldsymbol{\beta}(T \restriction \rho_{\mathbf{S},\mathbf{u}}) \geq \ell\ ]$$

$$= 2^{\ell} \Pr[\ |\boldsymbol{\beta}(T) \cap \mathbf{S}| \geq \ell\ ]$$

$$\leq 2^{\ell} \mathrm{Ex}\left[\binom{\#\boldsymbol{\beta}(T)}{\ell} p^{\ell}\right]$$

$$\leq 2^{\ell}\, p^{\ell}\, O(k2^k)^{\ell}$$

Q.E.D.

A Different Approach

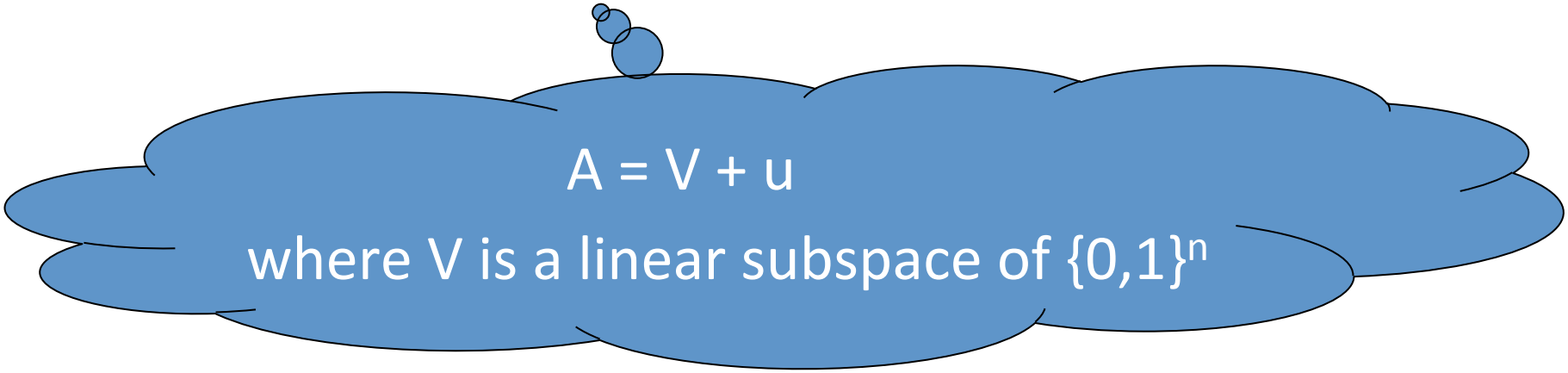
1. Decision Tree Switching Lemma
2. k-Clipped Decision Trees
3. Arbitrary Distribution of Stars
4. ***Switching Lemma for Affine Restrictions***
5. Tseitin Expander Switching Lemma

- Restrictions $[n] \to \{0,1,\star\}$ are in 1-1 correspondence with ***subcubes*** of $\{0,1\}^n$

- What about the complexity of $F \restriction \mathbf{A}$ (e.g. for F a k-DNF) for a random ***affine subspace*** of $\mathbf{A} \subseteq \{0,1\}^n$?

- Restrictions $[n] \to \{0,1,\star\}$ are in 1-1 correspondence with ***subcubes*** of $\{0,1\}^n$

- What about the complexity of $F \restriction \mathbf{A}$ (e.g. for F a k-DNF) for a random ***affine subspace*** of $\mathbf{A} \subseteq \{0,1\}^n$?



- Restrictions $[n] \to \{0,1,\star\}$ are in 1-1 correspondence with ***subcubes*** of $\{0,1\}^n$

- What about the complexity of $F \restriction \mathbf{A}$ (e.g. for F a k-DNF) for a random ***affine subspace*** of $\mathbf{A} \subseteq \{0,1\}^n$?

Affine Switching Lemma

If F is a k-DNF and **A** is a "p-bounded" random affine subset of $\{0,1\}^n$, then

$$\Pr[\ DT_{depth}(F \restriction \mathbf{A}) \geq \ell\ ] = O(pk2^k)^{\ell}$$

Applying an Affine Restriction

- Consider an affine set $A \subseteq \{0,1\}^n$
- For $f : \{0,1\}^n \to \{0,1\}$, we define:

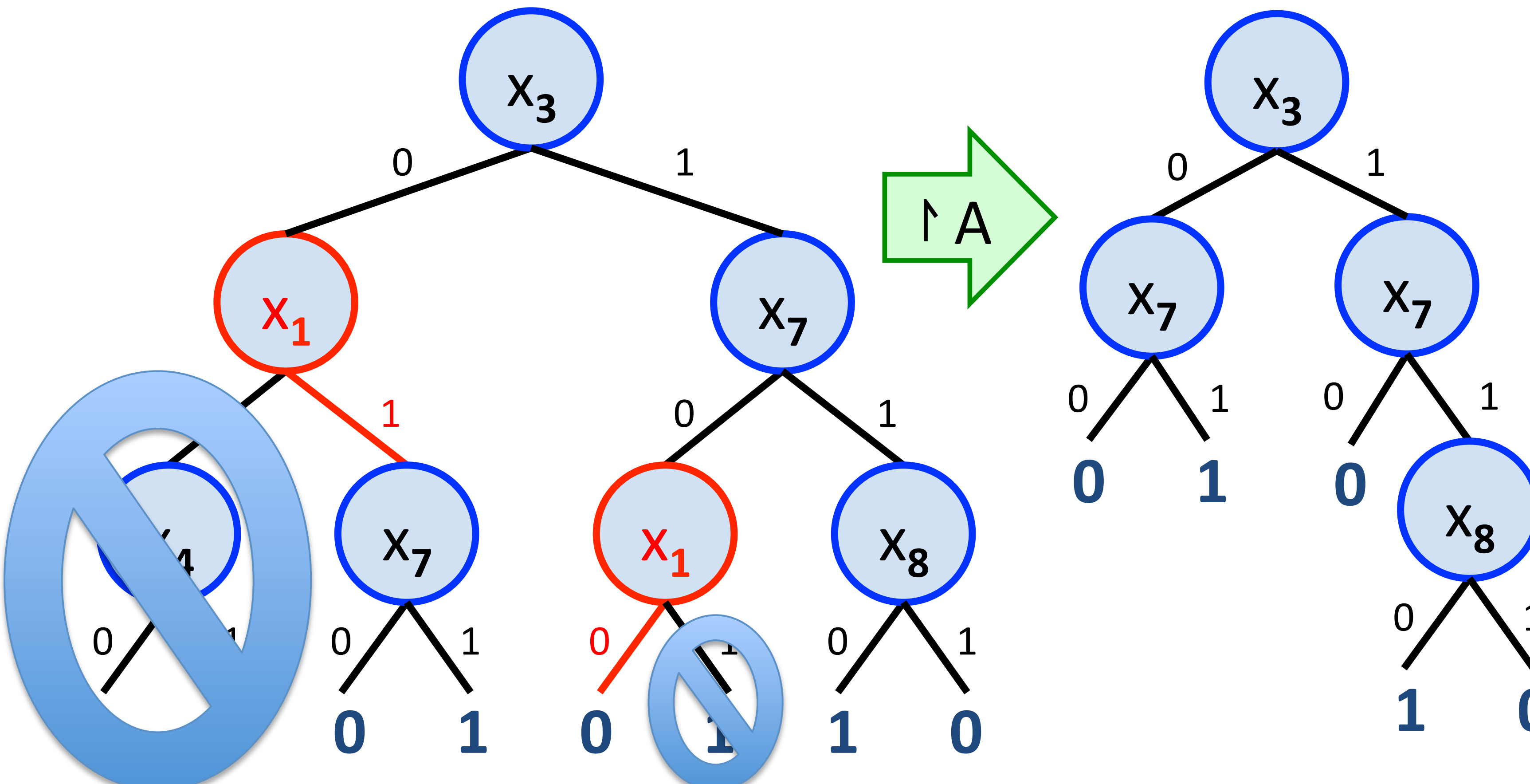
$$f \restriction A : A \to \{0,1\},$$

$DT_{depth}(f \restriction A) =$ min. depth of a decision tree T such that $f(x) = T(x)$ for all $x \in A$

- We also have a *syntactic* operation $T \mapsto T \restriction A$ on decision trees

Applying an Affine Restriction

- <u>Example</u>: $A = \{ x \in \{0,1\}^n \mid x_1 \neq x_3 \}$



- Let $\mathbf{S} \subseteq [n]$ be an *arbitrary* dist. of "stars"

- Let $\mathbf{u} \in_{unif} \{0,1\}^n$
- Consider random restriction $\rho_{\mathbf{S},\mathbf{u}}(i) = \begin{cases} \star & \text{if } i \in \mathbf{S}, \\ \mathbf{u}_i & \text{otherwise.} \end{cases}$

- ~~Let $\mathbf{S} \subseteq [n]$ be an *arbitrary* dist. of "stars"~~

  Let $\mathbf{V}$ be an *arbitrary* dist. on linear subspaces of $\{0,1\}^n$

- Let $\mathbf{u} \in_{unif} \{0,1\}^n$

- Consider random restriction $\rho_{\mathbf{S},\mathbf{u}}(i) = \begin{cases} \star & \text{if } i \in \mathbf{S}, \\ \mathbf{u}_i & \text{otherwise.} \end{cases}$

- ~~Let **S** $\subseteq$ [n] be an *arbitrary* dist. of "stars"~~

  Let **V** be an *arbitrary* dist. on linear subspaces of $\{0,1\}^n$

- Let $\mathbf{u} \in_{unif} \{0,1\}^n$

- ~~Consider random restriction $\rho_{\mathbf{S},\mathbf{u}}(i) =$ $\begin{cases} \star & \text{if } i \in \mathbf{S}, \\ \mathbf{u}_i & \text{otherwise.} \end{cases}$~~

  Consider random affine space **V** + **u**

- ~~Let **S** ⊆ [n] be an *arbitrary* dist. of "stars"~~

  Let **V** be an *arbitrary* dist. on linear subspaces of $\{0,1\}^n$

- Let $\mathbf{u} \in_{unif} \{0,1\}^n$

- ~~Consider random restriction $\rho_{\mathbf{S},\mathbf{u}}(i) = \begin{cases} \star & \text{if } i \in \mathbf{S}, \\ \mathbf{u}_i & \text{otherwise.} \end{cases}$~~

  Consider random affine space **V** + **u**

V is the arrangement of "stars"

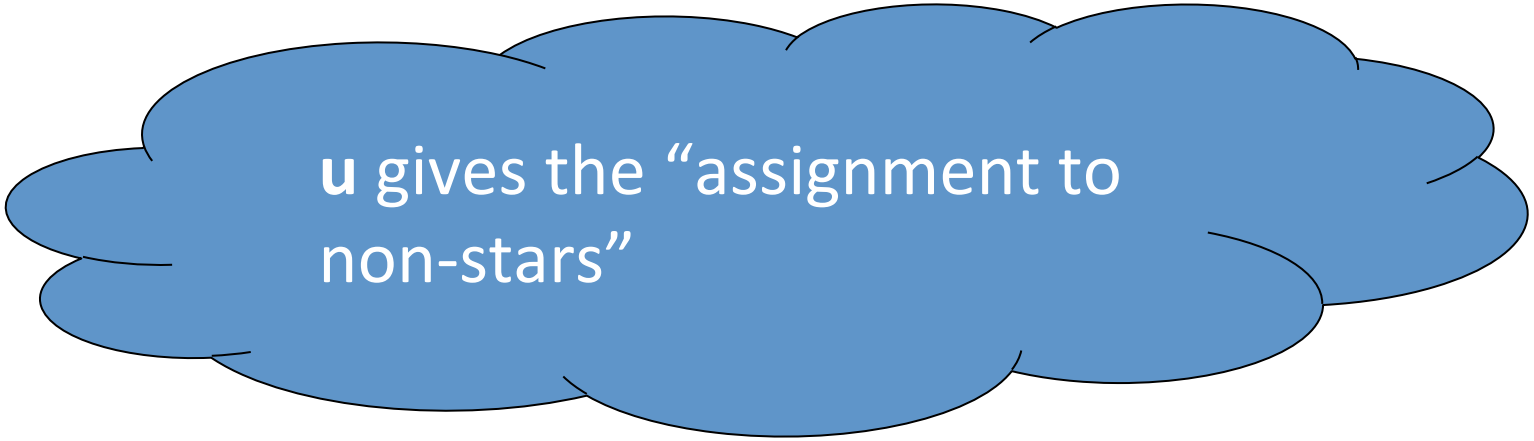
- ~~Let **S** ⊆ [n] be an *arbitrary* dist. of "stars"~~

  Let **V** be an *arbitrary* dist. on linear subspaces of $\{0,1\}^n$

- Let **u** $\in_{unif} \{0,1\}^n$

- ~~Consider random restriction $\rho_{\mathbf{S},\mathbf{u}}(i) =$ $\begin{cases} \star & \text{if } i \in \mathbf{S}, \\ \mathbf{u}_i & \text{otherwise.} \end{cases}$~~

  Consider random affine space **V** + **u**



- Let $\mathbf{S} \subseteq [n]$ be an *arbitrary* dist. of "stars"

  Let $\mathbf{V}$ be an *arbitrary* dist. on linear subspaces of $\{0,1\}^n$

- Let $\mathbf{u} \in_{unif} \{0,1\}^n$

- ~~Consider random restriction $\rho_{\mathbf{S},\mathbf{u}}(i) =$ $\begin{cases} \star & \text{if } i \in \mathbf{S}, \\ \mathbf{u}_i & \text{otherwise.} \end{cases}$~~

  Consider random affine space $\mathbf{V} + \mathbf{u}$

$\{b_1, \ldots, b_n\}$ = standard basis for $\{0,1\}^n$

if $\mathbf{V} = \text{Span}\{ b_i \mid i \in \mathbf{S} \}$, then $\mathbf{V} + \mathbf{u}$ is the subcube defined by $\rho_{\mathbf{S},\mathbf{u}}$

Definition

A random set $\mathbf{S} \subseteq [n]$ is p-*bounded* if, for all $J \subseteq [n]$,

$$\Pr[\, J \subseteq \mathbf{S} \,] \leq p^{|J|}$$

Definition

A random linear subspace $\mathbf{V} \subseteq \{0,1\}^n$ is p-*bounded* if, for all $J \subseteq [n]$,

$$\Pr[\, \mathbf{V} \text{ shatters } J \,] \leq p^{|J|}$$

Definition

A random set $\mathbf{S} \subseteq [n]$ is p-*bounded* if, for all $J \subseteq [n]$,

$$\Pr[\, J \subseteq \mathbf{S} \,] \leq p^{|J|}$$

Definition

A random linear subspace $\mathbf{V} \subseteq \{0,1\}^n$ is p-*bounded* if, for all $J \subseteq [n]$,

$$\Pr[\, \mathbf{V} \text{ shatters } J \,] \leq p^{|J|}$$

$\forall I \subseteq J \;\; \exists v \in \mathbf{V}$ such that

- $v_i = 1$ for all $i \in I$
- $v_j = 0$ for all $j \in J \setminus I$

Definition

A rand[illegible]

V shatters J ⊆ [n]

⇔

J is independent in the *matroid* associated with V

Definition

A random linear subspace $\mathbf{V} \subseteq \{0,1\}^n$ is p-*bounded* if, for all J ⊆ [n],

$$\Pr[\ \mathbf{V} \text{ shatters } J\ ] \le p^{|J|}$$

$\forall I \subseteq J \quad \exists v \in \mathbf{V}$ such that

- $v_i = 1$ for all $i \in I$
- $v_j = 0$ for all $j \in J \setminus I$

Definition

A random set $\mathbf{S} \subseteq [n]$ is p-*bounded* if, for all $J \subseteq [n]$,

$$\Pr[\, J \subseteq \mathbf{S} \,] \leq p^{|J|}$$

Definition

A random linear subspace $\mathbf{V} \subseteq \{0,1\}^n$ is p-*bounded* if, for all $J \subseteq [n]$,

$$\Pr[\, \mathbf{V} \text{ shatters } J \,] \leq p^{|J|}$$

equivalent if $\mathbf{V} = \mathrm{Span}\{\, b_i \mid i \in \mathbf{S} \,\}$

Suppose $\mathbf{A} = \mathbf{V} + \mathbf{u}$ where

- $\mathbf{V}$ is a p-bounded random linear subspace of $\{0,1\}^n$
- $\mathbf{u} \in_{unif} \{0,1\}^n$

Theorem For every k-clipped decision tree T,

$$\Pr[\ \mathrm{depth}(T \restriction \mathbf{A}) \geq \ell\ ] = O(pk2^k)^{\ell}$$

essentially the same proof as the Switching Lemma for $\rho_{\mathbf{S},\mathbf{u}}$

Suppose $\mathbf{A} = \mathbf{V} + \mathbf{u}$ where

- $\mathbf{V}$ is a p-bounded random linear subspace of $\{0,1\}^n$
- $\mathbf{u} \in_{unif} \{0,1\}^n$

Theorem For every k-clipped decision tree T,

$$\Pr[\ \mathrm{depth}(T \restriction \mathbf{A}) \geq \ell\ ] = O(pk2^k)^{\ell}$$

Corollary (Affine Switching Lemma)

For every k-DNF F, $\Pr[\ \mathrm{DT}_{\mathrm{depth}}(F \restriction \mathbf{A}) \geq \ell\ ] = O(pk2^k)^{\ell}$

Suppose $\mathbf{A} = \mathbf{V} + \mathbf{u}$ where

- $\mathbf{V}$ is a p-bounded random linear subspace of $\{0,1\}^n$
- $\mathbf{u} \in_{unif} \{0,1\}^n$

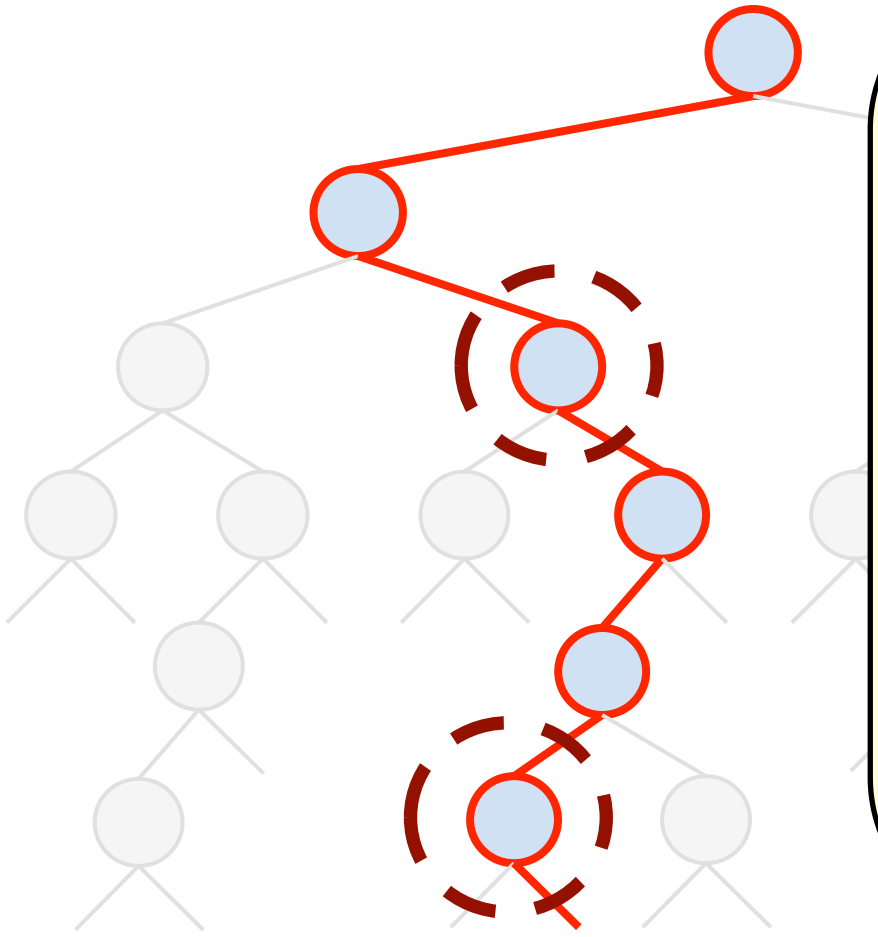
Theorem For every k-clipped decision tree T,

$$\Pr[\ \mathrm{depth}(T \restriction \mathbf{A}) \geq \ell\ ] = O(pk2^k)^\ell$$

Corollary (Affine Switching Lemma)

For every k-DNF F, $\Pr[\ \mathrm{DT}_{\mathrm{depth}}(F \restriction \mathbf{A}) \geq \ell\ ] = O(pk2^k)^\ell$

Conjecture: $O(pk)^\ell$



For every fixed V (and random $\mathbf{u} \in \{0,1\}^n$), the following are equivalent:

1. $\boldsymbol{\beta}(T \restriction (V + \mathbf{u}))$

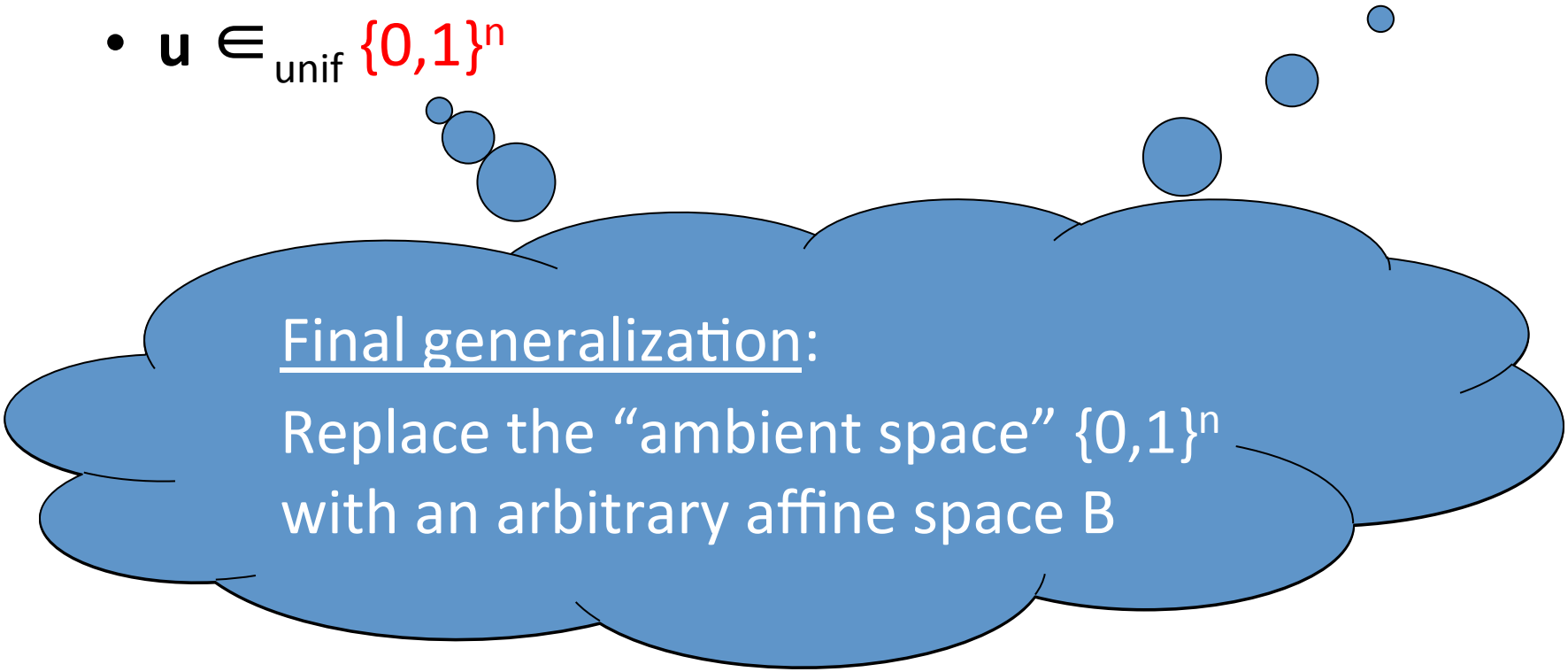
   $\#\boldsymbol{\beta}(T \restriction (V + \mathbf{u}))$

2. "greedy basis" of $\boldsymbol{\beta}(T)$ in the V-matroid

   $\text{rank}_V(\boldsymbol{\beta}(T))$

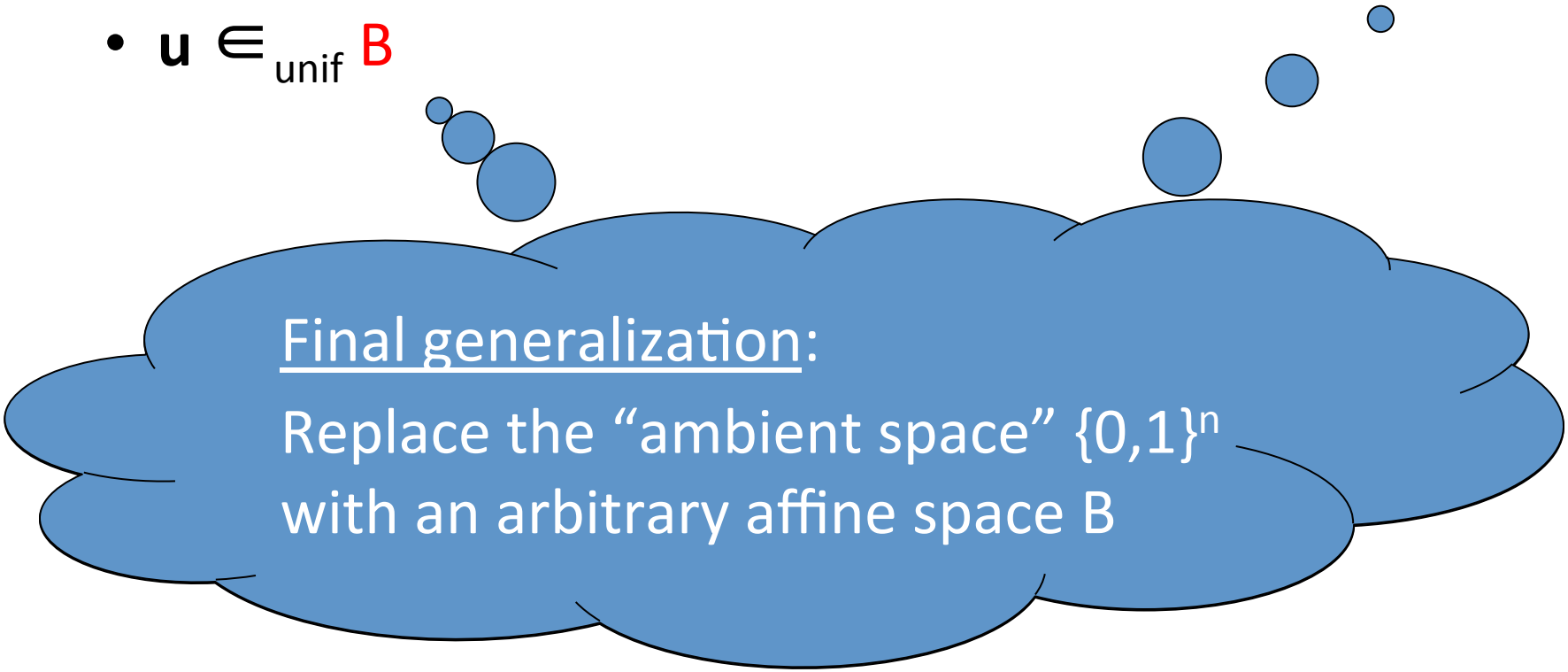
Suppose **A** = **V** + **u** where

- **V** is a p-bounded random linear subspace of $\{0,1\}^n$
- $\mathbf{u} \in_{\text{unif}} \{0,1\}^n$



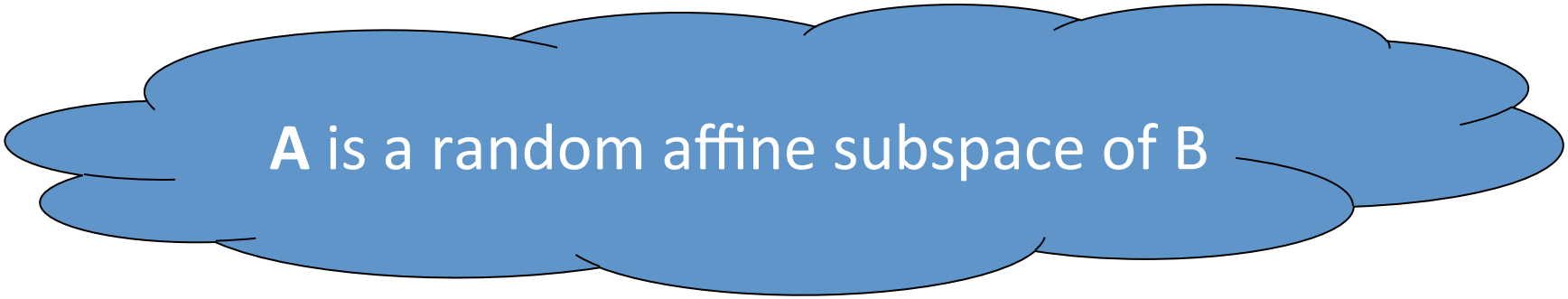
Suppose **A** = **V** + **u** where

- **V** is a p-bounded random linear subspace of B
- $\mathbf{u} \in_{unif} B$



Suppose **A** = **V** + **u** where

- **V** is a p-bounded random linear subspace of B
- $\mathbf{u} \in_{unif} B$



Suppose **A** = **V** + **u** where

- **V** is a p-bounded random linear subspace of B
- $\mathbf{u} \in_{unif} B$

Theorem

For every B-*independent* k-clipped decision tree T,

$$\Pr[\ \mathrm{depth}(T \restriction \mathbf{A}) \geq \ell\ ] = O(pk2^k)^{\ell}$$

Suppose **A** = **V** + **u** where

- **V** is a p-bounded random linear subspace of B
- $\mathbf{u} \in_{unif} B$

Theorem

For every B-*independent* k-clipped decision tree T,

$$\Pr[\ \mathrm{depth}(T \restriction \mathbf{A}) \geq \ell\ ] = O(pk2^k)^{\ell}$$

Every branch $\beta \subseteq [n]$ of T is "shattered" by B

(i.e. β is independent in the matroid associated with $\mathrm{Lin}(B) = \{ x - y \mid x,y \in B\}$)

A Different Approach

1. Decision Tree Switching Lemma
2. k-Clipped Decision Trees
3. Arbitrary Distribution of Stars
4. *Switching Lemma for Affine Restrictions*
5. **Tseitin Expander Switching Lemma**

Tseitin Expander Switching Lemma

Theorem (Pitassi-R.-Servedio-Tan '16)

Depth-d AC^0 Frege proofs of Tseitin(3-regular expander) require size $\exp\left(\Omega\left(\left(\frac{\log n}{d}\right)^2\right)\right)$

Theorem (Beame-Pitassi-Impagliazzo '93, Ben-Sasson '02)

Depth-d AC^0 Frege proofs of Tseitin(3-regular expander) require size $\exp\left(\Omega\left(n^{1/2^d}\right)\right)$

Tseitin Expander Switching Lemma

Theorem (Pitassi-R.-Servedio-Tan '16)

Depth-d AC^0 Frege proofs of Tseitin(3-regular expander) require size $\exp\left(\Omega\left(\left(\frac{\log n}{d}\right)^2\right)\right)$

The

Improving the AFFINE SWITCHING LEMMA would yield $\exp(\Omega(n^{1/d}))$

Suppose $\mathbf{A} = \mathbf{V} + \mathbf{u}$ where

- $\mathbf{V}$ is a p-bounded random linear subspace of $\{0,1\}^n$
- $\mathbf{u} \in_{unif} \{0,1\}^n$

Affine Switching Lemma for k-DNFs

For every k-DNF F,

$$\Pr[\, DT_{depth}(F \restriction \mathbf{A}) \geq \ell \,] \leq O(pk2^k)^{\ell}$$

Conjecture: $O(pk)^{\ell}$

Stay Tuned…

- Toni Pitassi: Expander S.L. & AC^0-Frege lower bound
- Johan Hastad, Avishay Tal: Correlation bounds from improved switching lemmas
- Johan Hastad, Rocco Servedio: Random projections, depth hierarchy theorem
- Srikanth Srinivasan: Adaptive random restrictions (against AC^0 with few threshold gates)
- …

Thanks!