Restriction-Based Methods

Benjamin Rossman

University of Toronto

Restrictions

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

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

independently for each variable x_i

Lower Bounds from Restrictions

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

- Recipe for lower bounds:

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

Types of Restrictions $R \subseteq \{0,1\}^n$

(increasing order of generality)

subcube	$x_i = 0,\ \ x_i = 1$
mon. projection	$x_i = 0,\ \ x_i = 1,\ \ x_i = x_j$
projection	$x_i = 0,\ \ x_i = 1,\ \ x_i = x_j,\ \ x_i \neq x_j$
affine	$x_{i\_1} \oplus \cdots \oplus x_{i\_k} = 0,\ \ x_{i\_1} \oplus \cdots \oplus x_{i\_k} = 1$
low-degree variety	$P(x_1,\dots,x_n) = 0$ where $\deg(P) \leq d$

Outline

- Background (circuit complexity, gate elimination arguments)
- The Switching Lemma & **a new "entropy" proof**
- Recent applications of stronger Switching Lemmas (**criticality of AC^0 functions**, #SAT algorithms,bounds on Fourier spectrum)
- Tour of other random restrictions (Hastad's Tseitin grid projections)

Circuit Complexity

Circuit Complexity

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

- Goal is to prove ***unconditional lower bounds***, which do not rely on any unproven assumptions

Circuit Complexity

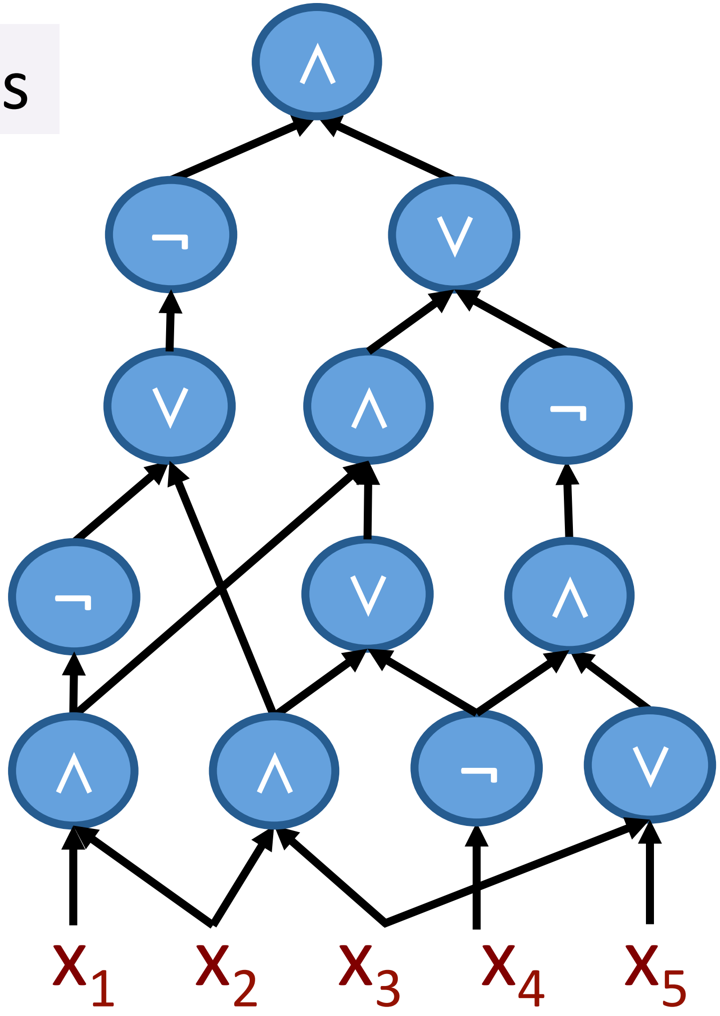
- Studies the complexity of specific **problems** (e.g. PARITY, MATRIX MULTIPLICATION, etc.) in ***combinatorial models of computation***, most importantly Boolean circuits

- Go

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

Boolean Circuits

size = # of AND and OR gates



Boolean Circuits

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

Boolean Circuits

- An n-variable Boolean circuit computes an n-variable Boolean function $\{0,1\}^n \rightarrow \{0,1\}$

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

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

Circuit Size

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

- Theorem [Shannon 1949, Lupanov 1958]

  Almost all Boolean functions have circuit size $\Theta(2^n/n)$

- The goal in Circuit Complexity is proving lower bounds for ***explicit*** Boolean functions (e.g. k-CLIQUE)

Circuit Size

- Theorem [Schnorr 1976, Fischer-Pippenger 1979]

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

- Corollary

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

Circuit Size

- Theorem [Schnorr 1976, Fischer-Pippenger 1979]

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

- Corollary

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

Circuit Complexity is widely believed to be the most viable approach to $P \neq NP$

Circuit Size

- Holy Grail (P ≠ NP)

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

Circuit Size

- Holy Grail ($P \neq NP$)

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

- Best known lower bound

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

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

[Find-Golovnev-Hirsch-Kulikov ’16]

circuit

- Best known lower bound

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

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

[Find-Golovnev-Hirsch-Kulikov ’16]

circuit

Gate-elimination arguments

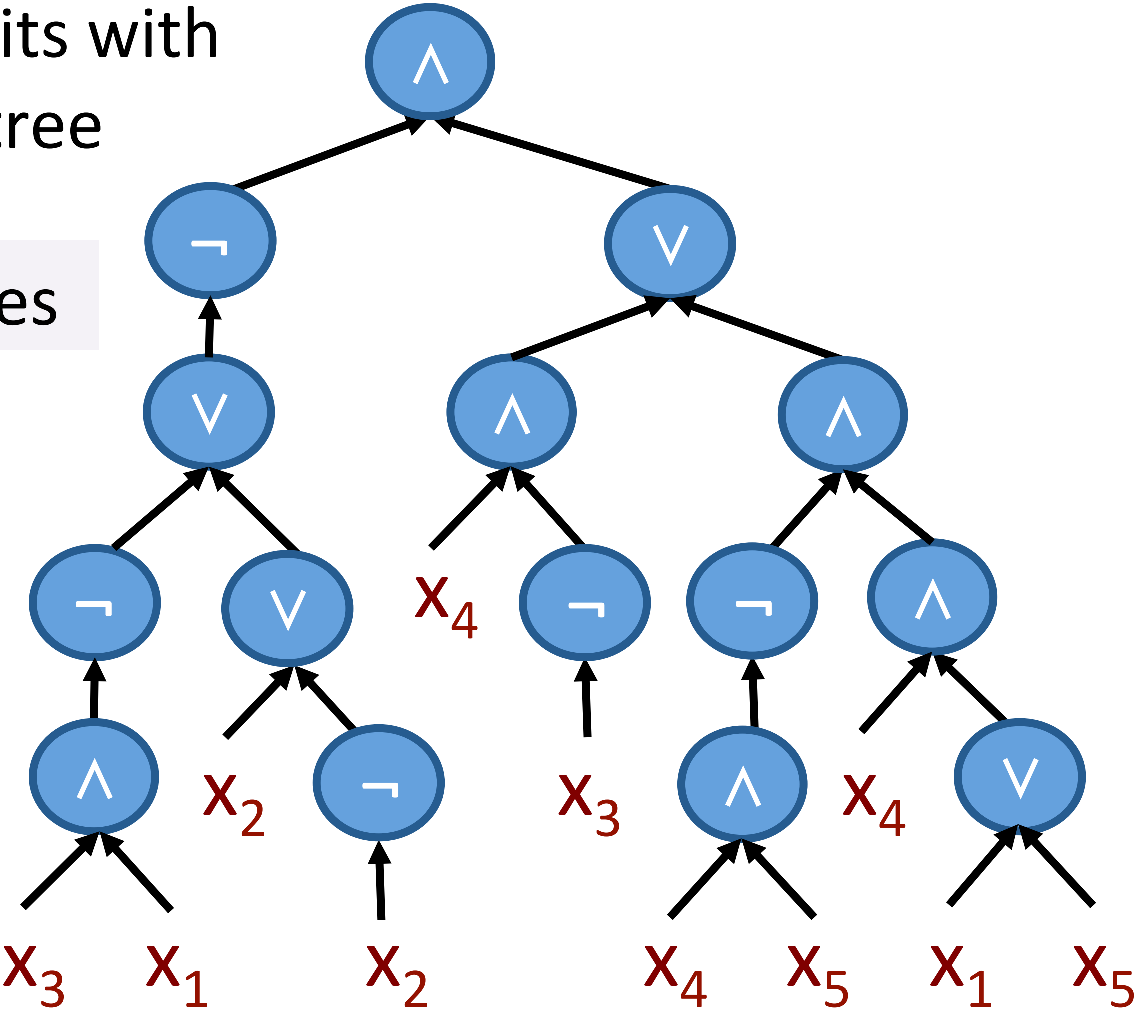
(subcube and affine restrictions)

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

(DeMorgan) Formulas

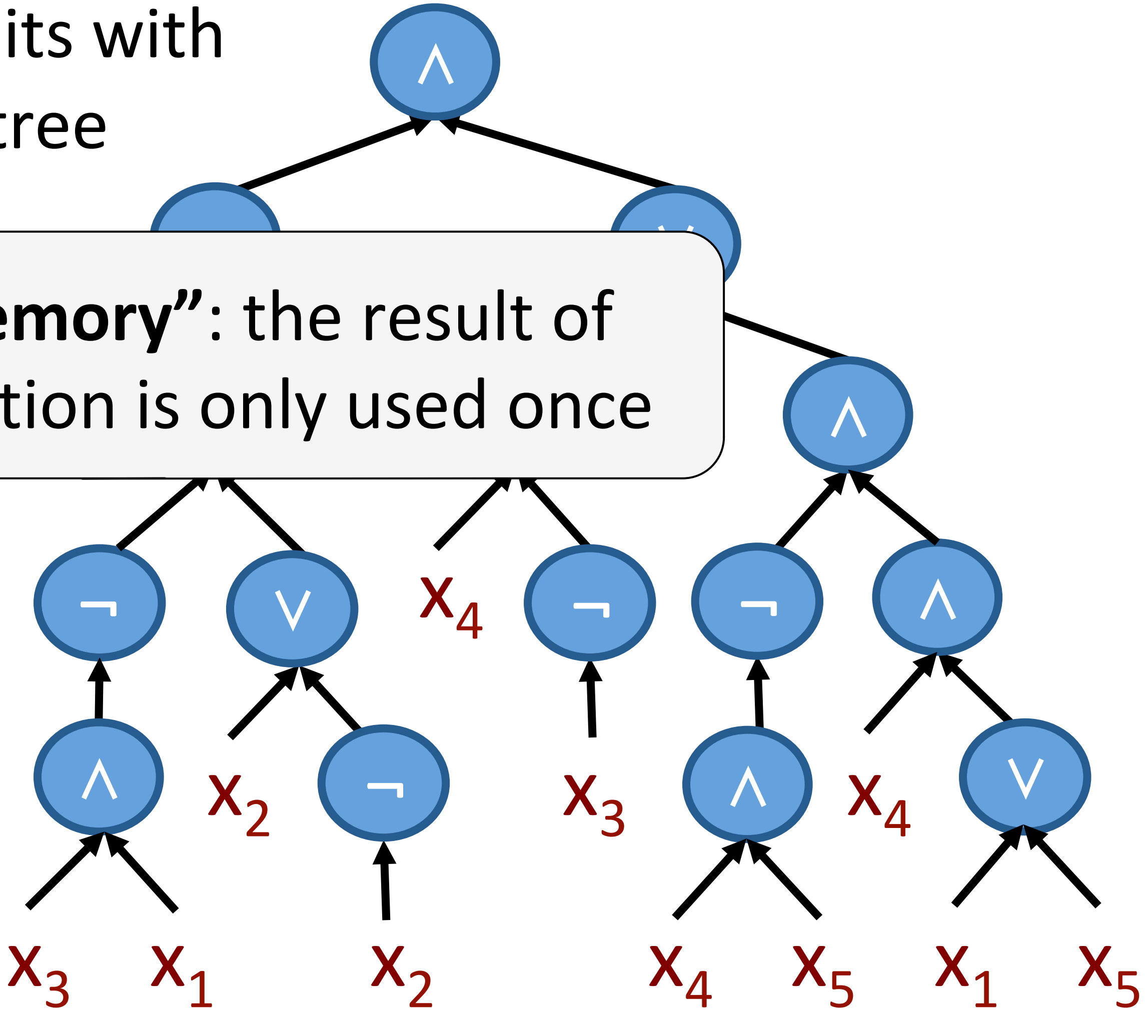
Formulas are circuits with the structure of a tree

leafsize = # of leaves



(DeMorgan) Formulas

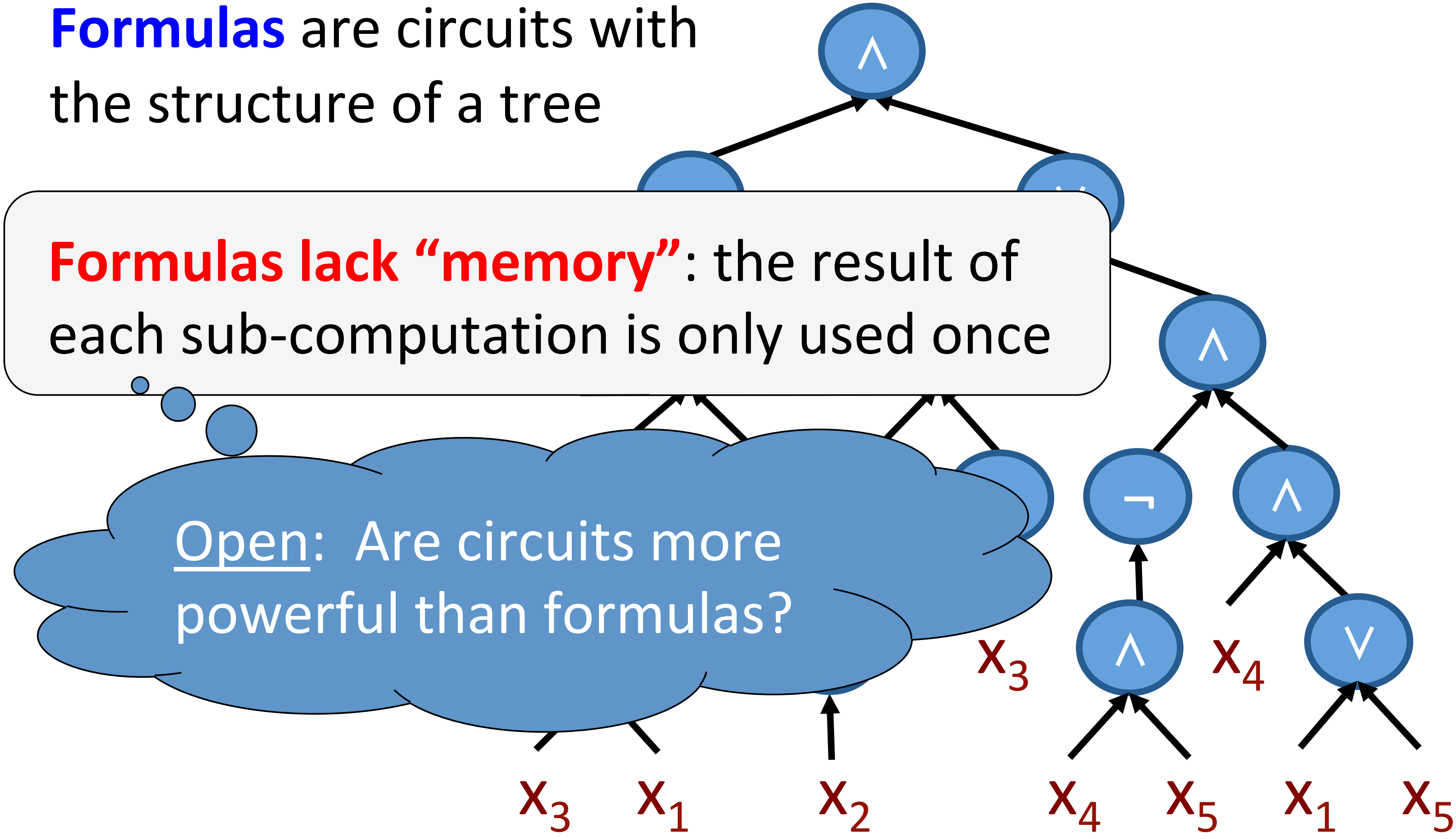
Formulas are circuits with the structure of a tree



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

(DeMorgan) Formulas

Formulas are circuits with the structure of a tree



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

Open: Are circuits more powerful than formulas?

Formulas vs. Circuits

- A Pret-ty Holy Grail (NC^1 ≠ P)

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

Formulas vs. Circuits

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

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

- Best known formula size lower bound

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

(log-factor improvement [Tal'14])

Formulas vs. Circuits

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

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

Shrinkage of DeMorgan formulas

(simplification under p-random restrictions)

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

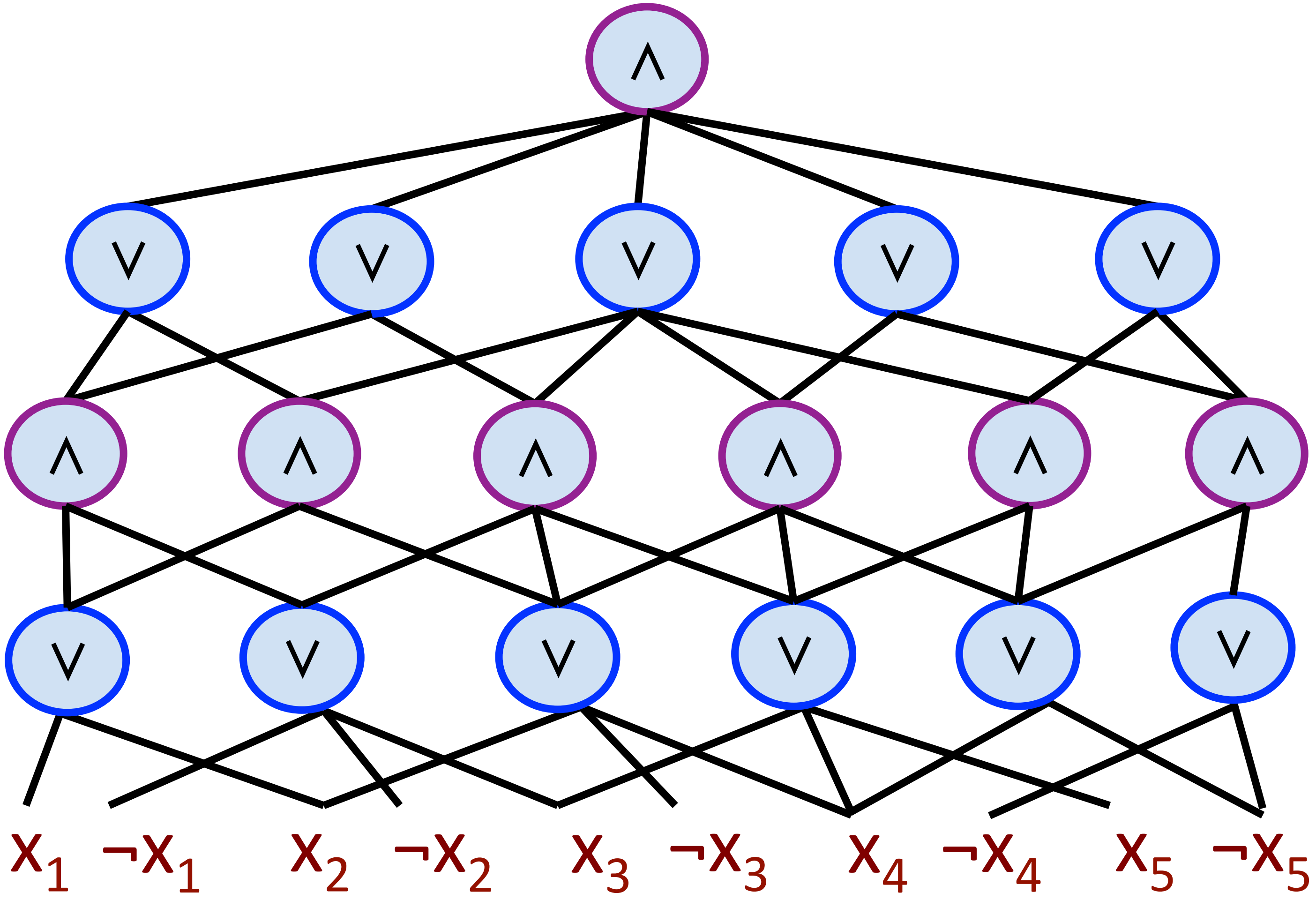
(log-factor improvement [Tal'14])

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

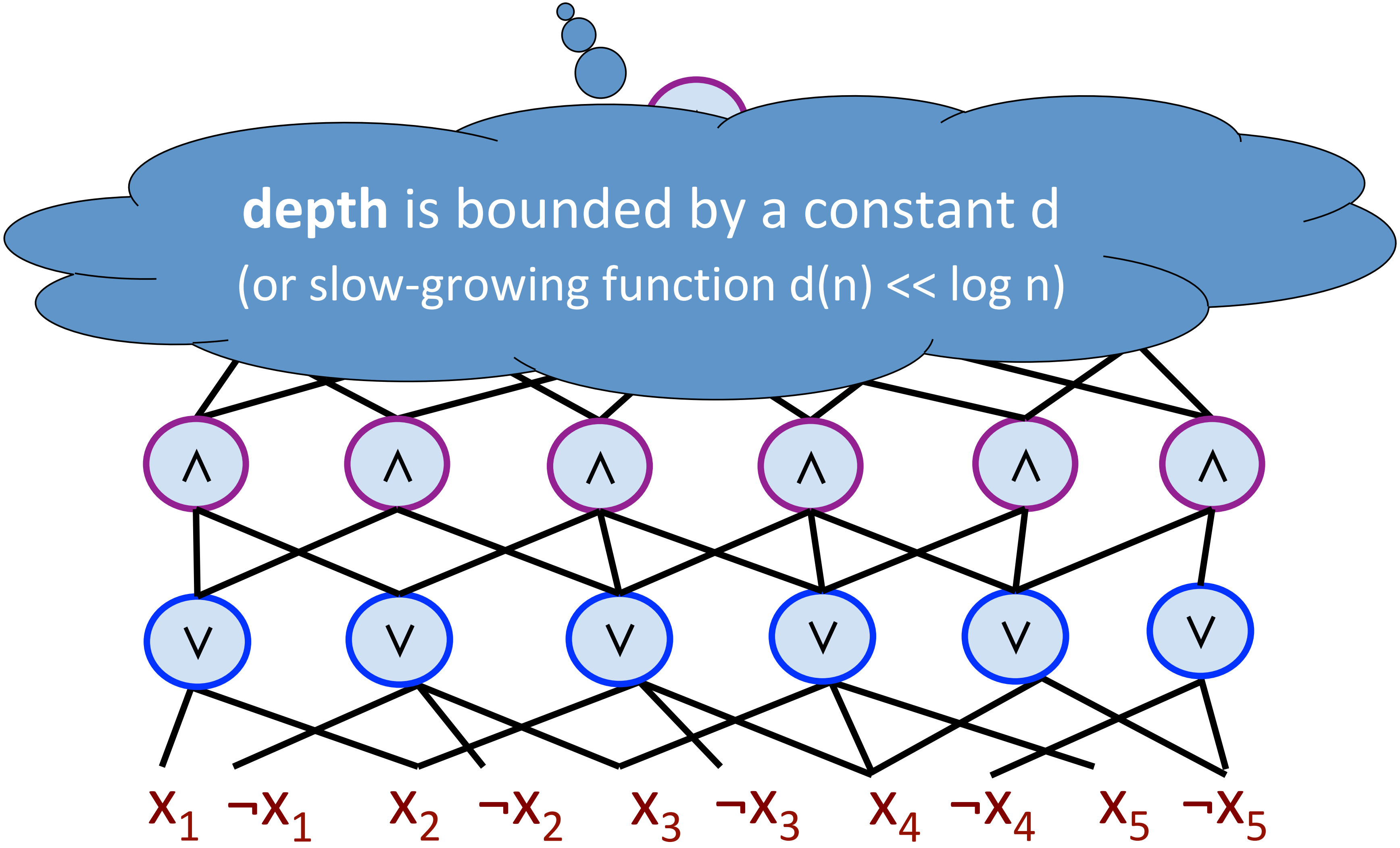
Restricted Classes

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

AC^0 Circuits



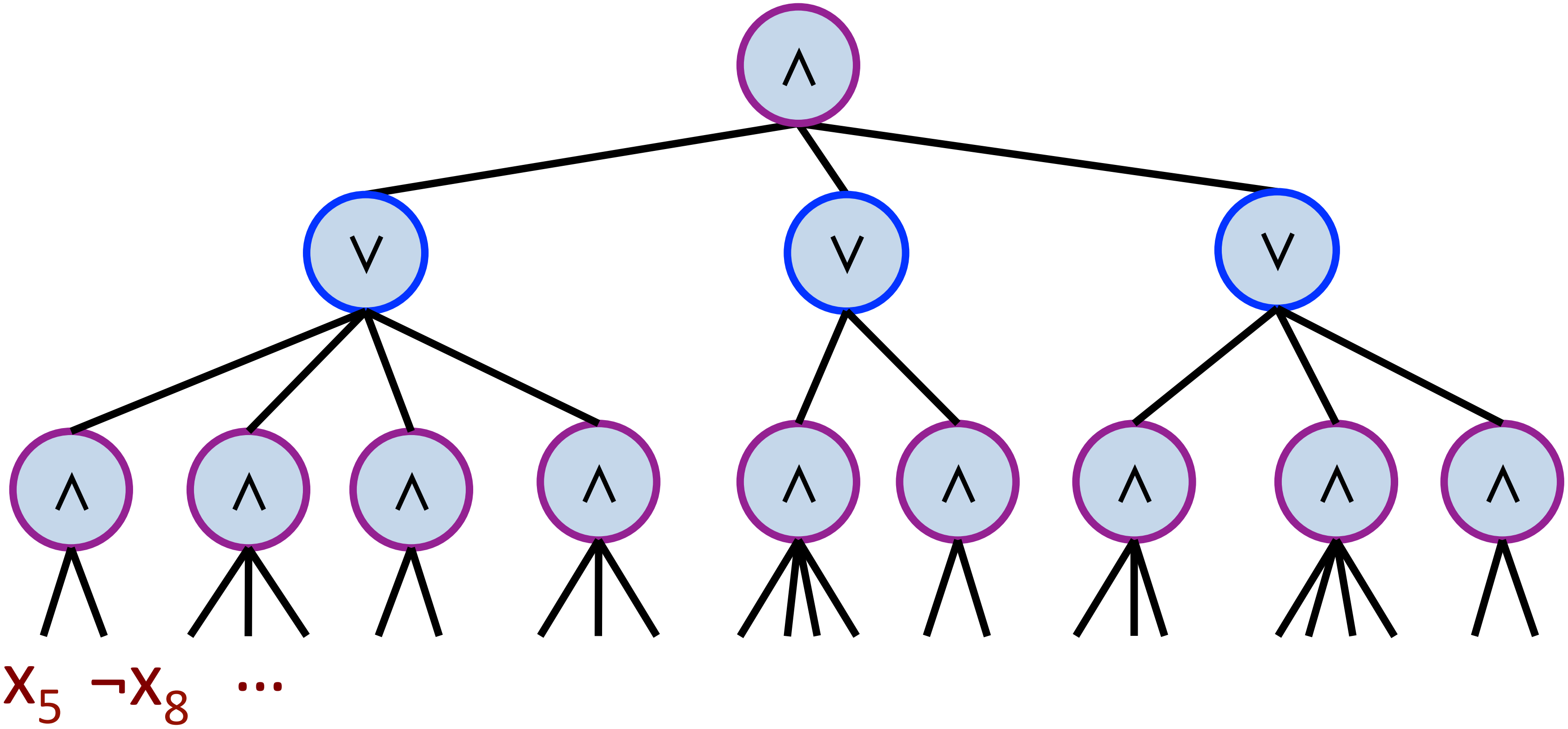
AC^0 Circuits


∧
∧
∧
∧
∧
∧
∨
∨
∨
∨
∨
∨
x_1 $\neg x_1$ x_2 $\neg x_2$ x_3 $\neg x_3$ x_4 $\neg x_4$ x_5 $\neg x_5$

depth is bounded by a constant d

(or slow-growing function d(n) << log n)

AC^0 Formulas



AC^0 Lower Bounds

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

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

AC^0 Lower Bounds

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

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

Switching Lemma

(simplification under p-random restrictions)

AC^0 Lower Bounds

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

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

The "size-depth tradeoff" is a limitation of lower bounds via Switching Lemmas (which become trivial before depth d = log n)

Lower Bound Techniques

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

Monotone Lower Bounds

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

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

Gate Elimination Arguments & Shrinkage

Restrictions

- Consider a Boolean function

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

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

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

Restrictions

- Consider a Boolean function

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

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

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

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

Restrictions

- Consider a Boolean function

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

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

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

- Applying R to f, we get a Boolean function

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

R		⋆	1	⋆	⋆	1	0	⋆	1	⋆	1	0	0	⋆	⋆	0	⋆	0	⋆	⋆	⋆	0	⋆	0	
$f\restriction R$	(	0		1	0			0		0				1	1		1		1	0	1		1		)
f	(	0	1	1	0	1	0	0	1	0	1	0	0	1	1	0	1	0	1	0	1	0	1	0	)

Restrictions

- Consider a Boolean function

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

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

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

- Applying R to f, we get a Boolean function

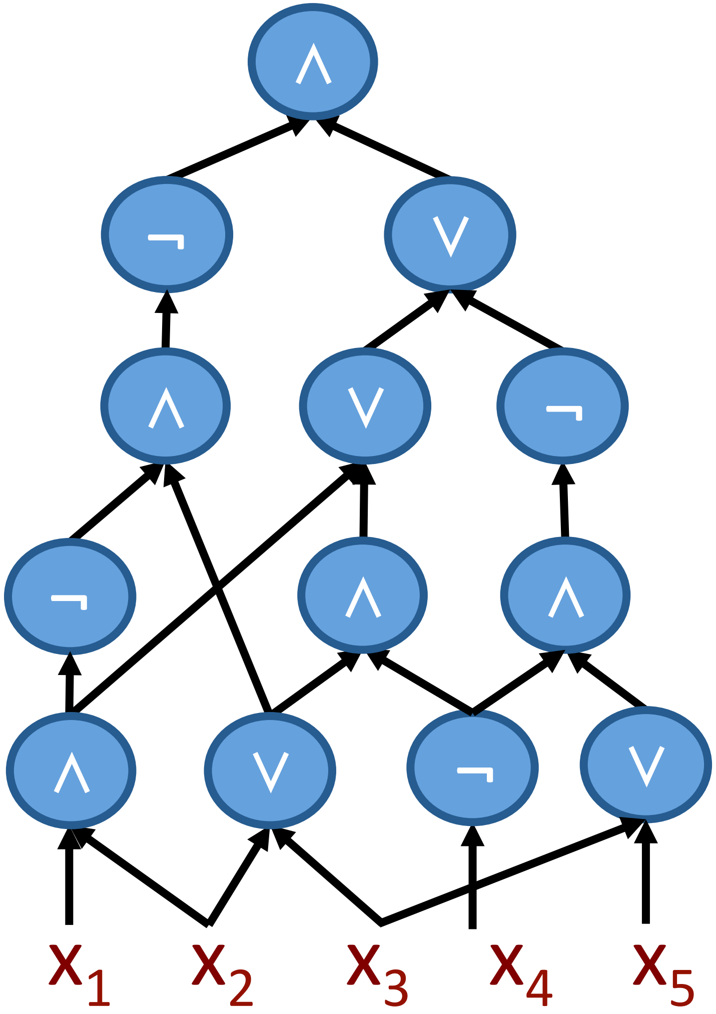
$$f \upharpoonright R : \{0,1\}^{\mathrm{Stars}(R)} \rightarrow \{0,1\}$$

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

Restricting a Circuit

- Consider the 1-bit restriction

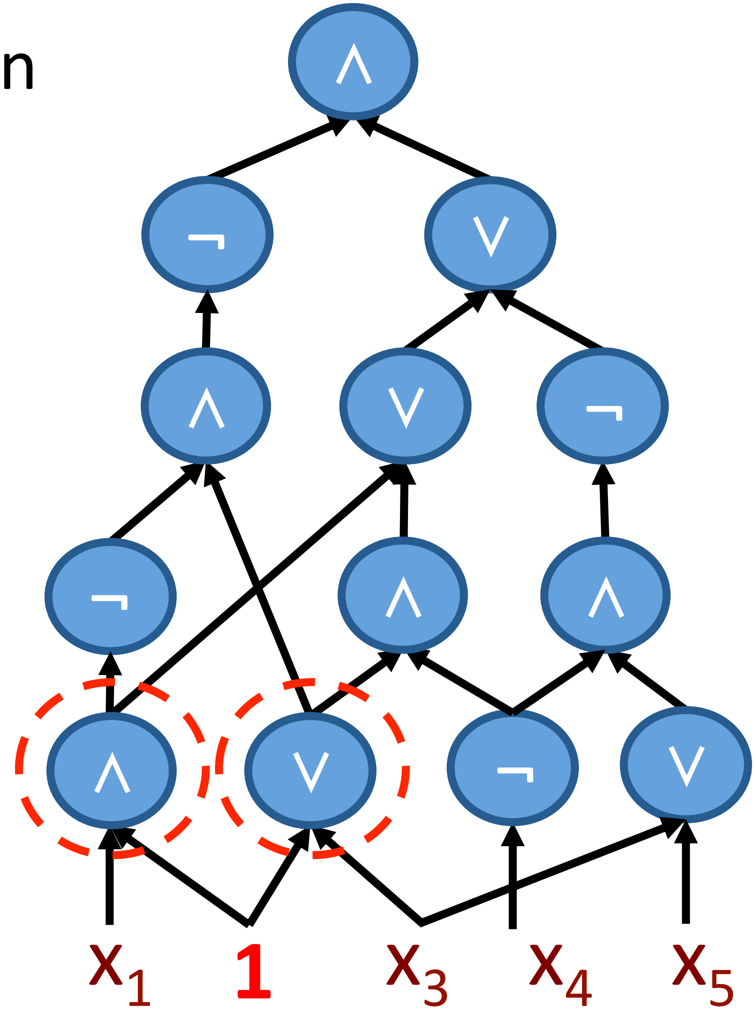
  $R = \{ x_2 \mapsto 1 \}$



Restricting a Circuit

- Consider the 1-bit restriction

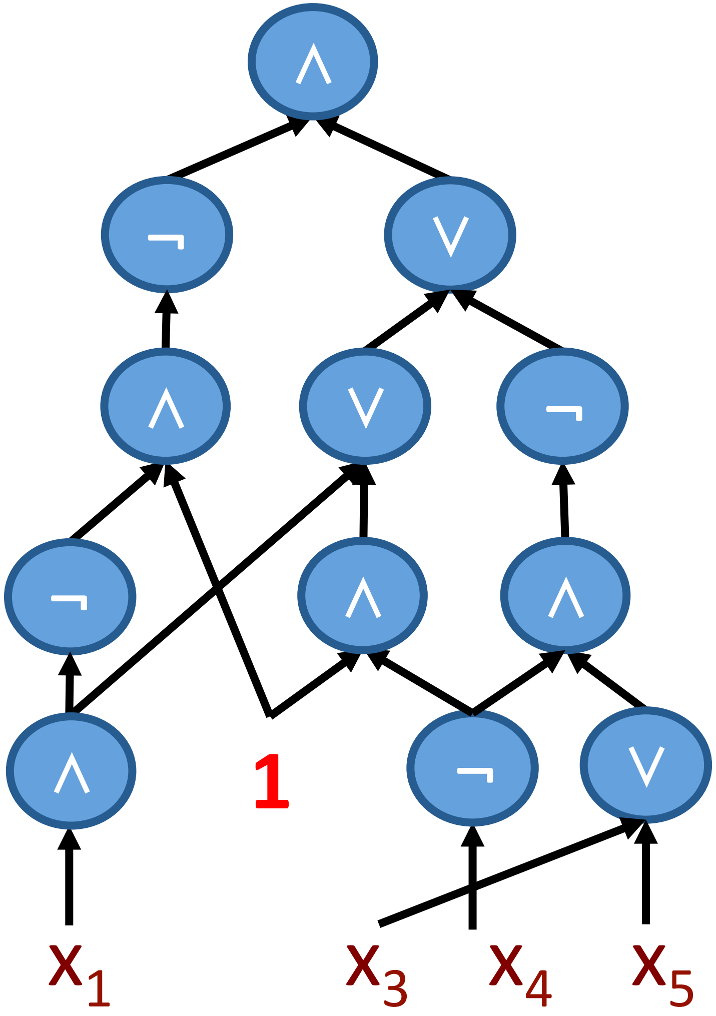
  $R = \{ x_2 \mapsto 1 \}$



Restricting a Circuit

- Consider the 1-bit restriction

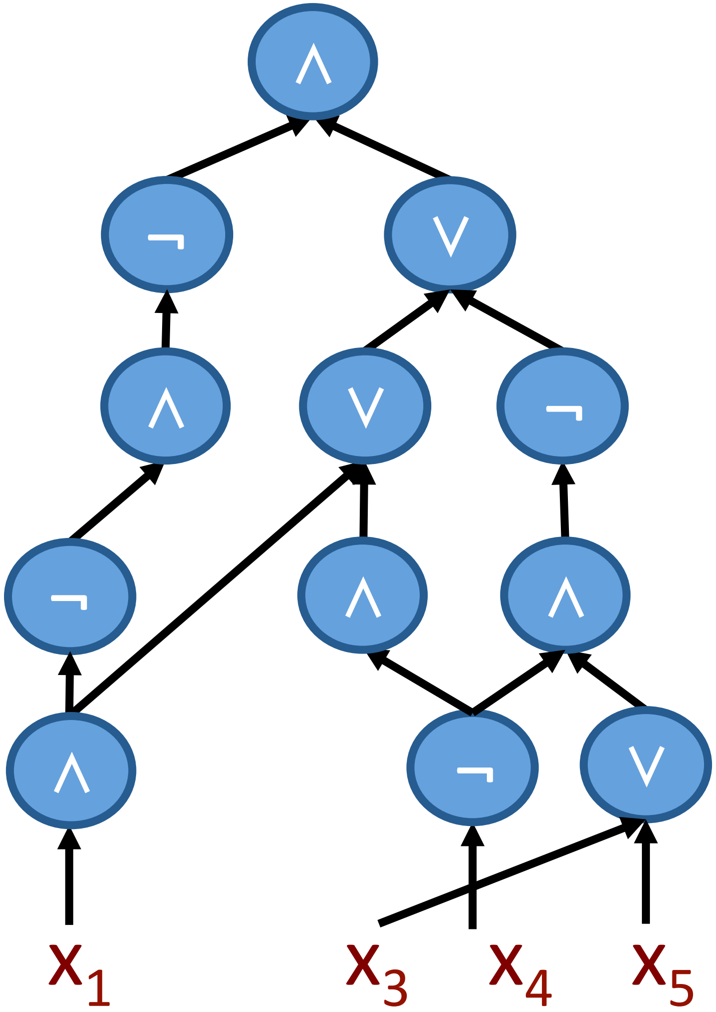
  $R = \{ x_2 \mapsto 1 \}$



Restricting a Circuit

- Consider the 1-bit restriction

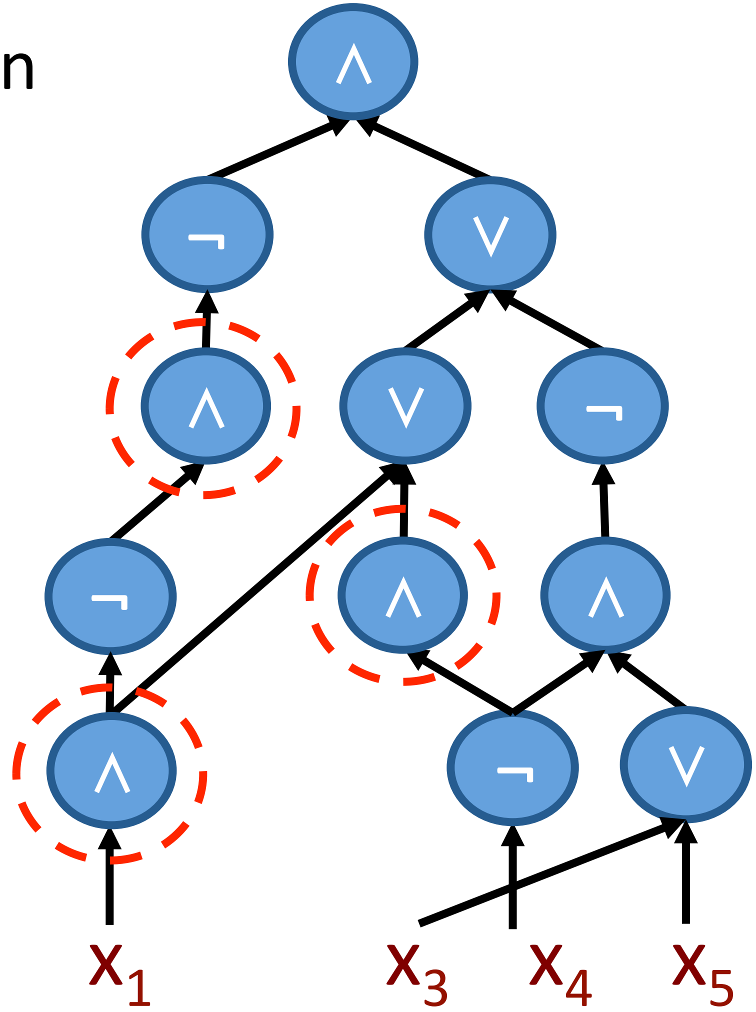
  $R = \{ x_2 \mapsto 1 \}$



Restricting a Circuit

- Consider the 1-bit restriction

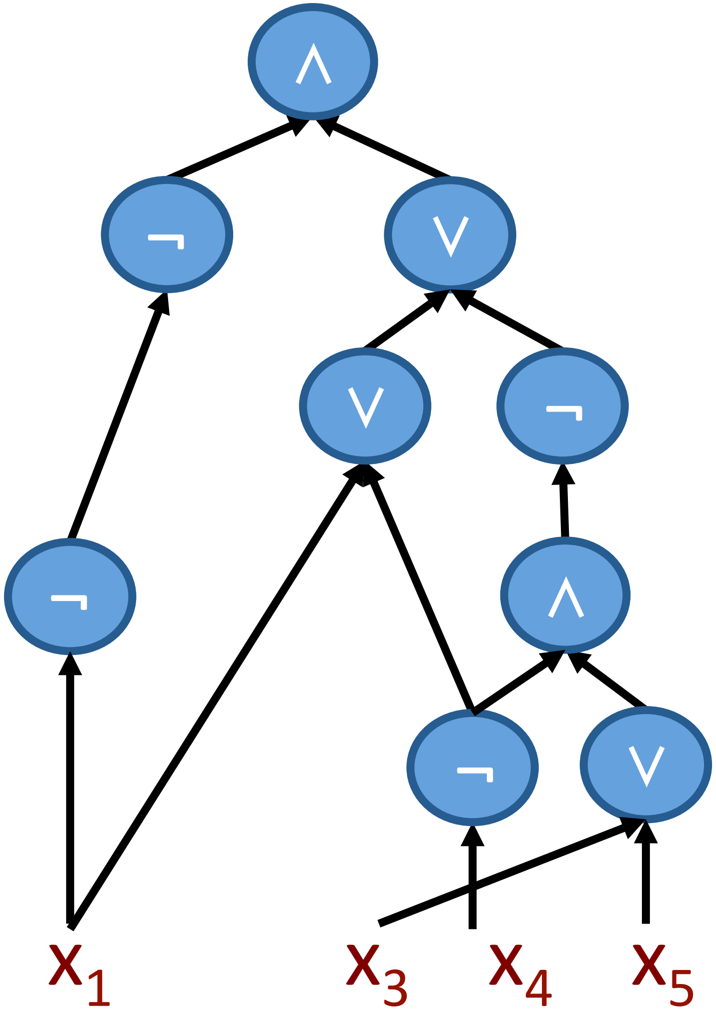
  $R = \{ x_2 \mapsto 1 \}$



Restricting a Circuit

- Consider the 1-bit restriction

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



Gate Elimination

- Lemma [Schnorr '76]

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

- Corollary

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

Gate Elimination

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

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

[Iwama-Lachish-Morizumi-Raz ‘02]

≈3.01n full binary basis

[Find-Golovnev-Hirsch-Kulikov ’16]

Gate Elimination

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

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

[Iwama-Lachish-Morizumi-Raz ‘02]

$\approx 3.01n$ full binary basis

[Find-Golovnev-Hirsch-Kulikov ’16]

uses affine restrictions

Gate Elimination

- Theorem [Chaudhuri-Radhakrishnan ’96]

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

- Theorem [Koppary-Srinivasan ’12]

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

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

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

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

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

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

- For $0 \le p \le 1$, let **R**

Convention:

Random objects written in **boldface**

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

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

Effect of $\mathbf{R}_p$

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

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

- Subbotovskaya '61

  If F is an n-variable DeMorgan formula, then

  $$\text{Ex}[\ \text{leafsize}(F \restriction \textbf{random 1-bit rest.})\ ]$$

  $$\leq (1-n)^{1.5}\ \text{leafsize}(F)$$

- As a consequence,

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

- Hastad '98, Tal '14

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

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

- Subbotovskaya '61

  If F is an n-variable DeMorgan formula, then

  $\mathrm{Ex}[\ \mathrm{leafsize}(F \upharpoonright \textbf{random 1-bit rest.})\ ]$

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

- Hastad '98, Tal '14

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

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

- Implies lower bounds:

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

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

- Hastad '98, Tal '14

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

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

- Implies lower bounds:

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

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

current frontier

- <u>Hastad '98, Tal '14</u>

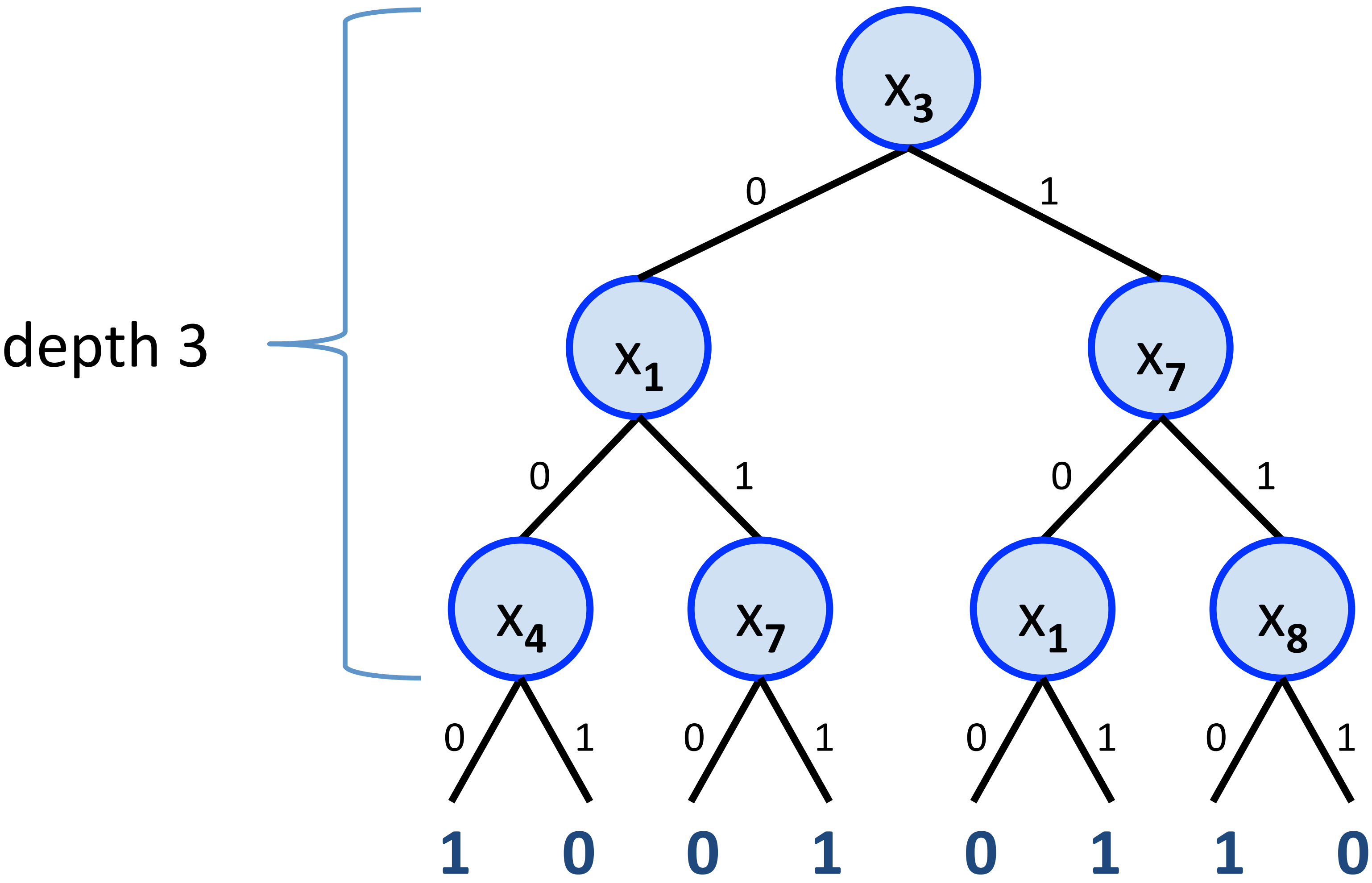
$$\text{Ex}[\ \text{leafsize}(F \restriction \mathbf{R}_p)\ ] \leq O(p^2\,\text{leafsize}(F) + 1)$$

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

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

The Switching Lemma

Decision Trees



Decision Trees

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

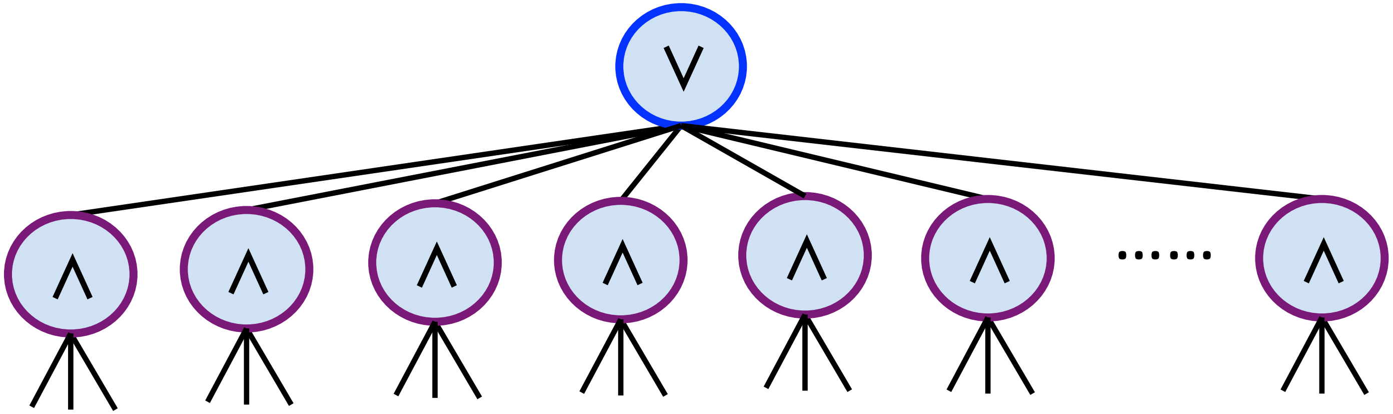
$$f : \{0,1\}^n \rightarrow \{0,1\}$$

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

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

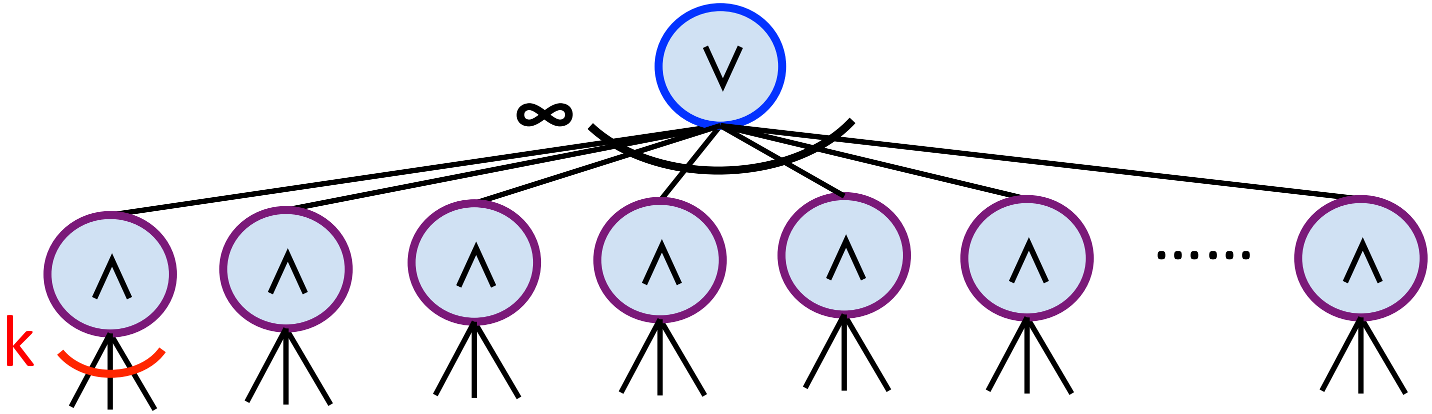
Depth-2 Formulas (DNFs and CNFs)

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



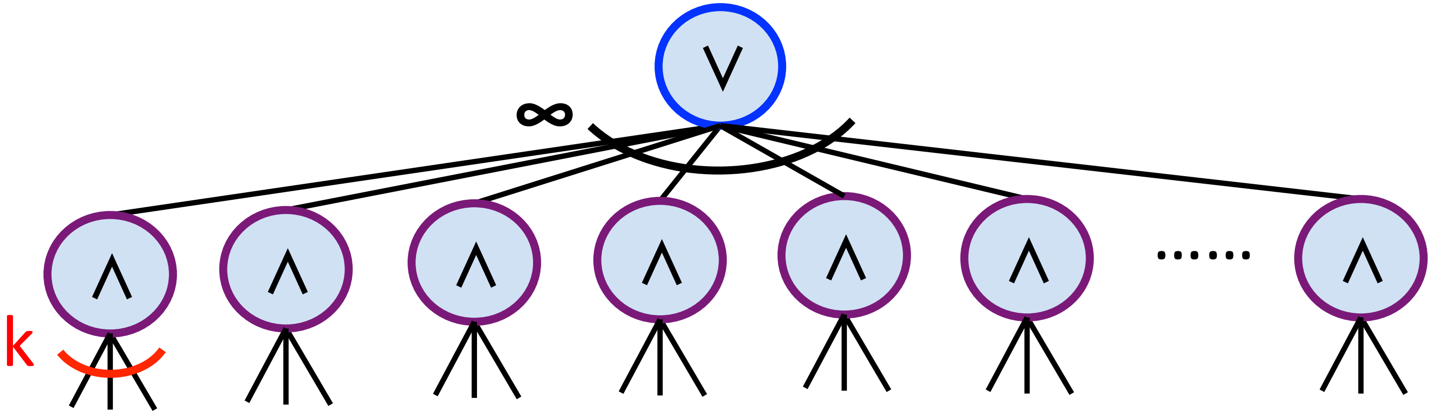
Depth-2 Formulas (DNFs and CNFs)

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



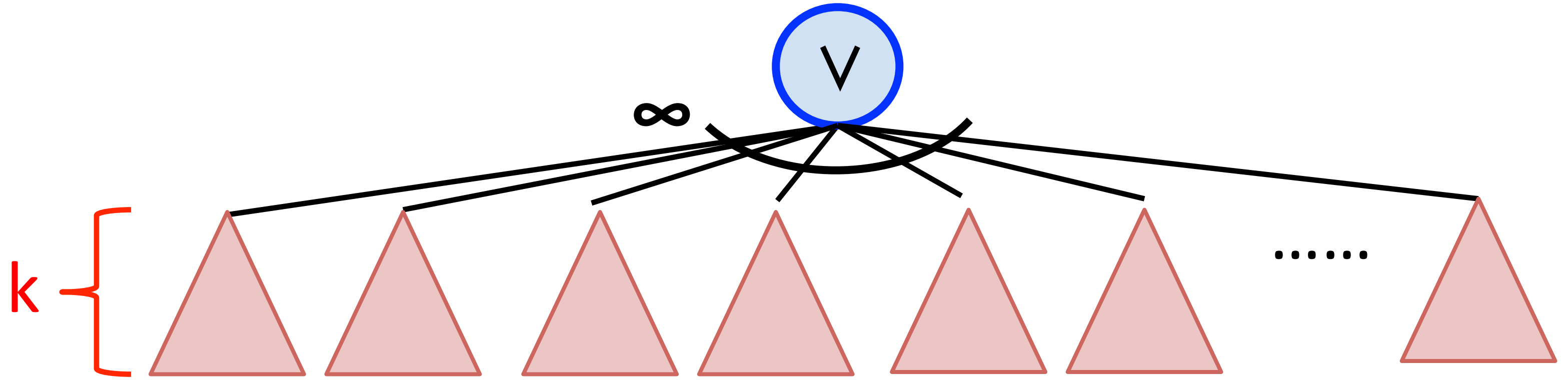
Depth-2 Formulas (DNFs and CNFs)

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



Depth-2 Formulas (DNFs and CNFs)

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



Depth-2 Formulas (DNFs and CNFs)

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

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

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

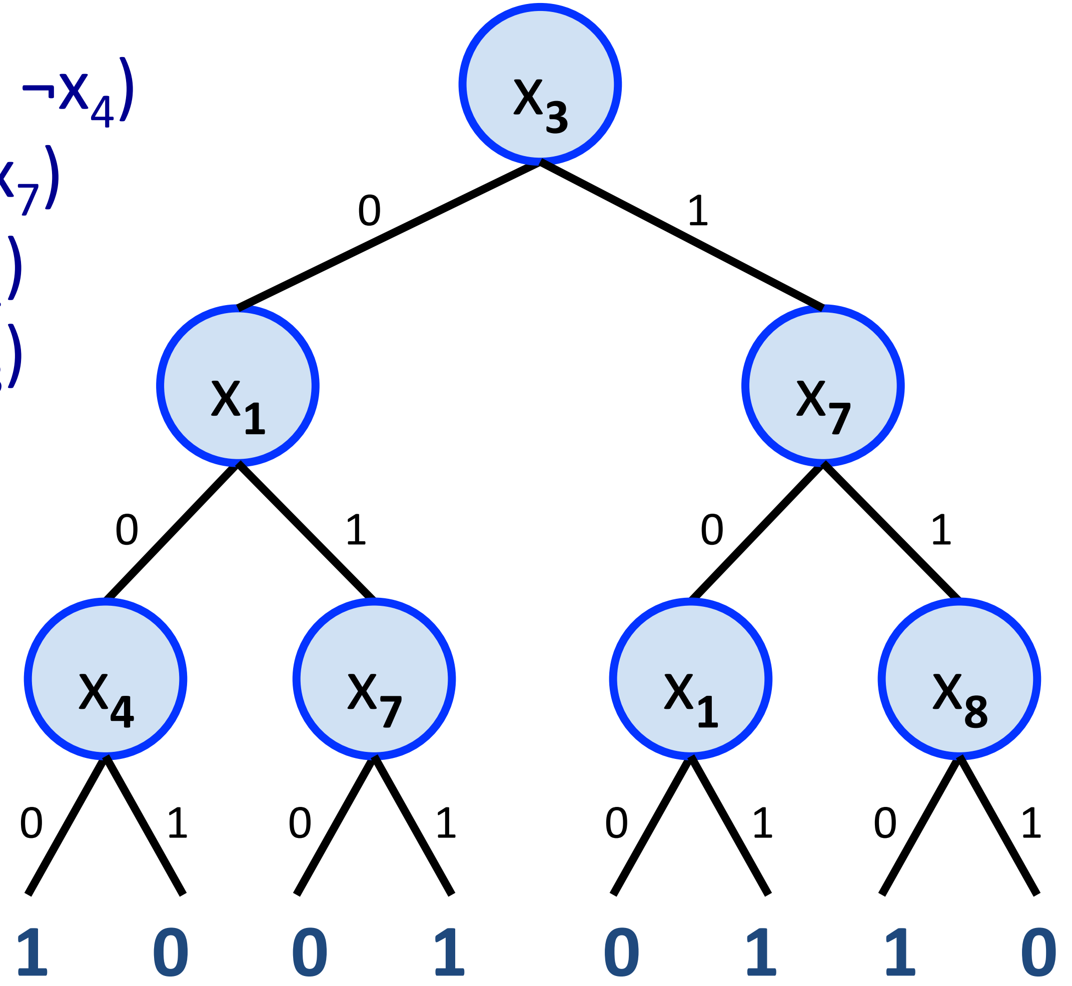
Decision Tree to DNF

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

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

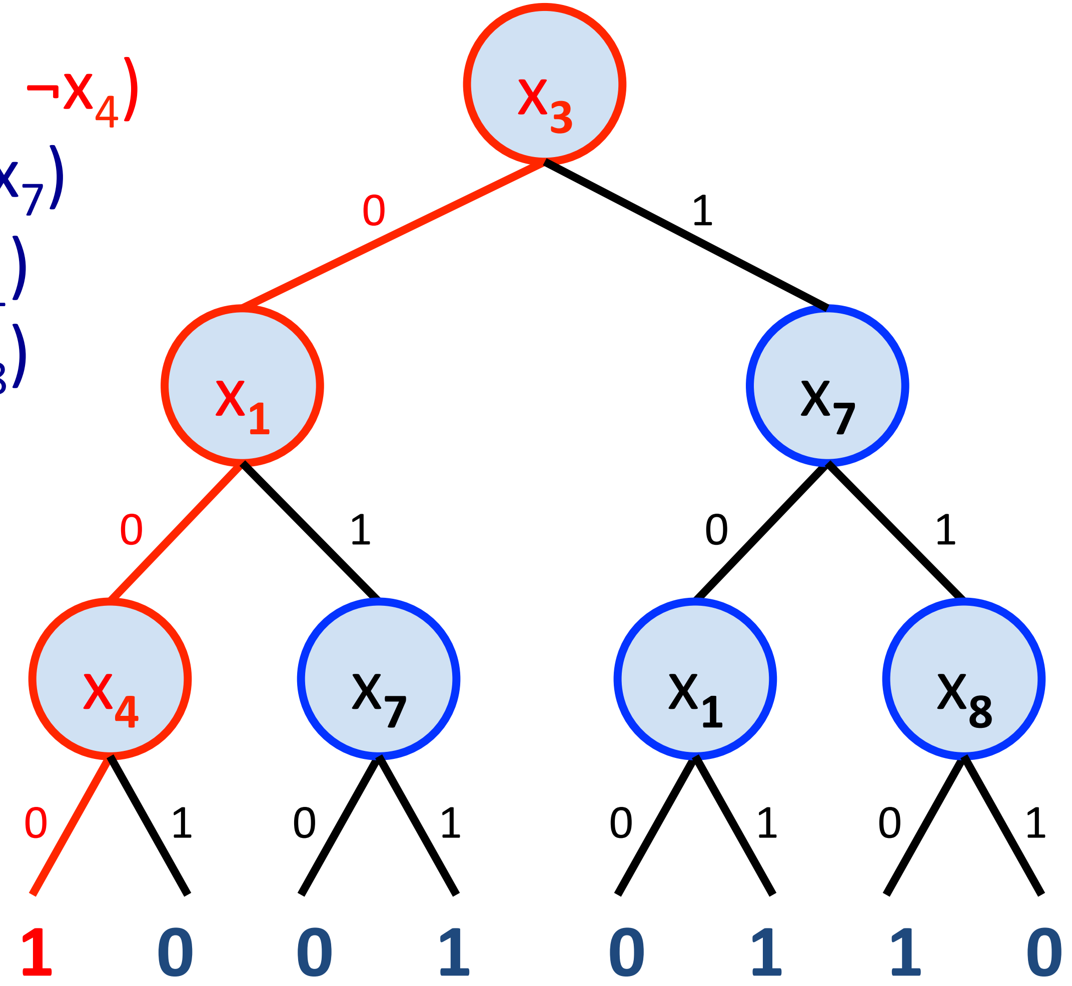
$\vee\ (x_3 \wedge x_7 \wedge x_1)$

$\vee\ (x_3 \wedge x_7 \wedge x_8)$



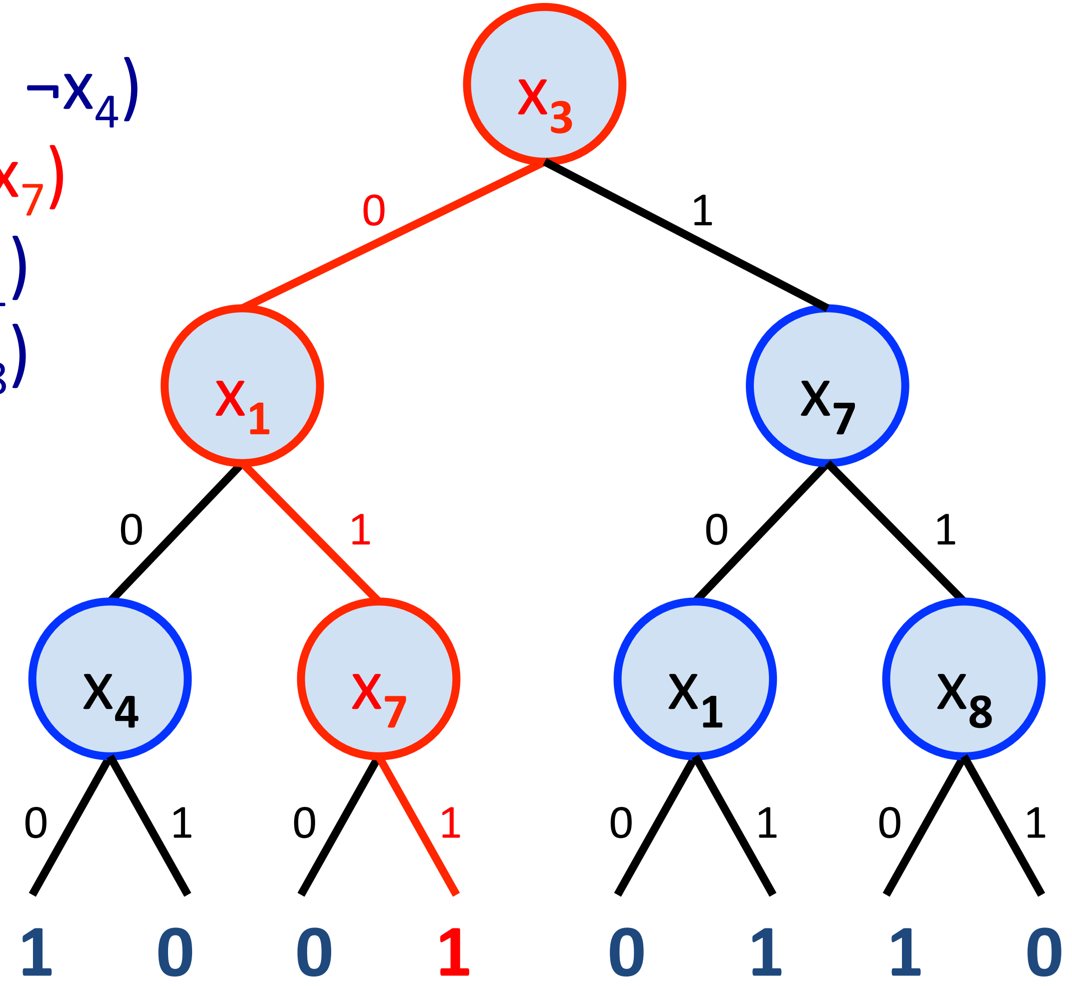
Decision Tree to DNF

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



Decision Tree to DNF

$$
\begin{aligned}
&(\neg x_3 \wedge \neg x_1 \wedge \neg x_4)\\
\vee\ &(\neg x_3 \wedge x_1 \wedge x_7)\\
\vee\ &(x_3 \wedge x_7 \wedge x_1)\\
\vee\ &(x_3 \wedge x_7 \wedge x_8)
\end{aligned}
$$



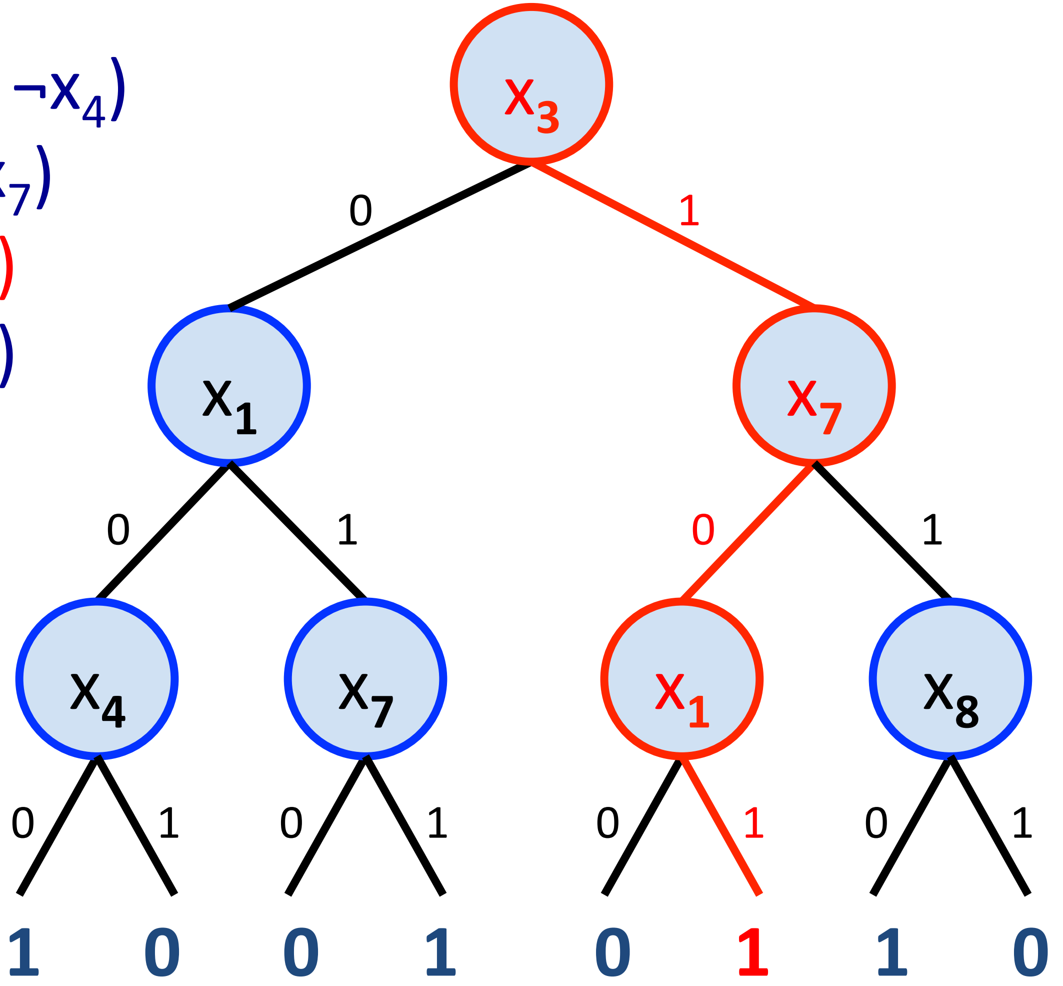
Decision Tree to DNF

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

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

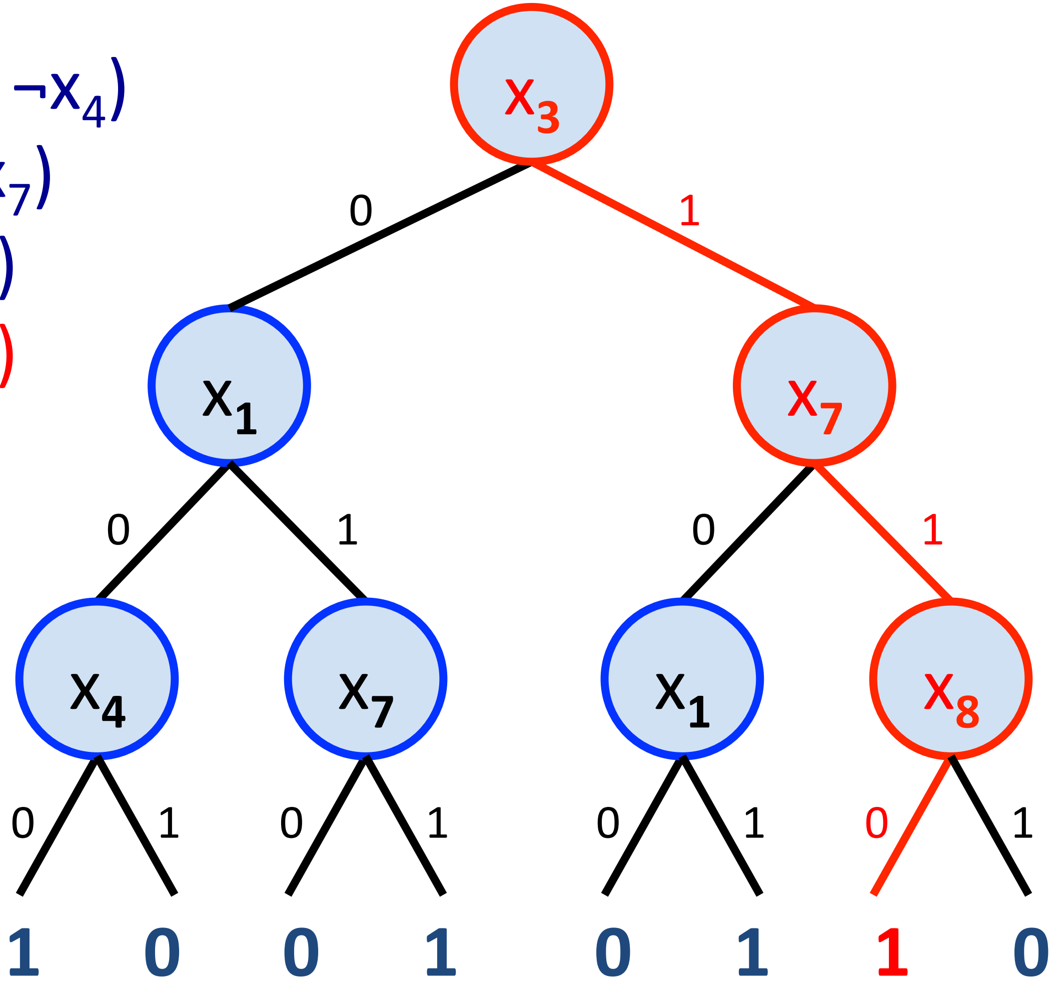
$\vee\ (x_3 \wedge x_7 \wedge x_1)$

$\vee\ (x_3 \wedge x_7 \wedge x_8)$



Decision Tree to DNF

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



k-DNF Switching Lemma

Hastad's Switching Lemma (1986)

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

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

k-DNF Switching Lemma

Hastad's Switching Lemma (1986)

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

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

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

k-DNF Switching Lemma

Hastad's Switching Lemma (1986)

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

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

Dual CNF version

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

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

k-DNF Switching Lemma

Hastad's Switching Lemma (1986)

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

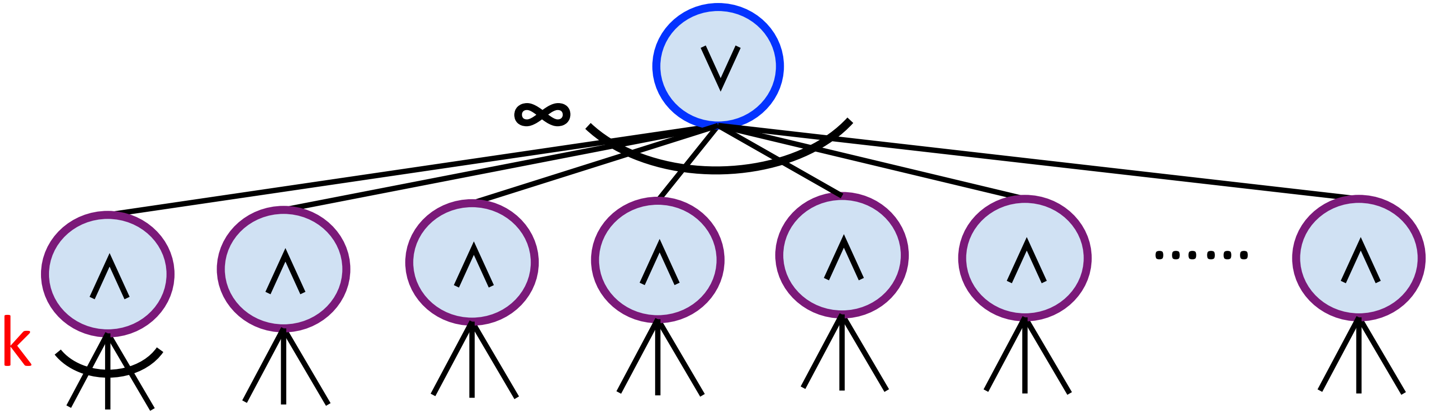
$$\Pr[\ \mathrm{DT}_{\mathrm{depth}}(F \restriction \mathbf{R}_p) \geq t\ ] \leq (5pk)^t$$

Corollary (usual statement of the S.L.)

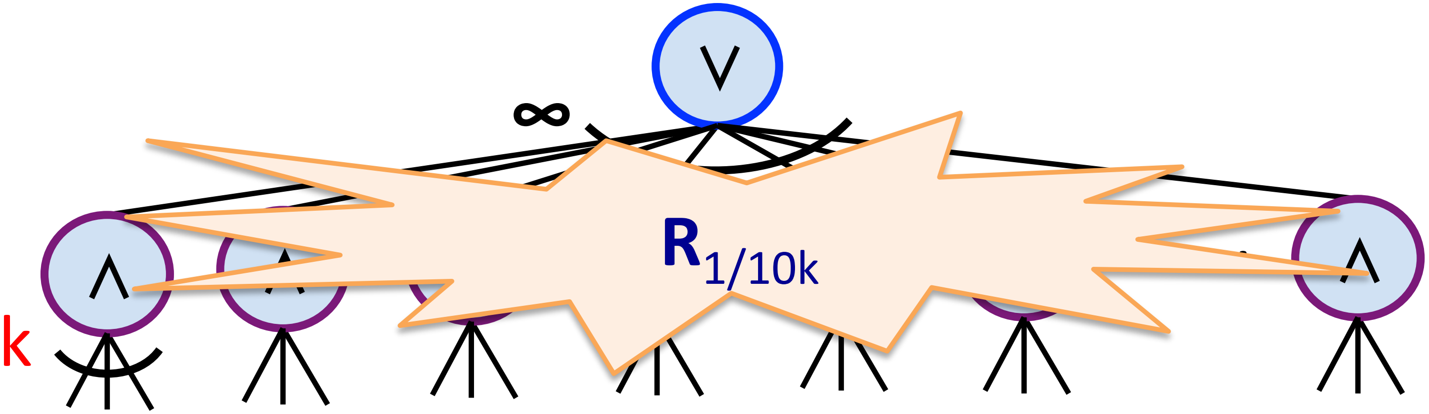
If F is a k-DNF, then

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

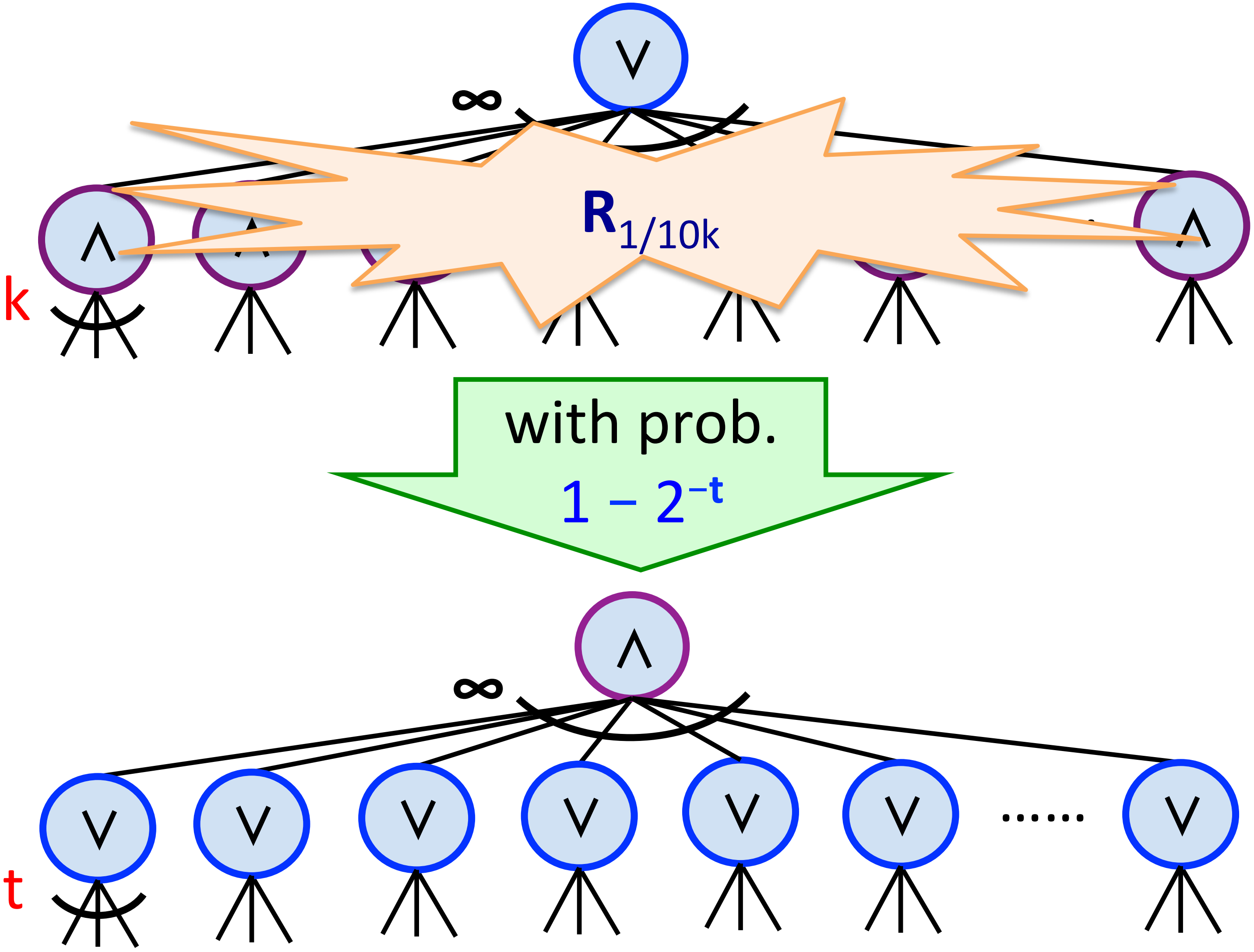
k-DNF Switching Lemma



k-DNF Switching Lemma



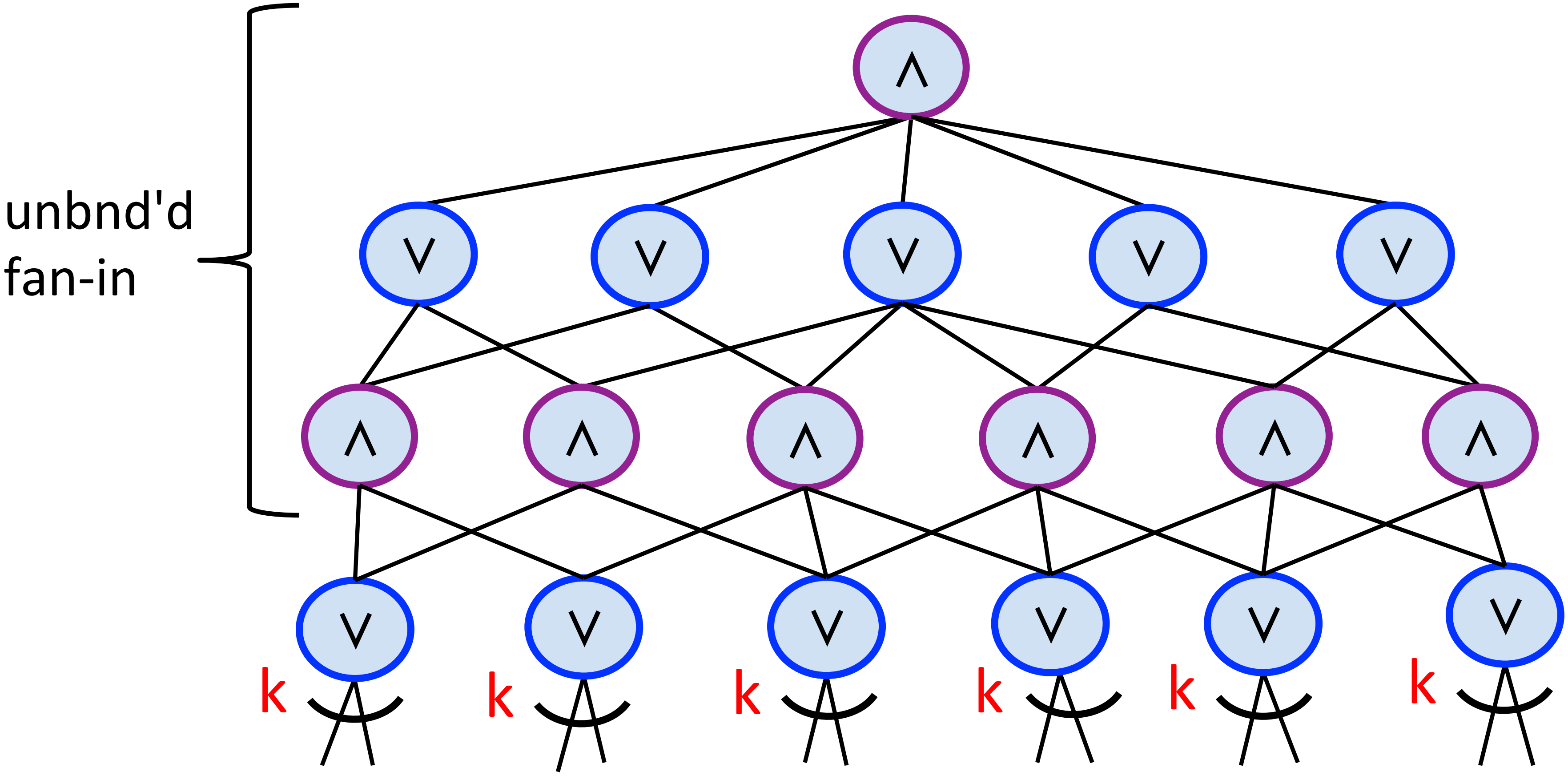
k-DNF Switching Lemma



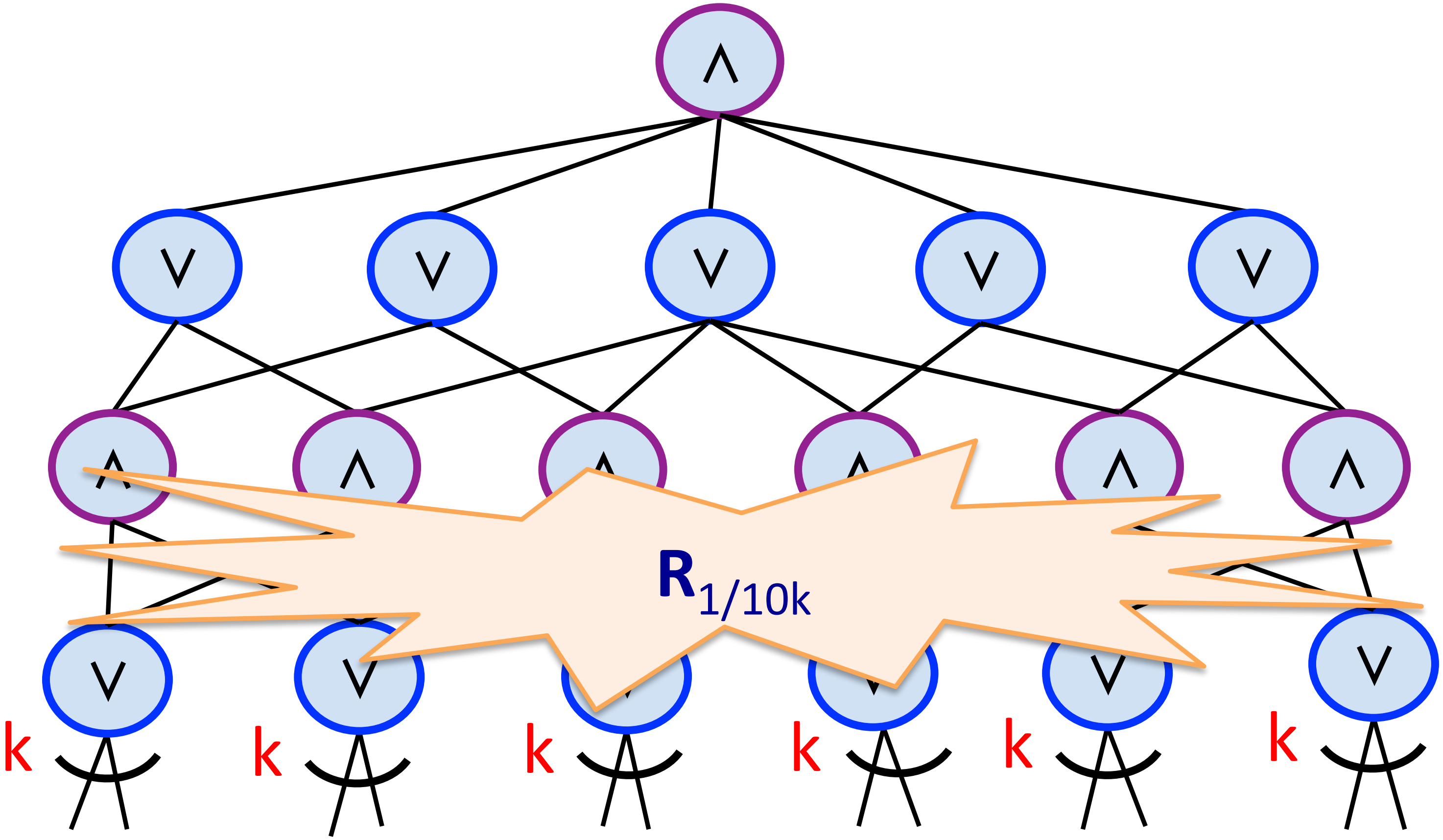
with prob.

$1 - 2^{-t}$

Depth Reduction

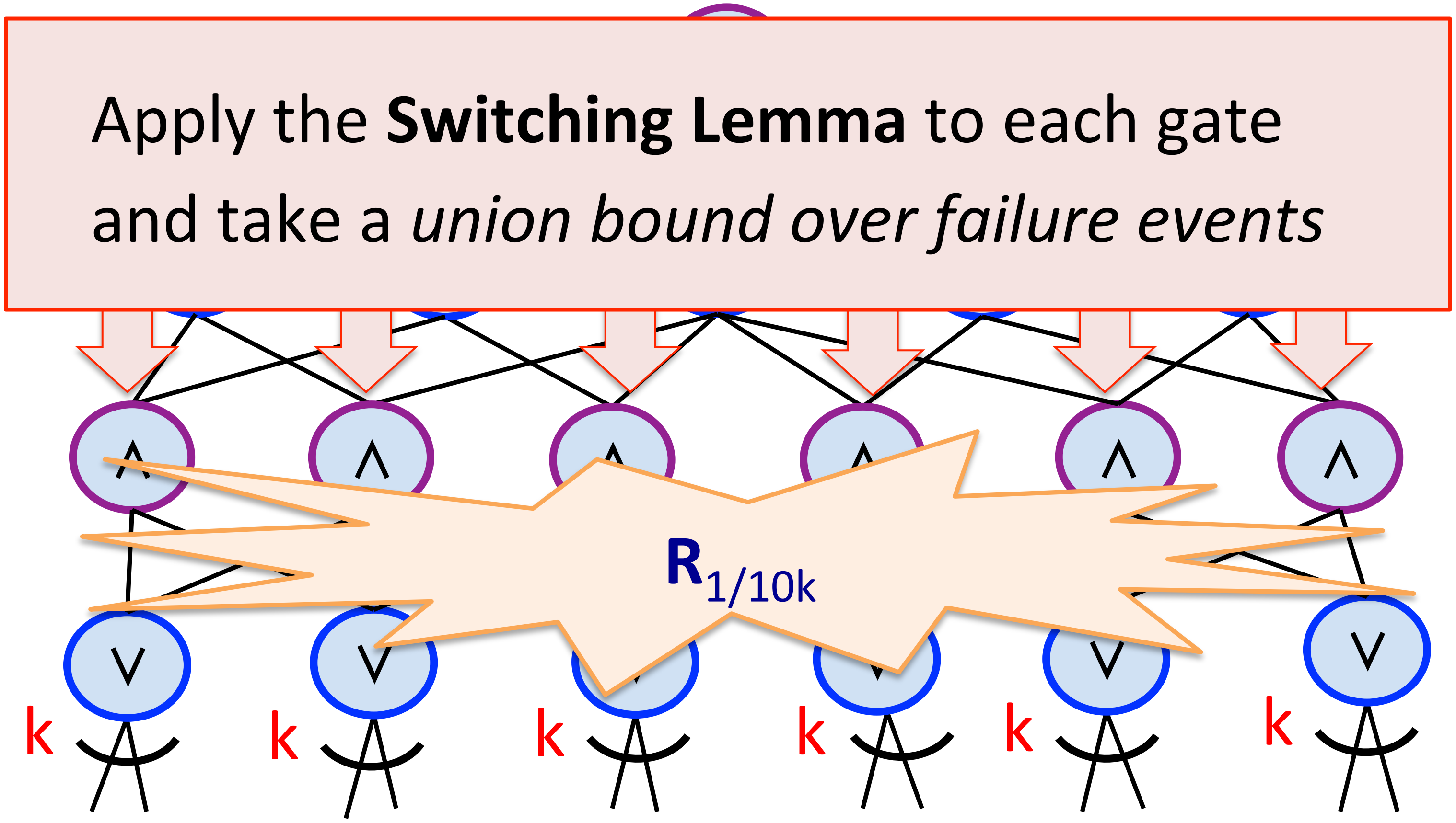


Depth Reduction



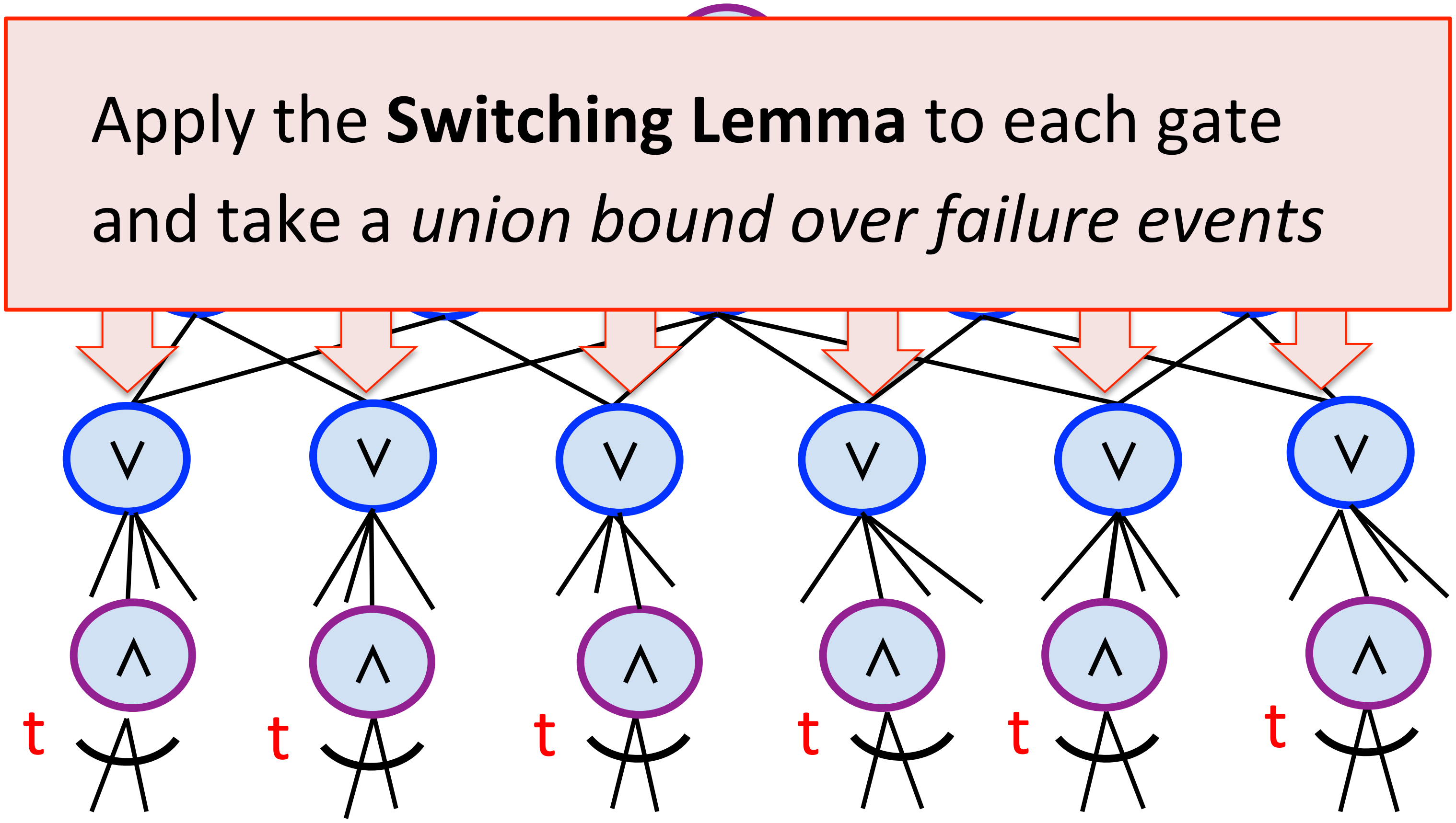
Depth Reduction

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

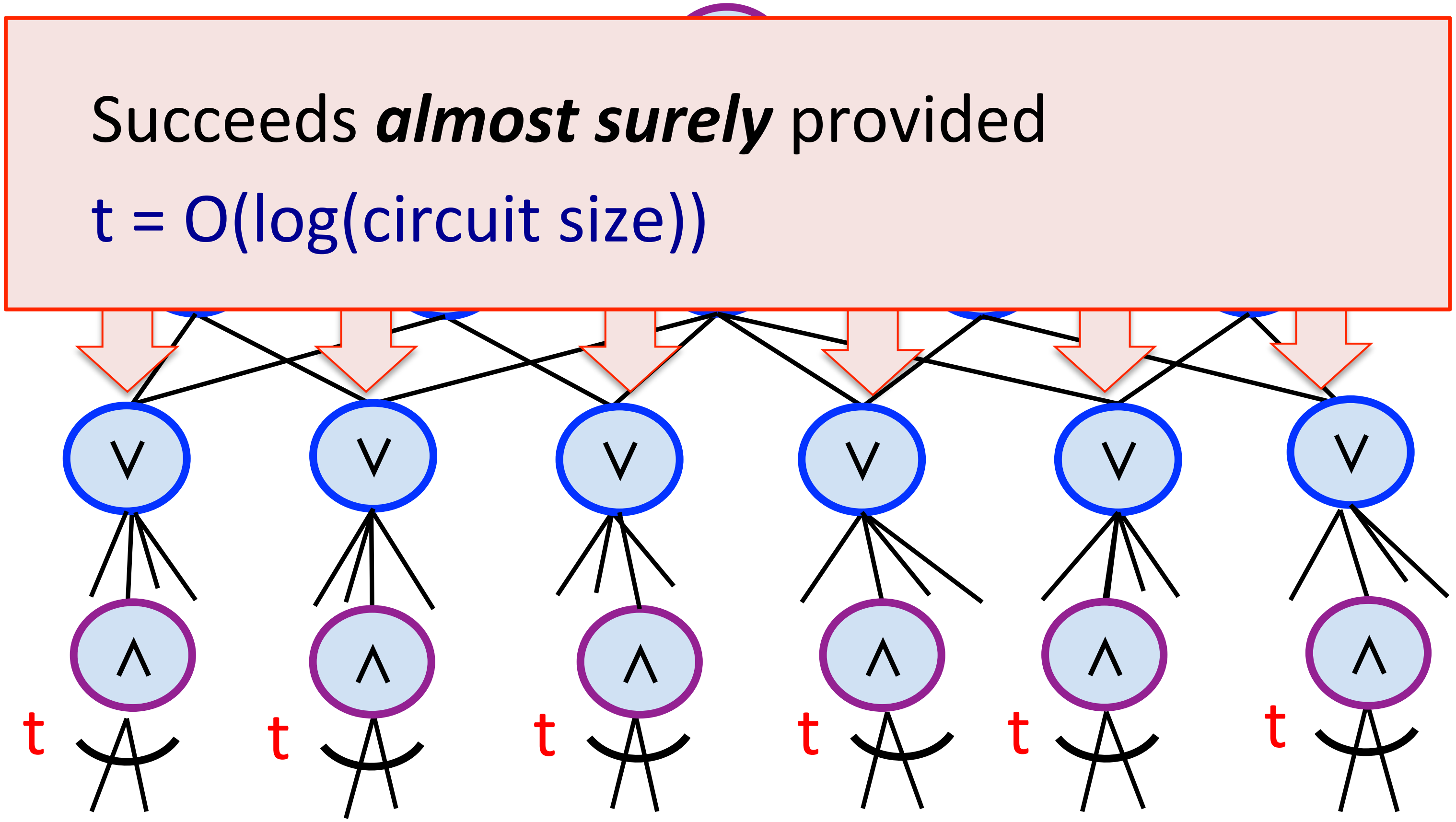


Depth Reduction

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



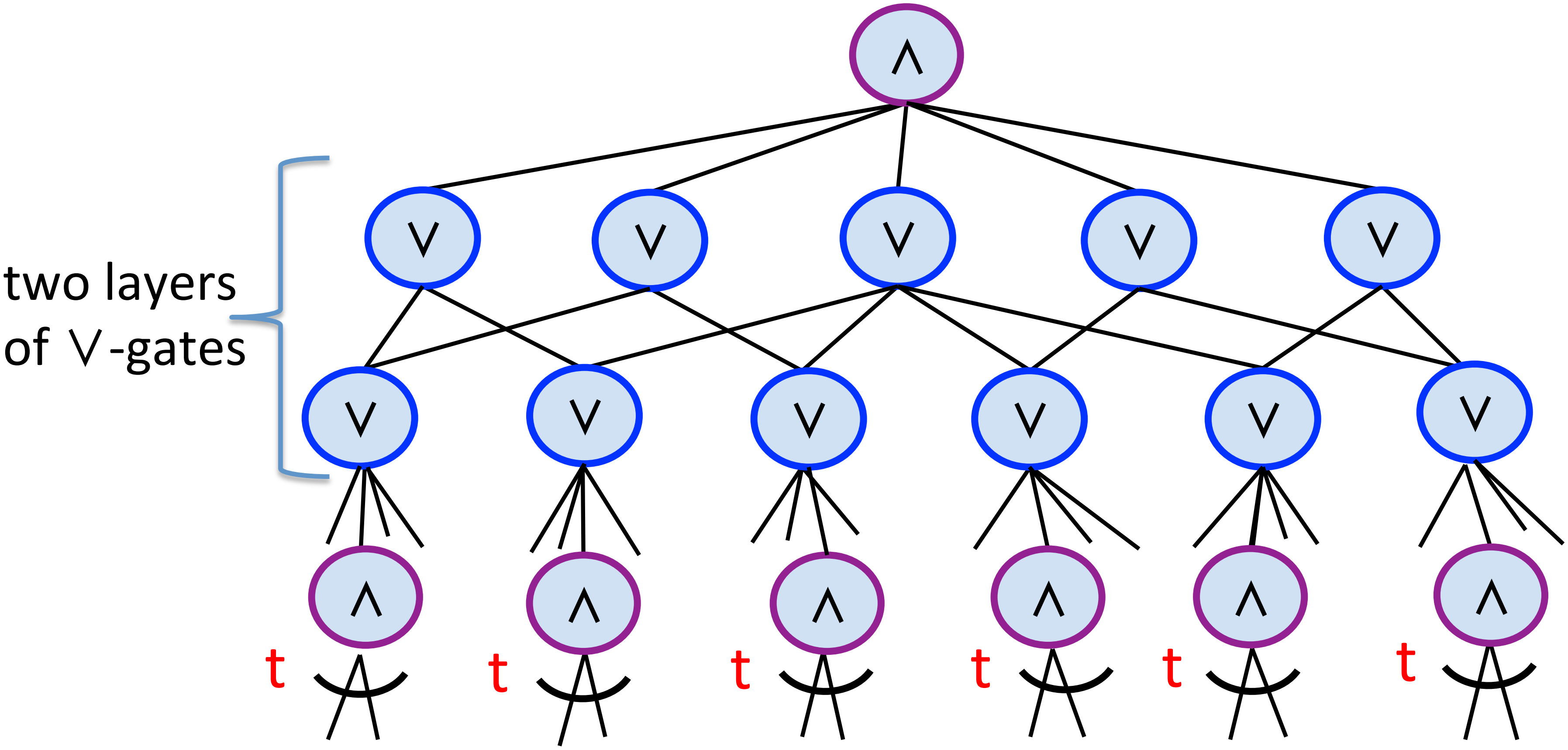
Depth Reduction



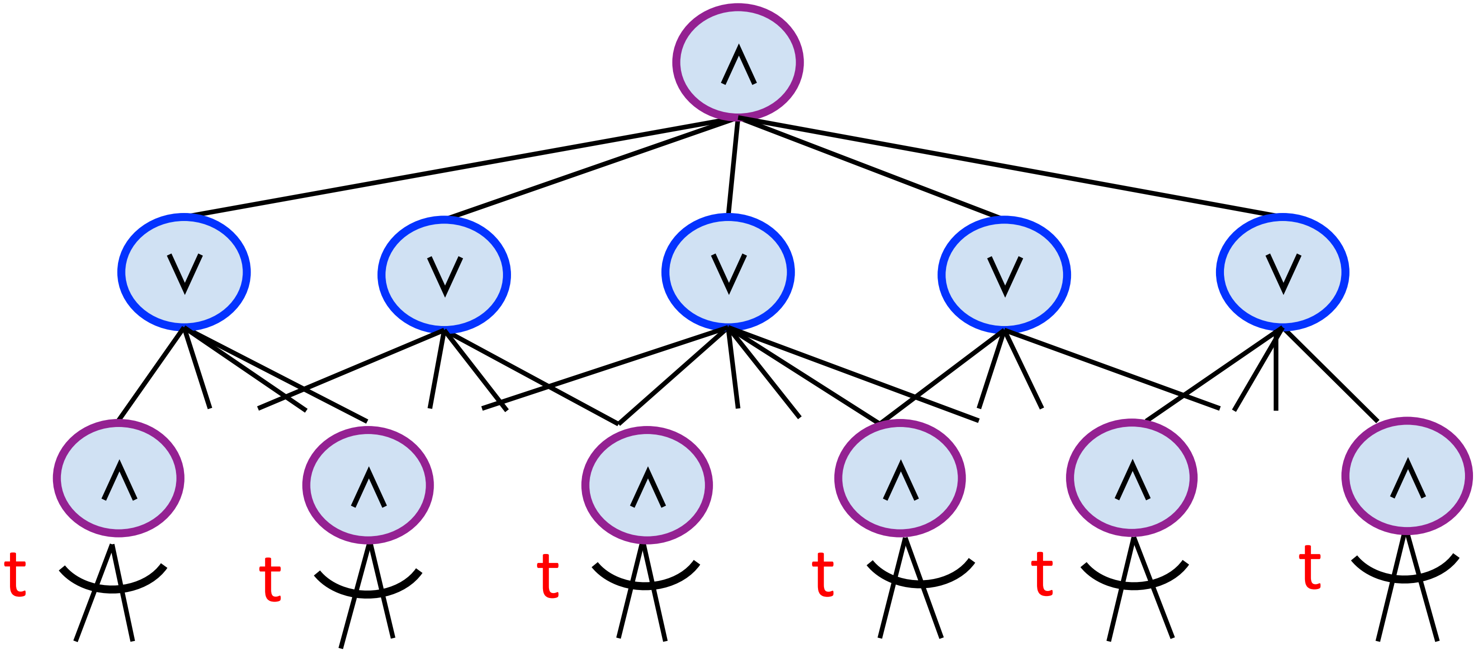
Succeeds ***almost surely*** provided

t = O(log(circuit size))

Depth Reduction



Depth Reduction



PARITY Lower Bound

Theorem [Hastad ’86]

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

Matching Upper Bound

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

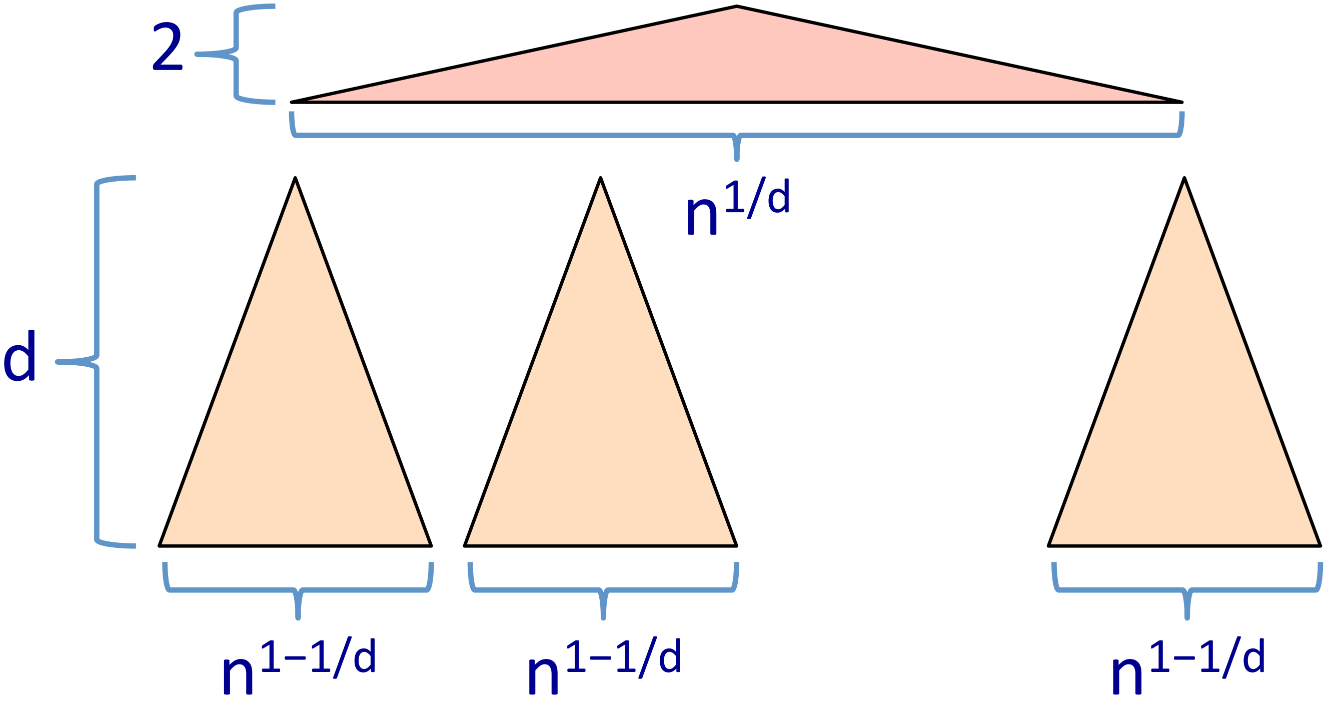
Theorem [Hastad '86]

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

Matching Upper Bound

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

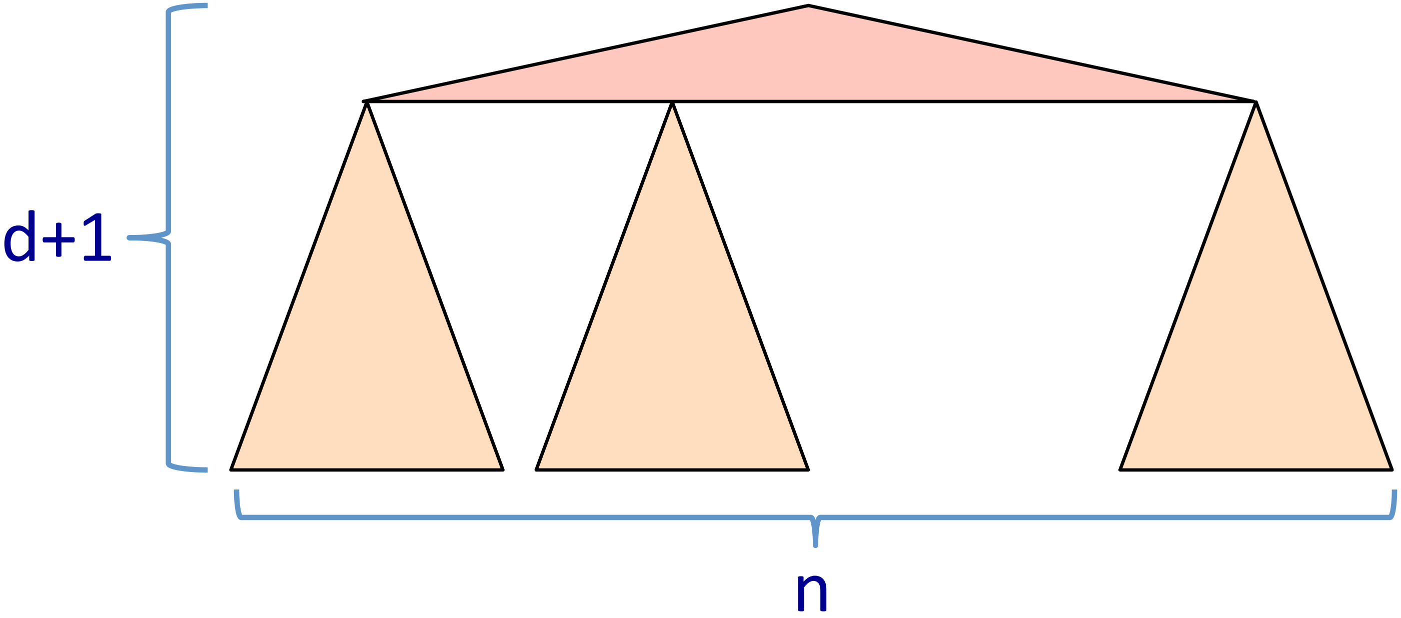
- depth 2 circuits of size $O(2^n)$ (brute-force CNF/DNF)
- for $d+1 \geq 3$, divide and conquer:



Matching Upper Bound

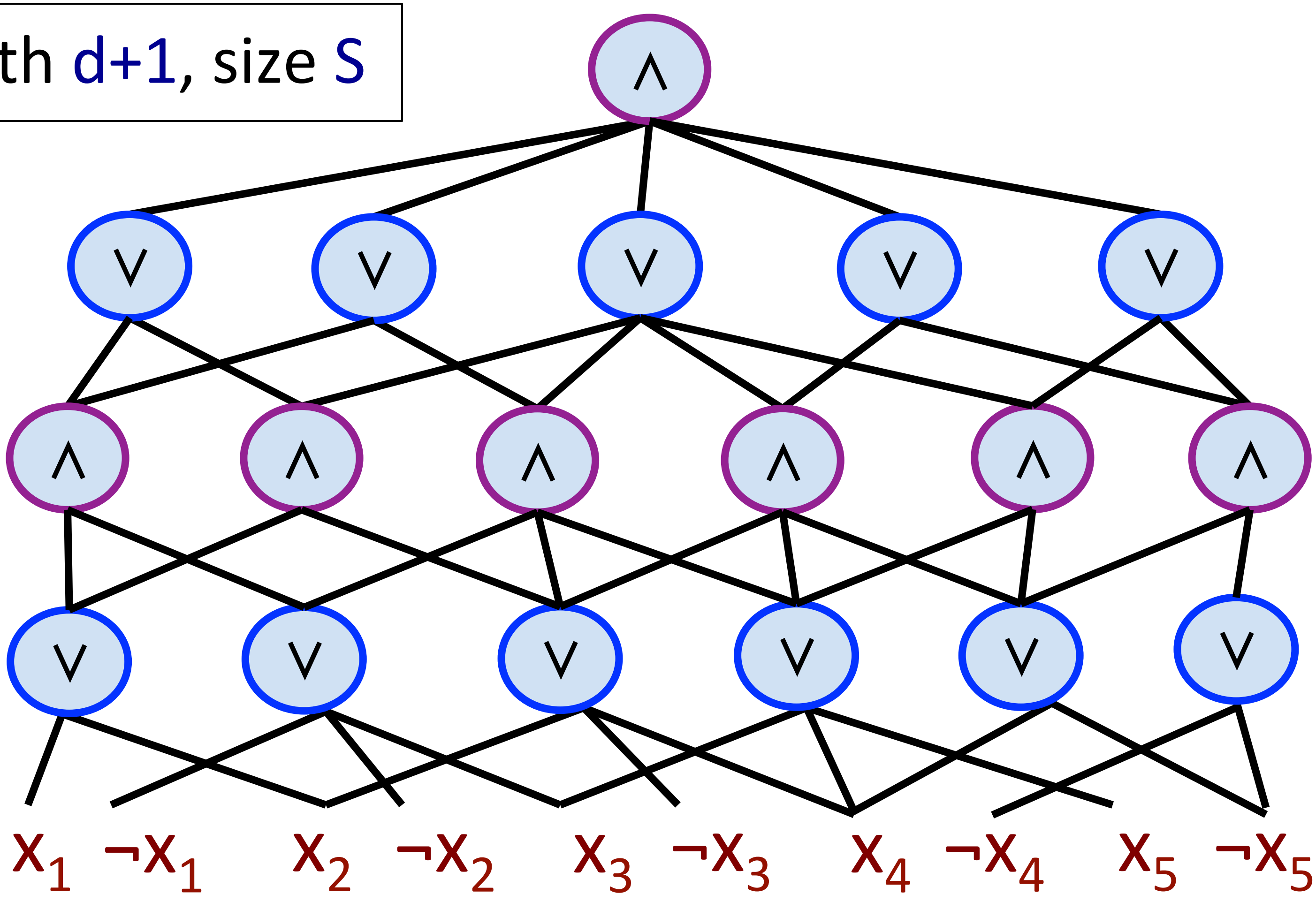
PARITY_n has depth $d+1$ **circuits** of size $\exp(O(n^{1/d}))$

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

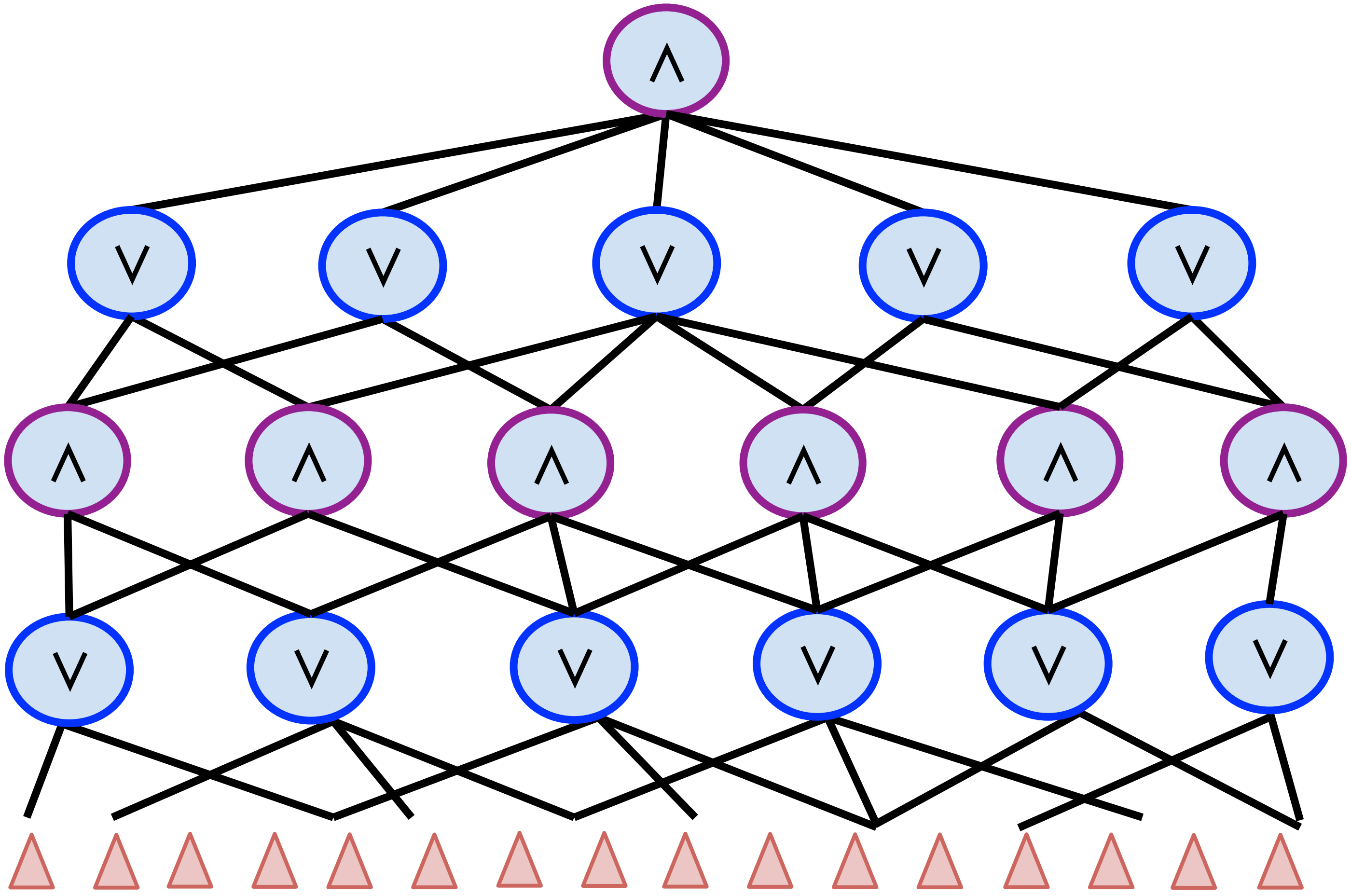


PARITY Lower Bound

depth d+1, size S

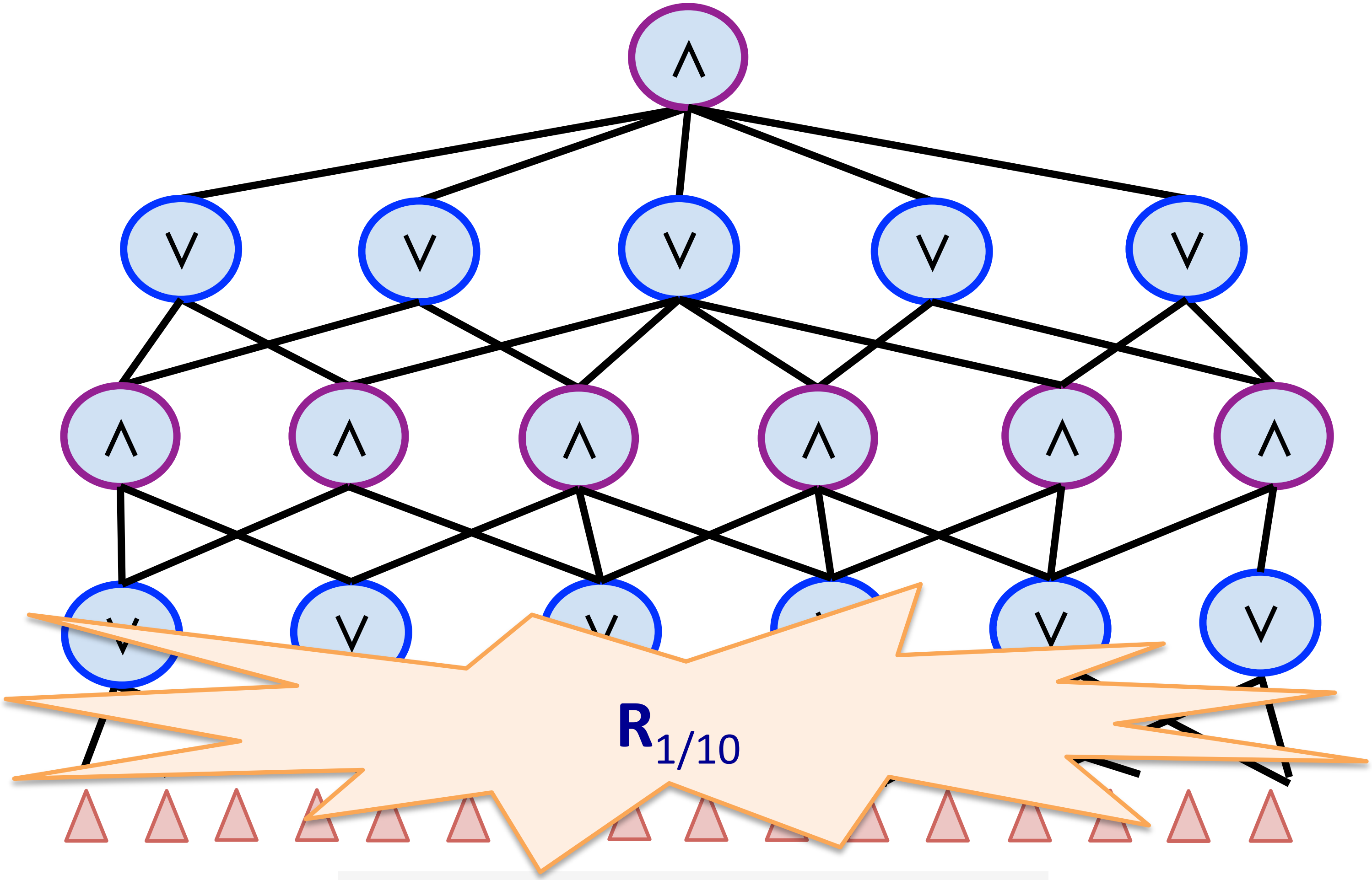

∧
∨
∨
∨
∨
∨
∧
∧
∧
∧
∧
∧
∨
∨
∨
∨
∨
∨
x_1 $\neg x_1$ x_2 $\neg x_2$ x_3 $\neg x_3$ x_4 $\neg x_4$ x_5 $\neg x_5$

PARITY Lower Bound



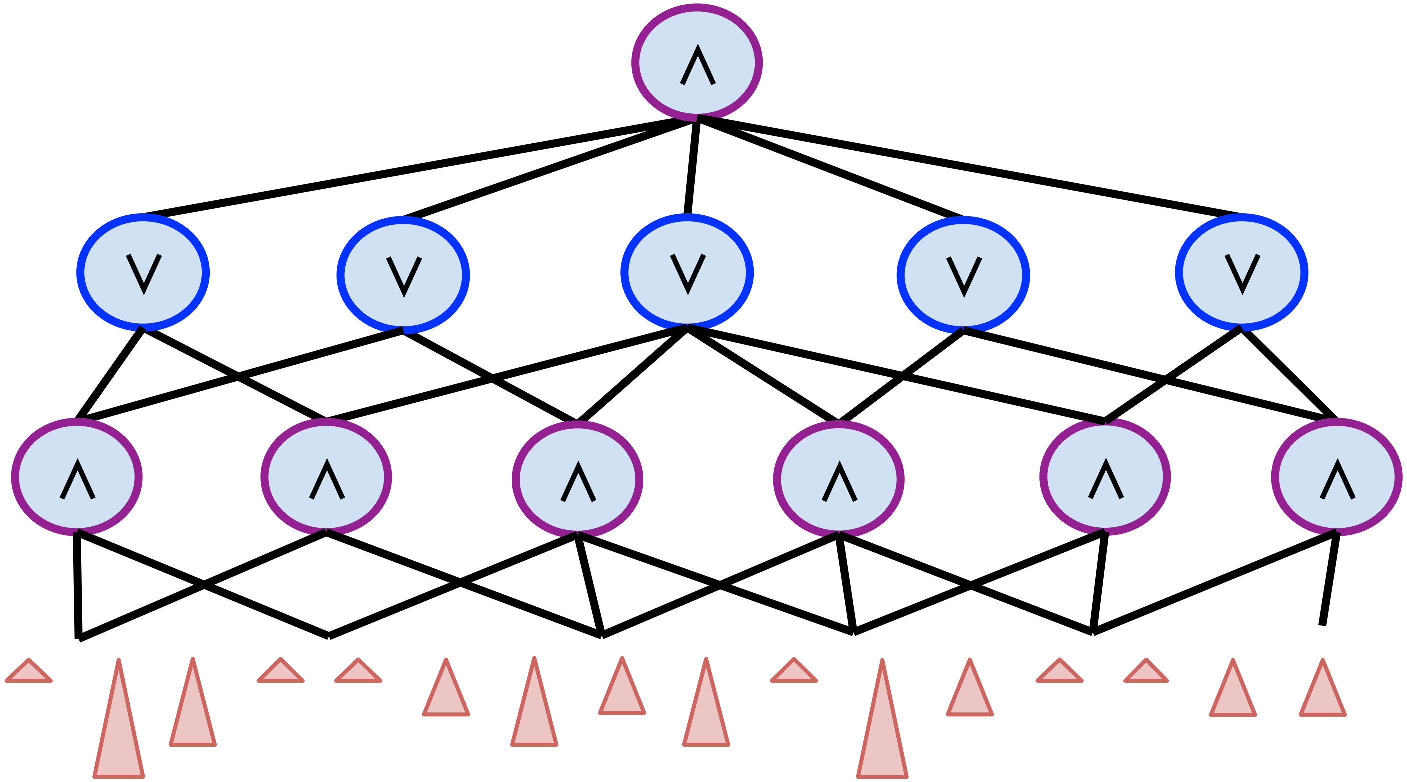
depth-1 decision trees

PARITY Lower Bound



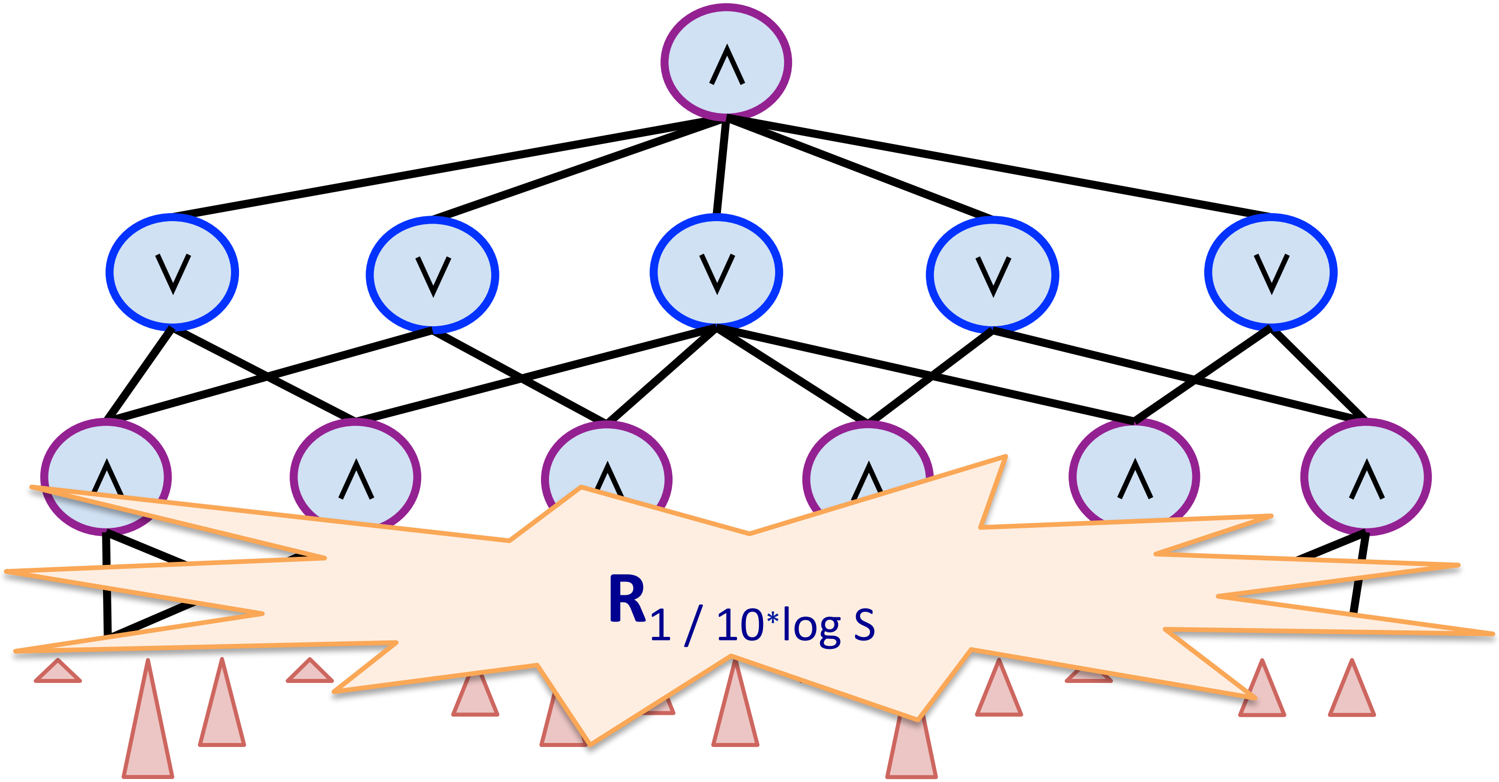
depth-1 decision trees

PARITY Lower Bound



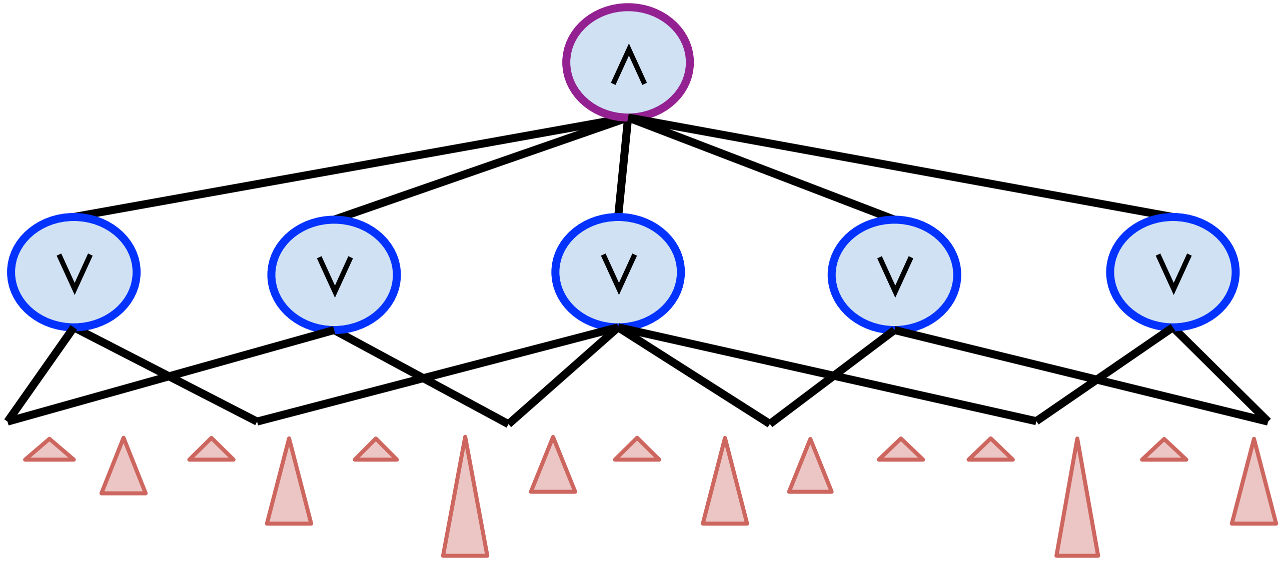
depth O(log S) decision trees (w.h.p.)

PARITY Lower Bound



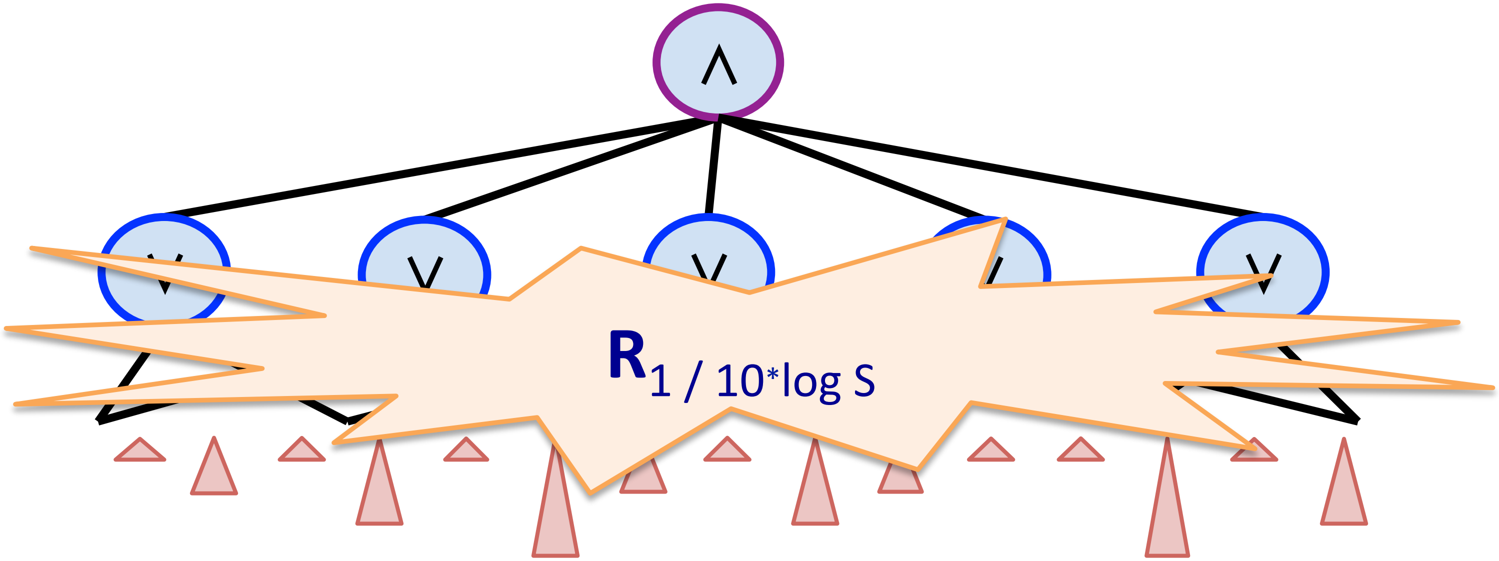
depth O(log S) decision trees (w.h.p.)

PARITY Lower Bound



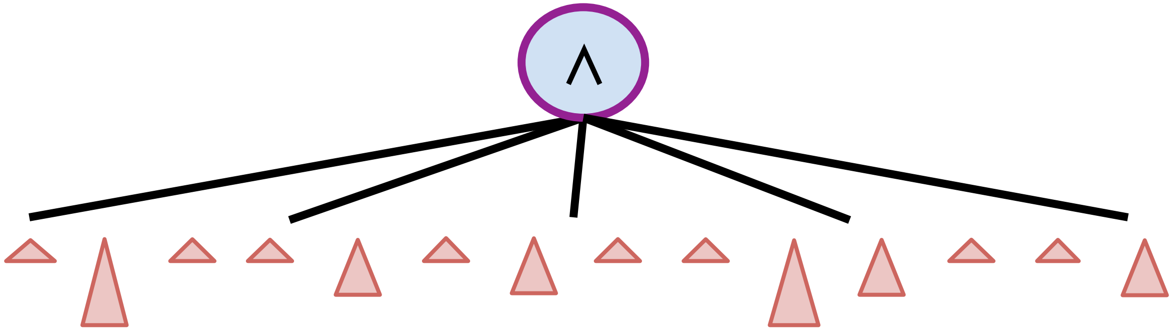
depth O(log S) decision trees (w.h.p.)

PARITY Lower Bound



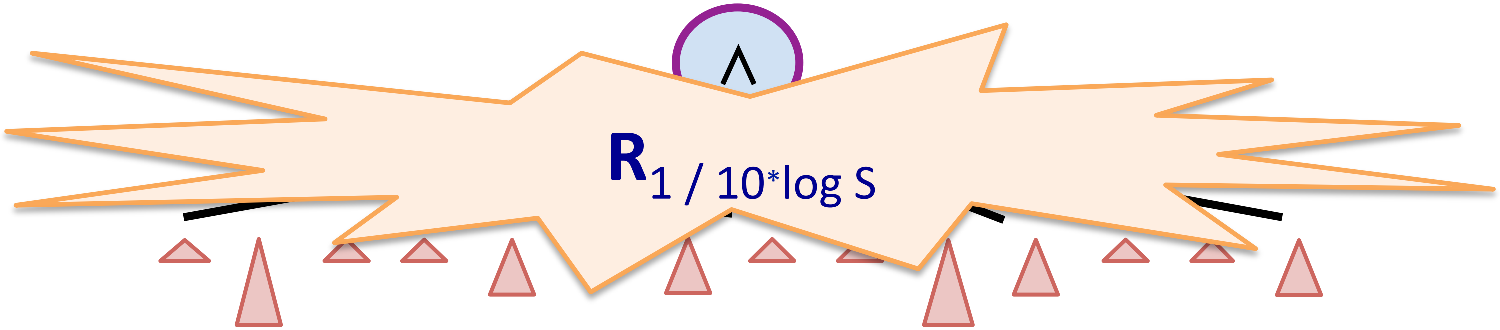
depth O(log S) decision trees (w.h.p.)

PARITY Lower Bound



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

PARITY Lower Bound



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

PARITY Lower Bound

constant function (w.h.p.)

PARITY Lower Bound

constant function (w.h.p.)

decision tree of depth:

- 0 with high prob.
- 1 with prob. $\leq \varepsilon$
- 2 with prob. $\leq \varepsilon^2$
- $\vdots$

PARITY Lower Bound

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

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

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

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

PARITY Lower Bound

- (AC^0 circuit of depth $d+1$ and size S) $\upharpoonright \mathbf{R}_{1/O(\log S)^d}$ is almost surely **constant**

- On the other hand, $\mathrm{PARITY}_n \upharpoonright \mathbf{R}_p$ is almost surely **non-constant** for $p = \omega(1/n)$

PARITY Lower Bound

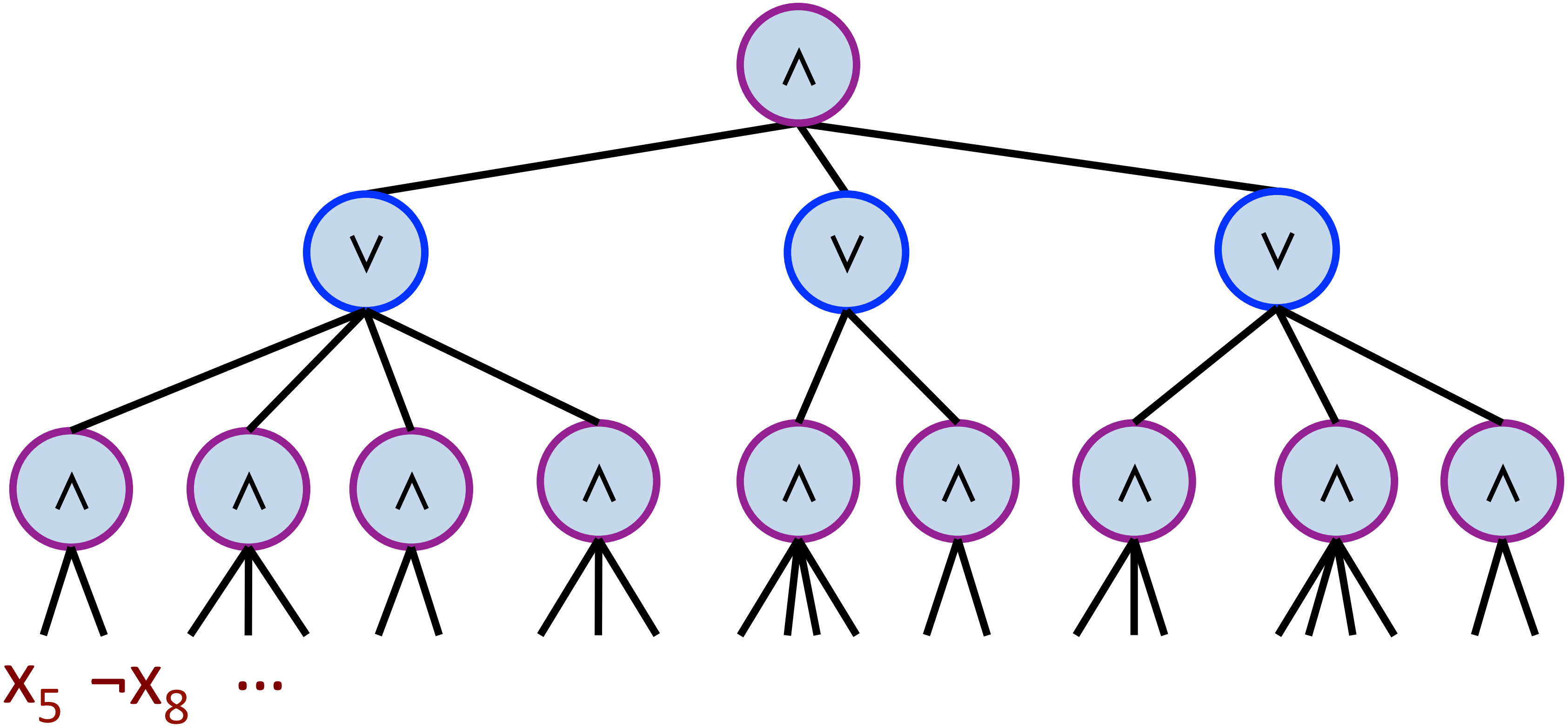
- (AC^0 circuit of depth $d+1$ and size S) $\upharpoonright$ $\mathbf{R}_{1/O(\log S)^d}$ is almost surely **constant**
- On the other hand, $\mathrm{PARITY}_n \upharpoonright \mathbf{R}_p$ is almost surely **non-constant** for $p = \omega(1/n)$

PARITY_m or $1 - \mathrm{PARITY}_m$ on $m =$ **Binomial**(n,p) variables

PARITY Lower Bound

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

Recall: AC^0 Formulas



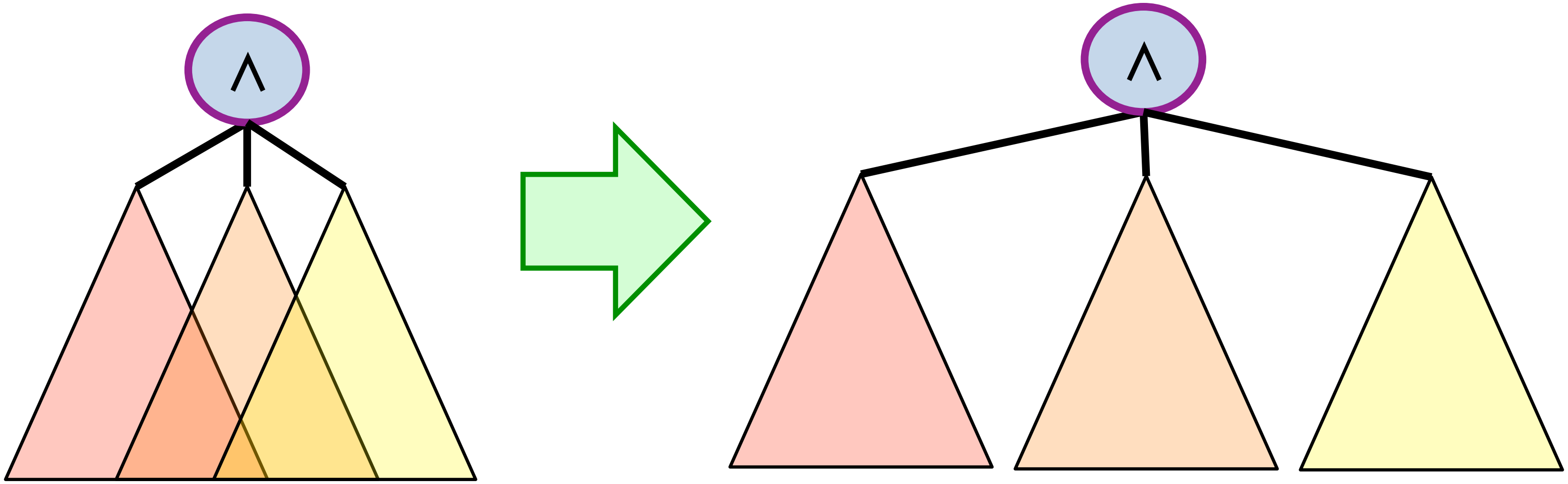
Upper Bound

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

Upper Bound

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

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



Upper Bound

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

Theorem [Hastad '86]

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

Upper Bound

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

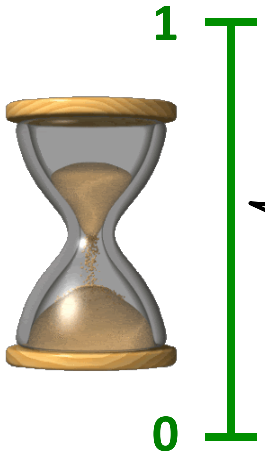
Theorem [Hastad ’86]

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

Theorem [R.’15]

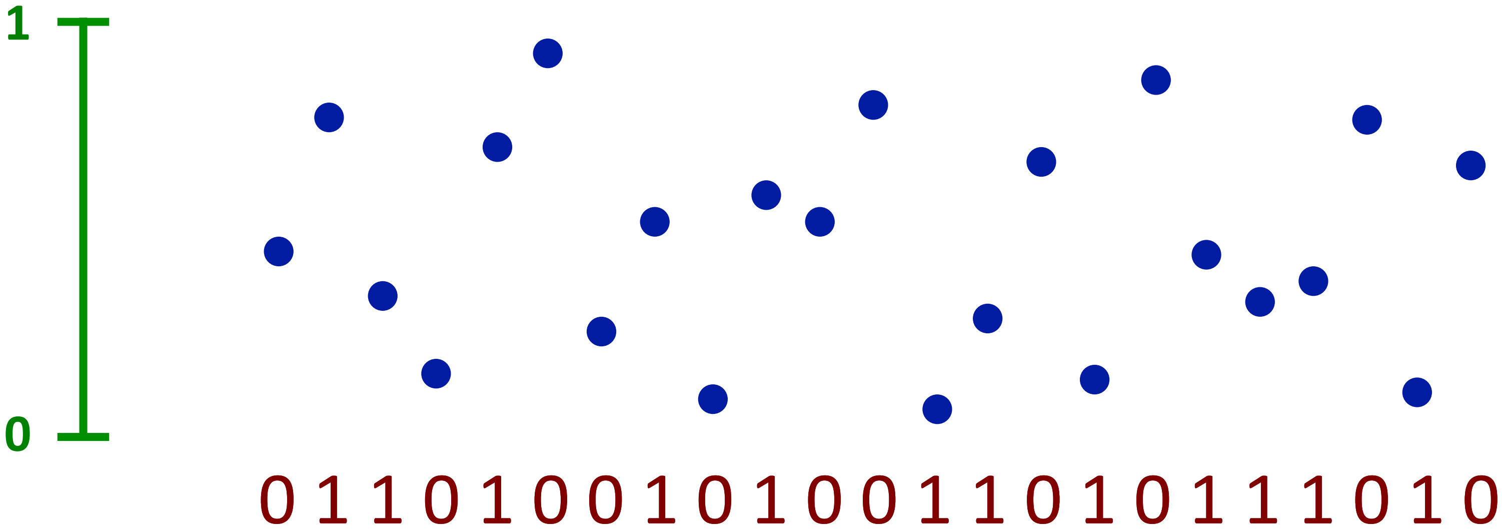
Depth $d+1$ **formulas** for PAR. have size $\exp(\Omega(dn^{1/d}))$

Dynamic View of $\mathbf{R}_p$



“time” p runs from 1 to 0

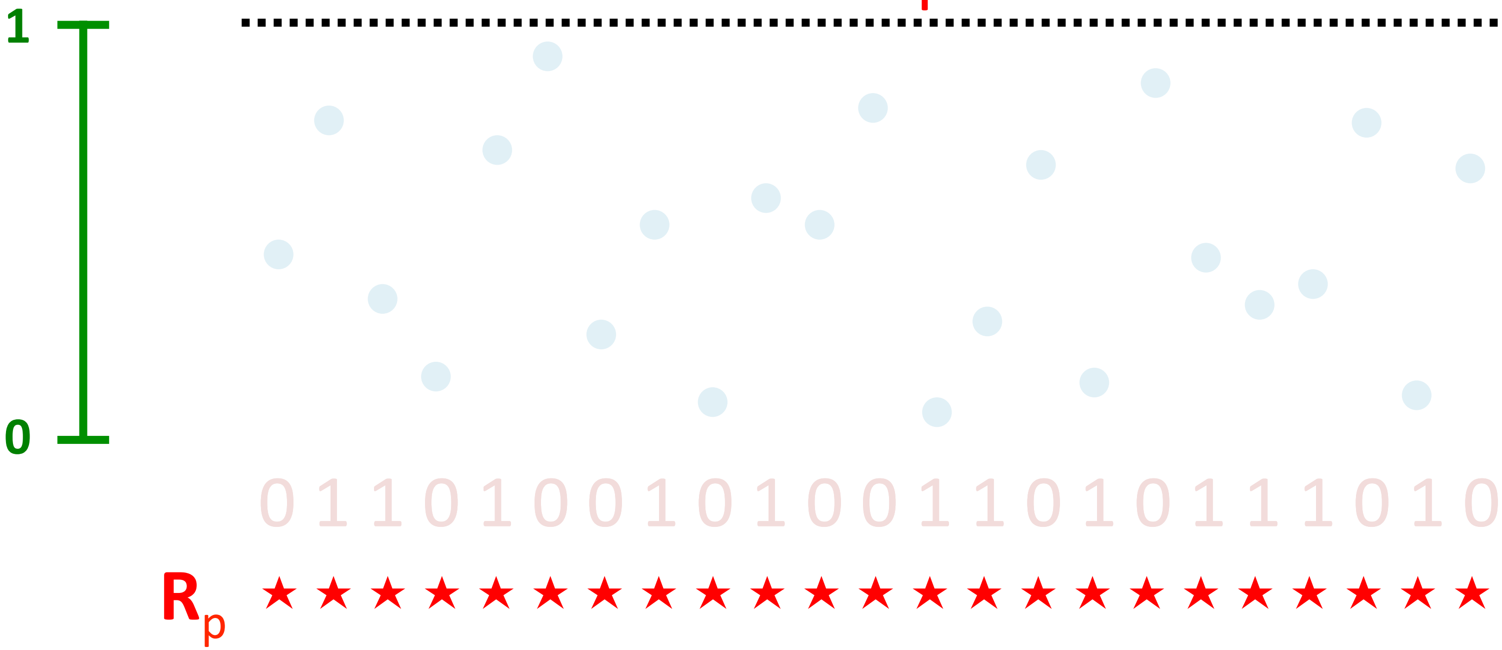
We view the random restriction $\mathbf{R}_p : \{x_1,\ldots,x_n\} \to \{0,1,\star\}$ as a process



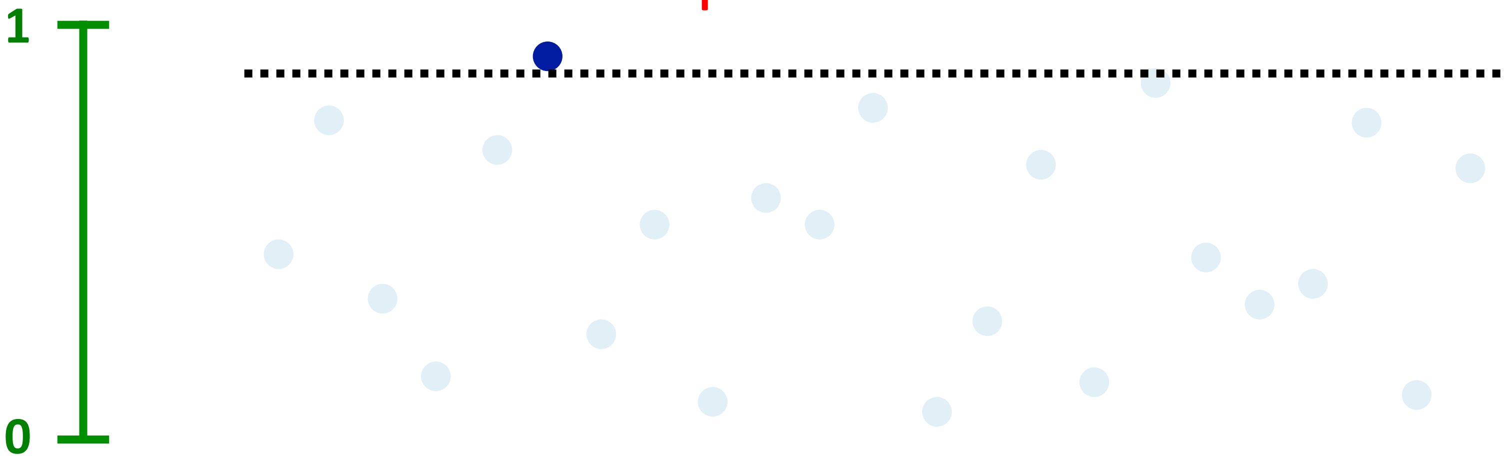
for each variable, we generate a random

- **value** in {0,1}
- **timestamp** in [0,1]

initial time $p = 1$



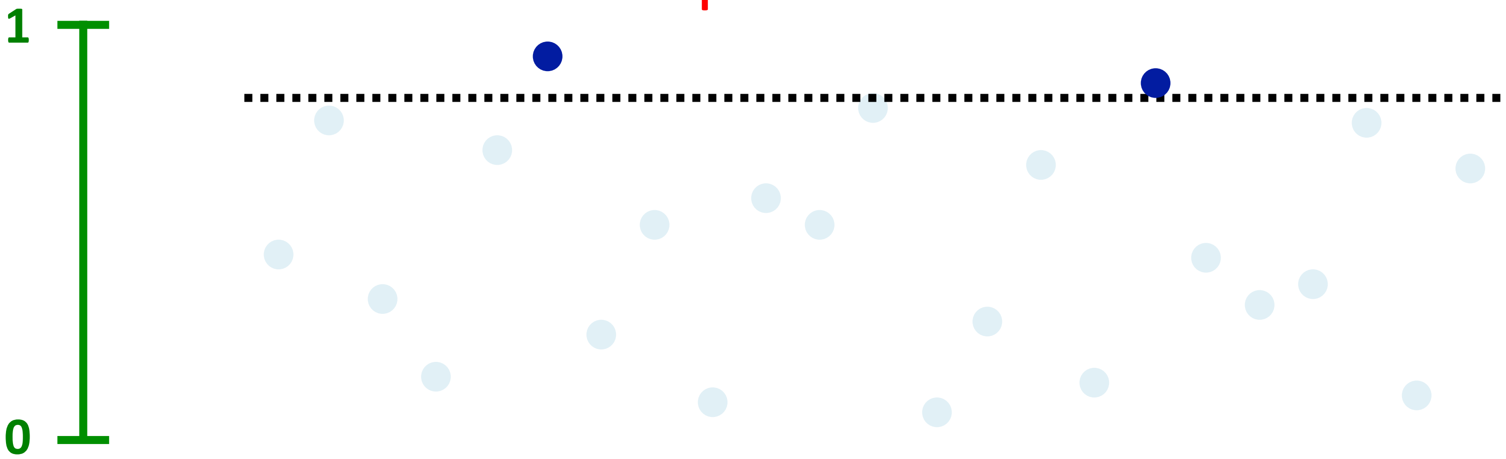
$p = 0.99$



0 1 1 0 1 0 0 1 0 1 0 0 1 1 0 1 0 1 1 1 0 1 0

R_p ★ ★ ★ ★ ★ 0 ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★

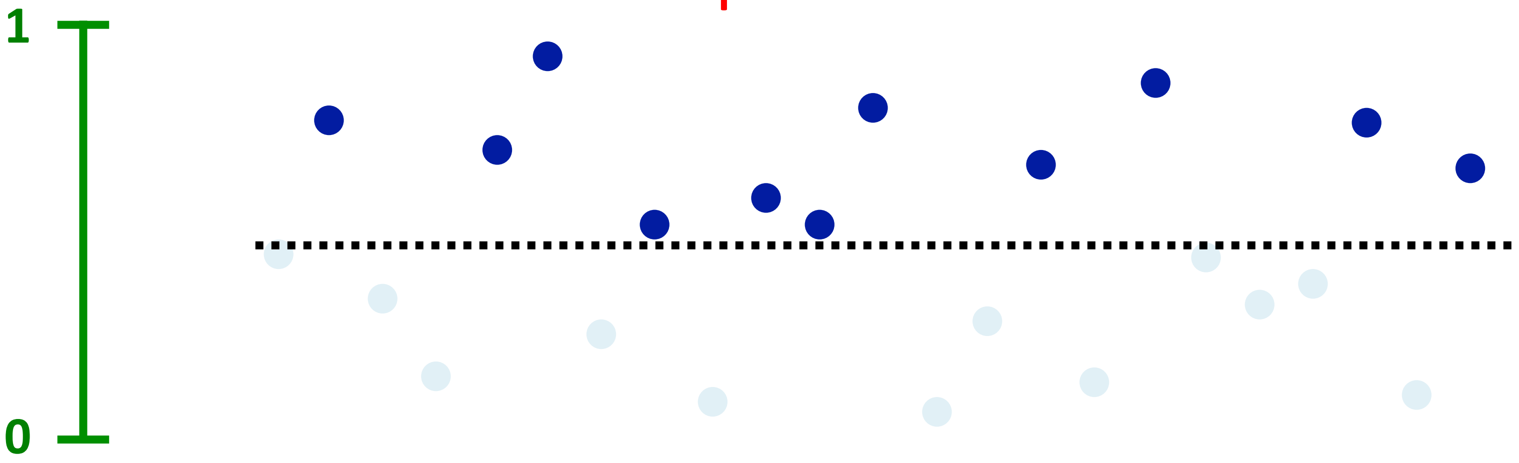
$p = 0.98$



0 1 1 0 1 0 0 1 0 1 0 0 1 1 0 1 0 1 1 1 0 1 0

R_p ★ ★ ★ ★ ★ 0 ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ 0 ★ ★ ★ ★ ★ ★

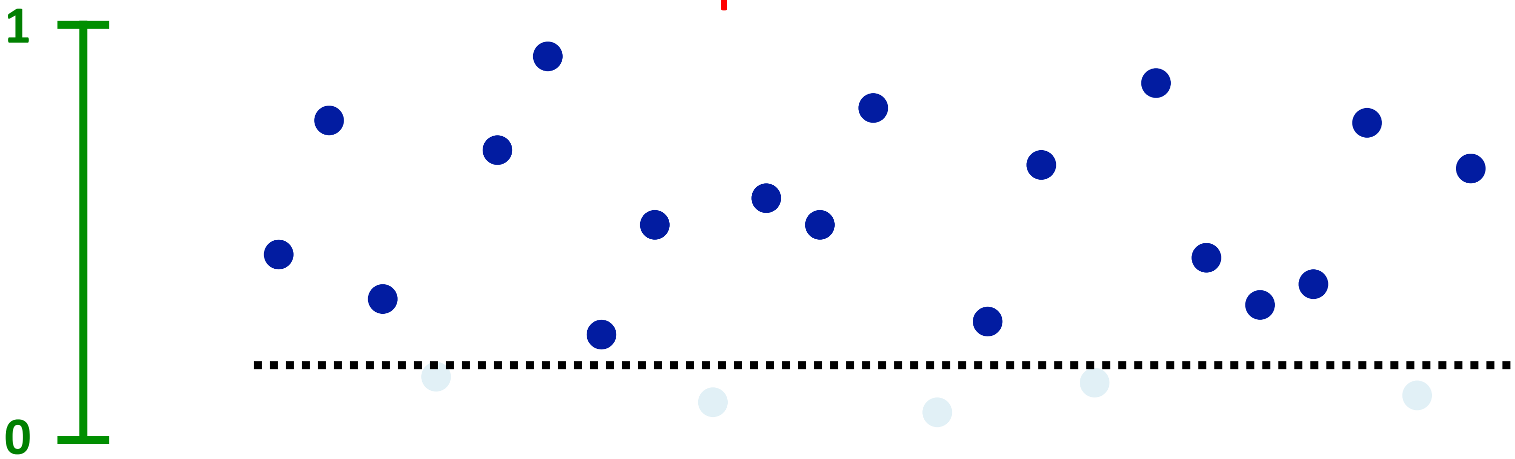
p = 0.5



0 1 1 0 1 0 0 1 0 1 0 0 1 1 0 1 0 1 1 1 0 1 0

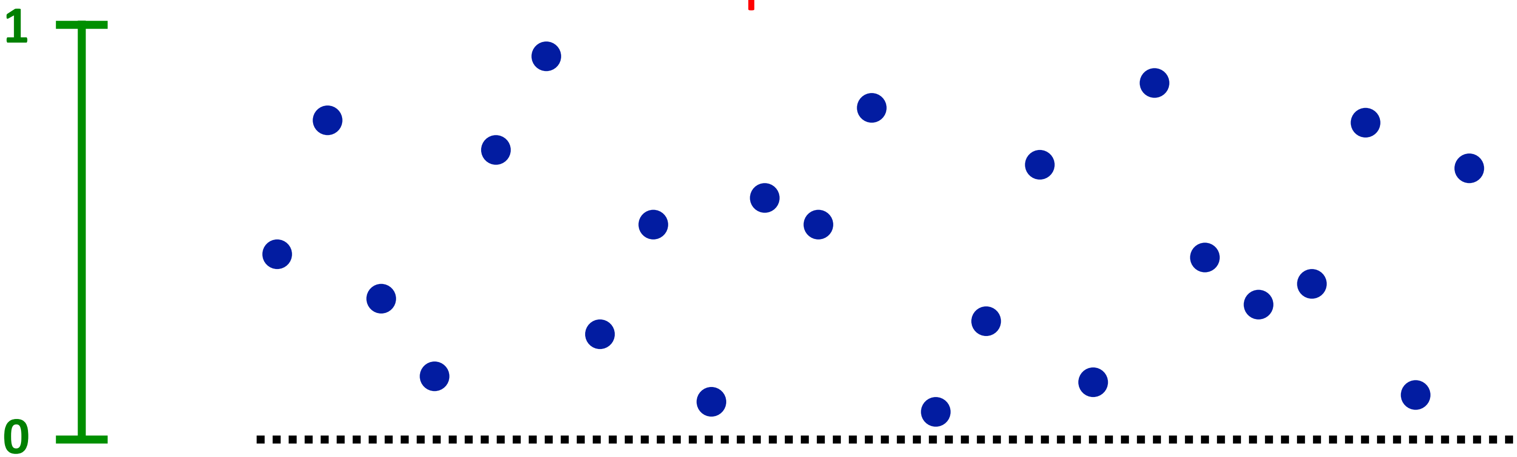
R_p ★ 1 ★ ★ 1 0 ★ 1 ★ 1 0 0 ★ ★ 0 ★ 0 ★ ★ ★ 0 ★ 0

$p = 0.1$



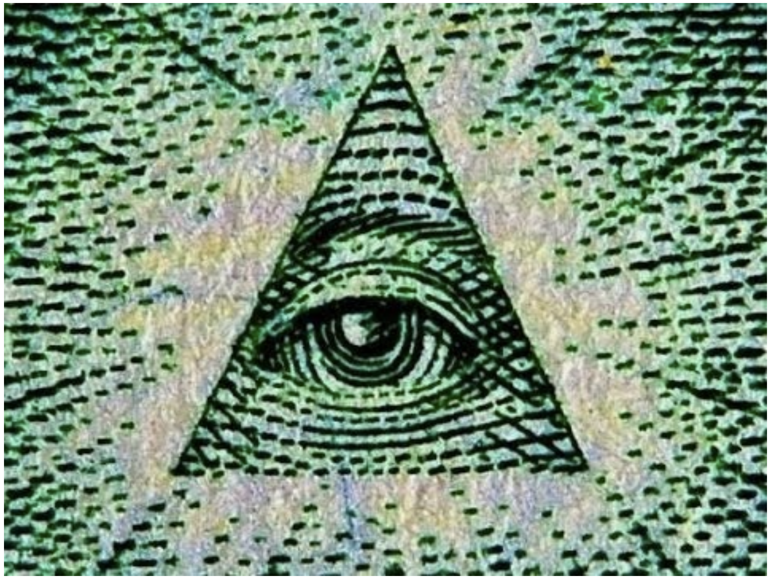
0 1 1 0 1 0 0 1 0 1 0 0 1 1 0 1 0 1 1 1 0 1 0

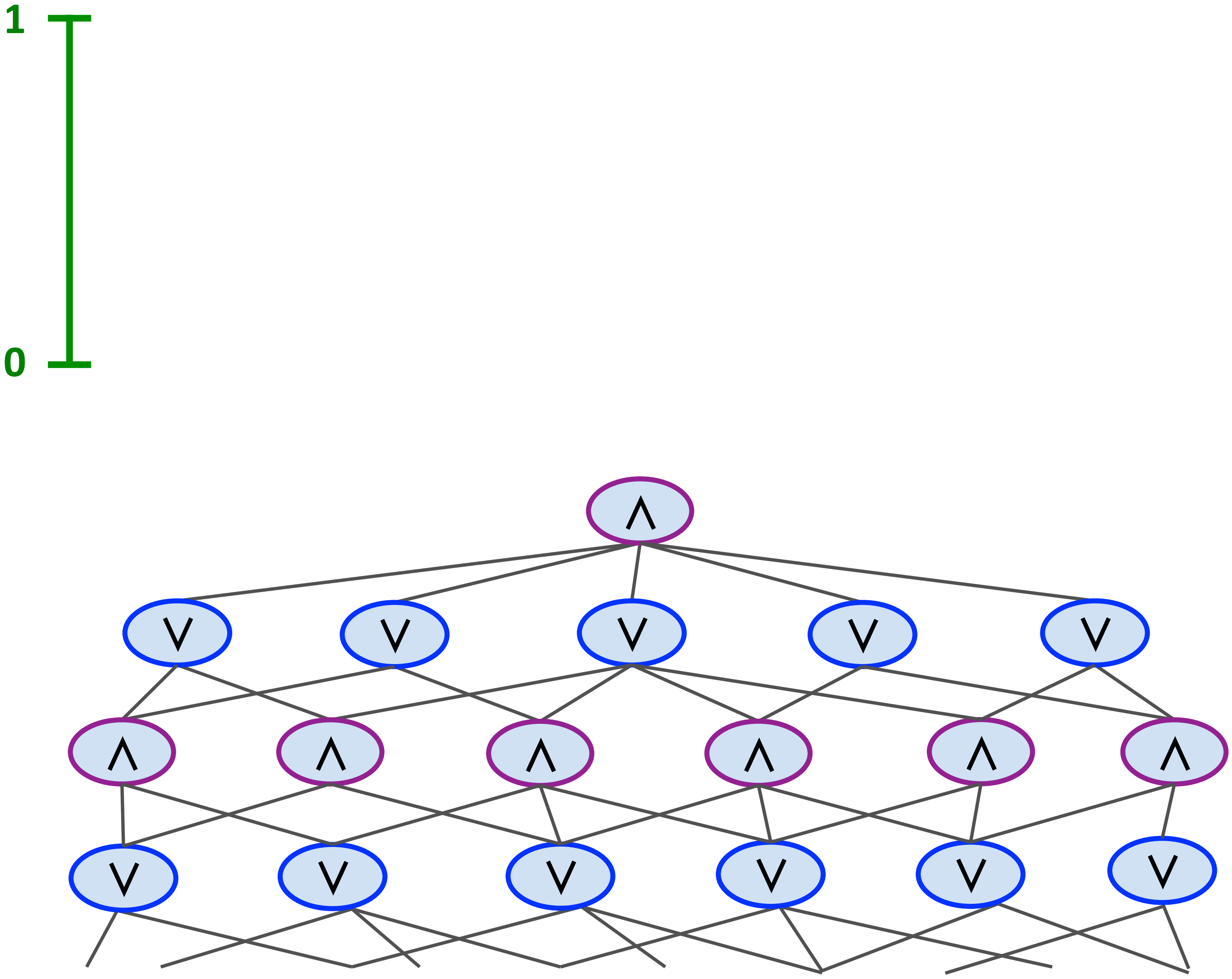
R_p 0 1 1 ★ 1 0 0 1 ★ 1 0 0 ★ 1 0 ★ 0 1 1 1 0 ★ 0 p = 0

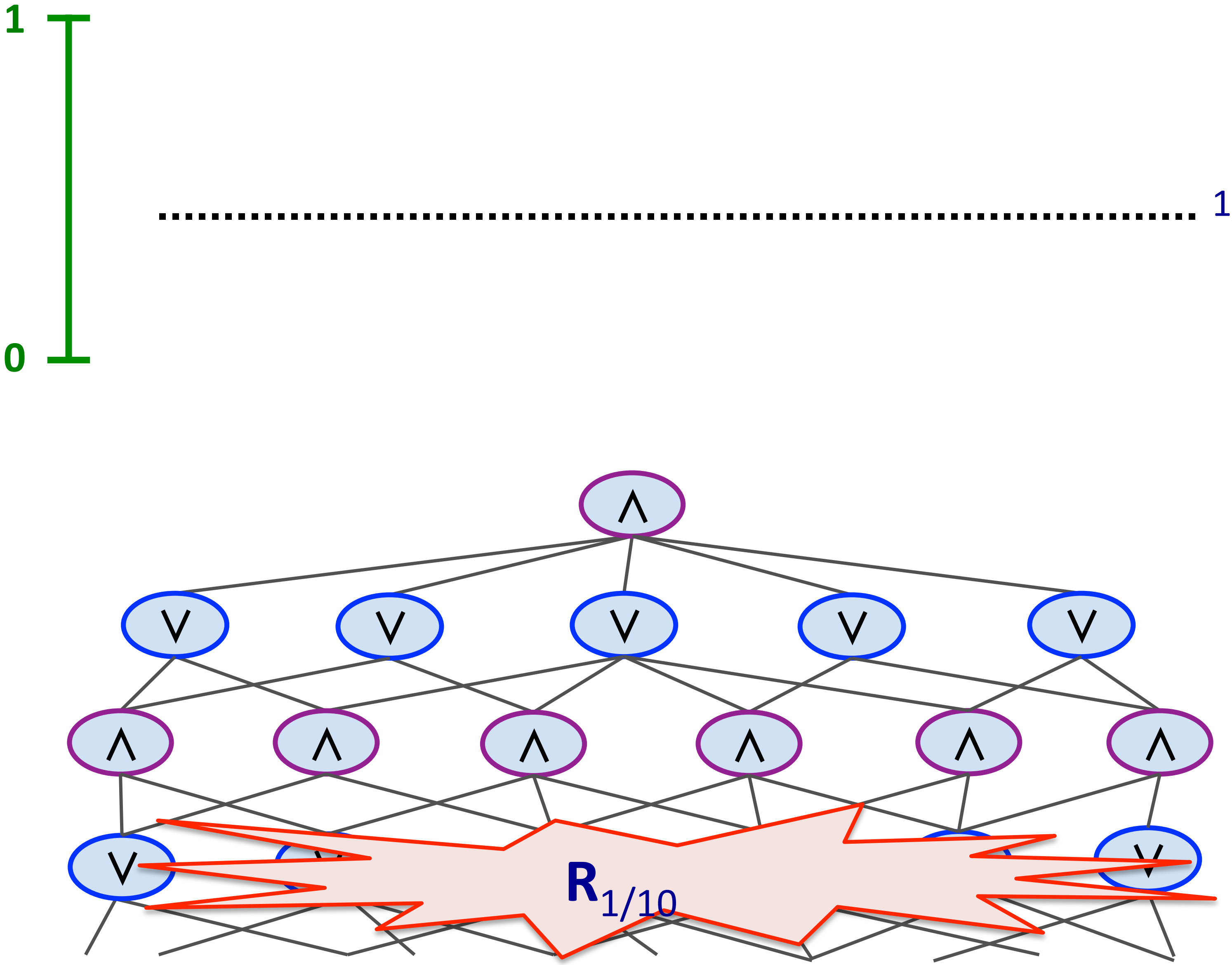


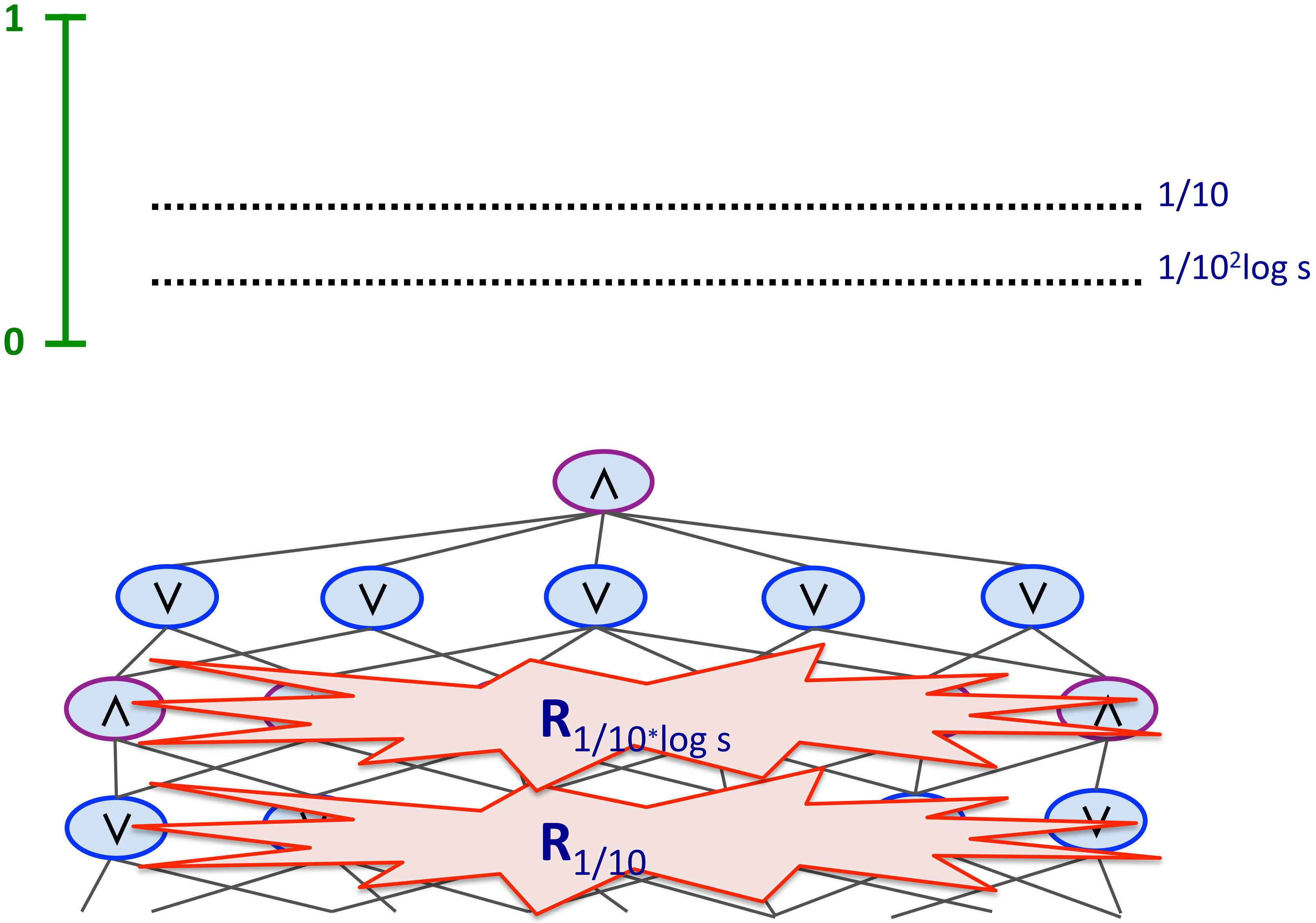
0 1 1 0 1 0 0 1 0 1 0 0 1 1 0 1 0 1 1 1 0 1 0

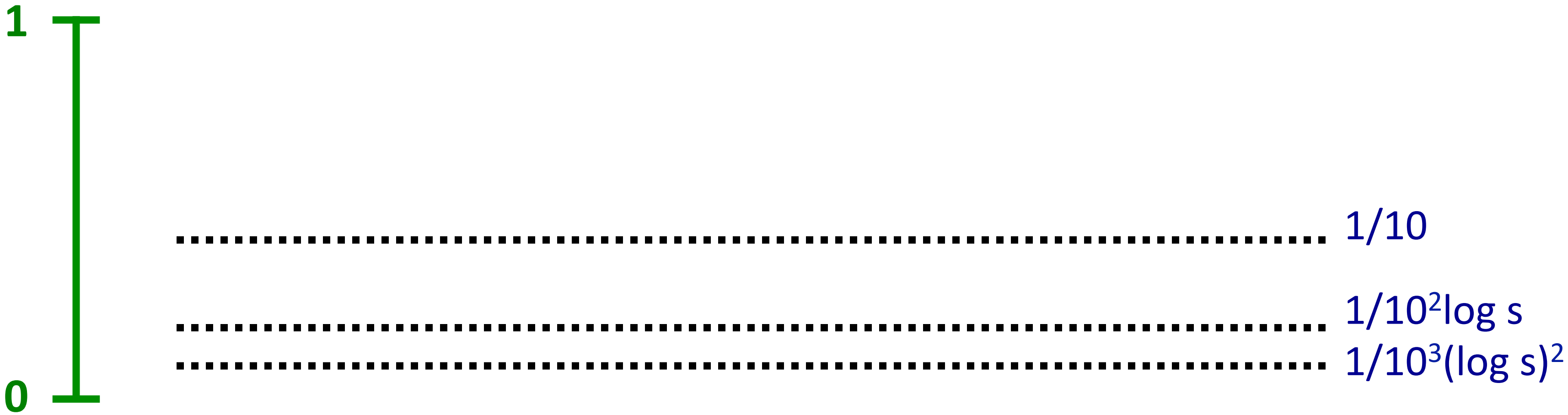
R_p 0 1 1 0 1 0 0 1 0 1 0 0 1 1 0 1 0 1 1 1 0 1 0




1
0
∧
∨ ∨ ∨ ∨ ∨
∧ ∧ ∧ ∧ ∧ ∧
∨ ∨ ∨ ∨ ∨ ∨


1
1/10
0
∧
∨ ∨ ∨ ∨ ∨
∧ ∧ ∧ ∧ ∧ ∧
∨ ∨
R1/10


1
0
1/10
1/10²log s
∧
∨
∨
∨
∨
∨
∧
∧
∨
∨
R1/10*log s
R1/10



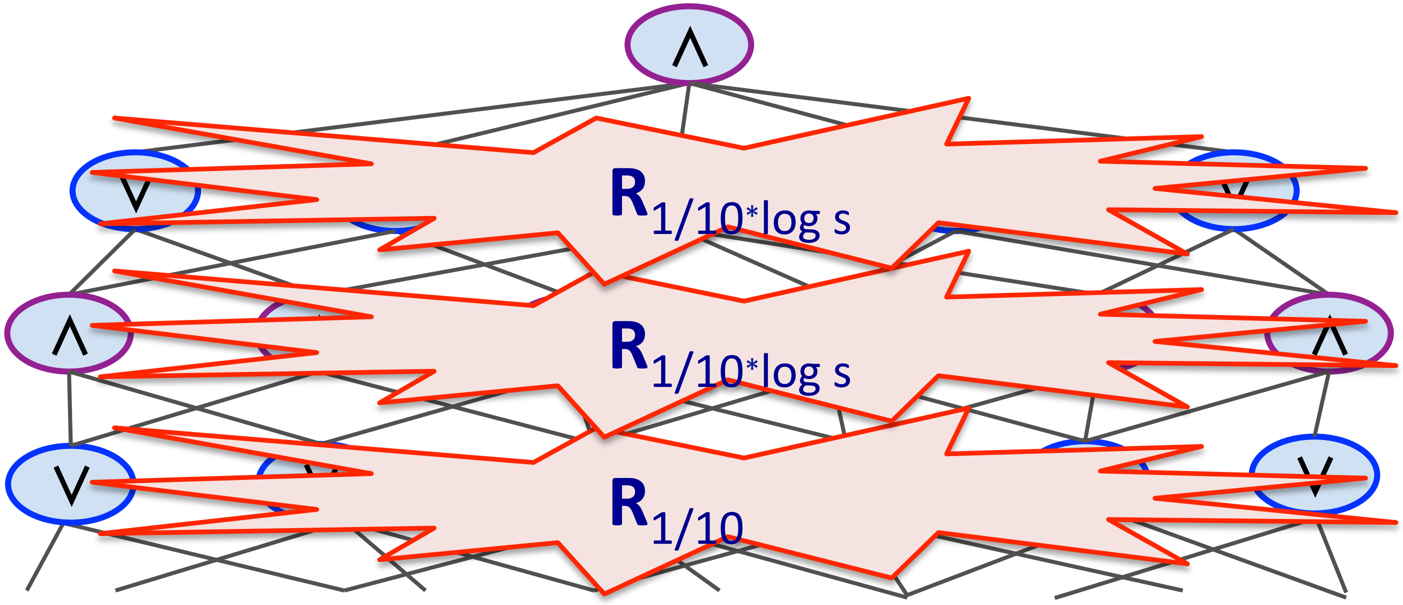
1

0

1/10

$1/10^2\log s$

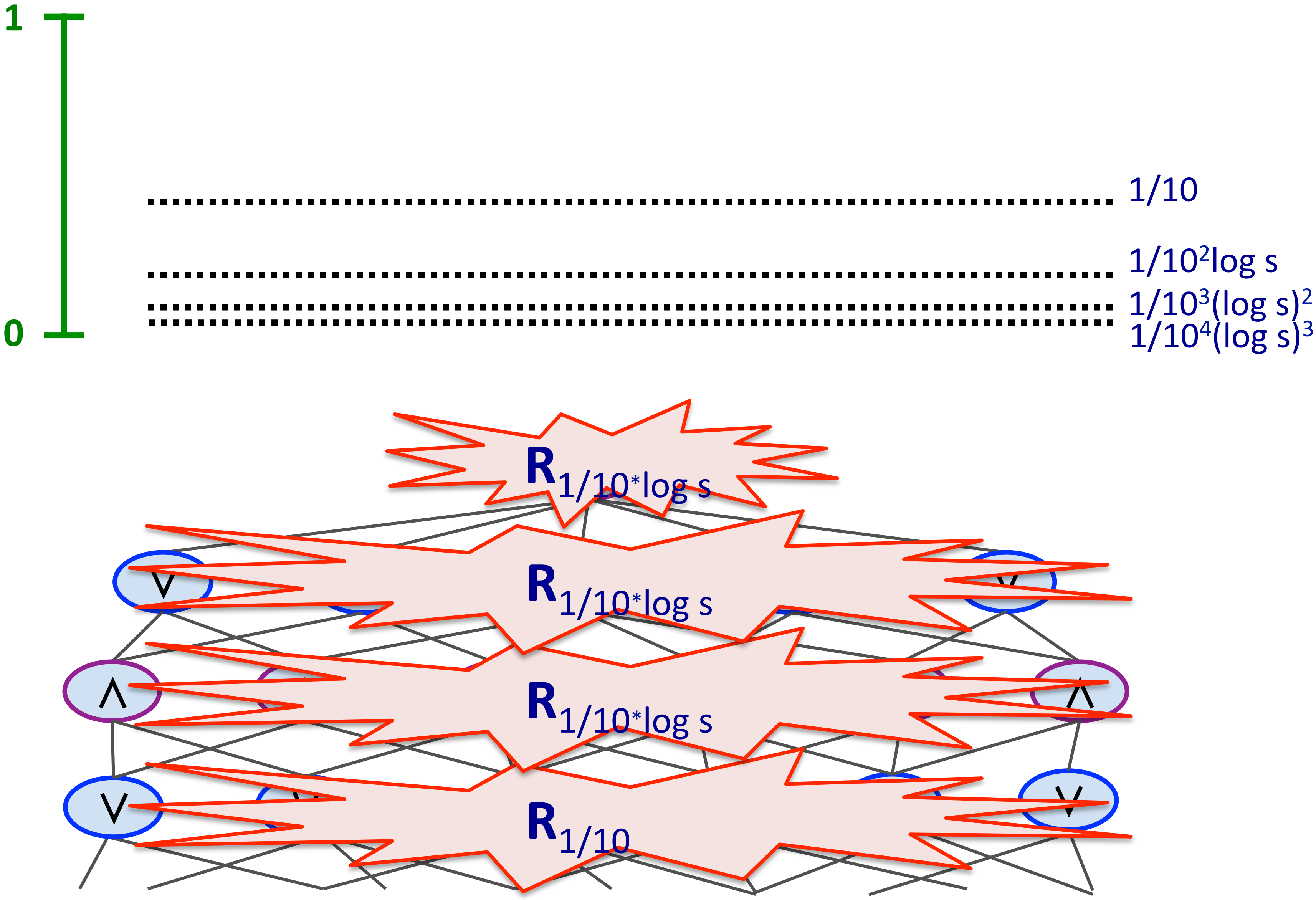
$1/10^3(\log s)^2$

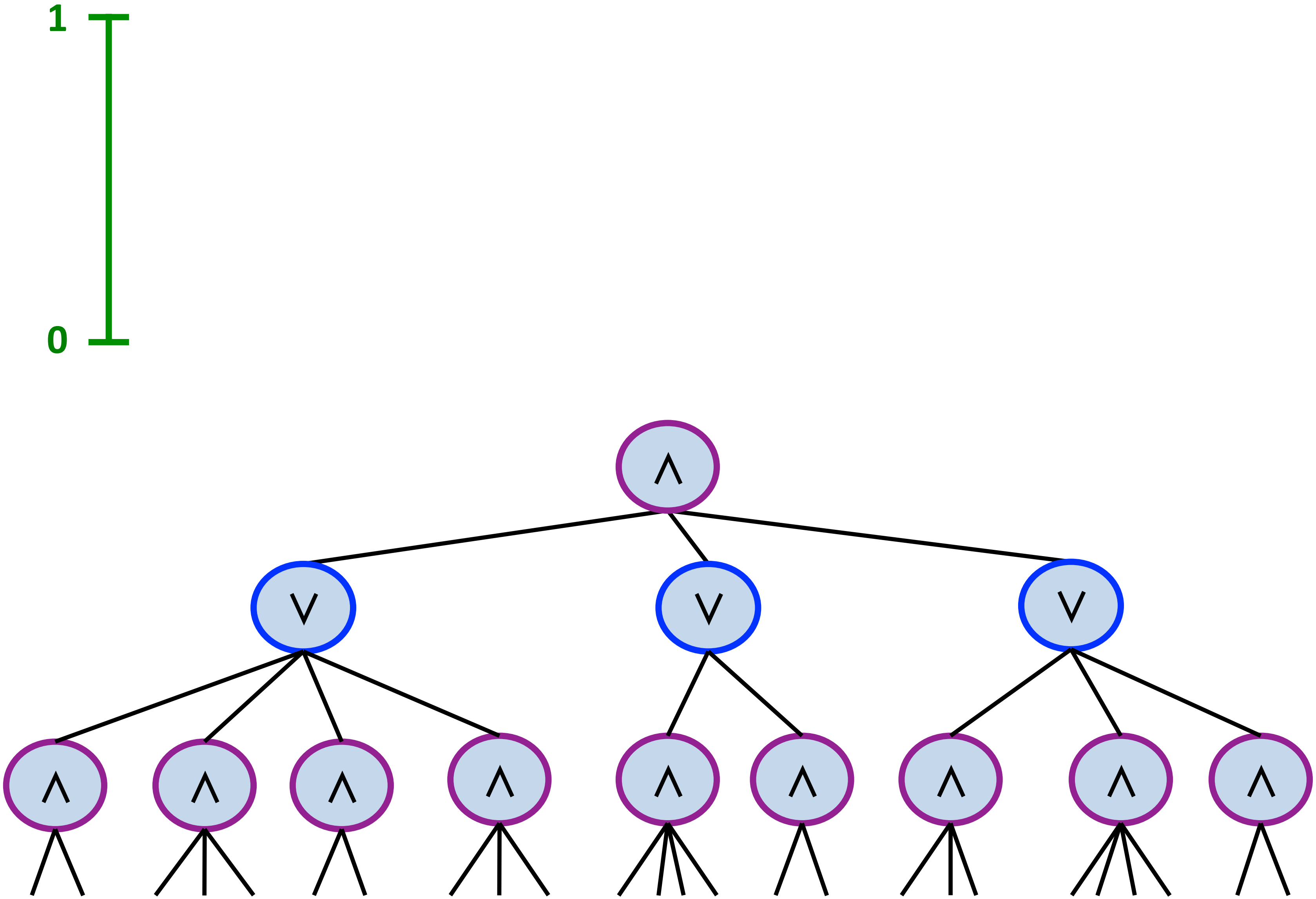


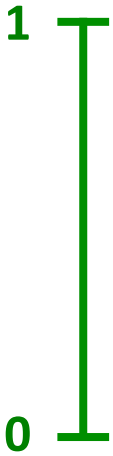
$\mathbf{R}_{1/10^*\log s}$

$\mathbf{R}_{1/10^*\log s}$

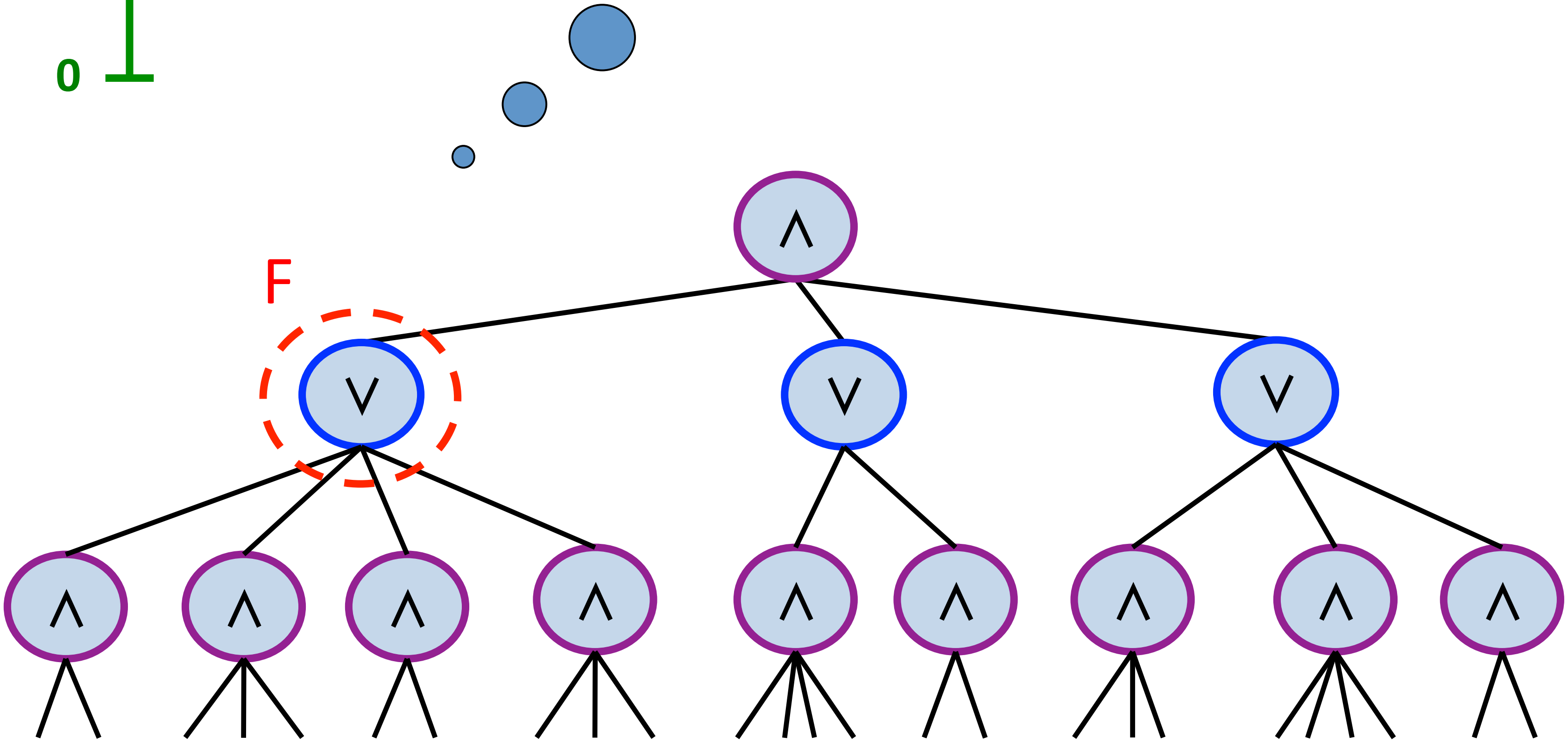
$\mathbf{R}_{1/10}$

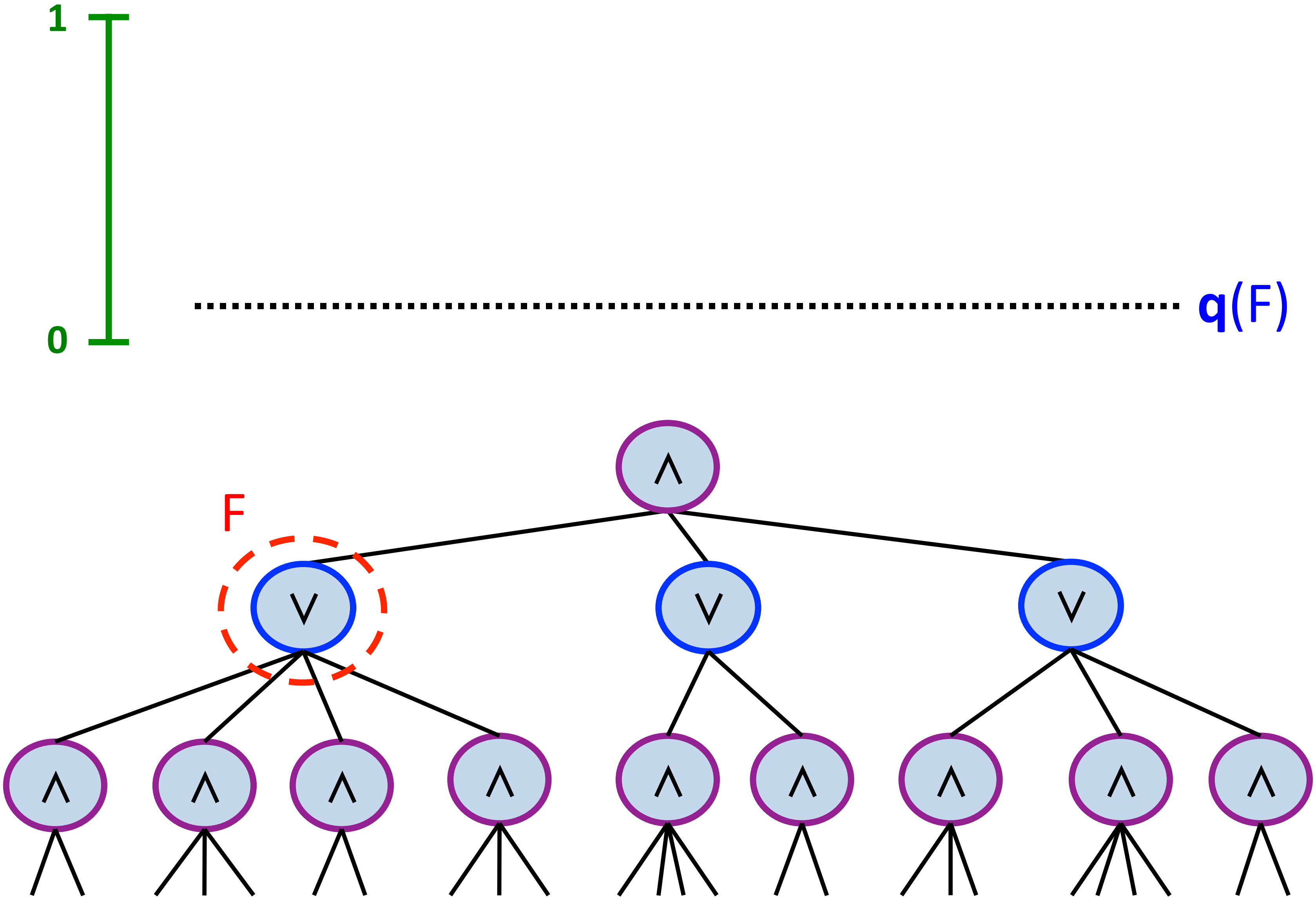

1
0
$1/10$
$1/10^2 \log s$
$1/10^3 (\log s)^2$
$1/10^4 (\log s)^3$
$R_{1/10^* \log s}$
$R_{1/10^* \log s}$
$R_{1/10^* \log s}$
$R_{1/10}$
$\vee$
$\wedge$
$\vee$
$\vee$
$\wedge$
$\vee$

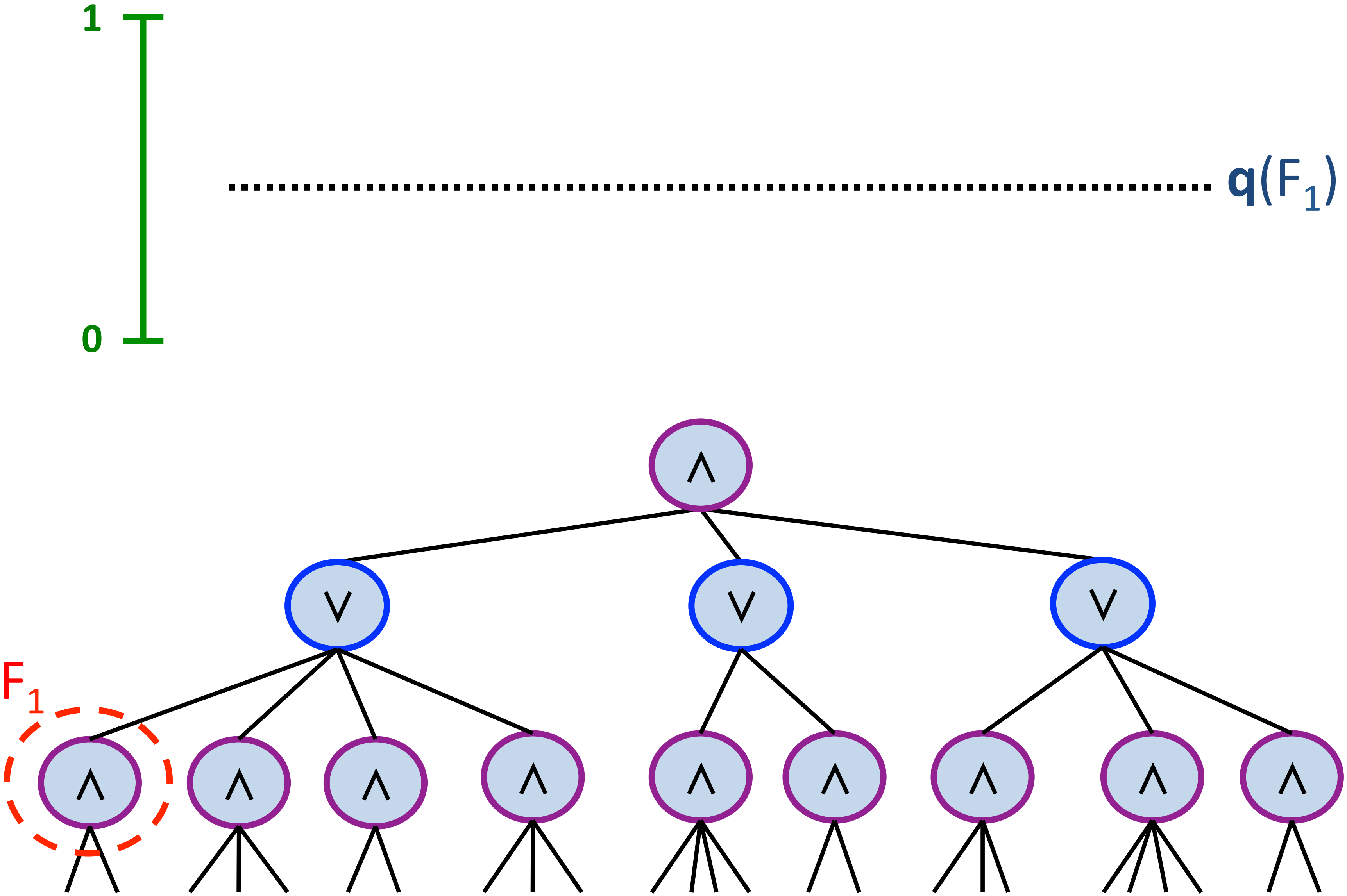

1
0
∧
∨
∨
∨
∧
∧
∧
∧
∧
∧
∧
∧
∧

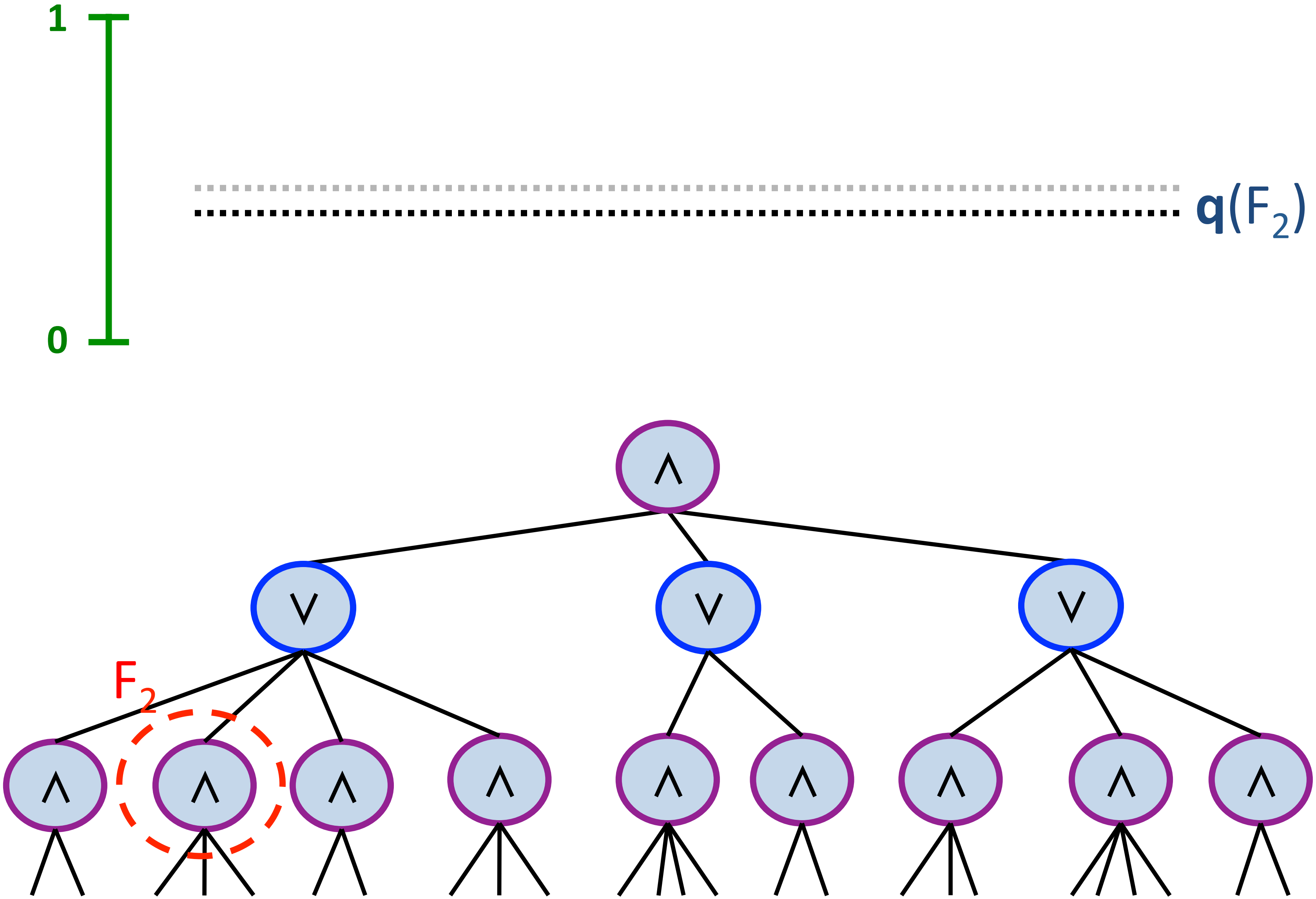


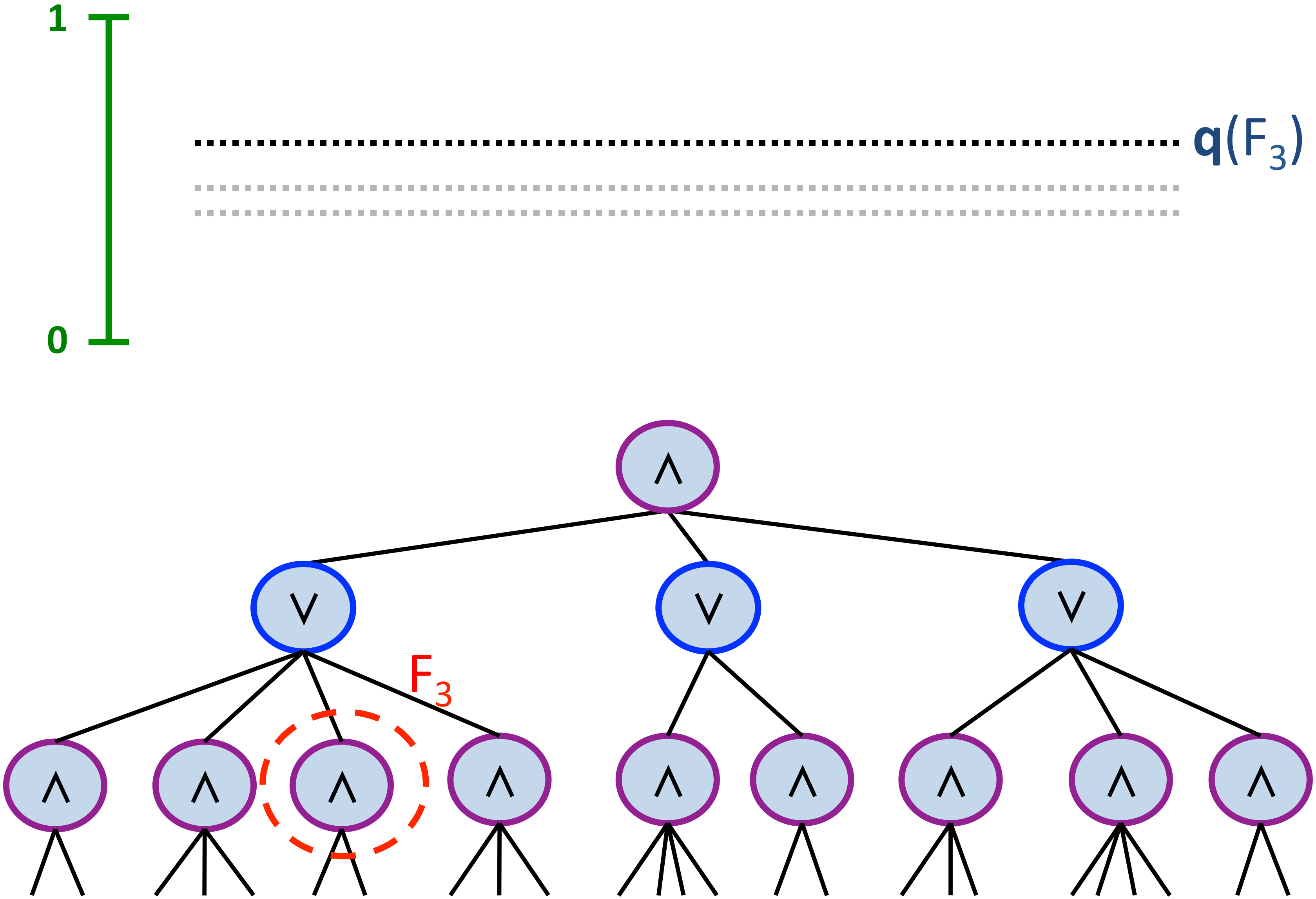
Idea: Dynamically assign each sub-formula F its own “stopping time” **q**(F)

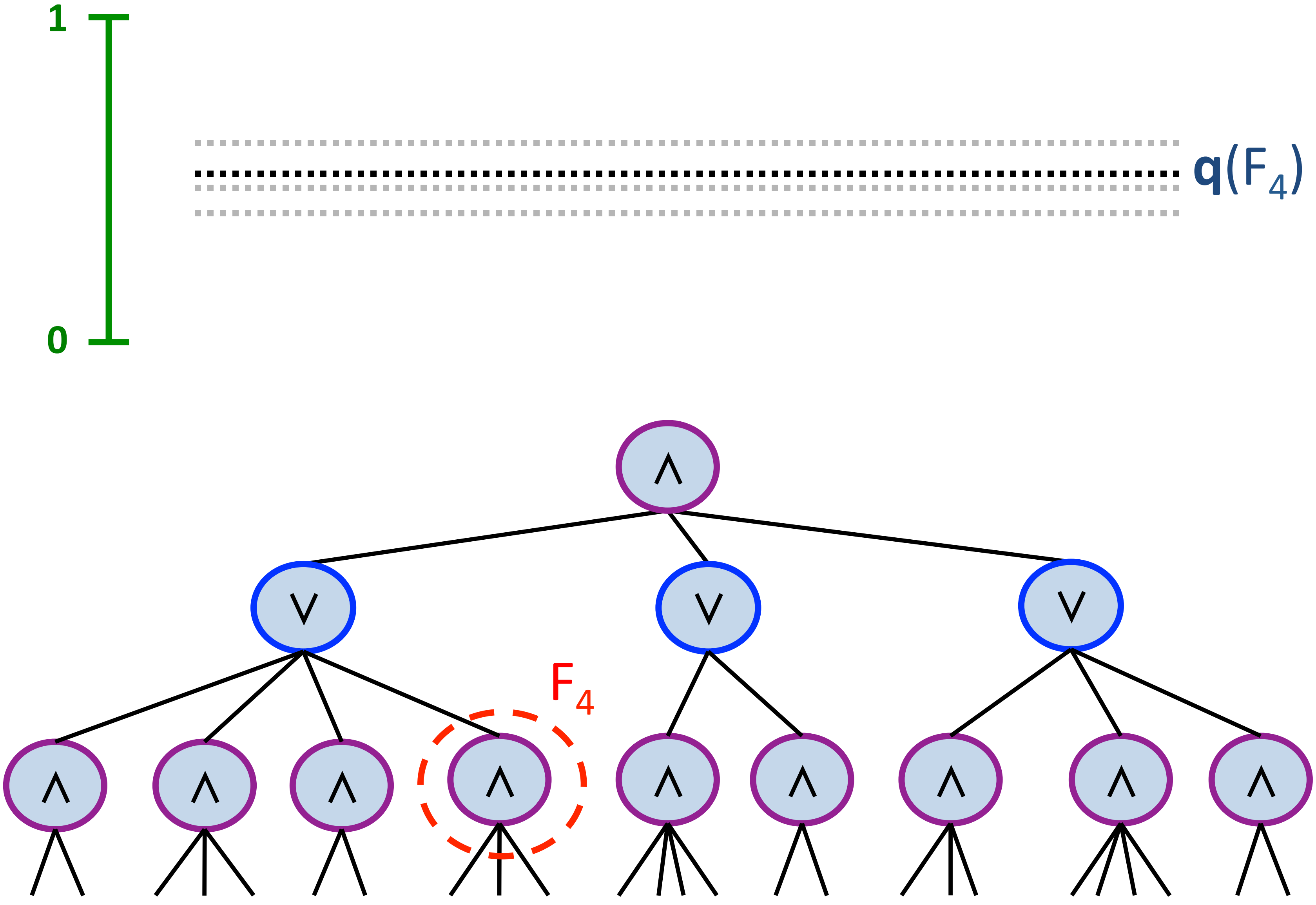



1
0
q(F)
F
∧
∨
∨
∨
∧
∧
∧
∧
∧
∧
∧
∧
∧

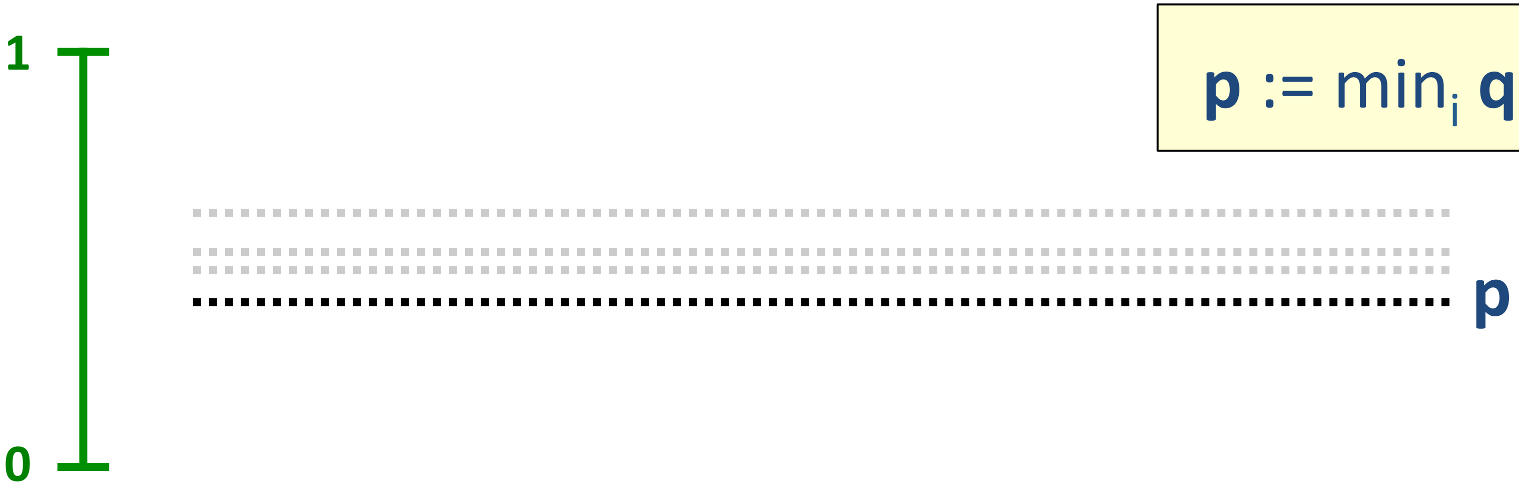

1
0
q(F1)
∧
∨
∨
∨
F1
∧
∧
∧
∧
∧
∧
∧
∧
∧

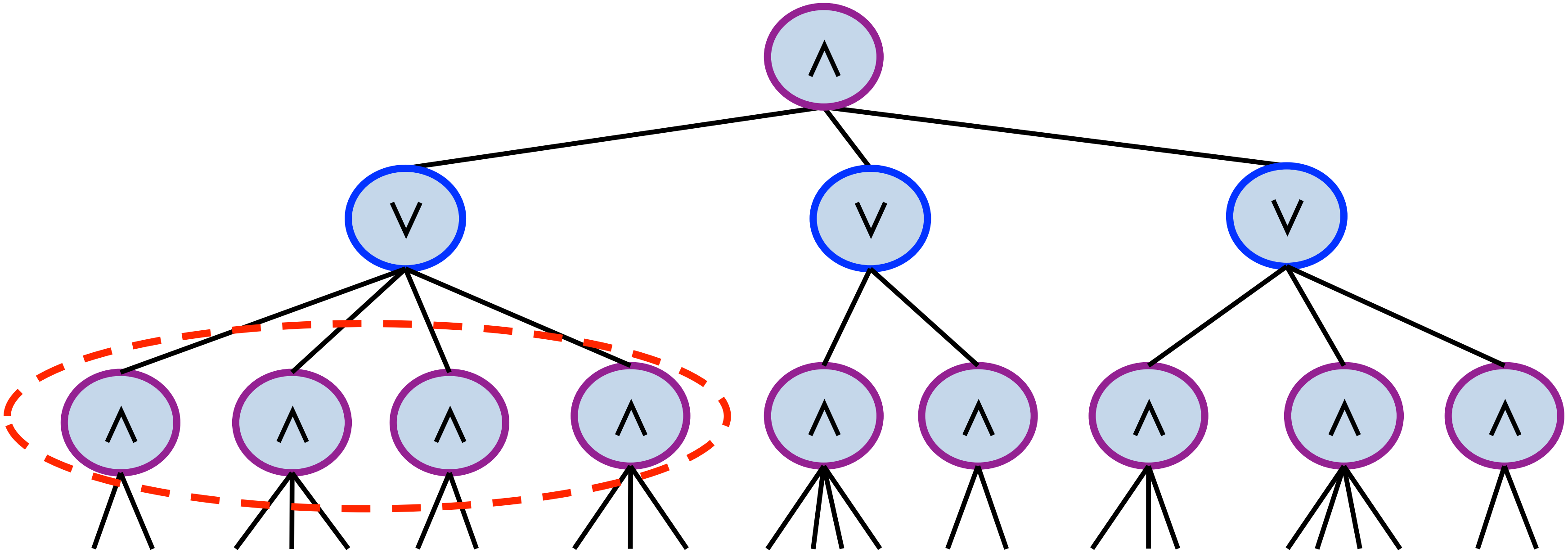

1
0
q(F2)
∧
∨
∨
∨
F2
∧
∧
∧
∧
∧
∧
∧
∧
∧


1
0
q(F_3)
∧
∨
∨
∨
F_3
∧
∧
∧
∧
∧
∧
∧
∧
∧

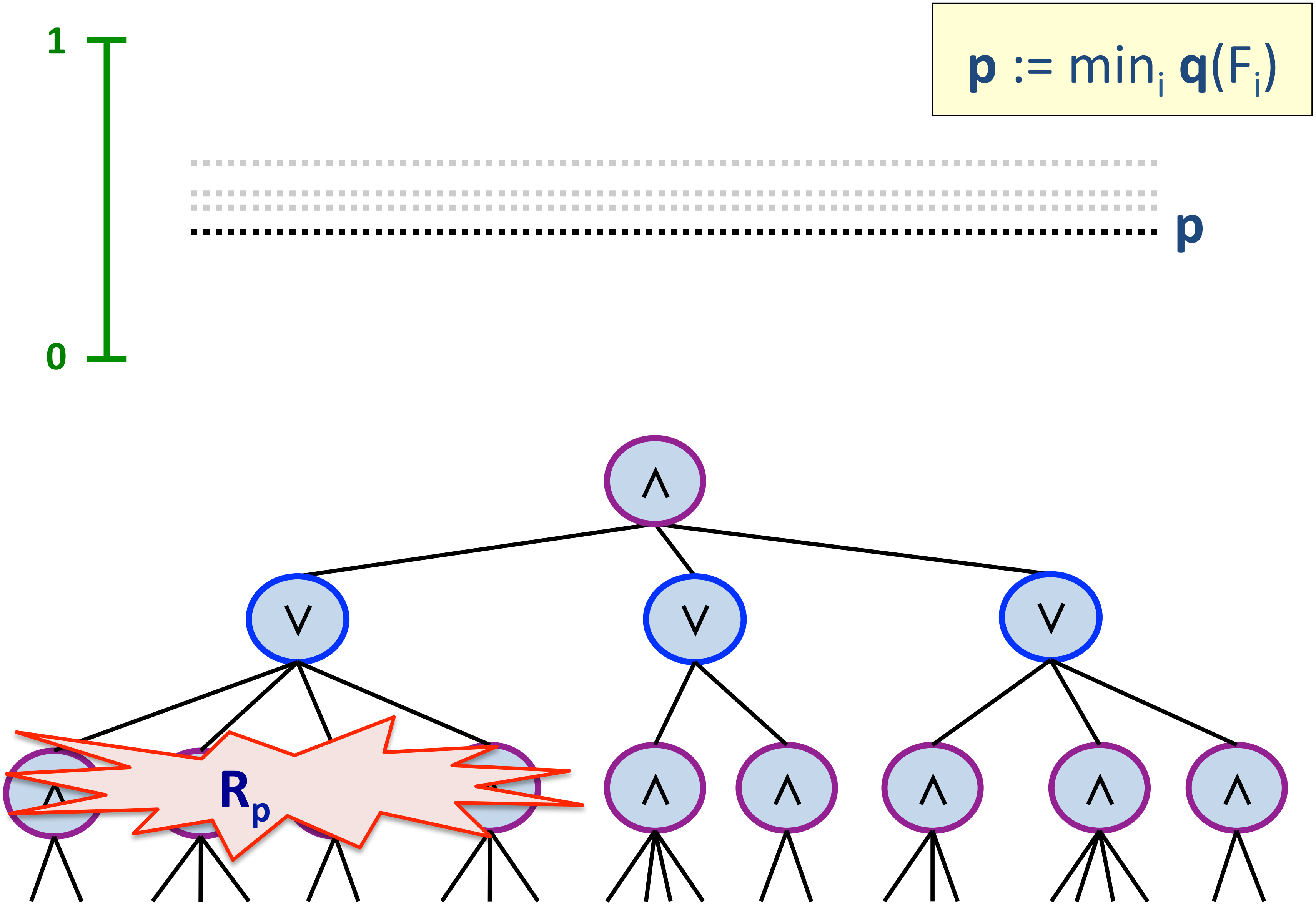

1
0
$\mathbf{q}(F_4)$
∧
∨
∨
∨
F_4
∧
∧
∧
∧
∧
∧
∧
∧
∧

$\mathbf{p} := \min_i \mathbf{q}(F_i)$

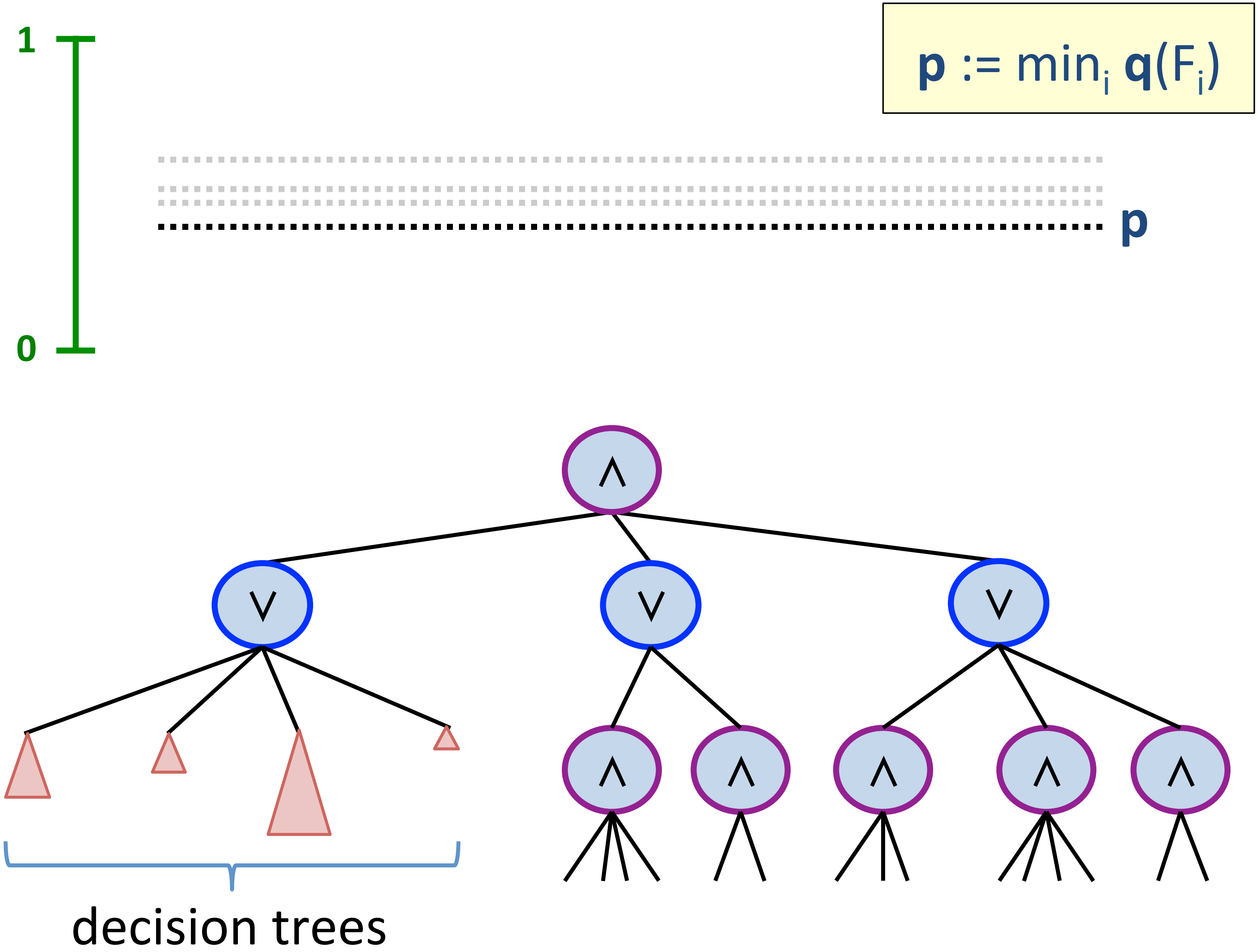




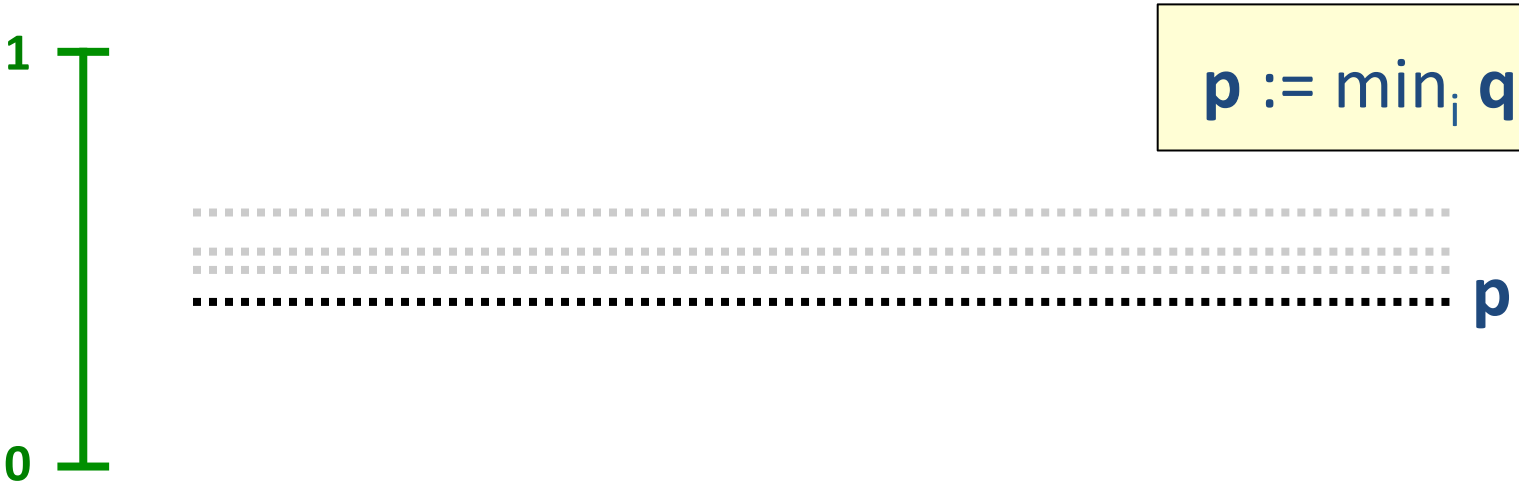
$\mathbf{p} := \min_i \mathbf{q}(F_i)$

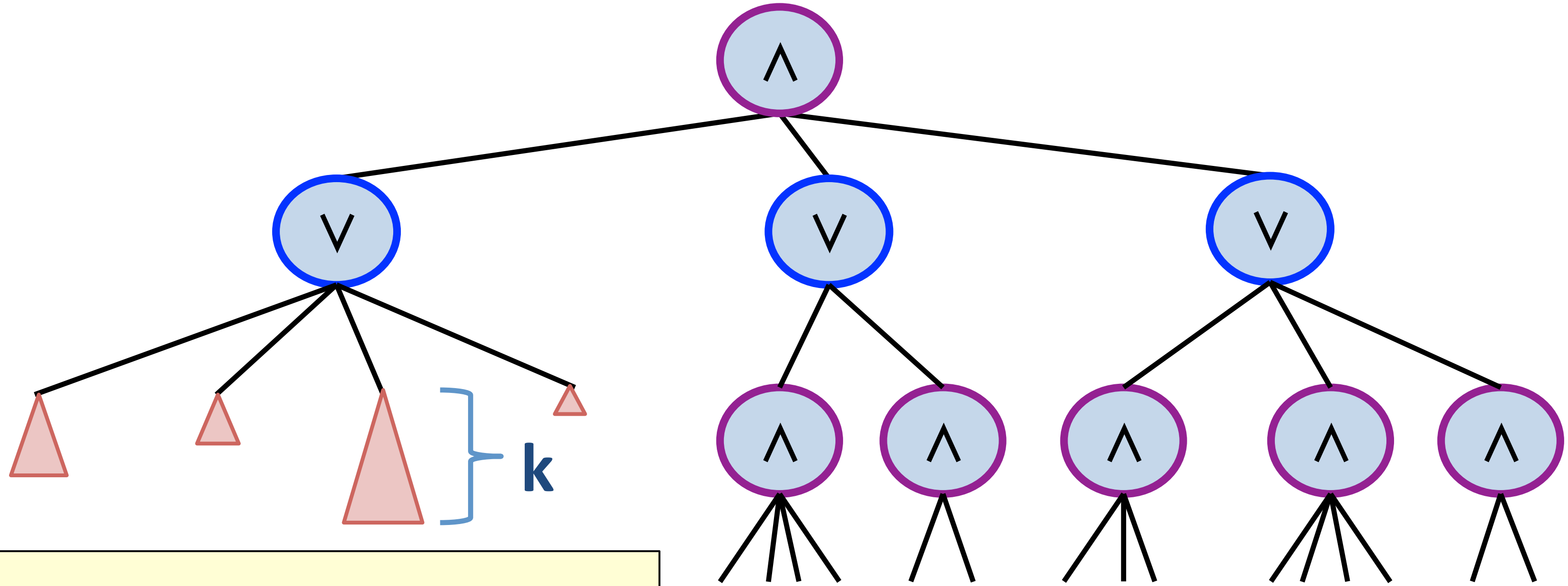


$$\mathbf{p} := \min_i \mathbf{q}(F_i)$$



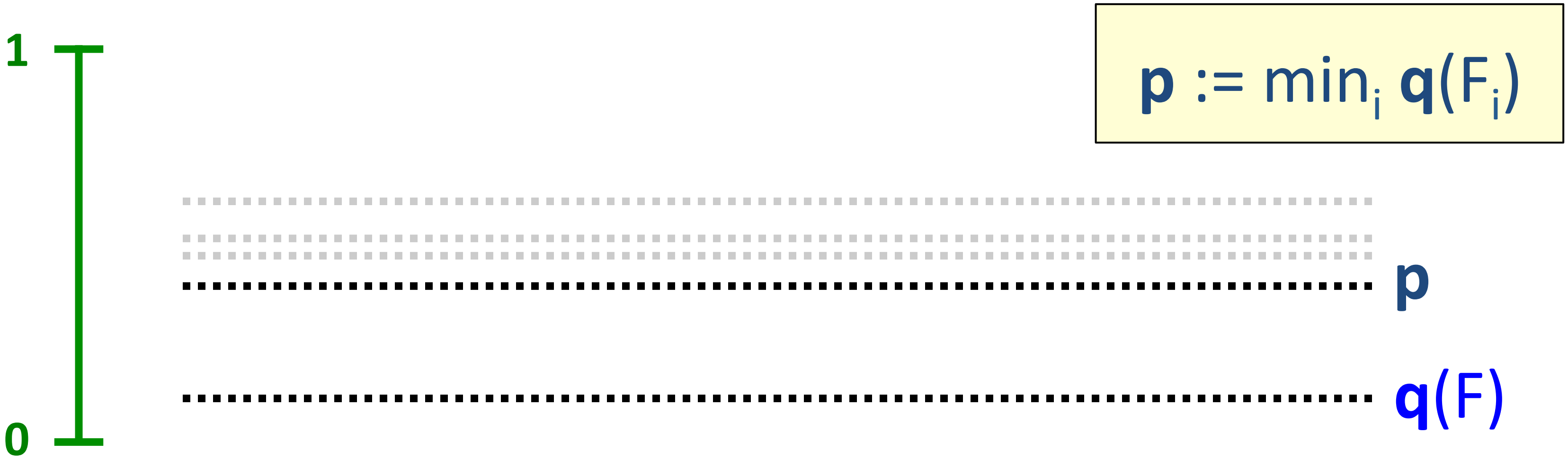
$\mathbf{p} := \min_i \mathbf{q}(F_i)$



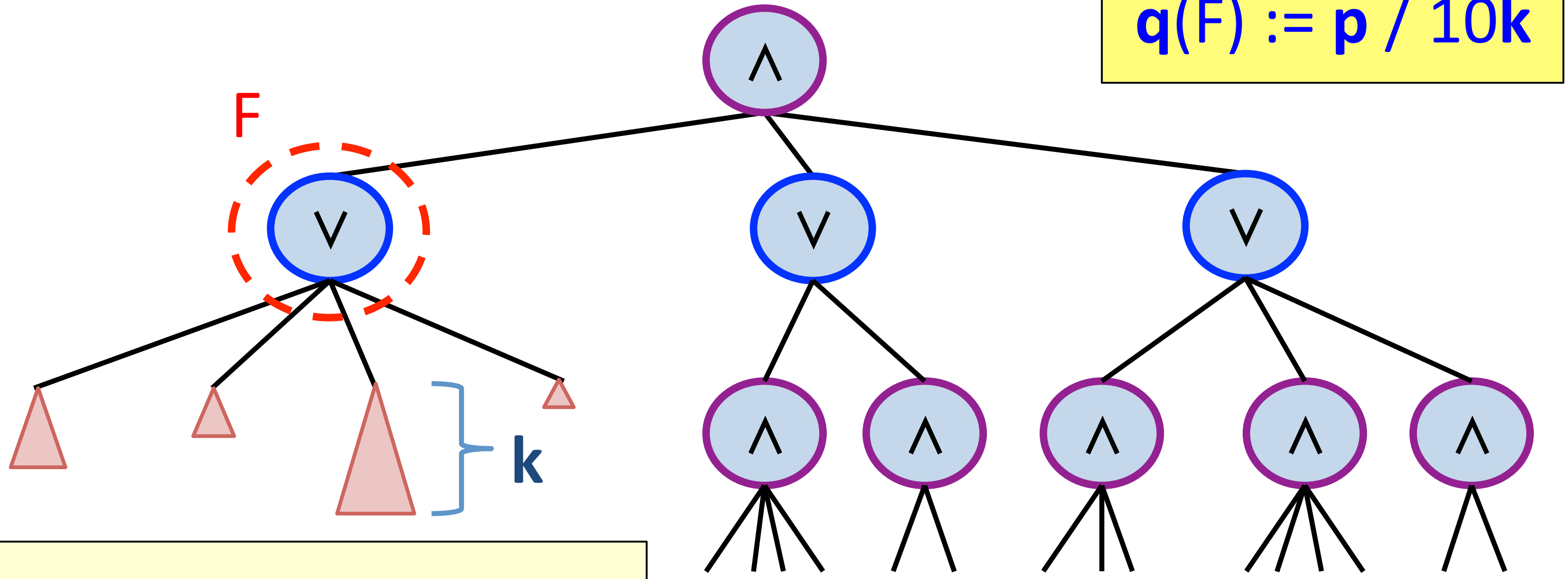


$\mathbf{k} := \max_i \mathrm{DT}_{\mathrm{depth}}(F_i \upharpoonright \mathbf{R_p})$

$\mathbf{p} := \min_i \mathbf{q}(F_i)$



$\mathbf{q}(F) := \mathbf{p} \,/\, 10\mathbf{k}$



$\mathbf{k} := \max_i \mathrm{DT}_{\mathrm{depth}}(F_i \upharpoonright \mathbf{R_p})$

Theorem [Hastad '86]

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

Theorem [R.'15]

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

Theorem [Hastad '86, Boppana '87]

Depth $d+1$ **circuits** of size S have average sensitivity $O(\log S)^d$

Theorem [R.'15]

Depth $d+1$ **formulas** of size S have average sensitivity $O((\log S)/d)^d$

$$\mathrm{AveSens}(f) := \mathop{\mathbb{E}}_{\mathbf{x} \in \{0,1\}^n} \#\{\, i \in [n] : f(\mathbf{x}) \neq f(\mathbf{x}^{(i)}) \,\}$$

Theorem [Hastad ’86, Boppana ‘87]

Depth $d+1$ **circuits** of size S have average sensitivity $O(\log S)^d$

Theorem [R.’15]

Depth $d+1$ **formulas** of size S have average sensitivity $O((\log S)/d)^d$

$$\mathrm{AveSens}(f) := \mathop{\mathbb{E}}_{\mathbf{x}\in\{0,1\}^n} \#\{\, i \in [n] : f(\mathbf{x}) \neq f(\mathbf{x}^{(i)}) \,\}$$

x with ith bit flipped

Proof of the Switching Lemma

DNF formula $F = C_1 \vee \cdots \vee C_m$

Each clause C_ℓ is a conjunction of literals (e.g. $x_1 \wedge \neg x_3 \wedge x_4$).

Easy observation: $\mathrm{AveSens}(\text{any } k\text{-DNF}) \leq 2k$ (in fact $\leq k$ [Amano 11])

We will show: $\mathrm{AveSens}(F) \leq 2\log(m+1)$

DNF formula $F = C_1 \vee \cdots \vee C_m$

Each clause C_ℓ is a conjunction of literals (e.g. $x_1 \wedge \neg x_3 \wedge x_4$).

Let $\widetilde{F} : \{0,1\}^n \to [m+1]$ be the "first witness function":

$$\widetilde{F}(x) := \begin{cases} \text{the index of the first satisfied clause} & \text{if } F(x) = 1, \\ m+1 & \text{if } F(x) = 0. \end{cases}$$

DNF formula $F = C_1 \vee \cdots \vee C_m$

Each clause C_ℓ is a conjunction of literals (e.g. $x_1 \wedge \neg x_3 \wedge x_4$).

Let $\widetilde{F} : \{0,1\}^n \to [m+1]$ be the "first witness function":

$$\widetilde{F}(x) := \begin{cases} \text{the index of the first satisfied clause} & \text{if } F(x) = 1, \\ m+1 & \text{if } F(x) = 0. \end{cases}$$

Claim. $\mathrm{AveSens}(F) \leq 2 \cdot \mathsf{H}(\widetilde{F}) \leq 2 \cdot \log(m+1)$

where $\mathsf{H}(\widetilde{F})$ is the entropy of the random variable $\widetilde{F}(\boldsymbol{x})$ where $\boldsymbol{x} \in_{\text{uniform}} \{0,1\}^n$

$$\begin{aligned}
\mathrm{AveSens}(F) &= \sum_{i\in[n]} \mathbb{P}\left[\, F(\boldsymbol{x}) \neq F(\boldsymbol{x}^{(i)}) \,\right] \\
&\leq \sum_{i\in[n]} \mathbb{P}\left[\, \widetilde{F}(\boldsymbol{x}) \neq \widetilde{F}(\boldsymbol{x}^{(i)}) \,\right] \\
&= \sum_{i\in[n]} 2\,\mathbb{P}\left[\, \widetilde{F}(\boldsymbol{x}) < \widetilde{F}(\boldsymbol{x}^{(i)}) \,\right] \\
&= \sum_{i\in[n]} 2 \sum_{\ell\in[m]} \mathbb{P}\left[\, \widetilde{F}(\boldsymbol{x}) = \ell \text{ and } \widetilde{F}(\boldsymbol{x}^{(i)}) > \ell \,\right] \\
&= 2 \sum_{\ell\in[m]} \mathbb{P}\left[\, \widetilde{F}(\boldsymbol{x}) = \ell \,\right] \sum_{i\in[n]} \underbrace{\mathbb{P}\left[\, \widetilde{F}(\boldsymbol{x}^{(i)}) > \ell \;\middle|\; \widetilde{F}(\boldsymbol{x}) = \ell \,\right]}_{\text{this probability is 0 unless } C_\ell \text{ contains } x_i \text{ or } \neg x_i}
\end{aligned}$$

$$
\begin{aligned}
\mathrm{AveSens}(F) &= \sum_{i\in[n]} \mathbb{P}\left[\, F(\boldsymbol{x}) \neq F(\boldsymbol{x}^{(i)}) \,\right] \\
&\leq \sum_{i\in[n]} \mathbb{P}\left[\, \widetilde{F}(\boldsymbol{x}) \neq \widetilde{F}(\boldsymbol{x}^{(i)}) \,\right] \\
&= \sum_{i\in[n]} 2\,\mathbb{P}\left[\, \widetilde{F}(\boldsymbol{x}) < \widetilde{F}(\boldsymbol{x}^{(i)}) \,\right] \\
&= \sum_{i\in[n]} 2 \sum_{\ell\in[m]} \mathbb{P}\left[\, \widetilde{F}(\boldsymbol{x}) = \ell \text{ and } \widetilde{F}(\boldsymbol{x}^{(i)}) > \ell \,\right] \\
&= 2 \sum_{\ell\in[m]} \mathbb{P}\left[\, \widetilde{F}(\boldsymbol{x}) = \ell \,\right] \sum_{i\in[n]} \mathbb{P}\left[\, \widetilde{F}(\boldsymbol{x}^{(i)}) > \ell \;\middle|\; \widetilde{F}(\boldsymbol{x}) = \ell \,\right] \\
&\leq 2 \sum_{\ell\in[m]} \mathbb{P}\left[\, \widetilde{F}(\boldsymbol{x}) = \ell \,\right] \cdot |\mathrm{Vars}(C_\ell)|
\end{aligned}
$$

$$
\begin{aligned}
\mathrm{AveSens}(F) &= \sum_{i\in[n]} \mathbb{P}\left[\, F(\boldsymbol{x}) \neq F(\boldsymbol{x}^{(i)}) \,\right] \\
&\leq \sum_{i\in[n]} \mathbb{P}\left[\, \widetilde{F}(\boldsymbol{x}) \neq \widetilde{F}(\boldsymbol{x}^{(i)}) \,\right] \\
&= \sum_{i\in[n]} 2\,\mathbb{P}\left[\, \widetilde{F}(\boldsymbol{x}) < \widetilde{F}(\boldsymbol{x}^{(i)}) \,\right] \\
&= \sum_{i\in[n]} 2 \sum_{\ell\in[m]} \mathbb{P}\left[\, \widetilde{F}(\boldsymbol{x}) = \ell \text{ and } \widetilde{F}(\boldsymbol{x}^{(i)}) > \ell \,\right] \\
&= 2 \sum_{\ell\in[m]} \mathbb{P}\left[\, \widetilde{F}(\boldsymbol{x}) = \ell \,\right] \sum_{i\in[n]} \mathbb{P}\left[\, \widetilde{F}(\boldsymbol{x}^{(i)}) > \ell \;\middle|\; \widetilde{F}(\boldsymbol{x}) = \ell \,\right] \\
&\leq 2 \sum_{\ell\in[m]} \mathbb{P}\left[\, \widetilde{F}(\boldsymbol{x}) = \ell \,\right] \cdot |\mathrm{Vars}(C_\ell)| \\
&\leq 2 \sum_{\ell\in[m]} \mathbb{P}\left[\, \widetilde{F}(\boldsymbol{x}) = \ell \,\right] \cdot \log\left(\frac{1}{\mathbb{P}[\, \widetilde{F}(\boldsymbol{x}) = \ell \,]}\right)
\end{aligned}
$$

$$
\left(\text{since } \mathbb{P}[\, \widetilde{F}(\boldsymbol{x}) = \ell \,] \leq \mathbb{P}[\, C_\ell(\boldsymbol{x}) = 1 \,] = 2^{-|\mathrm{Vars}(C_\ell)|}\right)
$$

$$
\begin{aligned}
\mathrm{AveSens}(F) &= \sum_{i\in[n]} \mathbb{P}\left[\, F(\boldsymbol{x}) \neq F(\boldsymbol{x}^{(i)}) \,\right] \\
&\leq \sum_{i\in[n]} \mathbb{P}\left[\, \widetilde{F}(\boldsymbol{x}) \neq \widetilde{F}(\boldsymbol{x}^{(i)}) \,\right] \\
&= \sum_{i\in[n]} 2\,\mathbb{P}\left[\, \widetilde{F}(\boldsymbol{x}) < \widetilde{F}(\boldsymbol{x}^{(i)}) \,\right] \\
&= \sum_{i\in[n]} 2 \sum_{\ell\in[m]} \mathbb{P}\left[\, \widetilde{F}(\boldsymbol{x}) = \ell \text{ and } \widetilde{F}(\boldsymbol{x}^{(i)}) > \ell \,\right] \\
&= 2 \sum_{\ell\in[m]} \mathbb{P}\left[\, \widetilde{F}(\boldsymbol{x}) = \ell \,\right] \sum_{i\in[n]} \mathbb{P}\left[\, \widetilde{F}(\boldsymbol{x}^{(i)}) > \ell \;\middle|\; \widetilde{F}(\boldsymbol{x}) = \ell \,\right] \\
&\leq 2 \sum_{\ell\in[m]} \mathbb{P}\left[\, \widetilde{F}(\boldsymbol{x}) = \ell \,\right] \cdot |\mathrm{Vars}(C_\ell)| \\
&\leq 2 \sum_{\ell\in[m]} \mathbb{P}\left[\, \widetilde{F}(\boldsymbol{x}) = \ell \,\right] \cdot \log\left(\frac{1}{\mathbb{P}[\, \widetilde{F}(\boldsymbol{x}) = \ell \,]}\right) \\
&\leq 2{\cdot}\mathsf{H}(\widetilde{F})
\end{aligned}
$$

DNF formula $F = C_1 \vee \cdots \vee C_m$

Switching Lemma. $\mathbb{P}[\ \mathsf{DT}_{\mathsf{depth}}(F{\upharpoonright}\boldsymbol{R}_p) \geq t\ ] = O(p \log m)^t$

DNF formula $F = C_1 \vee \cdots \vee C_m$

Switching Lemma. $\mathbb{P}[\ \mathsf{DT}_{\mathsf{depth}}(F{\upharpoonright}\boldsymbol{R}_p) \geq t\ ] = O(p \log m)^t$

Proof based on analysis of the ***canonical decision tree*** for $F{\upharpoonright}\boldsymbol{R}_p$. We actually show

$$\mathbb{P}[\ \text{CanonicalDT}(F{\upharpoonright}\boldsymbol{R}_p) \text{ has depth } t\ ] = O(p \log m)^t.$$

DNF formula $F = C_1 \vee \cdots \vee C_m$

Switching Lemma. $\mathbb{P}[\ \mathsf{DT}_{\mathsf{depth}}(F{\restriction}\boldsymbol{R}_p) \geq t\ ] = O(p \log m)^t$

High-level sketch

- $\mathrm{Bad}_t :=$ {restrictions ϱ such that $\mathrm{CanonicalDT}(F{\restriction}\varrho)$ has depth t}
- Suffices to show $\mathbb{P}[\ \boldsymbol{R}_p \in \mathrm{Bad}_t\ ] = O(p \log m)^t$
- For each $\varrho \in \mathrm{Bad}_t$, we define an extended restriction ϱ^* fixing t additional variables.
- $$\begin{aligned} \mathbb{P}[\ \boldsymbol{R}_p \in \mathrm{Bad}_t\ ] &= \sum_{\varrho \in \mathrm{Bad}_t} \mathbb{P}[\ \boldsymbol{R}_p = \varrho\ ] \\ &= \sum_{\varrho \in \mathrm{Bad}_t} \left(\tfrac{2p}{1-p}\right)^t \mathbb{P}[\ \boldsymbol{R}_p = \varrho^*\ ] \\ &= \sum_{\sigma} \left(\tfrac{2p}{1-p}\right)^t \mathbb{P}[\ \boldsymbol{R}_p = \sigma\ ] \cdot |\{\varrho \in \mathrm{Bad}_t : \varrho^* = \sigma\}| \\ &= \left(\tfrac{2p}{1-p}\right)^t \mathbb{E}\,|\{\varrho \in \mathrm{Bad}_t : \varrho^* = \boldsymbol{R}_p\}| \end{aligned}$$

DNF formula $F = C_1 \vee \cdots \vee C_m$

Switching Lemma. $\mathbb{P}[\ \mathsf{DT}_{\mathsf{depth}}(F{\upharpoonright}\boldsymbol{R}_p) \geq t\ ] = O(p \log m)^t$

High-level sketch

- $\mathrm{Bad}_t :=$ {restrictions ϱ such that $\mathrm{CanonicalDT}(F{\upharpoonright}\varrho)$ has depth t}
- Suffices to show $\mathbb{P}[\ \boldsymbol{R}_p \in \mathrm{Bad}_t\ ] = O(p \log m)^t$
- For each $\varrho \in \mathrm{Bad}_t$, we define an extended restriction ϱ^* fixing t additional variables.
- $\mathbb{P}[\ \boldsymbol{R}_p \in \mathrm{Bad}_t\ ] = O(p)^t \cdot \mathbb{E}\,|\{\varrho \in \mathrm{Bad}_t : \varrho^* = \boldsymbol{R}_p\}|$

DNF formula $F = C_1 \vee \cdots \vee C_m$

Switching Lemma. $\mathbb{P}[\ \mathsf{DT}_{\mathsf{depth}}(F\upharpoonright \boldsymbol{R}_p) \geq t\ ] = O(p \log m)^t$

HIGH-LEVEL SKETCH

- $\mathrm{Bad}_t :=$ {restrictions ϱ such that $\mathrm{CanonicalDT}(F\upharpoonright\varrho)$ has depth t}
- Suffices to show $\mathbb{P}[\ \boldsymbol{R}_p \in \mathrm{Bad}_t\ ] = O(p \log m)^t$
- For each $\varrho \in \mathrm{Bad}_t$, we define an extended restriction ϱ^* fixing t additional variables.
- $\mathbb{P}[\ \boldsymbol{R}_p \in \mathrm{Bad}_t\ ] = O(p)^t \cdot \mathbb{E}\,|\{\varrho \in \mathrm{Bad}_t : \varrho^* = \boldsymbol{R}_p\}|$
- Finally, we show

$$\mathbb{E}\,|\{\varrho \in \mathrm{Bad}_t : \varrho^* = \boldsymbol{R}_p\}| = O(\log m)^t.$$

(Argument is similar to $\mathrm{AveSens}(F) \leq 2{\cdot}\mathsf{H}(\widetilde{F})$, but rather than entropy we use Jensen's inequality for the concave function $x \mapsto (\frac{1}{t}\ln(x) + 1)^t$.)

DNF formula $F = C_1 \vee \cdots \vee C_m$

Switching Lemma. $\mathbb{P}[\ \mathsf{DT}_{\mathsf{depth}}(F{\upharpoonright}\boldsymbol{R}_p) \geq t\ ] = O(p \log m)^t$

High-level sketch

- $\mathrm{Bad}_t :=$ {restrictions ϱ such that $\mathrm{CanonicalDT}(F{\upharpoonright}\varrho)$ has depth t}
- Suffices to show $\mathbb{P}[\ \boldsymbol{R}_p \in \mathrm{Bad}_t\ ] = O(p \log m)^t$
- For each $\varrho \in \mathrm{Bad}_t$, we define an extended restriction ϱ^* fixing t additional variables.
- $\mathbb{P}[\ \boldsymbol{R}_p \in \mathrm{Bad}_t\ ] = O(p)^t \cdot \mathbb{E}\,|\{\varrho \in \mathrm{Bad}_t : \varrho^* = \boldsymbol{R}_p\}|$
- If F has width k, we get **Håstad's Switching Lemma**:

  The map $\varrho \mapsto \varrho^*$ is $O(k)^t$-to-1 over Bad_t.

  Therefore, $\mathbb{E}\,|\{\varrho \in \mathrm{Bad}_t : \varrho^* = \boldsymbol{R}_p\}| = O(k)^t$.

  Therefore, $\mathbb{P}[\ \boldsymbol{R}_p \in \mathrm{Bad}_t\ ] = O(pk)^t$.

DNF formula $F = C_1 \vee \cdots \vee C_m, \quad V_\ell := \mathrm{Vars}(C_\ell)$

DNF formula $F = C_1 \vee \cdots \vee C_m, \quad V_\ell := \mathrm{Vars}(C_\ell)$

Canonical decision tree $\mathrm{CanonicalDT}(F{\upharpoonright}\varrho)$**:**

- If any clause is satisfied (forced to 1) by ϱ, output 1.
- If all clauses are falsified (forced to 0) by ϱ, output 0.
- Otherwise:

  Let $\ell \in [m]$ be the index of the first "relevant" clause C_ℓ not forced by ϱ.

  Let $s \geq 1$ be the number of surviving variables of $C_\ell{\upharpoonright}\varrho$.

  Let $Q \in \binom{V_\ell}{s}$ be the set of surviving variables of $C_\ell{\upharpoonright}\varrho$.

  Query the variables of Q in order, receiving answers $A \in \{0,1\}^s$.

  Proceed as $\mathrm{CanonicalDT}(F{\upharpoonright}\varrho \cup \{Q \leftarrow A\})$.

  (Obs: C_ℓ is forced to 0 or 1 by $\varrho \cup \{Q \leftarrow A\}$, so this process eventually terminates.)

DNF formula $F = C_1 \vee \cdots \vee C_m, \quad V_\ell := \mathrm{Vars}(C_\ell)$

Branch data. Each branch of $\mathrm{CanonicalDT}(F{\upharpoonright}\varrho)$ of length t (with t total queries) is characterized by:

- $r \in \{1, \ldots, t\}$ # of relevant clauses
- $\ell_i \in [m] \quad (1 \leq \ell_1 < \cdots < \ell_r \leq m)$ location of i^{th} relevant clause
- $s_i \geq 1 \quad (s_1 + \cdots + s_r = t)$ # of queried variables from C_{ℓ_i}
- $Q_i \in \binom{V_{\ell_i} \setminus (V_{\ell_1} \cup \cdots \cup V_{\ell_{i-1}})}{s_i}$ set of queried variables from C_{ℓ_i}
- $A_i \in \{0,1\}^{s_i}$ answers to queries Q_i

DNF formula $F = C_1 \vee \cdots \vee C_m, \quad V_\ell := \mathrm{Vars}(C_\ell)$

Branch data. Each branch of $\mathrm{CanonicalDT}(F{\restriction}\varrho)$ of length t (with t total queries) is characterized by:

- $r \in \{1, \ldots, t\}$ # of relevant clauses
- $\ell_i \in [m] \quad (1 \le \ell_1 < \cdots < \ell_r \le m)$ location of i^{th} relevant clause
- $s_i \ge 1 \quad (s_1 + \cdots + s_r = t)$ # of queried variables from C_{ℓ_i}
- $Q_i \in \binom{V_{\ell_i} \setminus (V_{\ell_1} \cup \cdots \cup V_{\ell_{i-1}})}{s_i}$ set of queried variables from C_{ℓ_i}
- $A_i \in \{0,1\}^{s_i}$ answers to queries Q_i

(i.e., surviving variables of $C_{\ell_i}{\restriction}_{Q_1 \leftarrow A_1, \ldots, Q_{i-1} \leftarrow A_{i-1}}$)

DNF formula $F = C_1 \vee \cdots \vee C_m, \quad V_\ell := \mathrm{Vars}(C_\ell)$

Branch data. Each branch of $\mathsf{CanonicalDT}(F{\upharpoonright}\varrho)$ of length t (with t total queries) is characterized by:

• $r \in \{1, \dots, t\}$	# of relevant clauses
• $\ell_i \in [m] \quad (1 \le \ell_1 < \cdots < \ell_r \le m)$	location of i^{th} relevant clause
• $s_i \ge 1 \quad (s_1 + \cdots + s_r = t)$	# of queried variables from C_{ℓ_i}
• $Q_i \in \binom{V_{\ell_i} \setminus (V_{\ell_1} \cup \cdots \cup V_{\ell_{i-1}})}{s_i}$	set of queried variables from C_{ℓ_i}
• $A_i \in \{0,1\}^{s_i}$	answers to queries Q_i

The map $\varrho \mapsto \varrho^*$. Let $(\vec{\ell}, \vec{s}, \vec{Q}, \vec{A})$ be the data associated with the longest branch of $\mathsf{CanonicalDT}(F{\upharpoonright}\varrho)$. Then

$$\varrho^* := \varrho \cup \{Q_1 \leftarrow A_1^*, \dots, Q_r \leftarrow A_r^*\}$$

where A_i^* are the unique answers to queries Q_i consistent with clause C_{ℓ_i}.

$\varrho \mapsto \varrho^*$

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

$\varrho \quad = \{\, x_1 \mapsto 1,\ x_4 \mapsto 0 \,\}$

$\varrho^* = \{\, x_1 \mapsto 1,\ x_4 \mapsto 0,\ \ldots \,\}$

$\varrho \mapsto \varrho^*$

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

$\varrho \;\;= \{\, x_1 \mapsto 1,\, x_4 \mapsto 0 \,\}$

$\varrho^* = \{\, x_1 \mapsto 1,\, x_4 \mapsto 0,\, \ldots \,\}$

$\varrho \mapsto \varrho^*$

$$F = \overset{1}{x_1}\, x_2\, \neg x_3 \vee \cancel{\overset{0}{\neg x_1}\, x_3\, x_5} \vee x_2\, \overset{1}{\neg x_4}\, x_5 \vee \cancel{x_3\, \overset{0}{x_4}\, \neg x_6} \vee \overset{1}{x_1}\, \overset{1}{\neg x_4}\, \neg x_7$$

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

$\varrho^* = \{ x_1 \mapsto 1, x_4 \mapsto 0, \ldots \}$

$\varrho \mapsto \varrho^*$

$$F = \overset{1}{x_1}\; x_2\; \neg x_3 \;\vee\; \cancel{\overset{0}{\neg x_1}\; x_3\; x_5} \;\vee\; x_2\; \overset{1}{\neg x_4}\; x_5 \;\vee\; \cancel{x_3\; \overset{0}{x_4}\; \neg x_6} \;\vee\; \overset{1}{x_1}\; \overset{1}{\neg x_4}\; \neg x_7$$

$\varrho \;\;= \{\, x_1 \mapsto 1,\, x_4 \mapsto 0 \,\}$

$\varrho^* = \{\, x_1 \mapsto 1,\, x_4 \mapsto 0,\, \ldots \,\}$

$\ell_1 = 1$

$s_1 = 2$

$Q_1 = \{\, x_2, x_3 \,\}$

$\varrho \mapsto \varrho^*$

$$F = (\overset{1}{x_1}\ x_2\ \neg x_3) \vee \cancel{\overset{0}{\neg x_1}\ x_3\ x_5} \vee x_2\ \overset{1}{\neg x_4}\ x_5 \vee \cancel{x_3\ \overset{0}{x_4}\ \neg x_6} \vee \overset{1}{x_1}\ \overset{1}{\neg x_4}\ \neg x_7$$

$\varrho \;\; = \{\, x_1 \mapsto 1,\ x_4 \mapsto 0 \,\}$

$\varrho^* = \{\, x_1 \mapsto 1,\ x_4 \mapsto 0,\ \ldots \,\}$

$\ell_1 = 1$

$s_1 = 2$

$Q_1 = \{\, x_2, x_3 \,\}$

$A_1 = \{\, x_2 \mapsto 1,\ x_3 \mapsto 1 \,\}$

✓

$$\varrho \mapsto \varrho^*$$

$$F = \overset{1}{x_1}\ \overset{1}{x_2}\ \overset{1}{\neg x_3} \lor \cancel{\overset{0}{\neg x_1}\ x_3\ x_5} \lor x_2\ \overset{1}{\neg x_4}\ x_5 \lor \cancel{x_3\ \overset{0}{x_4}\ \neg x_6} \lor \overset{1}{x_1}\ \overset{1}{\neg x_4}\ \neg x_7$$

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

$\varrho^* = \{ x_1 \mapsto 1, x_4 \mapsto 0, x_2 \mapsto 1, x_3 \mapsto 0, \ldots \}$

$\ell_1 = 1$

$s_1 = 2$

$Q_1 = \{ x_2, x_3 \}$

$A_1 = \{ x_2 \mapsto 1, x_3 \mapsto 1 \}$

$A_1{}^* = \{ x_2 \mapsto 1, x_3 \mapsto 0 \}$

$\varrho \mapsto \varrho^*$

$$F = \overset{1}{x_1}\ \overset{1}{x_2}\ \overset{0}{\neg x_3} \lor \cancel{\overset{0}{\neg x_1}\ x_3\ x_5} \lor \overset{1}{x_2}\ \overset{1}{\neg x_4}\ x_5 \lor \cancel{x_3\ \overset{0}{x_4}\ \neg x_6} \lor \overset{1}{x_1}\ \overset{1}{\neg x_4}\ \neg x_7$$

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

$$\varrho^* = \{\, x_1 \mapsto 1,\ x_4 \mapsto 0,\ x_2 \mapsto 1,\ x_3 \mapsto 0,\ \ldots \,\}$$

$$\ell_1 = 1$$

$$s_1 = 2$$

$$Q_1 = \{\, x_2, x_3 \,\}$$

$$A_1 = \{\, x_2 \mapsto 1,\ x_3 \mapsto 1 \,\}$$

$\varrho \mapsto \varrho^*$

$$F = \cancel{\overset{1}{x_1}\,\overset{1}{x_2}\,\overset{0}{\neg x_3}} \vee \cancel{\overset{0}{\neg x_1}\,x_3\,x_5} \vee (\overset{1}{x_2}\,\overset{1}{\neg x_4}\,x_5) \vee \cancel{x_3\,\overset{0}{x_4}\,\neg x_6} \vee \overset{1}{x_1}\,\overset{1}{\neg x_4}\,\neg x_7$$

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

$\varrho^* = \{ x_1 \mapsto 1, x_4 \mapsto 0, x_2 \mapsto 1, x_3 \mapsto 0, \ldots \}$

$\ell_1 = 1$

$s_1 = 2$

$Q_1 = \{ x_2, x_3 \}$

$A_1 = \{ x_2 \mapsto 1, x_3 \mapsto 1 \}$

$\varrho \mapsto \varrho^*$

$$F = \cancel{\overset{1}{x_1}\,\overset{1}{x_2}\,\overset{0}{\neg x_3}} \lor \cancel{\overset{0}{\neg x_1}\,x_3\,x_5} \lor \overset{1}{x_2}\,\overset{1}{\neg x_4}\,x_5 \lor \cancel{x_3\,\overset{0}{x_4}\,\neg x_6} \lor \overset{1}{x_1}\,\overset{1}{\neg x_4}\,\neg x_7$$

$\varrho \;\; = \{\, x_1 \mapsto 1,\, x_4 \mapsto 0 \,\}$

$\varrho^* = \{\, x_1 \mapsto 1,\, x_4 \mapsto 0,\, x_2 \mapsto 1,\, x_3 \mapsto 0,\, \ldots \,\}$

$\ell_1 = 1$	$\ell_2 = 3$
$s_1 = 2$	$s_2 = 1$
$Q_1 = \{\, x_2, x_3 \,\}$	$Q_2 = \{\, x_5 \,\}$
$A_1 = \{\, x_2 \mapsto 1,\, x_3 \mapsto 1 \,\}$	

$$\varrho \mapsto \varrho^*$$

$$F = \cancel{\overset{1}{x_1}\,\overset{1}{x_2}\,\overset{0}{\neg x_3}} \lor \cancel{\overset{0}{\neg x_1}\,x_3\,x_5} \lor (\overset{1}{x_2}\,\overset{1}{\neg x_4}\,x_5) \lor \cancel{\overset{0}{x_3}\,x_4\,\neg x_6} \lor \overset{1}{x_1}\,\overset{1}{\neg x_4}\,\neg x_7$$

$\varrho \;\; = \{\, x_1 \mapsto 1,\, x_4 \mapsto 0 \,\}$

$\varrho^* = \{\, x_1 \mapsto 1,\, x_4 \mapsto 0,\, x_2 \mapsto 1,\, x_3 \mapsto 0,\, \ldots \,\}$

$\ell_1 = 1$	$\ell_2 = 3$
$s_1 = 2$	$s_2 = 1$
$Q_1 = \{\, x_2, x_3 \,\}$	$Q_2 = \{\, x_5 \,\}$
$A_1 = \{\, x_2 \mapsto 1,\, x_3 \mapsto 1 \,\}$	$A_2 = \{\, x_5 \mapsto 0 \,\}$

$\varrho \mapsto \varrho^*$ ✓

$$F = \cancel{\overset{1}{x_1}\,\overset{1}{x_2}\,\overset{0}{\neg x_3}} \lor \cancel{\overset{0}{\neg x_1}\,x_3\,x_5} \lor \overset{1}{x_2}\,\overset{1}{\neg x_4}\,\overset{1}{x_5} \lor \cancel{\overset{0}{x_3}\,x_4\,\neg x_6} \lor \overset{1}{x_1}\,\overset{1}{\neg x_4}\,\neg x_7$$

$\varrho \;= \{\, x_1 \mapsto 1,\ x_4 \mapsto 0 \,\}$

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

$\ell_1 = 1$	$\ell_2 = 3$
$s_1 = 2$	$s_2 = 1$
$Q_1 = \{\, x_2, x_3 \,\}$	$Q_2 = \{\, x_5 \,\}$
$A_1 = \{\, x_2 \mapsto 1,\ x_3 \mapsto 1 \,\}$	$A_2 = \{\, x_5 \mapsto 0 \,\}$
	$A_2^* = \{\, x_5 \mapsto 1 \,\}$

DNF formula $F = C_1 \vee \cdots \vee C_m, \quad V_\ell := \mathrm{Vars}(C_\ell)$

$$\varrho^* := \varrho \cup \{Q_1 \leftarrow A_1^*, \ldots, Q_r \leftarrow A_r^*\}$$

DNF formula $F = C_1 \vee \cdots \vee C_m, \quad V_\ell := \mathrm{Vars}(C_\ell)$

$$\varrho^* := \varrho \cup \{Q_1 \leftarrow A_1^*, \dots, Q_r \leftarrow A_r^*\}$$

Key observation. Given knowledge of ϱ^* and $(\vec{s}, \vec{Q}, \vec{A})$, we can recover ϱ (as well as relevant clause indices $\vec{\ell}$) as follows:

DNF formula $F = C_1 \vee \cdots \vee C_m, \quad V_\ell := \mathrm{Vars}(C_\ell)$

$$\varrho^* := \varrho \cup \{Q_1 \leftarrow A_1^*, \ldots, Q_r \leftarrow A_r^*\}$$

Key observation. Given knowledge of ϱ^* and $(\vec{s}, \vec{Q}, \vec{A})$, we can recover ϱ (as well as relevant clause indices $\vec{\ell}$) as follows:

$$\begin{aligned} C_1, \ldots, C_{\ell_1 - 1} \restriction \varrho^* &\equiv 0 \\ C_{\ell_1} \restriction \varrho^* &\equiv 1 \end{aligned}$$

DNF formula $F = C_1 \vee \cdots \vee C_m, \quad V_\ell := \mathrm{Vars}(C_\ell)$

$$\varrho^* := \varrho \cup \{Q_1 \leftarrow A_1^*, \ldots, Q_r \leftarrow A_r^*\}$$

Key observation. Given knowledge of ϱ^* and $(\vec{s}, \vec{Q}, \vec{A})$, we can recover ϱ (as well as relevant clause indices $\vec{\ell}$) as follows:

$$\begin{aligned} C_1, \ldots, C_{\ell_1 - 1} {\restriction} \varrho^* &\equiv 0 \\ C_{\ell_1} {\restriction} \varrho^* &\equiv 1 \\ C_{\ell_1 + 1}, \ldots, C_{\ell_2 - 1} {\restriction} \varrho^{*(Q_1 \leftarrow A_1)} &\equiv 0 \\ C_{\ell_2} {\restriction} \varrho^{*(Q_1 \leftarrow A_1)} &\equiv 1 \end{aligned}$$

DNF formula $F = C_1 \vee \cdots \vee C_m, \quad V_\ell := \mathrm{Vars}(C_\ell)$

$$\varrho^* := \varrho \cup \{Q_1 \leftarrow A_1^*, \ldots, Q_r \leftarrow A_r^*\}$$

Key observation. Given knowledge of ϱ^* and $(\vec{s}, \vec{Q}, \vec{A})$, we can recover ϱ (as well as relevant clause indices $\vec{\ell}$) as follows:

$$\begin{aligned}
C_1, \ldots, C_{\ell_1 - 1} \restriction \varrho^* &\equiv 0 \\
C_{\ell_1} \restriction \varrho^* &\equiv 1 \\
C_{\ell_1 + 1}, \ldots, C_{\ell_2 - 1} \restriction \varrho^{*(Q_1 \leftarrow A_1)} &\equiv 0 \\
C_{\ell_2} \restriction \varrho^{*(Q_1 \leftarrow A_1)} &\equiv 1 \\
&\vdots \\
C_{\ell_{r-1}+1}, \ldots, C_{\ell_r - 1} \restriction \varrho^{*(Q_1 \leftarrow A_1, \ldots, Q_{r-1} \leftarrow A_{r-1})} &\equiv 0 \\
C_{\ell_r} \restriction \varrho^{*(Q_1 \leftarrow A_1, \ldots, Q_{r-1} \leftarrow A_{r-1})} &\equiv 1
\end{aligned}$$

DNF formula $F = C_1 \vee \cdots \vee C_m$, $\quad V_\ell := \mathrm{Vars}(C_\ell)$

$$\varrho^* := \varrho \cup \{Q_1 \leftarrow A_1^*, \ldots, Q_r \leftarrow A_r^*\}$$

Key observation. Given knowledge of ϱ^* and $(\vec{s}, \vec{Q}, \vec{A})$, we can recover ϱ (as well as relevant clause indices $\vec{\ell}$) as follows:

$$\begin{aligned}
C_1, \ldots, C_{\ell_1 - 1} \upharpoonright \varrho^* &\equiv 0 \\
C_{\ell_1} \upharpoonright \varrho^* &\equiv 1 \\
C_{\ell_1 + 1}, \ldots, C_{\ell_2 - 1} \upharpoonright \varrho^{*(Q_1 \leftarrow A_1)} &\equiv 0 \\
C_{\ell_2} \upharpoonright \varrho^{*(Q_1 \leftarrow A_1)} &\equiv 1 \\
&\vdots \\
C_{\ell_{r-1}+1}, \ldots, C_{\ell_r - 1} \upharpoonright \varrho^{*(Q_1 \leftarrow A_1, \ldots, Q_{r-1} \leftarrow A_{r-1})} &\equiv 0 \\
C_{\ell_r} \upharpoonright \varrho^{*(Q_1 \leftarrow A_1, \ldots, Q_{r-1} \leftarrow A_{r-1})} &\equiv 1
\end{aligned}$$

Therefore, the map $\varrho \mapsto (\varrho^*, \vec{s}, \vec{Q}, \vec{A})$ is 1-to-1.

DNF formula $F = C_1 \vee \cdots \vee C_m, \quad V_\ell := \mathrm{Vars}(C_\ell)$

$$\varrho^* := \varrho \cup \{Q_1 \leftarrow A_1^*, \ldots, Q_r \leftarrow A_r^*\}$$

Håstad's Switching Lemma. Assume F has width k.

DNF formula $F = C_1 \vee \cdots \vee C_m, \quad V_\ell := \mathrm{Vars}(C_\ell)$

$$\varrho^* := \varrho \cup \{Q_1 \leftarrow A_1^*, \ldots, Q_r \leftarrow A_r^*\}$$

Håstad's Switching Lemma. Assume F has width k.

- Instead of Q_i (the ***set*** of queried variables from C_{ℓ_i}), it suffices to know $Q'_i \in \binom{[k]}{s_i}$ (the ***location*** of queried variables within C_{ℓ_i}).

  Therefore, $\varrho \mapsto (\varrho^*, \vec{s}, \vec{Q}', \vec{A})$ is 1-to-1.

- There are only $O(k)^t$ possibilities for data $(\vec{s}, \vec{Q}', \vec{A})$ when $\varrho \in \mathrm{Bad}_t$.

  Therefore, $\varrho \mapsto \varrho^*$ is $O(k)^t$-to-1 over Bad_t.

  Therefore, $\mathbb{E}\,|\{\varrho \in \mathrm{Bad}_t : \varrho^* = \boldsymbol{R}_p\}| = O(k)^t$.

- As noted before, this implies

$$\mathbb{P}[\ \mathsf{DT}_{\mathsf{depth}}(F{\restriction}\boldsymbol{R}_p) \geq t\ ] = O(pk)^t$$

DNF formula $F = C_1 \vee \cdots \vee C_m, \quad V_\ell := \mathrm{Vars}(C_\ell)$

$$\varrho^* := \varrho \cup \{Q_1 \leftarrow A_1^*, \ldots, Q_r \leftarrow A_r^*\}$$

Håstad's Switching Lemma. ~~Assume F has width k.~~

We will show

$$\mathbb{E}\,|\{\varrho \in \mathrm{Bad}_t : \varrho^* = \boldsymbol{R}_p\}| = O(\log m)^t$$

Claim. $\mathbb{E}\,|\{\varrho \in \mathrm{Bad}_t : \varrho^* = \boldsymbol{R}_p\}| = O(\log m)^t$

We have

$$\underset{\boldsymbol{\sigma}\sim\boldsymbol{R}_p}{\mathbb{E}} |\{\varrho \in \mathrm{Bad}_t : \varrho^* = \boldsymbol{\sigma}\}|$$

$$= \sum_{\substack{\text{encoding data } (\vec{\ell},\vec{s},\vec{Q},\vec{A}) \\ \text{for branches of length } t}} \mathbb{P}\left[\begin{array}{l} \exists \varrho \in \mathrm{Bad}_t \text{ s.t. } \varrho^* = \boldsymbol{\sigma} \\ \text{with data } (\vec{\ell}, \vec{s}, \vec{Q}, \vec{A}) \end{array}\right]$$

Claim. $\mathbb{E}\,|\{\varrho \in \mathrm{Bad}_t : \varrho^* = \boldsymbol{R}_p\}| = O(\log m)^t$

We have

$$\begin{aligned}
&\mathop{\mathbb{E}}_{\boldsymbol{\sigma}\sim\boldsymbol{R}_p} |\{\varrho \in \mathrm{Bad}_t : \varrho^* = \boldsymbol{\sigma}\}| \\
&\qquad \le \sum_{(\vec{\ell},\vec{s},\vec{Q},\vec{A})} \mathbb{P}\left[\begin{array}{r} C_1,\ldots,C_{\ell_1-1}{\restriction}\boldsymbol{\sigma} \equiv 0 \\ C_{\ell_1}{\restriction}\boldsymbol{\sigma} \equiv 1 \\ C_{\ell_1+1},\ldots,C_{\ell_2-1}{\restriction}\boldsymbol{\sigma}^{(Q_1\leftarrow A_1)} \equiv 0 \\ C_{\ell_2}{\restriction}\boldsymbol{\sigma}^{(Q_1\leftarrow A_1)} \equiv 1 \\ \vdots \\ C_{\ell_r}{\restriction}\boldsymbol{\sigma}^{(Q_1\leftarrow A_1,\ldots,Q_{r-1}\leftarrow A_{r-1})} \equiv 1 \end{array}\right]
\end{aligned}$$

Claim. $\mathbb{E}\,|\{\varrho \in \mathrm{Bad}_t : \varrho^* = \boldsymbol{R}_p\}| = O(\log m)^t$

We have

$$\begin{aligned}
&\mathop{\mathbb{E}}_{\boldsymbol{\sigma}\sim\boldsymbol{R}_p} |\{\varrho \in \mathrm{Bad}_t : \varrho^* = \boldsymbol{\sigma}\}| \\
&\quad\le \sum_{(\vec{\ell},\vec{s},\vec{Q},\vec{A})} \mathbb{P}\left[\begin{array}{r}
C_1, \ldots, C_{\ell_1 - 1}\restriction\boldsymbol{\sigma} \equiv 0 \\
C_{\ell_1}\restriction\boldsymbol{\sigma} \equiv 1 \\
C_{\ell_1+1}, \ldots, C_{\ell_2 - 1}\restriction\boldsymbol{\sigma}^{(Q_1\leftarrow A_1)} \equiv 0 \\
C_{\ell_2}\restriction\boldsymbol{\sigma}^{(Q_1\leftarrow A_1)} \equiv 1 \\
\vdots\; \\
C_{\ell_r}\restriction\boldsymbol{\sigma}^{(Q_1\leftarrow A_1,\ldots,Q_{r-1}\leftarrow A_{r-1})} \equiv 1
\end{array}\right] \\
&\quad= \sum_{\substack{s_1+\cdots+s_r=t \\ \vec{A}\in\{0,1\}^t}} \sum_{(\vec{\ell},\vec{Q})} \mathbb{P}[\;''\;]
\end{aligned}$$

Claim. $\mathbb{E}\,|\{\varrho \in \mathrm{Bad}_t : \varrho^* = \boldsymbol{R}_p\}| = O(\log m)^t$

We have

$$
\begin{aligned}
&\mathop{\mathbb{E}}_{\boldsymbol{\sigma} \sim \boldsymbol{R}_p} |\{\varrho \in \mathrm{Bad}_t : \varrho^* = \boldsymbol{\sigma}\}| \\
&\qquad \le \sum_{(\vec{\ell},\vec{s},\vec{Q},\vec{A})} \mathbb{P}\left[\begin{array}{r}
C_1, \ldots, C_{\ell_1 - 1}\restriction \boldsymbol{\sigma} \equiv 0 \\
C_{\ell_1}\restriction \boldsymbol{\sigma} \equiv 1 \\
C_{\ell_1+1}, \ldots, C_{\ell_2 - 1}\restriction \boldsymbol{\sigma}^{(Q_1 \leftarrow A_1)} \equiv 0 \\
C_{\ell_2}\restriction \boldsymbol{\sigma}^{(Q_1 \leftarrow A_1)} \equiv 1 \\
\vdots \\
C_{\ell_r}\restriction \boldsymbol{\sigma}^{(Q_1 \leftarrow A_1, \ldots, Q_{r-1} \leftarrow A_{r-1})} \equiv 1
\end{array}\right] \\
&\qquad = \sum_{\substack{s_1+\cdots+s_r=t \\ \vec{A}\in\{0,1\}^t}} \sum_{(\vec{\ell},\vec{Q})} \mathbb{P}[\,''\,] \\
&\qquad \le 4^t \max_{\substack{s_1+\cdots+s_r=t \\ \vec{A}\in\{0,1\}^t}} \sum_{(\vec{\ell},\vec{Q})} \mathbb{P}[\,''\,] \qquad \text{(we can ignore factors of } O(1)^t\text{)}
\end{aligned}
$$

Claim. $\mathbb{E}\,|\{\varrho \in \mathrm{Bad}_t : \varrho^* = \boldsymbol{R}_p\}| = O(\log m)^t$

Fix any partition $s_1 + \cdots + s_r = t$ and answer sequence $\vec{A} \in \{0,1\}^t$.

It suffices to show

$$\sum_{(\vec{\ell},\vec{Q})} \mathbb{P}\left[\begin{array}{r} C_1, \ldots, C_{\ell_1 - 1}\restriction\boldsymbol{\sigma} \equiv 0 \\ C_{\ell_1}\restriction\boldsymbol{\sigma} \equiv 1 \\ C_{\ell_1+1}, \ldots, C_{\ell_2 - 1}\restriction\boldsymbol{\sigma}^{(Q_1 \leftarrow A_1)} \equiv 0 \\ C_{\ell_2}\restriction\boldsymbol{\sigma}^{(Q_1 \leftarrow A_1)} \equiv 1 \\ \vdots \\ C_{\ell_r}\restriction\boldsymbol{\sigma}^{(Q_1 \leftarrow A_1, \ldots, Q_{r-1} \leftarrow A_{r-1})} \equiv 1 \end{array}\right] = O(\log m)^t.$$

Claim. $\mathbb{E}\,|\{\varrho \in \mathrm{Bad}_t : \varrho^* = \boldsymbol{R}_p\}| = O(\log m)^t$

Fix any partition $s_1 + \cdots + s_r = t$ and answer sequence $\vec{A} \in \{0,1\}^t$.

It suffices to show

$$\sum_{(\vec{\ell},\vec{Q})} \mathbb{P}\left[\begin{array}{r} C_1, \ldots, C_{\ell_1 - 1} \restriction \boldsymbol{\sigma} \equiv 0 \\ C_{\ell_1} \restriction \boldsymbol{\sigma} \equiv 1 \\ C_{\ell_1+1}, \ldots, C_{\ell_2 - 1} \restriction \boldsymbol{\sigma}^{(Q_1 \leftarrow A_1)} \equiv 0 \\ C_{\ell_2} \restriction \boldsymbol{\sigma}^{(Q_1 \leftarrow A_1)} \equiv 1 \\ \vdots \quad \\ C_{\ell_r} \restriction \boldsymbol{\sigma}^{(Q_1 \leftarrow A_1, \ldots, Q_{r-1} \leftarrow A_{r-1})} \equiv 1 \end{array}\right] = O(\log m)^t.$$

Obs. Given $\ell_1, \ldots, \ell_r$, the number of choices for $Q_1, \ldots, Q_r$ is

$$\binom{|V_{\ell_1}|}{s_1}\binom{|V_{\ell_2} \setminus V_{\ell_1}|}{s_2} \cdots \binom{|V_{\ell_r} \setminus (V_{\ell_1} \cup \cdots \cup V_{\ell_{r-1}})|}{s_r}$$
$$\le \binom{|V_{\ell_1} \cup \cdots \cup V_{\ell_r}|}{t} \le \left(\frac{e|V_{\ell_1} \cup \cdots \cup V_{\ell_r}|}{t}\right)^t$$

We have

$$\sum_{(\vec{\ell},\vec{Q})} \mathbb{P}\left[\begin{aligned} C_1,\dots,C_{\ell_1-1}\restriction\boldsymbol{\sigma} &\equiv 0\\ C_{\ell_1}\restriction\boldsymbol{\sigma} &\equiv 1\\ C_{\ell_1+1},\dots,C_{\ell_2-1}\restriction\boldsymbol{\sigma}^{(Q_1\leftarrow A_1)} &\equiv 0\\ C_{\ell_2}\restriction\boldsymbol{\sigma}^{(Q_1\leftarrow A_1)} &\equiv 1\\ &\vdots\\ C_{\ell_r}\restriction\boldsymbol{\sigma}^{(Q_1\leftarrow A_1,\dots,Q_{r-1}\leftarrow A_{r-1})} &\equiv 1 \end{aligned}\right]$$

$$\leq \sum_{\vec{\ell}} \max_{\vec{Q}} \left(\frac{e|V_{\ell_1}\cup\cdots\cup V_{\ell_r}|}{t}\right)^t \mathbb{P}\left[\begin{aligned} C_1,\dots,C_{\ell_1-1}\restriction\boldsymbol{\sigma} &\equiv 0\\ C_{\ell_1}\restriction\boldsymbol{\sigma} &\equiv 1\\ C_{\ell_1+1},\dots,C_{\ell_2-1}\restriction\boldsymbol{\sigma}^{(Q_1\leftarrow A_1)} &\equiv 0\\ C_{\ell_2}\restriction\boldsymbol{\sigma}^{(Q_1\leftarrow A_1)} &\equiv 1\\ &\vdots\\ C_{\ell_r}\restriction\boldsymbol{\sigma}^{(Q_1\leftarrow A_1,\dots,Q_{r-1}\leftarrow A_{r-1})} &\equiv 1 \end{aligned}\right]$$

We have

$$\sum_{(\vec{\ell},\vec{Q})} \mathbb{P}\left[\begin{aligned} C_1,\ldots,C_{\ell_1-1}\upharpoonright\boldsymbol{\sigma} &\equiv 0\\ C_{\ell_1}\upharpoonright\boldsymbol{\sigma} &\equiv 1\\ C_{\ell_1+1},\ldots,C_{\ell_2-1}\upharpoonright\boldsymbol{\sigma}^{(Q_1\leftarrow A_1)} &\equiv 0\\ C_{\ell_2}\upharpoonright\boldsymbol{\sigma}^{(Q_1\leftarrow A_1)} &\equiv 1\\ &\vdots\\ C_{\ell_r}\upharpoonright\boldsymbol{\sigma}^{(Q_1\leftarrow A_1,\ldots,Q_{r-1}\leftarrow A_{r-1})} &\equiv 1 \end{aligned}\right]$$

$$\leq \max_{\vec{Q}}\sum_{\vec{\ell}}\left(\frac{e|V_{\ell_1}\cup\cdots\cup V_{\ell_r}|}{t}\right)^t \mathbb{P}\left[\begin{aligned} C_1,\ldots,C_{\ell_1-1}\upharpoonright\boldsymbol{\sigma} &\equiv 0\\ C_{\ell_1}\upharpoonright\boldsymbol{\sigma} &\equiv 1\\ C_{\ell_1+1},\ldots,C_{\ell_2-1}\upharpoonright\boldsymbol{\sigma}^{(Q_1\leftarrow A_1)} &\equiv 0\\ C_{\ell_2}\upharpoonright\boldsymbol{\sigma}^{(Q_1\leftarrow A_1)} &\equiv 1\\ &\vdots\\ C_{\ell_r}\upharpoonright\boldsymbol{\sigma}^{(Q_1\leftarrow A_1,\ldots,Q_{r-1}\leftarrow A_{r-1})} &\equiv 1 \end{aligned}\right]$$

letting Q_i range over ***functions*** $Q_i(\ell_1,\ldots,\ell_i)\in\binom{V_{\ell_i}\setminus(V_{\ell_1}\cup\cdots\cup V_{\ell_{i-1}})}{s_i}$.

Fix any choice of functions $Q_i(\ell_1, \ldots, \ell_i) \in \binom{V_{\ell_i} \setminus (V_{\ell_1} \cup \cdots \cup V_{\ell_{i-1}})}{s_i}$.

We have

$$\sum_{\vec{\ell}} \left(\frac{e|V_{\ell_1} \cup \cdots \cup V_{\ell_r}|}{t} \right)^t \mathbb{P} \left[\begin{array}{r} C_1, \ldots, C_{\ell_1 - 1} \restriction \boldsymbol{\sigma} \equiv 0 \\ C_{\ell_1} \restriction \boldsymbol{\sigma} \equiv 1 \\ C_{\ell_1+1}, \ldots, C_{\ell_2-1} \restriction \boldsymbol{\sigma}^{(Q_1 \leftarrow A_1)} \equiv 0 \\ C_{\ell_2} \restriction \boldsymbol{\sigma}^{(Q_1 \leftarrow A_1)} \equiv 1 \\ \vdots \quad \\ C_{\ell_r} \restriction \boldsymbol{\sigma}^{(Q_1 \leftarrow A_1, \ldots, Q_{r-1} \leftarrow A_{r-1})} \equiv 1 \end{array} \right]$$

Fix any choice of functions $Q_i(\ell_1, \dots, \ell_i) \in \binom{V_{\ell_i} \setminus (V_{\ell_1} \cup \cdots \cup V_{\ell_{i-1}})}{s_i}$.

We have

$$\sum_{\vec{\ell}} \left(\frac{e|V_{\ell_1} \cup \cdots \cup V_{\ell_r}|}{t} \right)^t \mathbb{P} \underbrace{\left[\begin{array}{r} C_1, \dots, C_{\ell_1 - 1} \upharpoonright \boldsymbol{\sigma} \equiv 0 \\ C_{\ell_1} \upharpoonright \boldsymbol{\sigma} \equiv 1 \\ C_{\ell_1+1}, \dots, C_{\ell_2 - 1} \upharpoonright \boldsymbol{\sigma}^{(Q_1 \leftarrow A_1)} \equiv 0 \\ C_{\ell_2} \upharpoonright \boldsymbol{\sigma}^{(Q_1 \leftarrow A_1)} \equiv 1 \\ \vdots \quad \\ C_{\ell_r} \upharpoonright \boldsymbol{\sigma}^{(Q_1 \leftarrow A_1, \dots, Q_{r-1} \leftarrow A_{r-1})} \equiv 1 \end{array} \right]}_{}$$

These events are **mutually exclusive** over choices of $1 \leq \ell_1 < \cdots < \ell_r \leq m$.

Therefore, $\sum_{\vec{\ell}} \mathbb{P}[\,''\,] \leq 1$.

Fix any choice of functions $Q_i(\ell_1, \dots, \ell_i) \in \binom{V_{\ell_i} \setminus (V_{\ell_1} \cup \cdots \cup V_{\ell_{i-1}})}{s_i}$.

We have

$$\sum_{\vec{\ell}} \left(\frac{e|V_{\ell_1} \cup \cdots \cup V_{\ell_r}|}{t} \right)^t \mathbb{P} \left[\begin{array}{rl} C_1, \dots, C_{\ell_1 - 1} \restriction \boldsymbol{\sigma} & \equiv 0 \\ C_{\ell_1} \restriction \boldsymbol{\sigma} & \equiv 1 \\ C_{\ell_1+1}, \dots, C_{\ell_2 - 1} \restriction \boldsymbol{\sigma}^{(Q_1 \leftarrow A_1)} & \equiv 0 \\ C_{\ell_2} \restriction \boldsymbol{\sigma}^{(Q_1 \leftarrow A_1)} & \equiv 1 \\ \vdots & \\ C_{\ell_r} \restriction \boldsymbol{\sigma}^{(Q_1 \leftarrow A_1, \dots, Q_{r-1} \leftarrow A_{r-1})} & \equiv 1 \end{array} \right]$$

$$= \left(\frac{e}{\ln 2} \right)^t \sum_{\vec{\ell}} \left(\frac{\ln(2^{|V_{\ell_1} \cup \cdots \cup V_{\ell_r}|})}{t} \right)^t \mathbb{P}[\,''\,]$$

Fix any choice of functions $Q_i(\ell_1, \dots, \ell_i) \in \binom{V_{\ell_i} \setminus (V_{\ell_1} \cup \cdots \cup V_{\ell_{i-1}})}{s_i}$.

We have

$$\sum_{\vec{\ell}} \left(\frac{e|V_{\ell_1} \cup \cdots \cup V_{\ell_r}|}{t} \right)^t \mathbb{P} \left[\begin{array}{r} C_1, \dots, C_{\ell_1 - 1} \restriction \boldsymbol{\sigma} \equiv 0 \\ C_{\ell_1} \restriction \boldsymbol{\sigma} \equiv 1 \\ C_{\ell_1+1}, \dots, C_{\ell_2 - 1} \restriction \boldsymbol{\sigma}^{(Q_1 \leftarrow A_1)} \equiv 0 \\ C_{\ell_2} \restriction \boldsymbol{\sigma}^{(Q_1 \leftarrow A_1)} \equiv 1 \\ \vdots \\ C_{\ell_r} \restriction \boldsymbol{\sigma}^{(Q_1 \leftarrow A_1, \dots, Q_{r-1} \leftarrow A_{r-1})} \equiv 1 \end{array} \right]$$

$$= \left(\frac{e}{\ln 2} \right)^t \sum_{\vec{\ell}} \underbrace{\left(\frac{\ln(2^{|V_{\ell_1} \cup \cdots \cup V_{\ell_r}|})}{t} \right)^t}_{x \mapsto \left(\frac{\ln(x)}{t} \right)^t \text{ is a } \textbf{concave} \text{ function}} \mathbb{P}[\,''\,]$$

(really: $x \mapsto \left(\frac{\ln(x)}{t} + 1 \right)^t$, but let's ignore this $+1$)

Fix any choice of functions $Q_i(\ell_1, \ldots, \ell_i) \in \binom{V_{\ell_i} \setminus (V_{\ell_1} \cup \cdots \cup V_{\ell_{i-1}})}{s_i}$.

We have

$$\sum_{\vec{\ell}} \left(\frac{e |V_{\ell_1} \cup \cdots \cup V_{\ell_r}|}{t} \right)^t \mathbb{P} \left[\begin{array}{r} C_1, \ldots, C_{\ell_1 - 1} \restriction \boldsymbol{\sigma} \equiv 0 \\ C_{\ell_1} \restriction \boldsymbol{\sigma} \equiv 1 \\ C_{\ell_1+1}, \ldots, C_{\ell_2 - 1} \restriction \boldsymbol{\sigma}^{(Q_1 \leftarrow A_1)} \equiv 0 \\ C_{\ell_2} \restriction \boldsymbol{\sigma}^{(Q_1 \leftarrow A_1)} \equiv 1 \\ \vdots \quad \\ C_{\ell_r} \restriction \boldsymbol{\sigma}^{(Q_1 \leftarrow A_1, \ldots, Q_{r-1} \leftarrow A_{r-1})} \equiv 1 \end{array} \right]$$

$$= \left(\frac{e}{\ln 2} \right)^t \sum_{\vec{\ell}} \left(\frac{\ln(2^{|V_{\ell_1} \cup \cdots \cup V_{\ell_r}|})}{t} \right)^t \mathbb{P}[\ '' \ ]$$

$$\leq \left(\frac{e}{\ln 2} \right)^t \left(\frac{1}{t} \ln \left(\sum_{\vec{\ell}} 2^{|V_{\ell_1} \cup \cdots \cup V_{\ell_r}|} \ \mathbb{P}[\ '' \ ] \right) \right)^t \quad \text{(Jensen's Inequality)}$$

Fix any choice of functions $Q_i(\ell_1, \ldots, \ell_i) \in \binom{V_{\ell_i} \backslash (V_{\ell_1} \cup \cdots \cup V_{\ell_{i-1}})}{s_i}$.

We have

$$\sum_{\vec{\ell}} \left(\frac{e|V_{\ell_1} \cup \cdots \cup V_{\ell_r}|}{t}\right)^t \mathbb{P}\left[\begin{array}{r} C_1, \ldots, C_{\ell_1 - 1} \restriction \boldsymbol{\sigma} \equiv 0 \\ C_{\ell_1} \restriction \boldsymbol{\sigma} \equiv 1 \\ C_{\ell_1+1}, \ldots, C_{\ell_2 - 1} \restriction \boldsymbol{\sigma}^{(Q_1 \leftarrow A_1)} \equiv 0 \\ C_{\ell_2} \restriction \boldsymbol{\sigma}^{(Q_1 \leftarrow A_1)} \equiv 1 \\ \vdots \\ C_{\ell_r} \restriction \boldsymbol{\sigma}^{(Q_1 \leftarrow A_1, \ldots, Q_{r-1} \leftarrow A_{r-1})} \equiv 1 \end{array}\right]$$

$$= \left(\frac{e}{\ln 2}\right)^t \sum_{\vec{\ell}} \left(\frac{\ln(2^{|V_{\ell_1} \cup \cdots \cup V_{\ell_r}|})}{t}\right)^t \mathbb{P}[\,''\,]$$

$$\leq \left(\frac{e}{\ln 2}\right)^t \left(\frac{1}{t} \ln \left(\sum_{\vec{\ell}} 2^{|V_{\ell_1} \cup \cdots \cup V_{\ell_r}|} \underbrace{\mathbb{P}[\,''\,]}_{\leq 2^{-|V_{\ell_1} \cup \cdots \cup V_{\ell_r}|}}\right)\right)^t$$

$$
\begin{aligned}
\mathbb{P}[\;''\;] &= \mathbb{P}\left[\begin{array}{rl}
C_1,\dots,C_{\ell_1-1}\restriction\boldsymbol{\sigma} & \equiv 0 \\
C_{\ell_1}\restriction\boldsymbol{\sigma} & \equiv 1 \\
C_{\ell_1+1},\dots,C_{\ell_2-1}\restriction\boldsymbol{\sigma}^{(Q_1\leftarrow A_1)} & \equiv 0 \\
C_{\ell_2}\restriction\boldsymbol{\sigma}^{(Q_1\leftarrow A_1)} & \equiv 1 \\
 & \vdots \\
C_{\ell_r}\restriction\boldsymbol{\sigma}^{(Q_1\leftarrow A_1,\dots,Q_{r-1}\leftarrow A_{r-1})} & \equiv 1
\end{array}\right] \\
&\le \mathbb{P}\left[\begin{array}{rl}
C_{\ell_1}\restriction\boldsymbol{\sigma} & \equiv 1 \\
C_{\ell_2}\restriction\boldsymbol{\sigma}^{(Q_1\leftarrow A_1)} & \equiv 1 \\
 & \vdots \\
C_{\ell_r}\restriction\boldsymbol{\sigma}^{(Q_1\leftarrow A_1,\dots,Q_{r-1}\leftarrow A_{r-1})} & \equiv 1
\end{array}\right] \\
&= \mathbb{P}\left[\begin{array}{l}
C_{\ell_1}\wedge C_{\ell_2}\restriction_{Q_1\leftarrow A_1}\wedge\cdots\wedge C_{\ell_r}\restriction_{Q_1\leftarrow A_1,\dots,Q_{r-1}\leftarrow A_{r-1}} \\
\text{is satisfied (forced to 1) by } \boldsymbol{\sigma}
\end{array}\right] \\
&\le 2^{-|V_{\ell_1}\cup\cdots\cup V_{\ell_r}|}.
\end{aligned}
$$

Finally, we bound:

$$\begin{aligned}
&\left(\frac{e}{\ln 2}\right)^t \left(\frac{1}{t}\ln\left(\sum_{\vec{\ell}} 2^{|V_{\ell_1}\cup\cdots\cup V_{\ell_r}|}\,\mathbb{P}[\,''\,]\right)\right)^t \\
&\leq \left(\frac{e}{\ln 2}\right)^t \left(\frac{1}{t}\ln\left(\sum_{\vec{\ell}} 1\right)\right)^t && \text{(recall: } 1 \leq \ell_1 < \cdots < \ell_r \leq m\text{)} \\
&\leq \left(\frac{e}{\ln 2}\right)^t \left(\frac{1}{t}\ln\binom{m}{r}\right)^t && \text{(recall: } r \leq t\text{)} \\
&\leq \left(\frac{e}{\ln 2}\right)^t \left(\frac{1}{t}\ln(m^t)\right)^t \\
&= (e\log m)^t
\end{aligned}$$

Finally, we bound:

$$\begin{aligned}
&\left(\frac{e}{\ln 2}\right)^t \left(\frac{1}{t}\ln\left(\sum_{\vec{\ell}} 2^{|V_{\ell_1}\cup\cdots\cup V_{\ell_r}|}\,\mathbb{P}[\ ''\ ]\right)\right)^t \\
\leq\ &\left(\frac{e}{\ln 2}\right)^t \left(\frac{1}{t}\ln\left(\sum_{\vec{\ell}} 1\right)\right)^t \qquad \text{(recall: } 1 \leq \ell_1 < \cdots < \ell_r \leq m) \\
\leq\ &\left(\frac{e}{\ln 2}\right)^t \left(\frac{1}{t}\ln\binom{m}{r}\right)^t \qquad \text{(recall: } r \leq t) \\
\leq\ &\left(\frac{e}{\ln 2}\right)^t \left(\frac{1}{t}\ln(m^t)\right)^t \\
=\ &(e\log m)^t
\end{aligned}$$

Therefore, $\mathbb{E}\,|\{\varrho \in \mathrm{Bad}_t : \varrho^* = \boldsymbol{R}_p\}| \leq (4e\log m)^t$.

Therefore, $\mathbb{P}[\ \mathsf{DT}_{\mathsf{depth}}(F\restriction\boldsymbol{R}_p) \geq t\ ] = O(p\log m)^t$. **Q.E.D.**

Recent Developments via “Multi-Switching Lemmas”

Recent Developments

- Optimal correlation bounds [Hastad '14]

  AC^0 circuits of depth $d+1$ and size S have correlation $\frac{1}{2} + 2^{-\varepsilon n}$ with PARITY$_n$ where $\varepsilon = 1 / O(\log S)^d$

Recent Developments

- Optimal correlation bounds [Hastad '14]

  AC^0 circuits of depth $d+1$ and size S have correlation $\frac{1}{2} + 2^{-\varepsilon n}$ with PARITY_n where $\varepsilon = 1 / O(\log S)^d$

via a "multi-switching lemma" that analyzes multiple DNFs at once

Recent Developments

- Optimal correlation bounds [Hastad '14]

  AC^0 circuits of depth $d+1$ and size S have correlation $½ + 2^{-\varepsilon n}$ with PARITY_n where $\varepsilon = 1 / O(\log S)^d$

- #SAT algorithm [Impagliazzo-Matthews-Paturi '12]

  Counting the satisfying assignments to AC^0 circuits of depth $d+1$ and size S in randomized time $2^{(1-\varepsilon)n}$

Recent Developments

- Optimal correlation bounds [Hastad '14]

  AC^0 circuits of depth $d+1$ and size S have correlation $½ + 2^{-\varepsilon n}$ with PARITY$_n$ where $\varepsilon = 1 / O(\log S)^d$

- #SAT algorithm [Impagliazzo-Matthews-Paturi '12]

  Counting the satisfying assignments to AC^0 circuits of depth $d+1$ and size S in randomized time $2^{(1-\varepsilon)n}$

via a similar "multi-switching lemma" (independently discovered)

Recent Developments

- Optimal correlation bounds [Hastad '14]

  AC^0 circuits of depth $d+1$ and size S have correlation $½ + 2^{-\varepsilon n}$ with PARITY_n where $\varepsilon = 1 / O(\log S)^d$

- #SAT algorithm [Impagliazzo-Matthews-Paturi '12]

  Counting the satisfying assignments to AC^0 circuits of depth $d+1$ and size S in randomized time $2^{(1-\varepsilon)n}$

- Optimal Linial-Mansour-Nisan Theorem [Tal '14]

  Tight bounds on the Fourier spectrum of AC^0 circuits

These results all follow from a bound on the ***criticality*** of AC^0 circuits.

- Optimal correlation bounds [Hastad '14]

  AC^0 circuits of depth $d+1$ and size S have correlation $½ + 2^{-\varepsilon n}$ with $PARITY_n$ where $\varepsilon = 1 / O(\log S)^d$

- #SAT algorithm [Impagliazzo-Matthews-Paturi '12]

  Counting the satisfying assignments to AC^0 circuits of depth $d+1$ and size S in randomized time $2^{(1-\varepsilon)n}$

- Optimal Linial-Mansour-Nisan Theorem [Tal '14]

  Tight bounds on the Fourier spectrum of AC^0 circuits

Criticality

Definition

A Boolean function f is λ-**critical** (where $\lambda \geq 1$) if

$$\Pr[\ \mathrm{DT}_{\mathrm{depth}}(f \upharpoonright \mathbf{R}_p) \geq t\ ] \leq (p\lambda)^t$$ for all p and t.

The **criticality** of f is the minimum real $\lambda \geq 1$ such that f is k-critical.

Criticality

Definition

A Boolean function f is λ-**critical** (where $\lambda \geq 1$) if

$$\Pr[\, \mathrm{DT}_{\mathrm{depth}}(f \upharpoonright \mathbf{R}_p) \geq t \,] \leq (p\lambda)^t \quad \text{for all } p \text{ and } t.$$

For example:

- Every n-var. function $f : \{0,1\}^n \rightarrow \{0,1\}$ is n-critical
- Every depth-k decision tree is k-critical
- Every width-k DNF is $O(k)$-critical
- Every m-clause DNF is $O(\log m)$-critical

Criticality

Definition

A Boolean function f is λ-**critical** (where $\lambda \geq 1$) if

$$\Pr[\, DT_{\mathrm{depth}}(f \upharpoonright \mathbf{R}_p) \geq t \,] \leq (p\lambda)^t \text{ for all } p \text{ and } t.$$

Proposition

If $f : \{0,1\}^n \to \{0,1\}$ is λ-critical, then

$$DT_{\mathrm{size}}(f) \leq O(2^{n - (n/2\lambda)}).$$

Upper bounds on ***criticality*** yield randomized constructions of decision trees, hence randomized #SAT algorithms

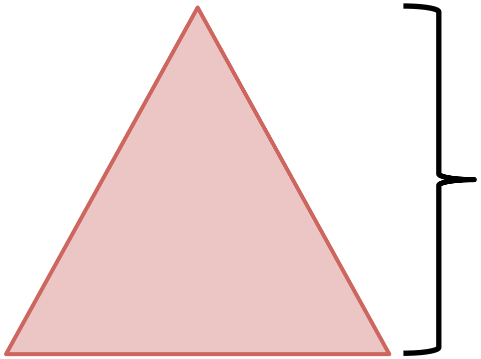
A

Pr[or all p and t.

<u>Proposition</u>

If $f : \{0,1\}^n \rightarrow \{0,1\}$ is λ-critical, then

$$\mathrm{DT}_{\mathrm{size}}(f) \leq O(2^{n - (n/2\lambda)}).$$

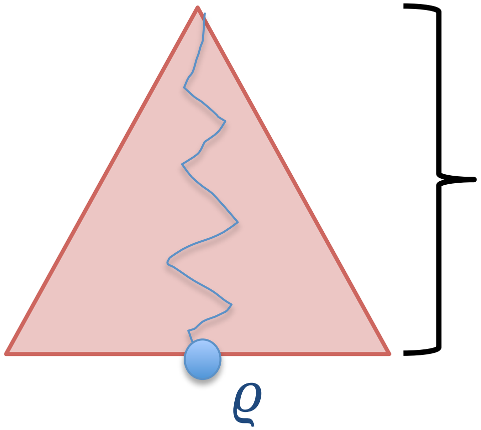


Query all variables from a random set of size $(1 - p)n$ where $p = 1 / 2.01\lambda$

Proposition

If $f : \{0,1\}^n \to \{0,1\}$ is λ-critical, then

$$\mathrm{DT}_{\mathrm{size}}(f) \le O(2^{n - (n/2\lambda)}).$$



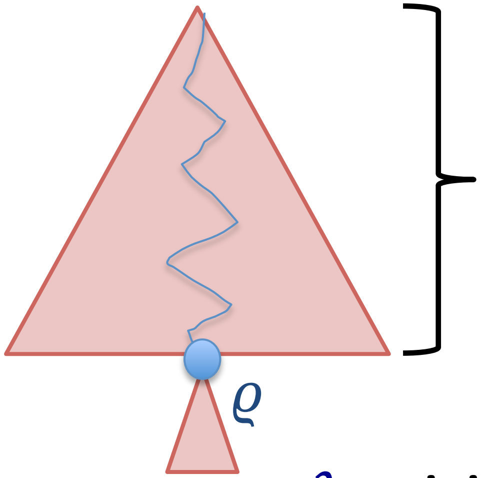
Query all variables from a random set of size $(1 - p)n$ where $p = 1 / 2.01\lambda$

a uniform random branch is a p-random restriction

Proposition

If $f : \{0,1\}^n \rightarrow \{0,1\}$ is λ-critical, then

$$\mathrm{DT}_{\mathrm{size}}(f) \leq O(2^{n - (n/2\lambda)}).$$



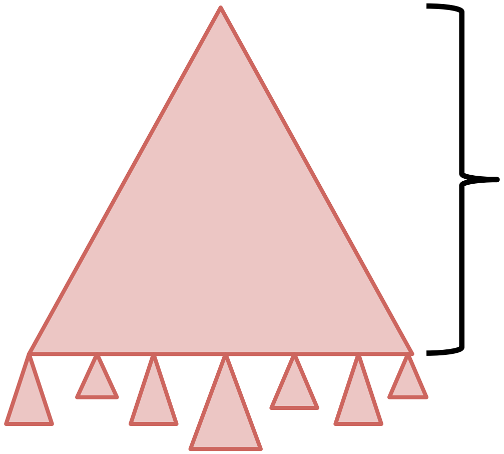
Query all variables from a random set of size $(1 - p)n$ where $p = 1 / 2.01\lambda$

λ-criticality of f implies $E[\ DT_{size}(f \upharpoonright \varrho)\ ] = O(1)$

Proposition

If $f : \{0,1\}^n \to \{0,1\}$ is λ-critical, then

$$DT_{size}(f) \leq O(2^{n - (n/2\lambda)}).$$



Query all variables from a random set of size $(1 - p)n$ where $p = 1 / 2.01\lambda$

w.h.p. we get a decision tree for f of size $O(2^{(1 - p)n})$

Proposition

If $f : \{0,1\}^n \rightarrow \{0,1\}$ is λ-critical, then

$$DT_{size}(f) \leq O(2^{n - (n/2\lambda)}).$$

Degree-Criticality

Definition

A Boolean function f is λ-**degree-critical** if

$$\Pr[\ \deg(f \upharpoonright \mathbf{R}_p) \geq t\ ] \leq (p\lambda)^t \quad \text{for all } p \text{ and } t.$$

Degree-Criticality

Definition

A Boolean function f is λ**-degree-critical** if

$$\Pr[\deg(f \upharpoonright \mathbf{R}_p) \geq t] \leq (p\lambda)^t \text{ for all } p \text{ and } t.$$

Obs λ-critical ⇒ λ-degree-critical

(since $\deg(.) \leq DT_{depth}(.)$)

Degree-Criticality

Definition

A Boolean function f is λ-**degree-critical** if

$$\Pr[\deg(f \restriction \mathbf{R}_p) \geq t] \leq (p\lambda)^t \text{ for all } p \text{ and } t.$$

Theorem [Tal 14]

- Circuits of depth d+1 and size S have degree-criticality $O(\log S)^d$.
- If f is any λ-degree-critical function, then for every k,

$$\sum_{|I|\geq k} \widehat{f}(I)^2 \leq O(e^{-k/\lambda}) \text{ and } \sum_{|I|=k} |\widehat{f}(I)| \leq O(\lambda)^k$$

Degree-Criticality

Definition

A Boolean function f is λ-**degree-critical** if

[Tal'14] also shows this condition is ***equivalent*** to degree-criticality $O(\lambda)$

T

- Circuits of depth $d+1$ have degree-criticality $O(\log S)^d$.
- If f is any λ-degree-critical function, then for every k,

$$\sum_{|I|\geq k} \widehat{f}(I)^2 \leq O(e^{-k/\lambda}) \quad \text{and} \quad \sum_{|I|=k} |\widehat{f}(I)| \leq O(\lambda)^k$$

Criticality of AC^0 Circuits

<u>Observation</u>

AC^0 circuits of depth $d+1$ and size S have criticality at most $\lambda = O(\log S)^d$

Criticality of AC^0 Circuits

<u>Observation</u>

AC^0 circuits of depth $d+1$ and size S have criticality at most $\lambda = O(\log S)^d$

Implies the results of [Hastad 14], [Impagliazzo-Matthews-Paturi 12], [Tal 14]

Criticality of AC^0 Circuits

Observation

AC^0 circuits of depth $d+1$ and size S have criticality at most $\lambda = O(\log S)^d$

- Hastad's Switching Lemma (1986) shows

$$\Pr[\, DT_{\text{depth}}(f \upharpoonright \mathbf{R}_p) \geq t \,] \leq (p\lambda/2)^t + (1/S)^{O(1)}$$
$$\leq (p\lambda)^t \quad \text{for all } t \leq \log S$$

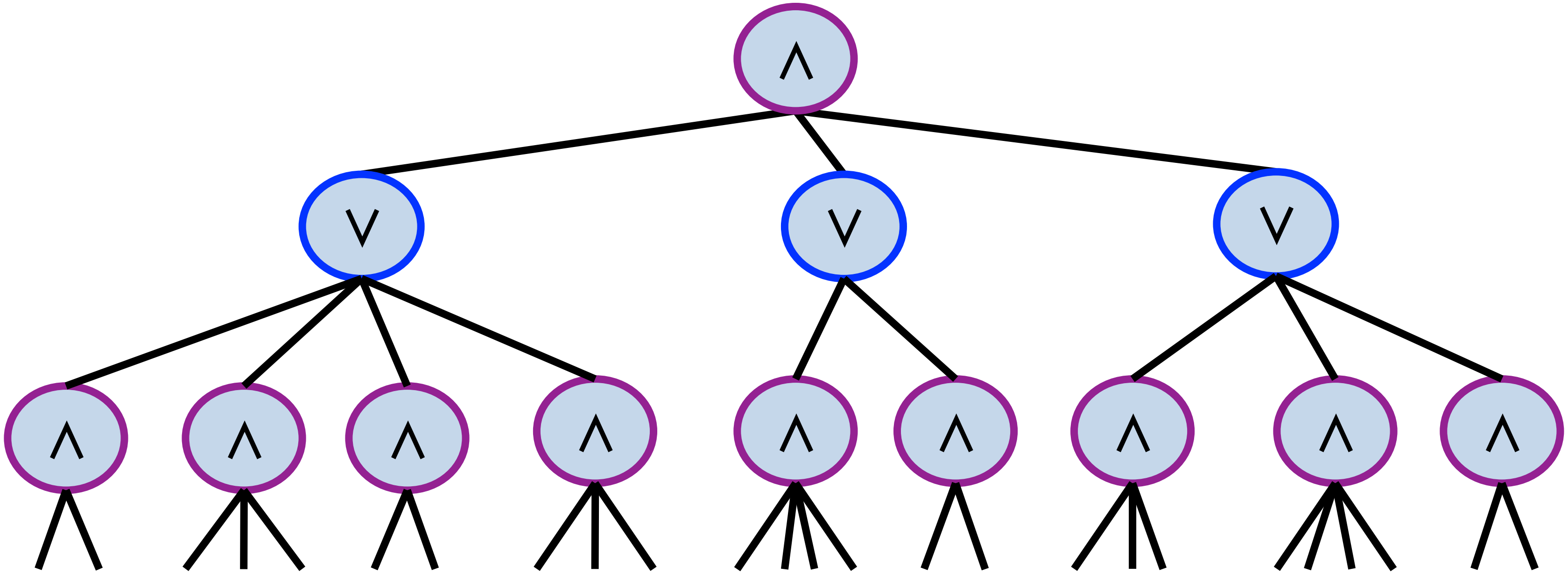
- Hastad's Multi-Switching Lemma (2014) shows

$$\Pr[\, DT_{\text{depth}}(f \upharpoonright \mathbf{R}_p) \geq t \,] \leq S * (p\lambda/2)^t$$
$$\leq (p\lambda)^t \quad \text{for all } t > \log S$$

Criticality of AC^0 Formulas

Conjecture

AC^0 formulas of depth d+1 and size S have criticality at most $\lambda = O((\log S)/d)^d$



Criticality of AC^0 Formulas

Conjecture

AC^0 formulas of depth $d+1$ and size S have criticality at most $\lambda = O((\log S)/d)^d$

- "Stopping time" technique of [R. 15] implies

  $\Pr[\ DT_{\mathrm{depth}}(f \upharpoonright \mathbf{R}_p) \geq t\ ] \leq (p\lambda)^t$ for all $t \leq \log S$

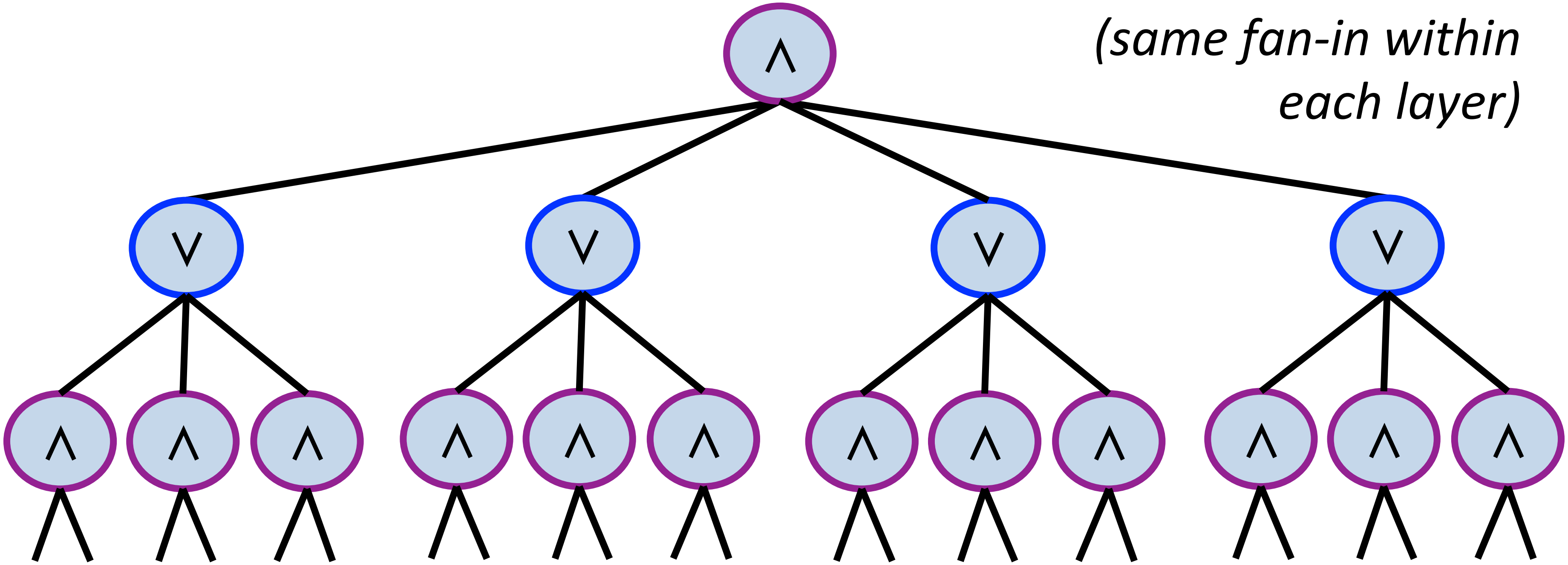
- Unfortunately, don't know how to show

  $\Pr[\ DT_{\mathrm{depth}}(f \upharpoonright \mathbf{R}_p) \geq t\ ] \leq (p\lambda)^t$ for all $t > \log S$

Criticality of ***Regular*** AC^0 Formulas

Theorem [R. 18]

Regular AC^0 formulas of depth d+1 and size S have criticality at most $O((\log S)/d)^d$



(same fan-in within each layer)

Criticality of ***Regular*** AC^0 Formulas

Theorem [R. 18]

Regular AC^0 formulas of depth d+1 and size S have criticality at most $O((\log S)/d)^d$

- Proof based on alternative analysis of the Switching Lemma with **log(size)** in place of **width**
- Introduces and analyses the ***canonical decision tree*** of an entire depth d+1 formula

Corollaries

- Optimal correlation bounds

  Regular AC^0 formulas of depth $d+1$ and size S have corr. $½ + 2^{-\varepsilon n}$ with PARITY_n where $\varepsilon = 1 / O((\log S)/d)^d$

- #SAT algorithm

  #SAT for **regular AC^0 formulas** of depth $d+1$ and size S is solvable in randomized time $2^{(1-\varepsilon)n}$

- Optimal Linial-Mansour-Nisan Theorem

  Tight bounds on the Fourier spectrum of **regular AC^0 formulas**

Corollaries

This improvement to [IMP12] has a further corollary:
an improved QBF-SAT algorithm

ave

corr. $\frac{1}{2}$ 2 $\varepsilon = 1 / O((\log S)/d)^d$

- <u>#SAT algorithm</u>

  #SAT for **regular AC^0 formulas** of depth $d+1$ and size S is solvable in randomized time $2^{(1-\varepsilon)n}$

- <u>Optimal Linial-Mansour-Nisan Theorem</u>

  Tight bounds on the Fourier spectrum of **regular AC^0 formulas**

QBF-SAT

[Santhanam-Williams 14] give two rand. algorithms for **Quantified-CNF Satisfiability** with q quantifier alternations:

- Algorithm #1 has time $\mathrm{poly}(n) * 2^{n-\Omega(q)}$

  This beats exhaustive search when $q >> \log n$

- Algorithm #2 has time $\mathrm{poly}(n) * 2^{n-\Omega(n\hat{}(1/q))}$

  Beats exhaustive search when $q << \log n / \log \log n$

QBF-SAT

[Santhanam-Williams 14] give two rand. algorithms for **Quantified-CNF Satisfiability** with q quantifier alternations:

- Algorithm #1 has time $\text{poly}(n) * 2^{n-\Omega(q)}$

  This beats exhaustive search when q >> log n

- Algorithm #2 has time $\text{poly}(n) * 2^{n-\Omega(q * n \wedge (1/q))}$

  Beats exhaustive search when q << log n ~~/ log log n~~

We get an improvement to alg #2

Open Problems

- Show that AC^0 formulas of depth $d+1$ and size S have criticality at most $O((\log S)/d)^d$.
- If $f_1,\dots,f_m$ are λ-critical, is $AND(f_1,\dots,f_m)$ necessarily $O(\lambda * \log m)$-critical? (If so, this implies our result on regular AC^0 formulas.)
- We observed that λ-critical ⇒ λ-degree-critical. Does λ-degree-critical imply $O(\lambda)$-critical?

Tour of other switching lemmas

$\mathbf{Stars}_m$

- $\mathbf{Stars}_m : \{x_1,\ldots,x_n\} \rightarrow \{0,1,\star\}$ with exactly m stars (behaves similarly to $\mathbf{R}_{m/n}$)
- Switching Lemma

$$\Pr[\ \mathrm{DT}_{\mathrm{depth}}(k\text{-DNF} \restriction \mathbf{Stars}_m) \geq t\ ] \leq O((m/n)k)^t$$

$\mathbf{R}_{p,q}$

- q-biased p-restriction $\mathbf{R}_{p,q}$

$$\mathbf{R}_{p,q}(x_i) = \begin{cases} \star & \text{with prob. } p \\ 1 & \text{with prob. } (1-p)q \\ 0 & \text{with prob. } (1-p)(1-q) \end{cases}$$

- Switching Lemma (q ≤ ½)

$$\Pr[\ \mathrm{DT}_{\mathrm{depth}}(k\text{-DNF} \restriction \mathbf{R}_{p,q}) \geq t\ ] \leq O(pk/q)^t$$

- Used for ave-case lower bounds under q-biased distribution on $\{0,1\}^n$

$\textbf{Clique}_{p,q}$

- Beame ’90 proved a “clique switching lemma” for the random restriction on (n choose 2) variables where
  - stars are edges of a clique on a p-random set of vertices
  - non-stars are set to 1 with prob. q and 0 with prob. 1 – q
- Switching Lemma (q ≤ ½)

  $$\Pr[\, DT_{depth}(k\text{-DNF} \upharpoonright \textbf{Clique}_{p,q}) \geq t \,] \leq O(pk/q^{O(k+t)})^t$$

- This gives an $\mathbf{n^{\Omega(k/d\text{^}2)}}$ lower bound for $k\text{-CLIQUE}_n$ (moreover, in the *average-case* for G(n,q))

$\mathrm{Clique}_{p,q}$

- Beame ’90 proved a “clique switching lemma” for the random restriction on (n choose 2) variables where
  - stars are edges of a clique on a p-random set of vertices
  -

Dependence on d results from the standard depth-reduction argument

$$\Pr[\ \mathrm{DT}_{\mathrm{depth}}(\text{k-DNF} \restriction \mathrm{Clique}_{p,q}) \geq t\ ] \leq O(pk/q^{O(k+t)})^t$$

- This gives an $n^{\Omega(k/d^2)}$ lower bound for k-CLIQUE_n (moreover, in the *average-case* for G(n,q))

Variants of $\mathbf{R}_p$

- See Beame’s “Switching Lemma Primer” for an account of:

$\mathbf{Stars}_m$

$\mathbf{R}_{p,q}$

$\mathbf{Clique}_{p,q}$

Matching Restrictions (vs. Pigeonhole Principle)

Hastad’s Tseitin Grid Restrictions

AC^0-Frege

- Proof system whose lines are depth-d AC^0 formulas
- Generalizes RESOLUTION (essentially “depth-1 Frege”)

AC^0-Frege Lower Bounds

- Pitassi-Beame-Impagliazzo, Krajicek-Pudlak-Woods 90's

  $\exp(n^{1/\exp(\Omega(d))})$ lower bound for **Pigeonhole Principle**

AC^0-Frege Lower Bounds

- Pitassi-Beame-Impagliazzo, Krajicek-Pudlak-Woods 90's

  $\exp(n^{1/\exp(\Omega(d))})$ lower bound for **Pigeonhole Principle**

worse than the $\exp(\Omega(n^{1/d}))$ lower bounds for AC^0 circuits

AC^0-Frege Lower Bounds

- Pitassi-Beame-Impagliazzo, Krajicek-Pudlak-Woods 90's

  $\exp(n^{1/\exp(\Omega(d))})$ lower bound for **Pigeonhole Principle**

- Pitassi-R.-Servedio-Tan '16

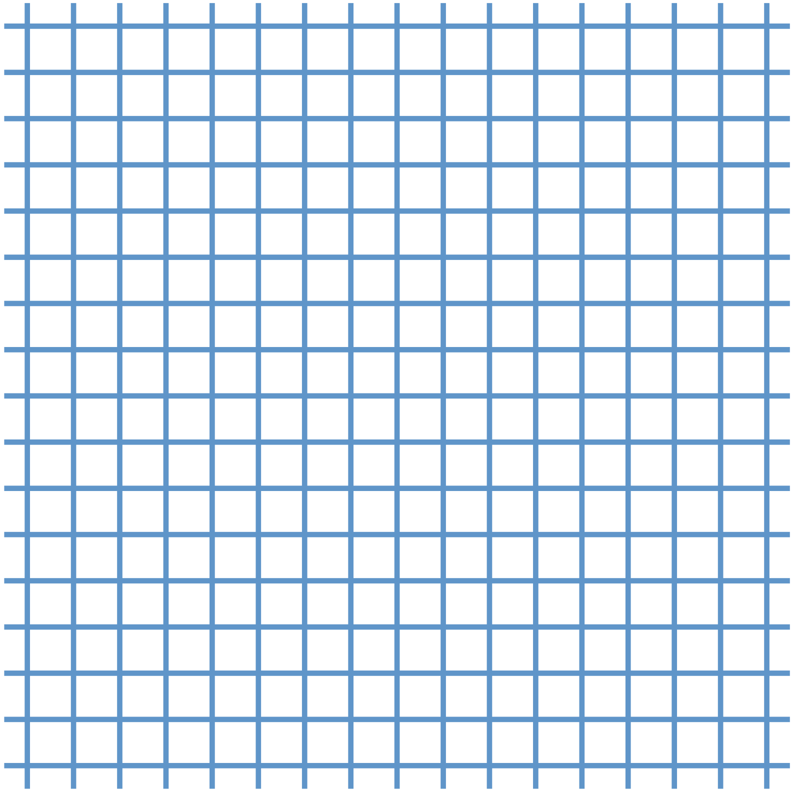
  Mild lower bound via new approach for **Tseitin** on expander graphs (using random projectins)

- Hastad '17

  $\exp(n^{\Omega(1/d)})$ lower bound for **Tseitin** on grids

Tseitin Contradiction

- $\text{Grid}_{n \times n}$ = 4-regular n×n (toroidal) grid graph, n *odd*



Tseitin Contradiction

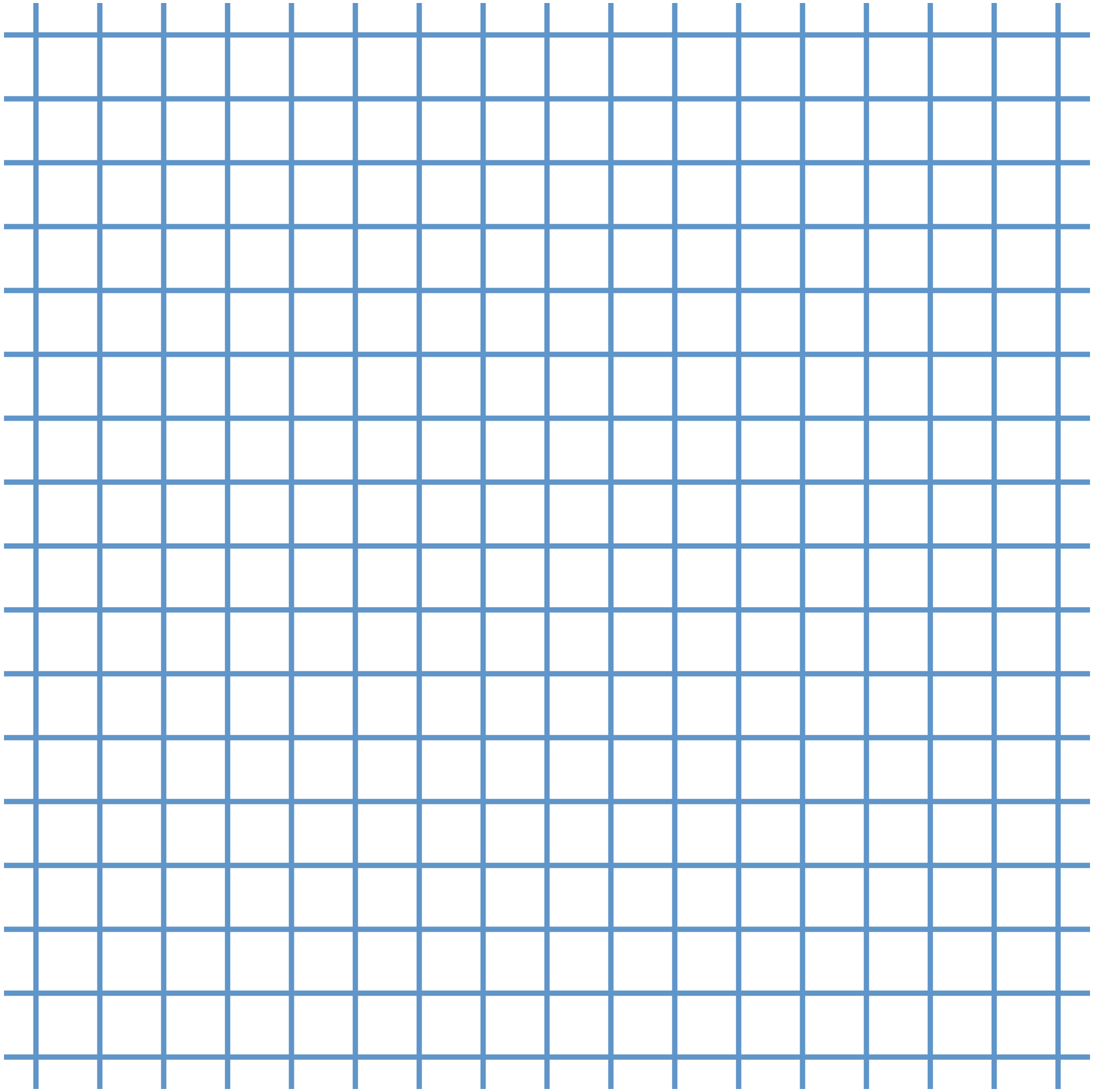
- $\mathrm{Grid}_{n\times n}$ = 4-regular n×n (toroidal) grid graph, n *odd*

- $\mathrm{Tseitin}(\mathrm{Grid}_{n\times n})$ is the *unsatisfiable* 4-DNF formula with variables X_e for each edge e and clauses

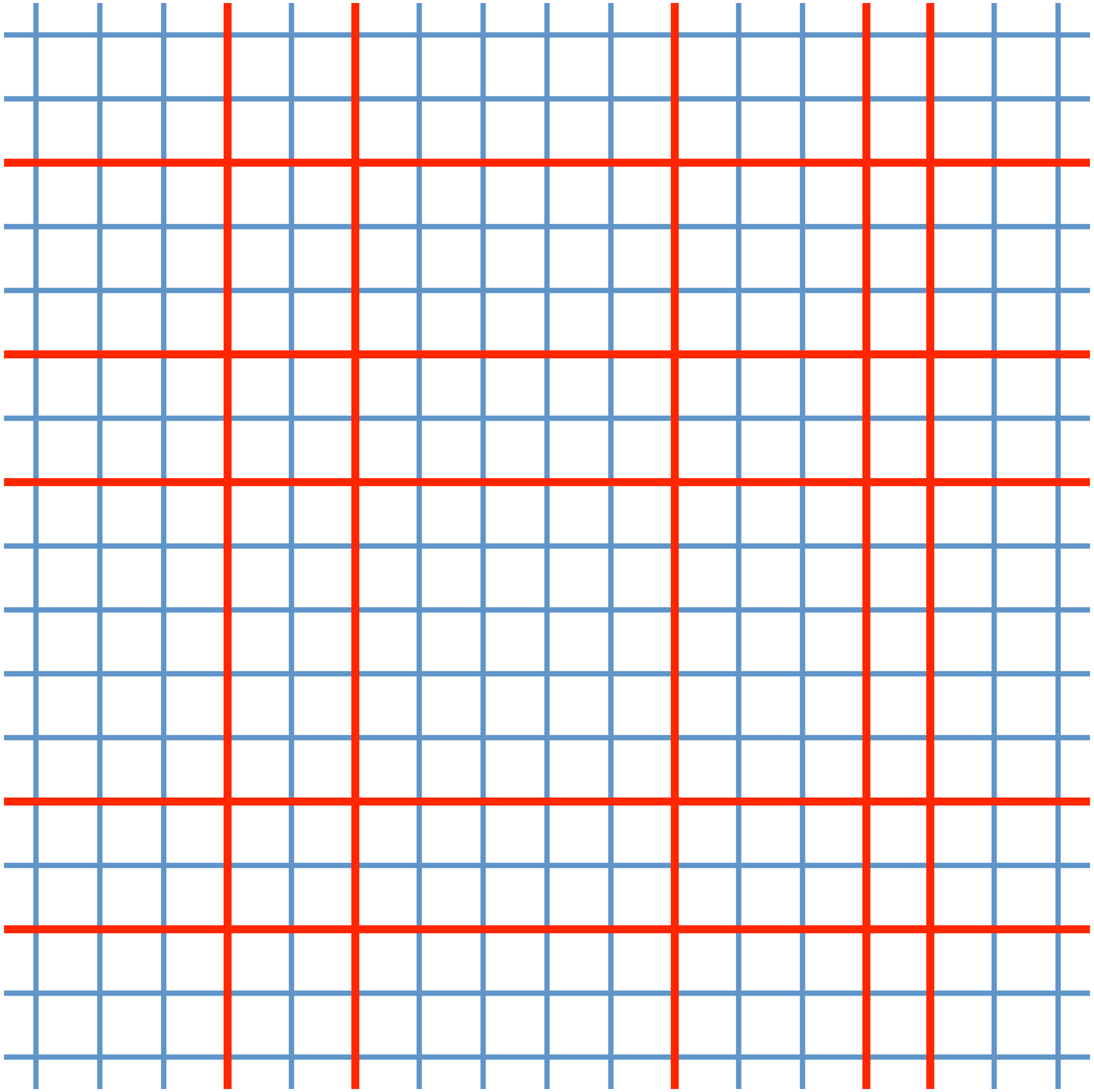
$$X_{e_1} \oplus X_{e_2} \oplus X_{e_3} \oplus X_{e_4} = 1$$

  for every four edges e_1, e_2, e_3, e_4 meeting a common vertex

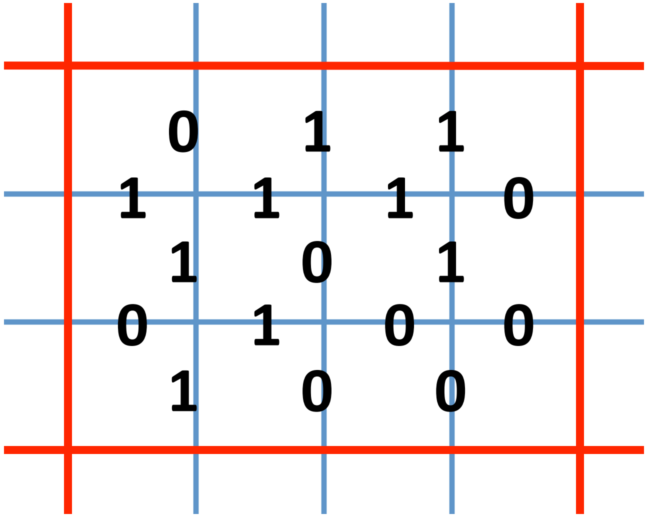
$\text{Grid}_{n\times n}$



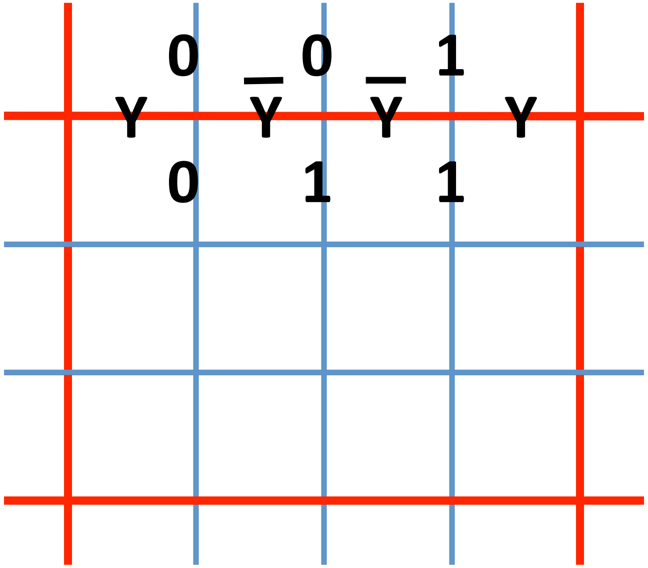
pick ℓ random rows and columns (ℓ *odd*)



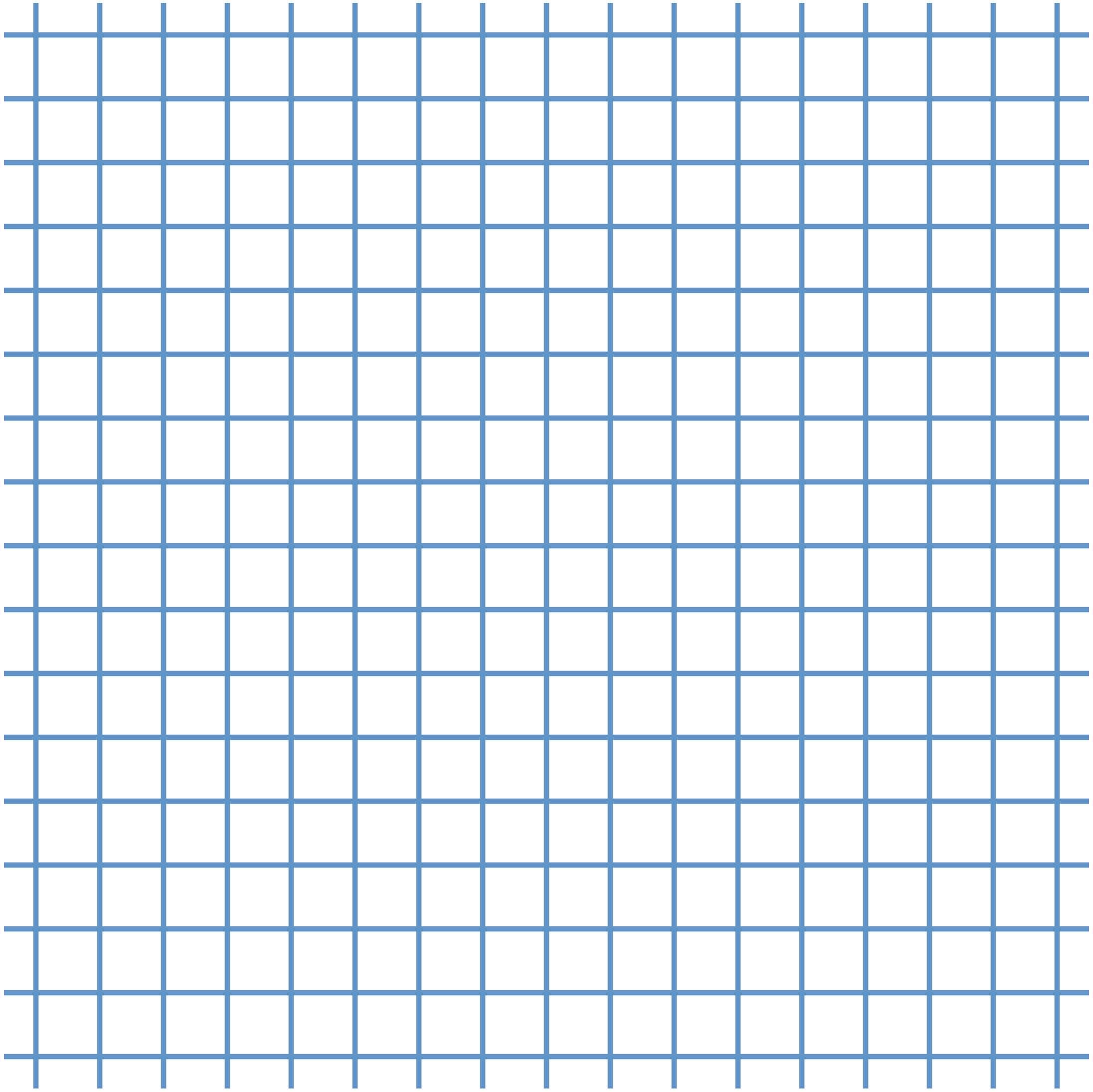
randomly set blue edges to 0 or 1
without violating any parity constraint



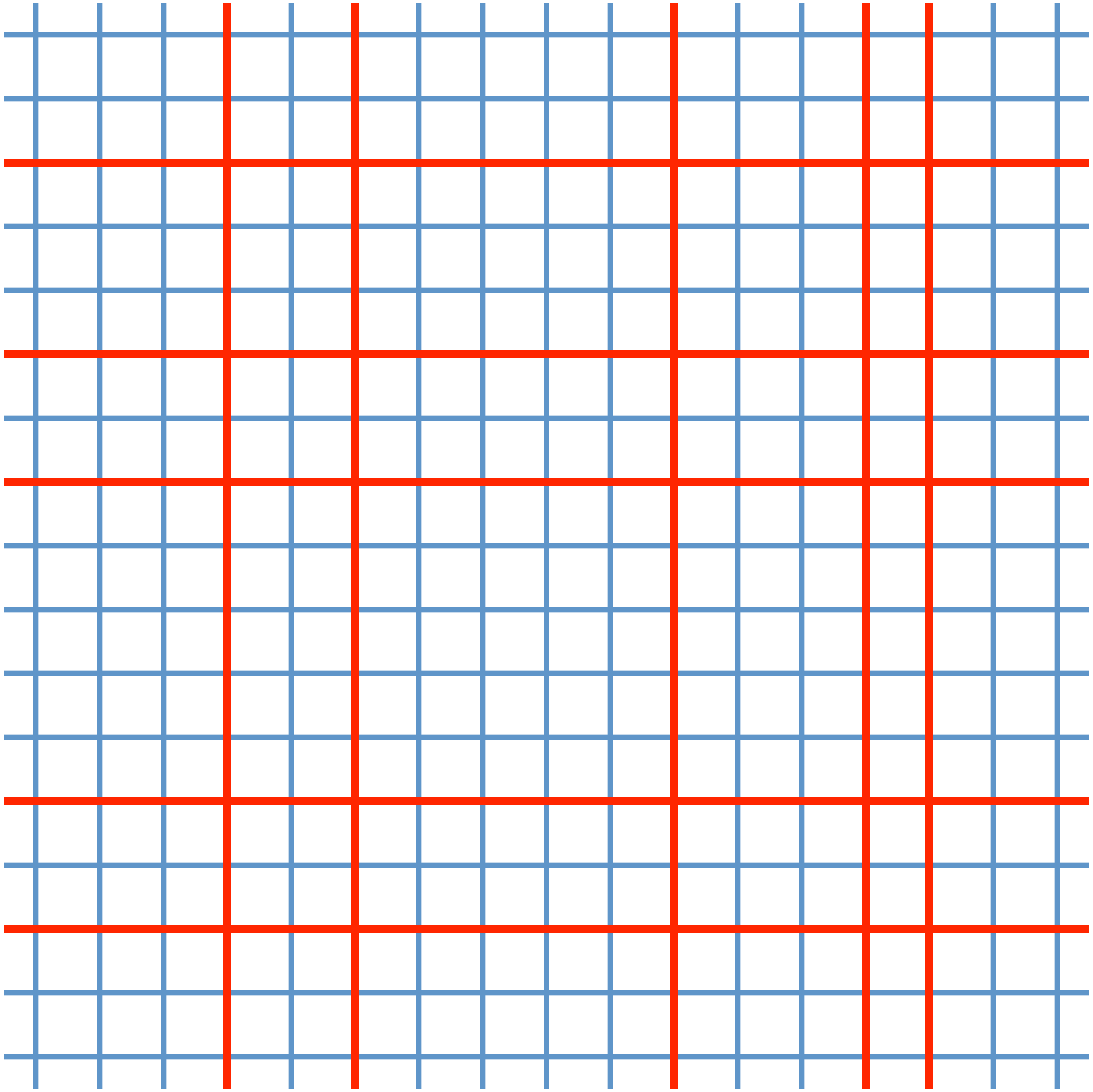
create a new Y-variable for each red "super-edge" and project each X-variables to Y or $\overline{Y}$ (as dictated by adjacent parity constraints)



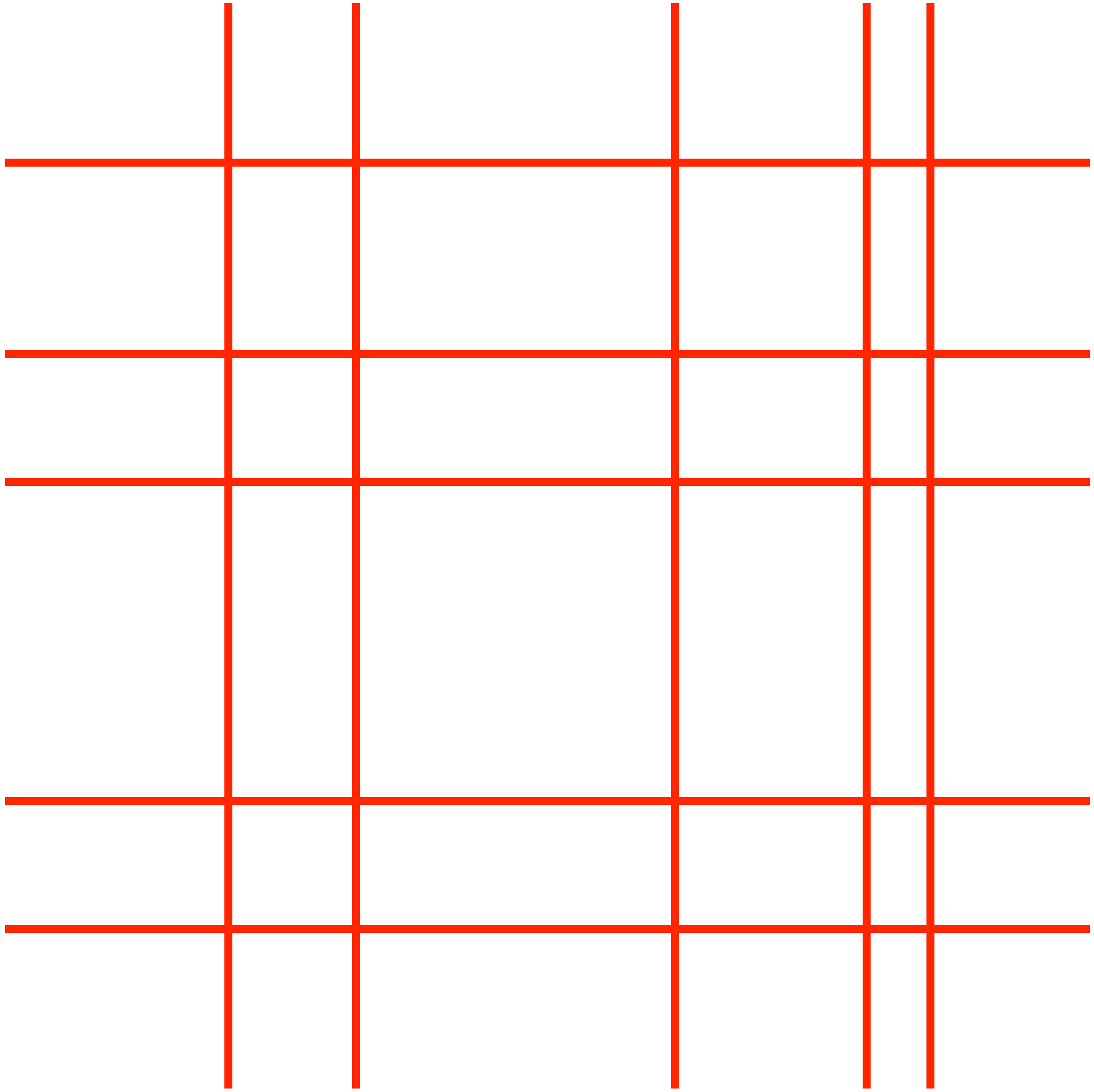
random projection from Tseitin($\mathrm{Grid}_{n\times n}$) to Tseitin($\mathrm{Grid}_{\ell\times\ell}$)



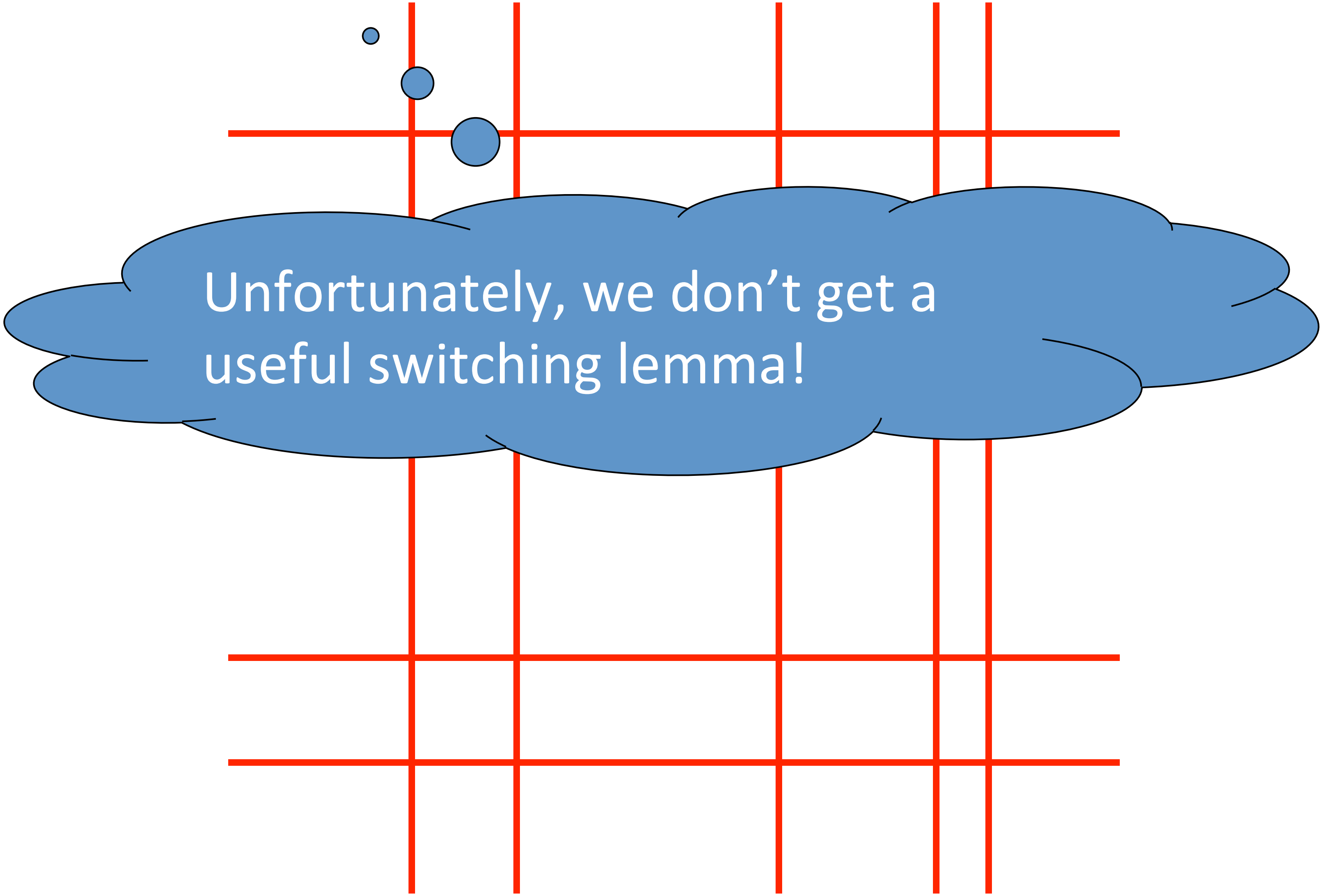
random projection from Tseitin($\mathrm{Grid}_{n\times n}$) to Tseitin($\mathrm{Grid}_{\ell\times\ell}$)



random projection from Tseitin($\text{Grid}_{n \times n}$) to Tseitin($\text{Grid}_{\ell \times \ell}$)

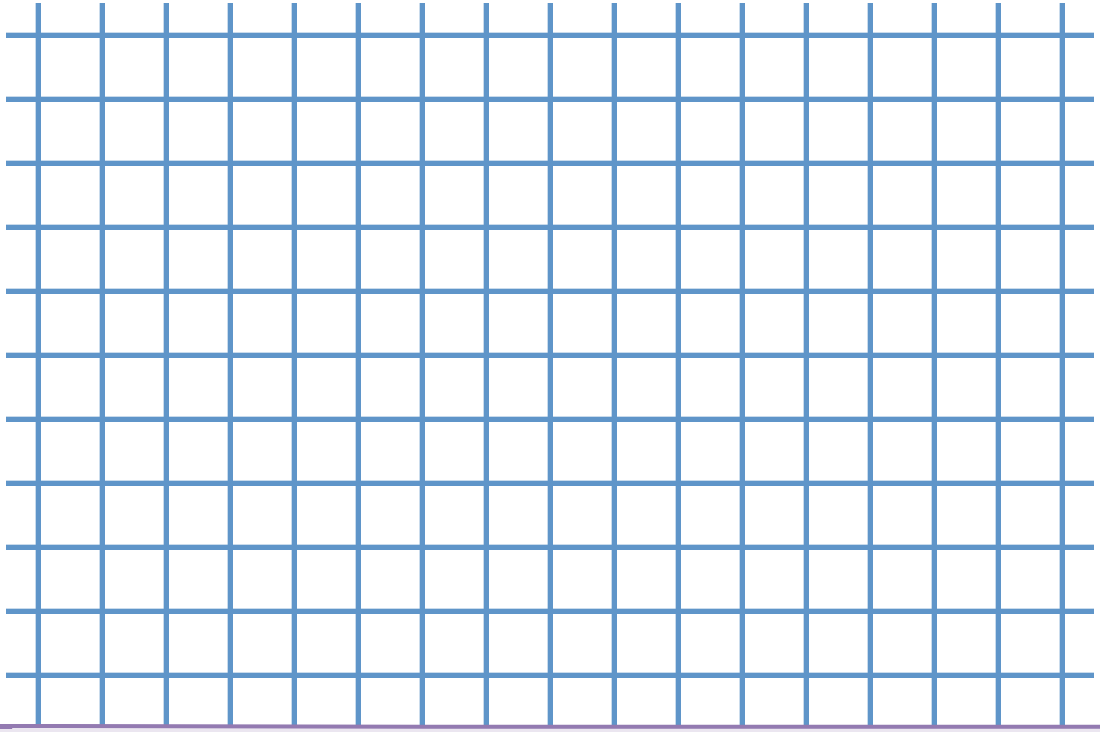


random projection from Tseitin($\mathrm{Grid}_{n\times n}$) to Tseitin($\mathrm{Grid}_{\ell\times\ell}$)



Unfortunately, we don't get a useful switching lemma!

random projection from Tseitin(Grid$_{n\times n}$) to Tseitin(Grid$_{\ell\times\ell}$)

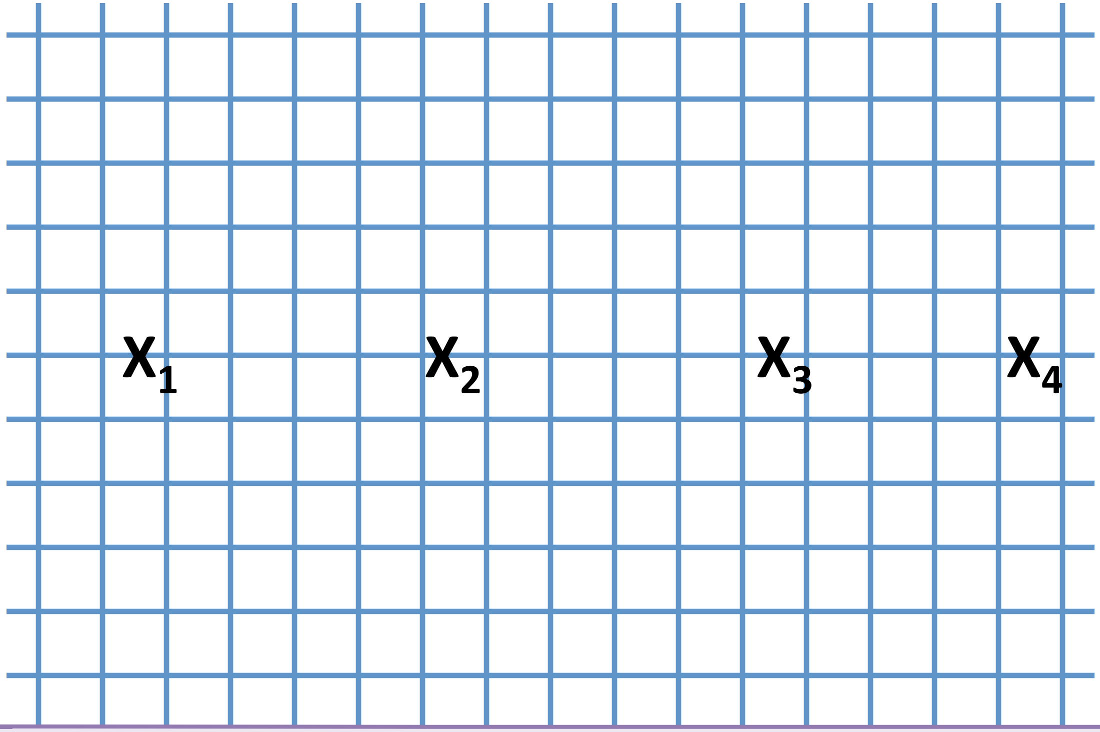


<u>Requirement for any useful switching lemma</u>:

Pr[any k given X-variables (i.e. edges of original grid) project to <u>distinct</u> Y-variables]

$\leq \varepsilon^k$ (for some $\varepsilon < 1$)

random projection from Tseitin($\mathrm{Grid}_{n\times n}$) to Tseitin($\mathrm{Grid}_{\ell\times\ell}$)

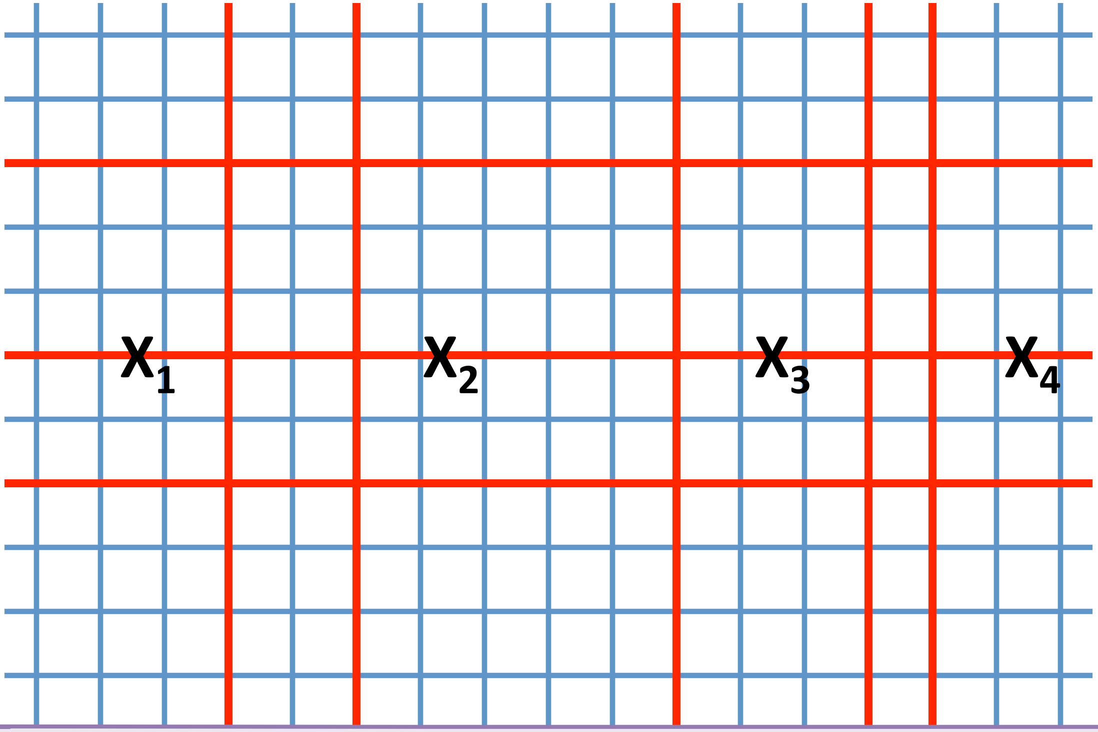


Requirement for any useful switching lemma:

Pr[any k given X-variables (i.e. edges of original grid) project to distinct Y-variables]

$\leq \varepsilon^k$ (for some $\varepsilon < 1$)

random projection from Tseitin(Grid$_{n\times n}$) to Tseitin(Grid$_{\ell\times\ell}$)

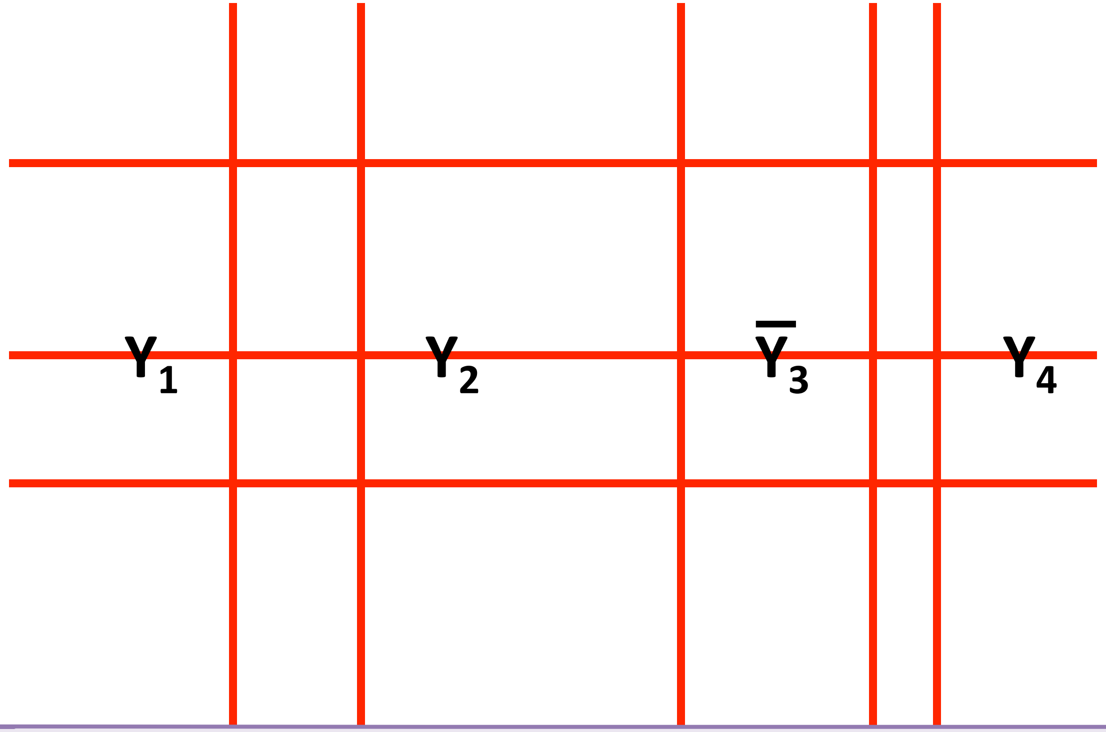


Requirement for any useful switching lemma:

Pr[any k given X-variables (i.e. edges of original grid) project to distinct Y-variables]

$\leq \varepsilon^k$ (for some $\varepsilon < 1$)

random projection from Tseitin(Grid$_{n\times n}$) to Tseitin(Grid$_{\ell\times\ell}$)

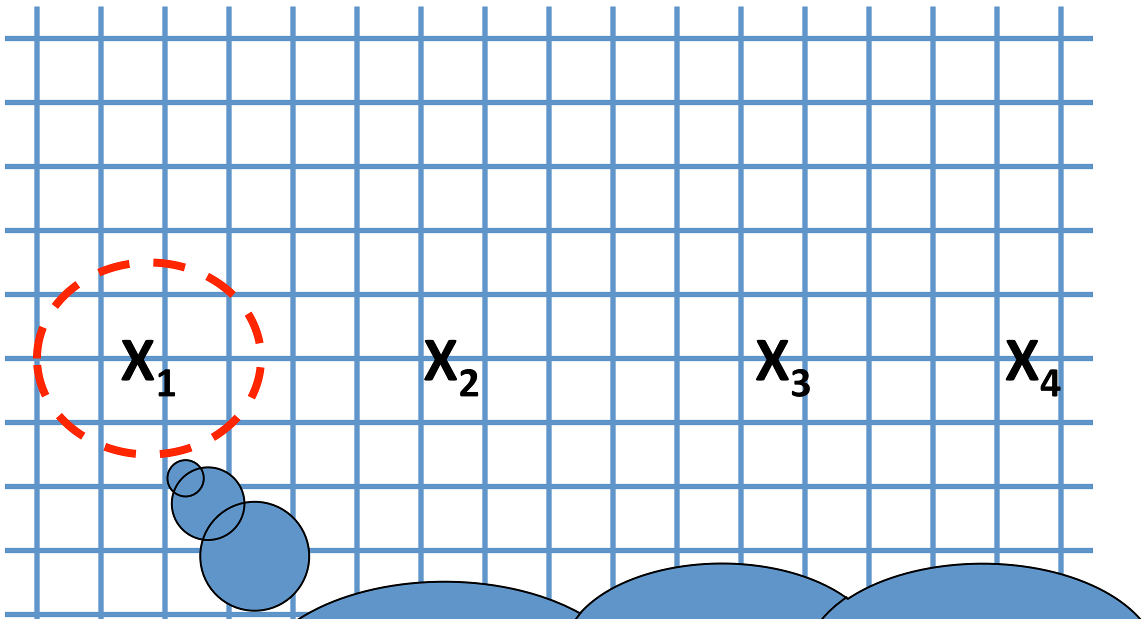


Requirement for any useful switching lemma:

Pr[any k given X-variables (i.e. edges of original grid) project to distinct Y-variables]

$\le \varepsilon^k$ (for some $\varepsilon < 1$)

random projection from Tseitin($\text{Grid}_{n\times n}$) to Tseitin($\text{Grid}_{\ell\times\ell}$)



If X_1 survives the projection, then w.h.p. all survive and map to distinct Y-variables (hence, no exponential tail bound in # of X-variables)

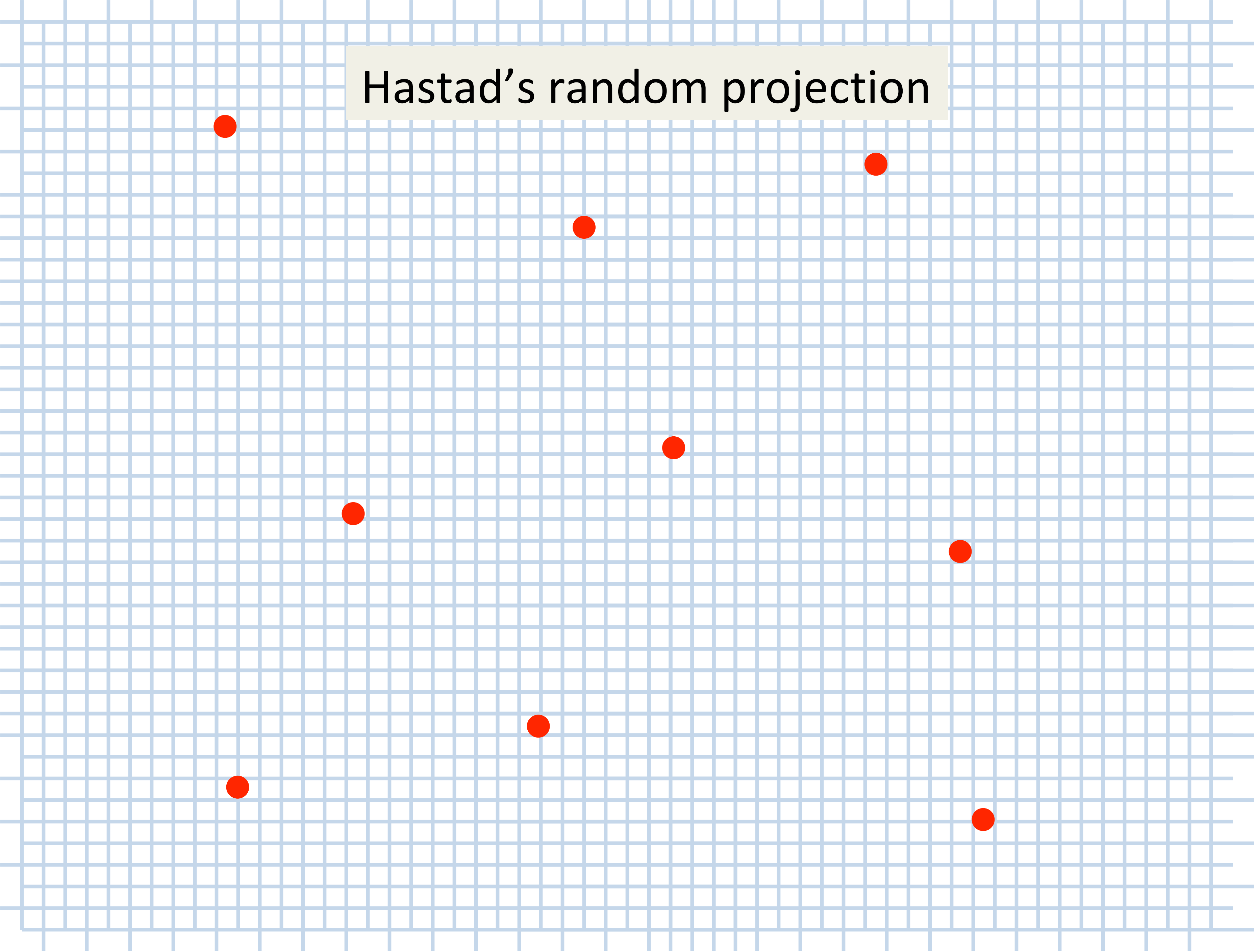
P

)

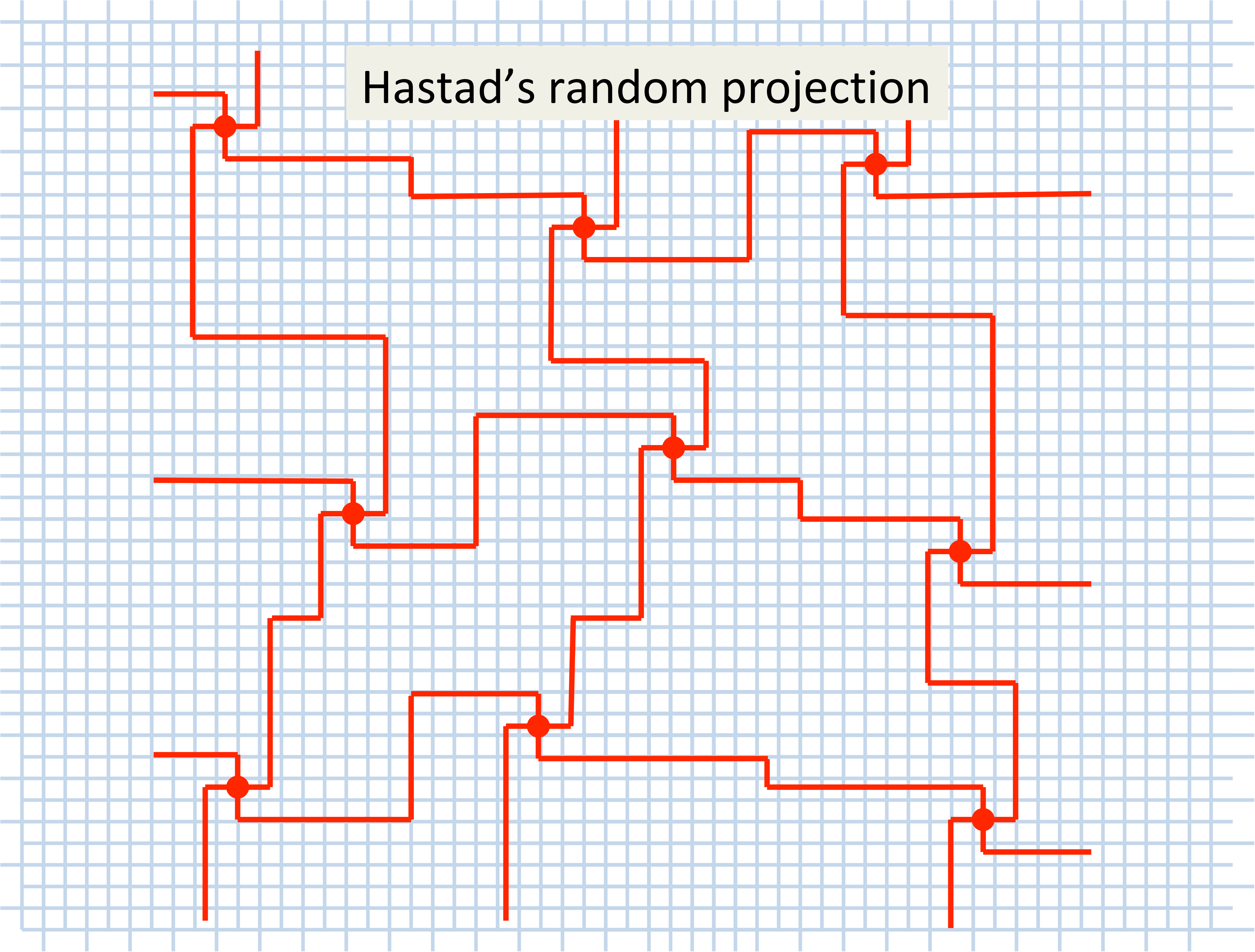
$\leq \varepsilon^k$ (

Hastad’s random projection

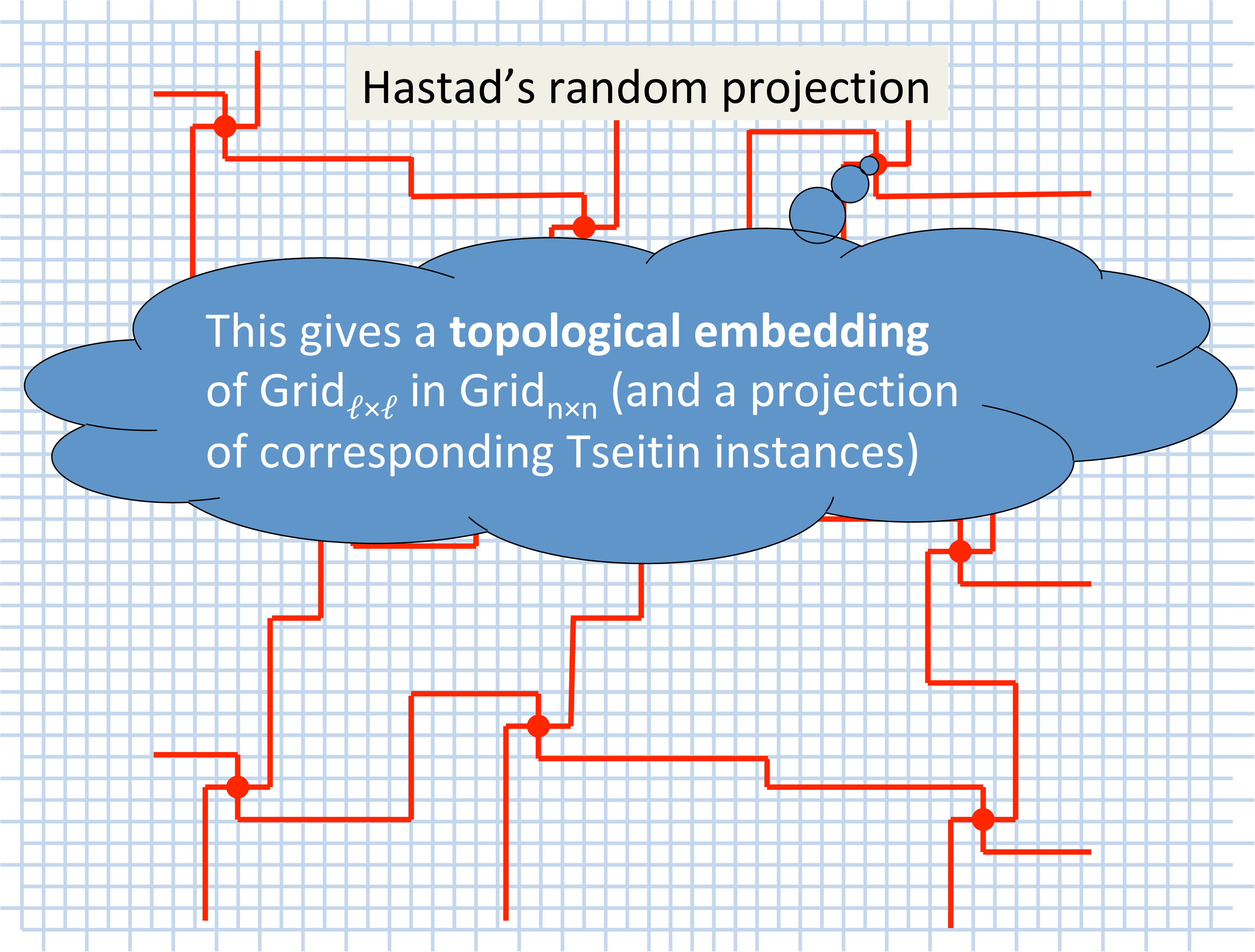
Hastad’s random projection



Hastad’s random projection

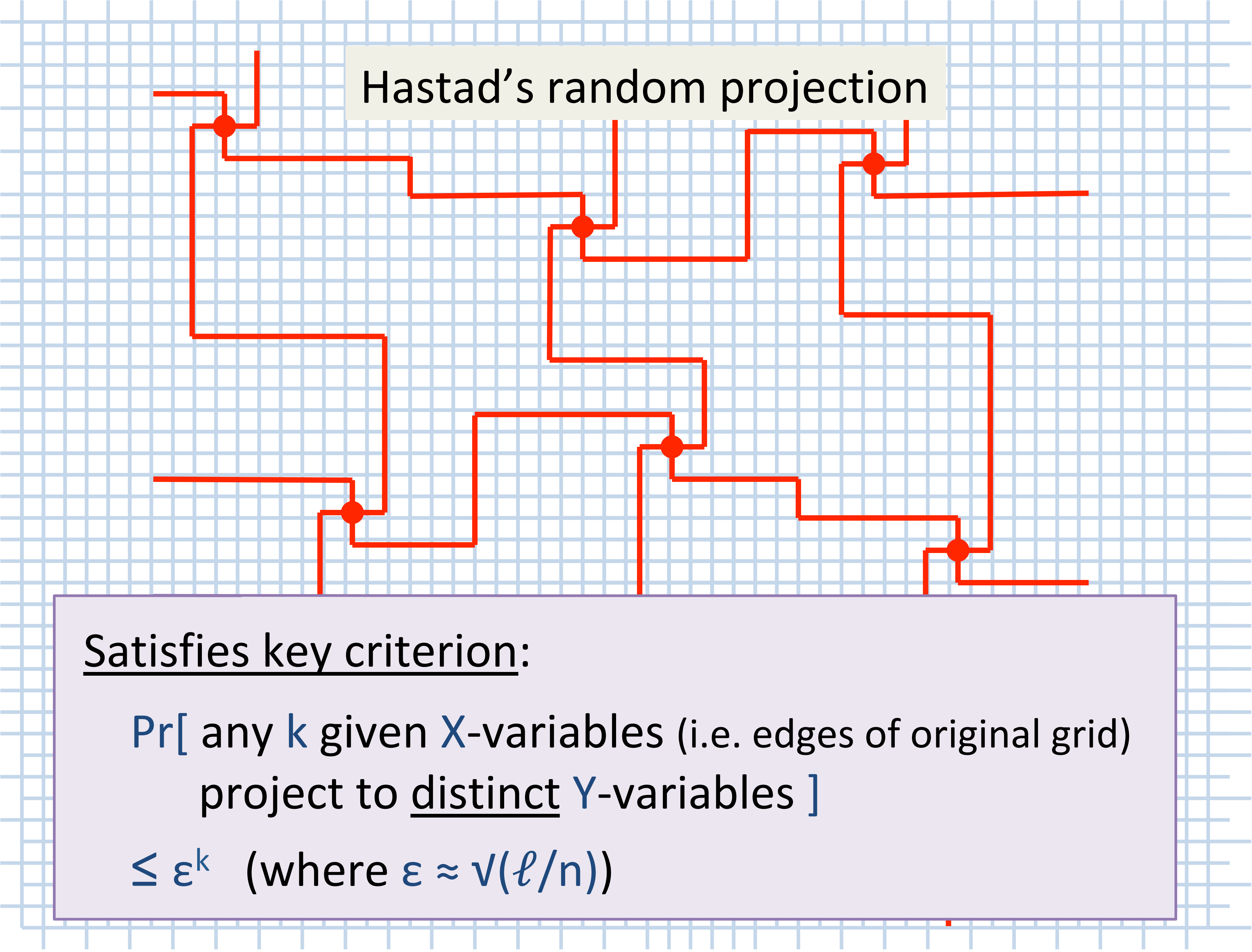


Hastad’s random projection



This gives a **topological embedding** of Grid$_{\ell\times\ell}$ in Grid$_{n\times n}$ (and a projection of corresponding Tseitin instances)

Hastad’s random projection

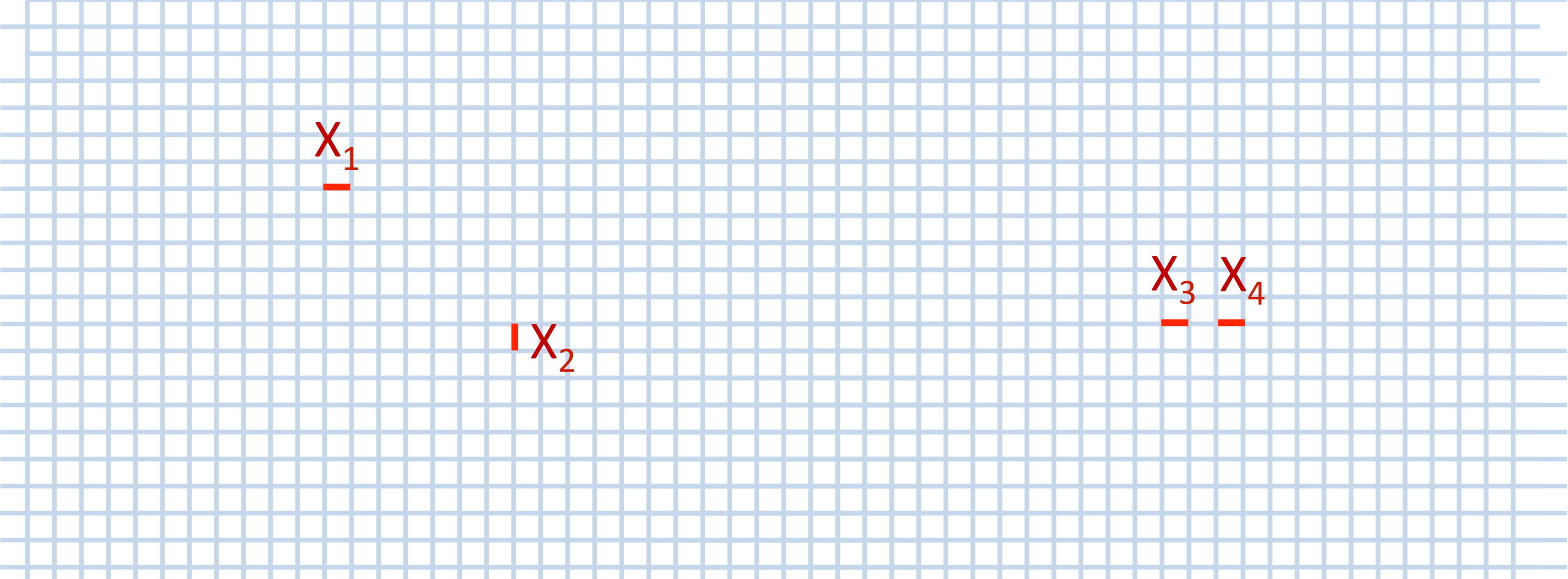


Satisfies key criterion:

Pr[any k given X-variables (i.e. edges of original grid) project to distinct Y-variables]

$\leq \varepsilon^k$ (where $\varepsilon \approx \sqrt{\ell/n}$)

$\Pr[\ X_1,\ldots,X_4$ project to *distinct* Y-variables $] \le p^4$

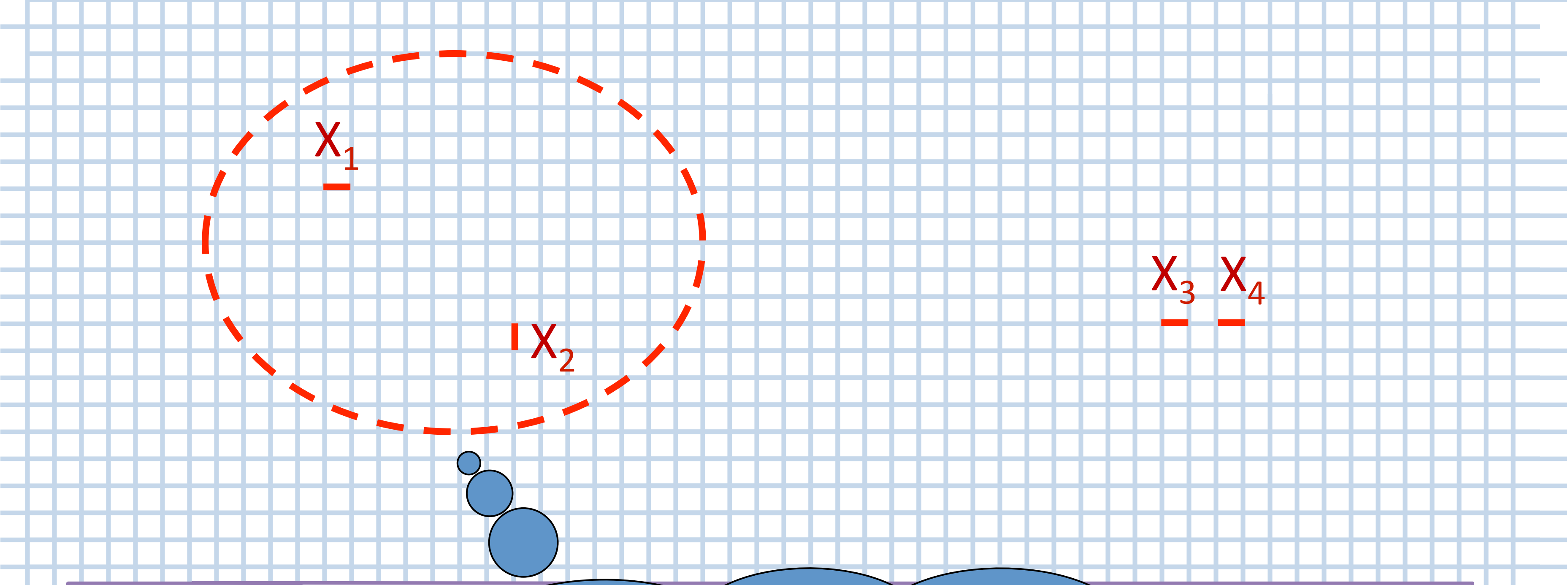


Satisfies key criterion:

Pr[any k given X-variables (i.e. edges of original grid)
project to distinct Y-variables]

$\le \varepsilon^k$ (where $\varepsilon \approx \sqrt{(\ell/n)}$)

Pr[$X_1,\ldots,X_4$ project to *distinct* Y-variables] $\leq p^4$



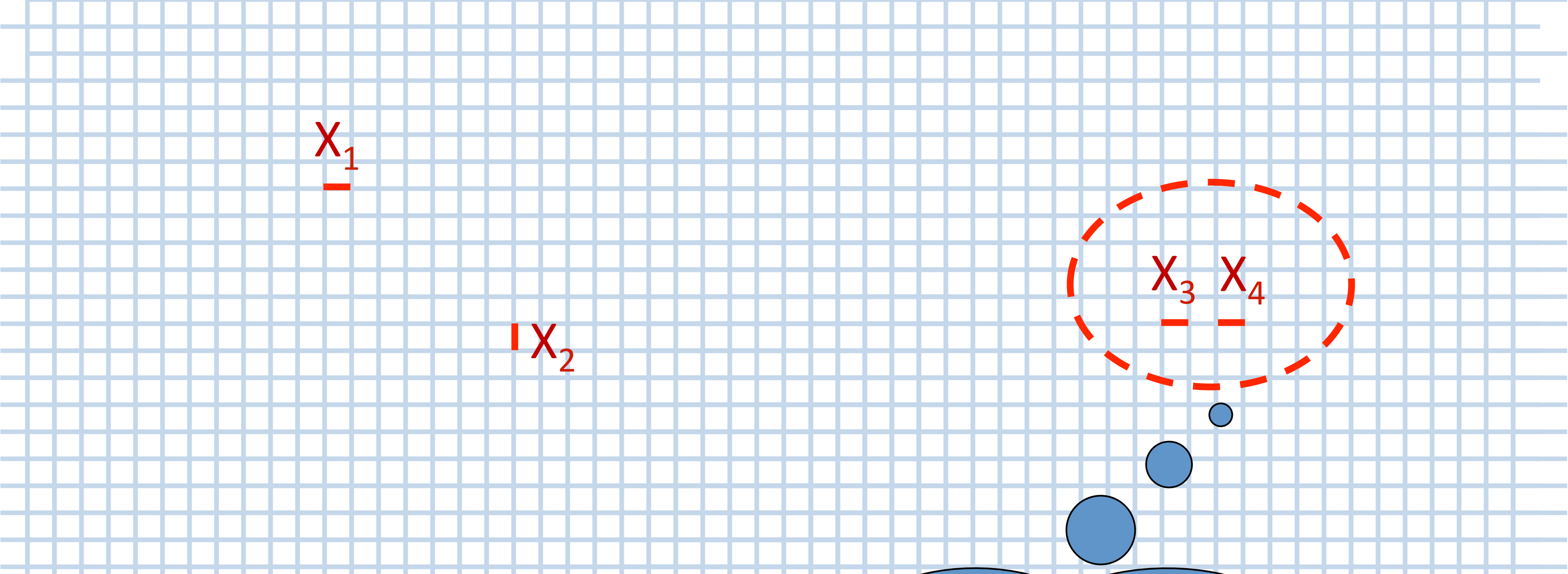
far apart edges ⇒ independent probability of surviving the projection

Satisf

al grid)

$\leq \varepsilon^k$ (

Pr[$X_1,\ldots,X_4$ project to *distinct* Y-variables] ≤ p^4



Satisfies key

Pr[a

pr

≤ ε^k (where

nearby edges ⇒

if both survive, likely to project to *same* Y-variable

Hastad’s depth reduction argument has two steps:

Hastad’s depth reduction argument has two steps:

① switching lemma with respect to a preliminary “partial restriction” (with greater independence properties, needed for the Razborov-style argument)

Hastad’s depth reduction argument has two steps:

① switching lemma with respect to a preliminary “partial restriction” (with greater independence properties, needed for the Razborov-style argument)

reduces the depth of each formula in an AC^0-Frege proof

Hastad’s depth reduction argument has two steps:

① switching lemma with respect to a preliminary “partial restriction” (with greater independence properties, needed for the Razborov-style argument)

② clean-up step: (arbitrary) completion of the “partial restriction” to an embedding of $\text{Tseitin}(\text{Grid}_{\ell\times\ell})$ in $\text{Tseitin}(\text{Grid}_{n\times n})$

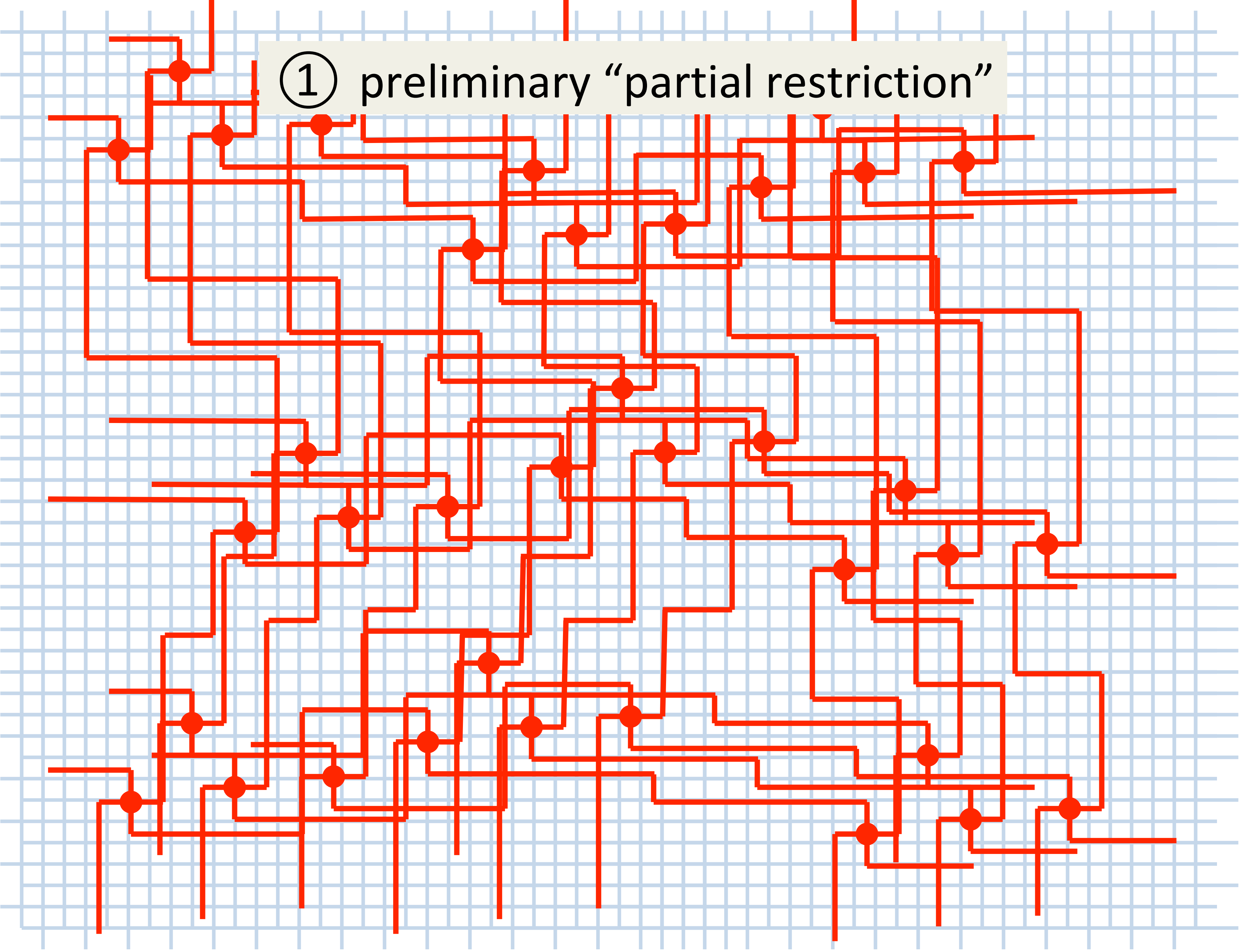
Hastad’s depth reduction argument has two steps:

① switching lemma with respect to a preliminary “partial restriction” (with greater independence properties, needed for the Razborov-style argument)

② clean-up step: (arbitrary) completion of the “partial restriction” to an embedding of $\mathrm{Tseitin}(\mathrm{Grid}_{\ell\times\ell})$ in $\mathrm{Tseitin}(\mathrm{Grid}_{n\times n})$

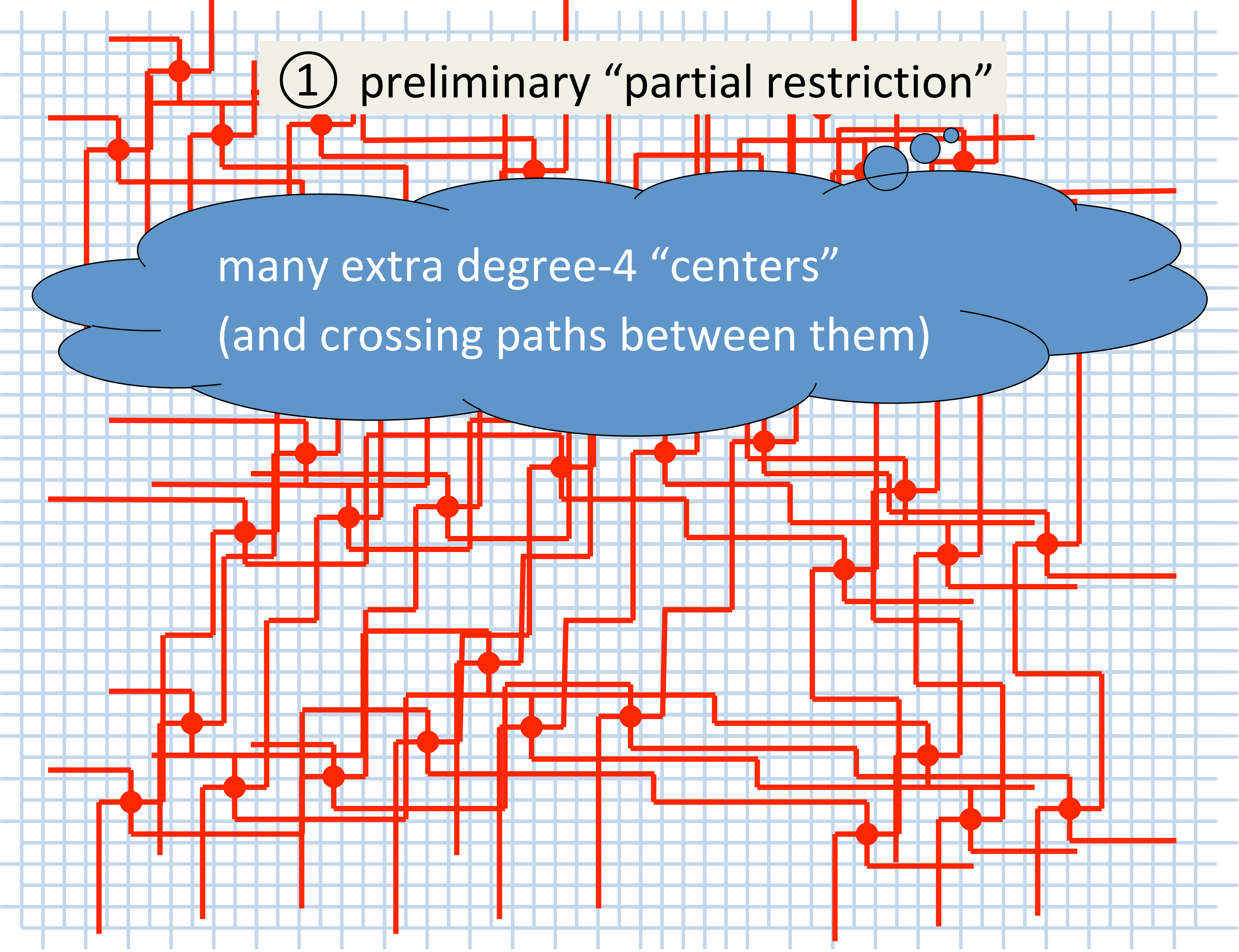
for purpose of induction

① preliminary “partial restriction”

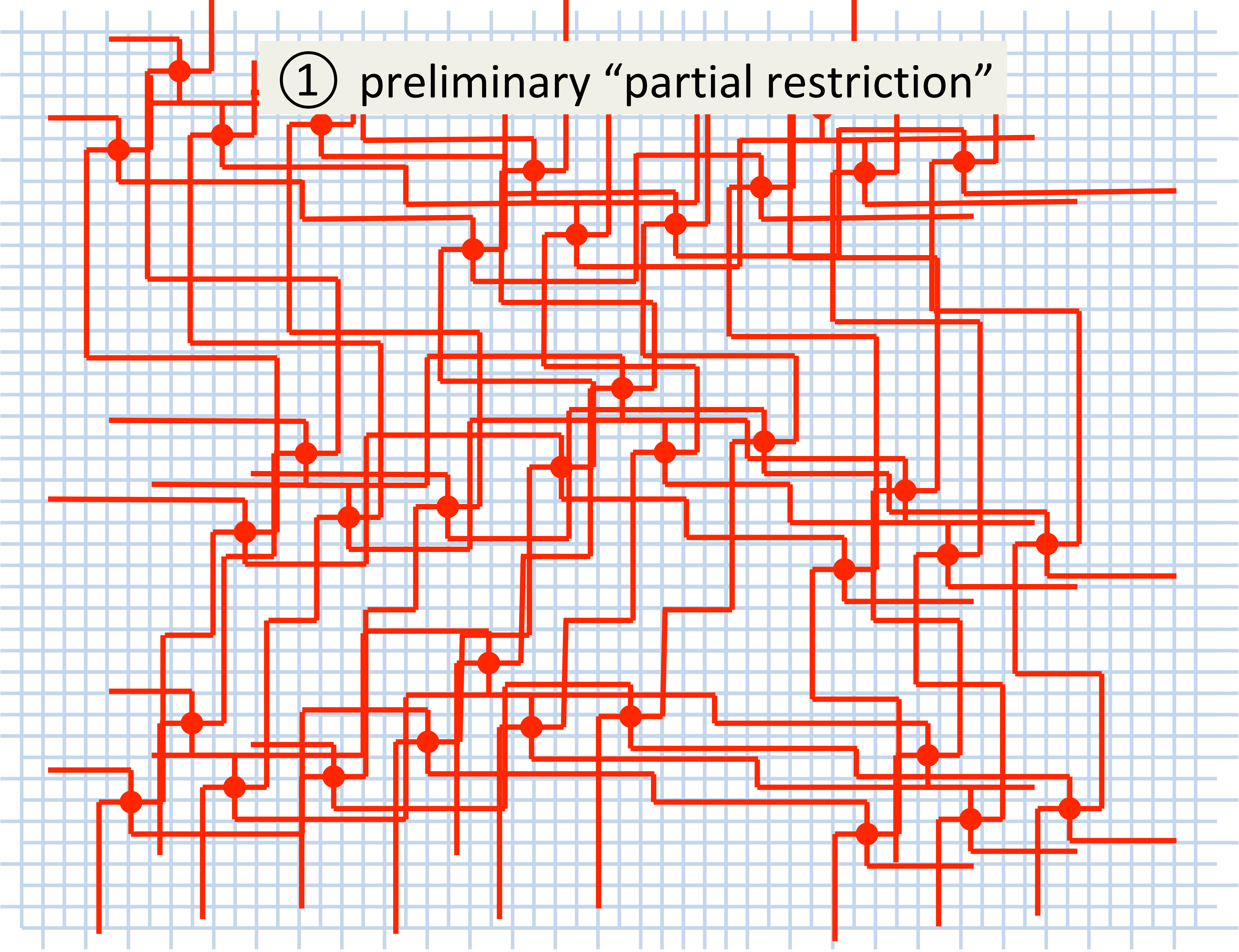


① preliminary “partial restriction”

① preliminary “partial restriction”

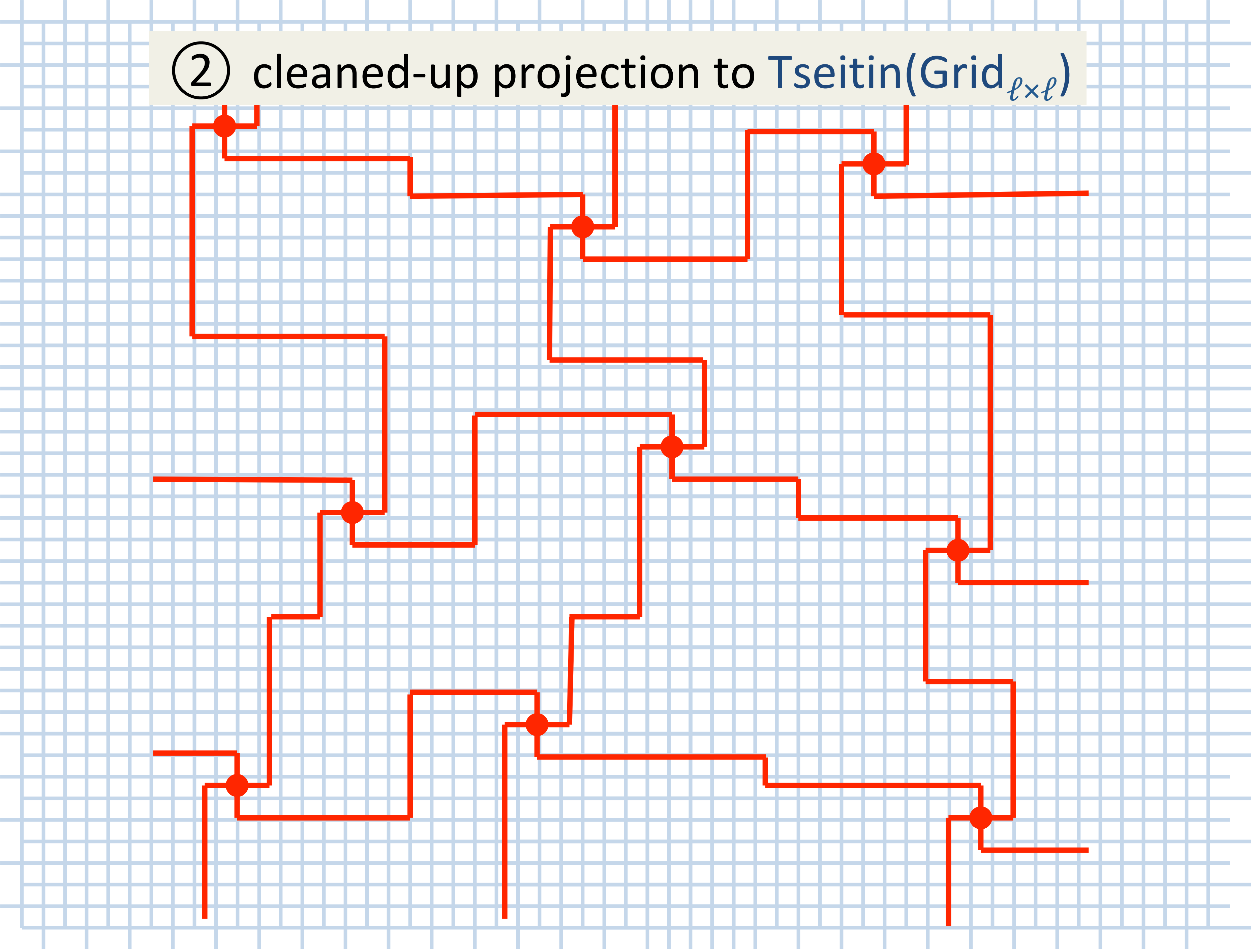


many extra degree-4 “centers”
(and crossing paths between them)



① preliminary “partial restriction”

② cleaned-up projection to Tseitin(Grid$_{\ell\times\ell}$)

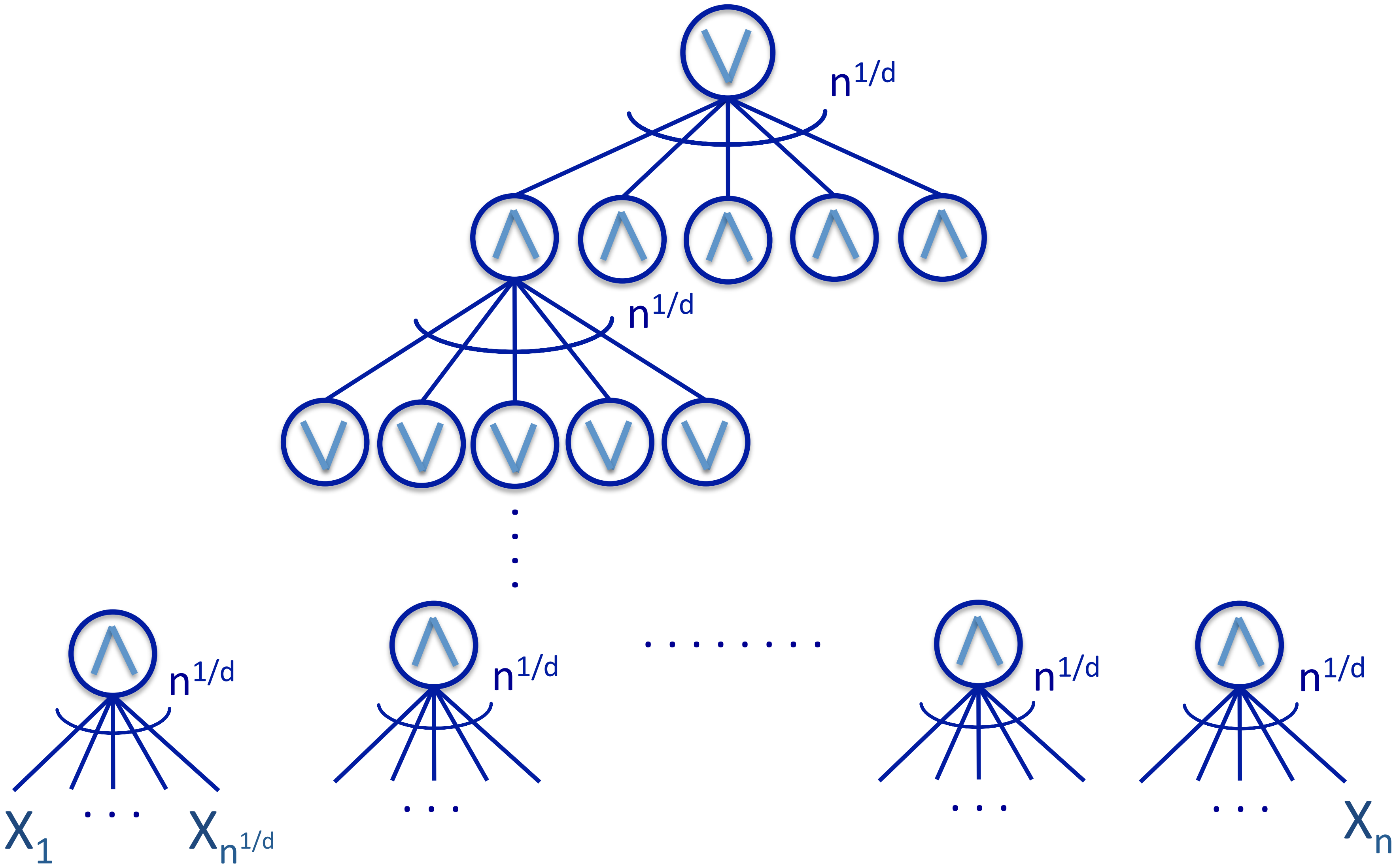


AC^0-Frege Depth Hierarchy?

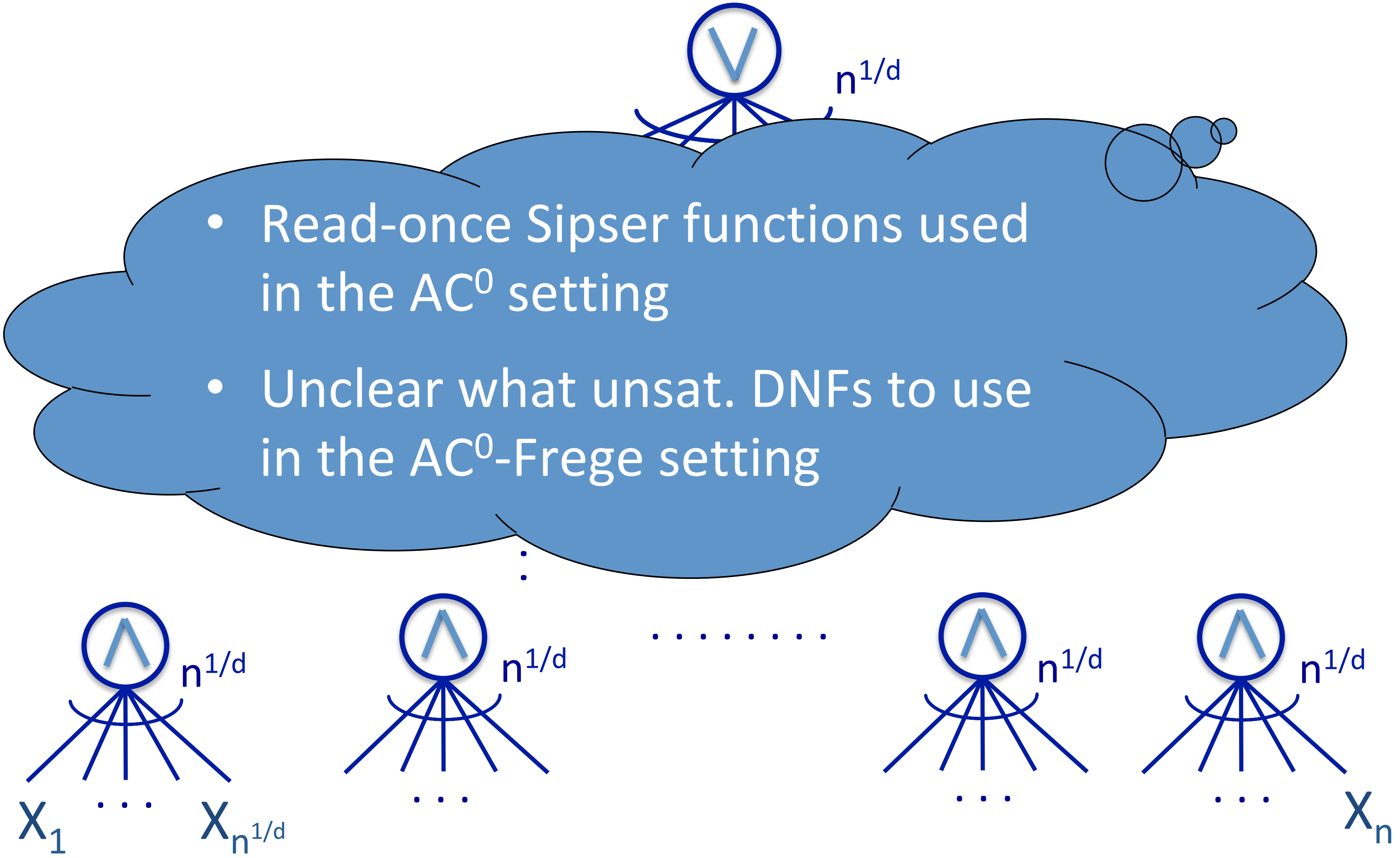
- Open Problem

  Find a family of unsatisfiable DNF formulas with poly(n)-size depth d+1 refutations, which require $\exp(n^{\Omega(1/d)})$-size depth d refutations.

AC^0 Depth Hierarchy



AC^0 Depth Hierarchy



- Read-once Sipser functions used in the AC^0 setting
- Unclear what unsat. DNFs to use in the AC^0-Frege setting

Thank You!