SMALL DEPTH CIRCUIT LOWER BOUNDS VIA THE SWITCHING LEMMA

SRIKANTH SRINIVASAN

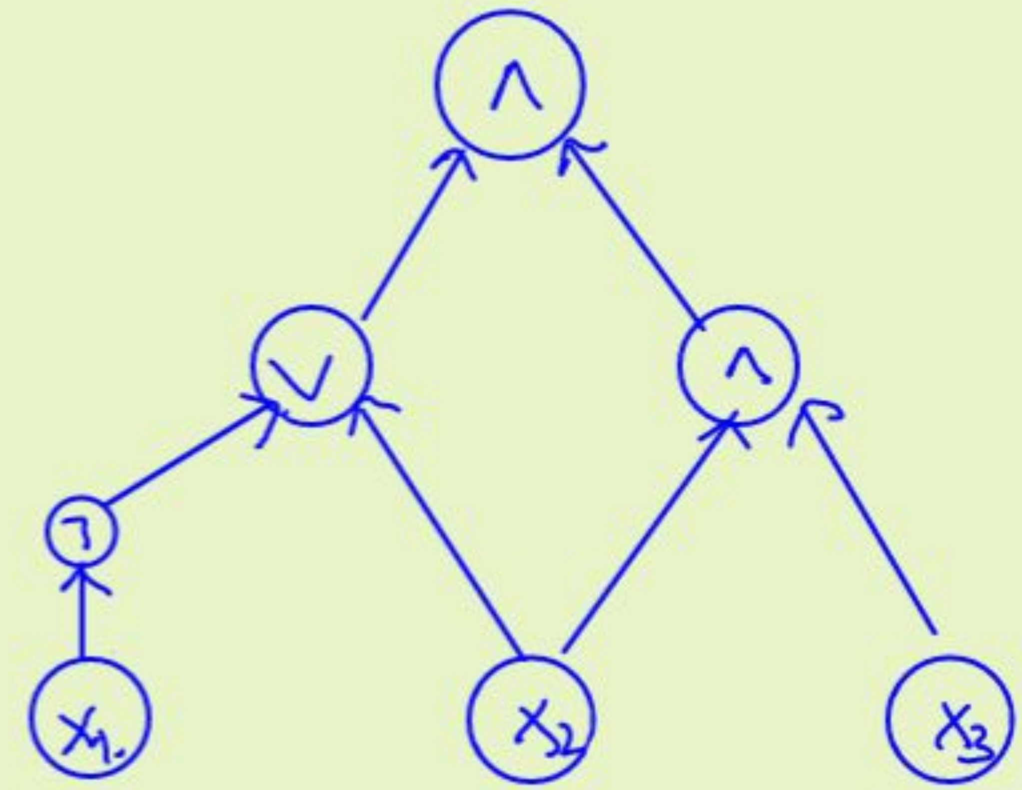
UNIV. OF COPENHAGEN

Circuit Complexity

→ Boolean circuit

De Morgan basis

AND / OR / NOT

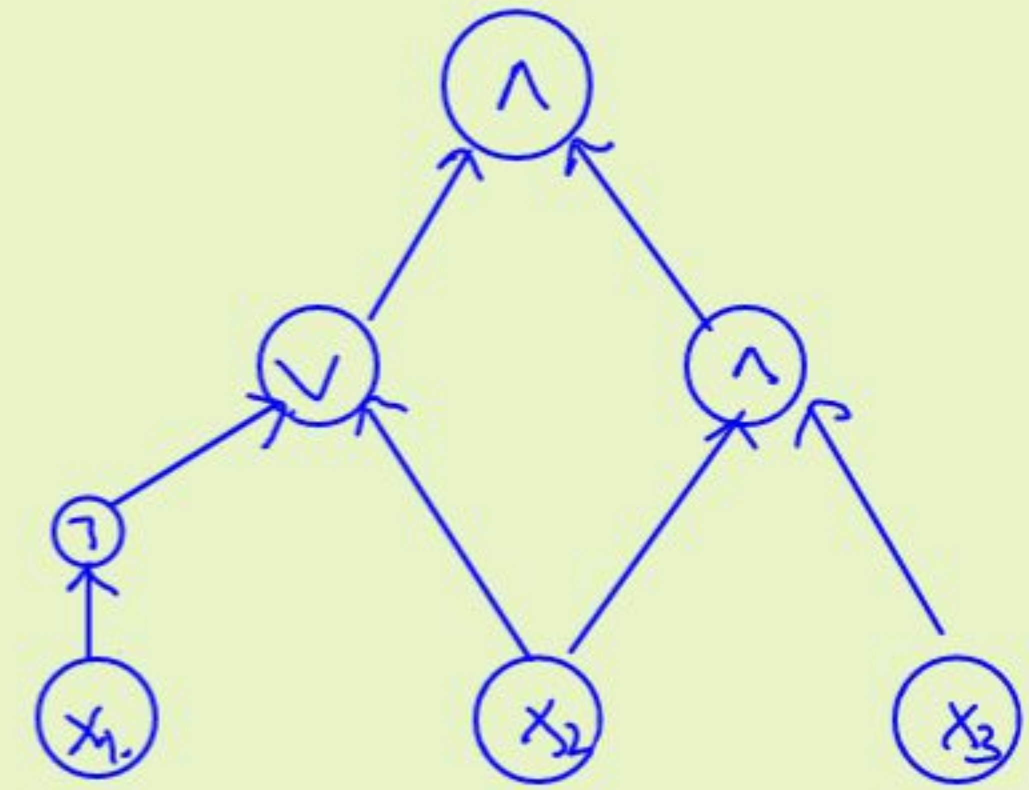


Circuit Complexity

→ Boolean circuit

De Morgan basis

AND / OR / NOT



Size = # of gates = 6

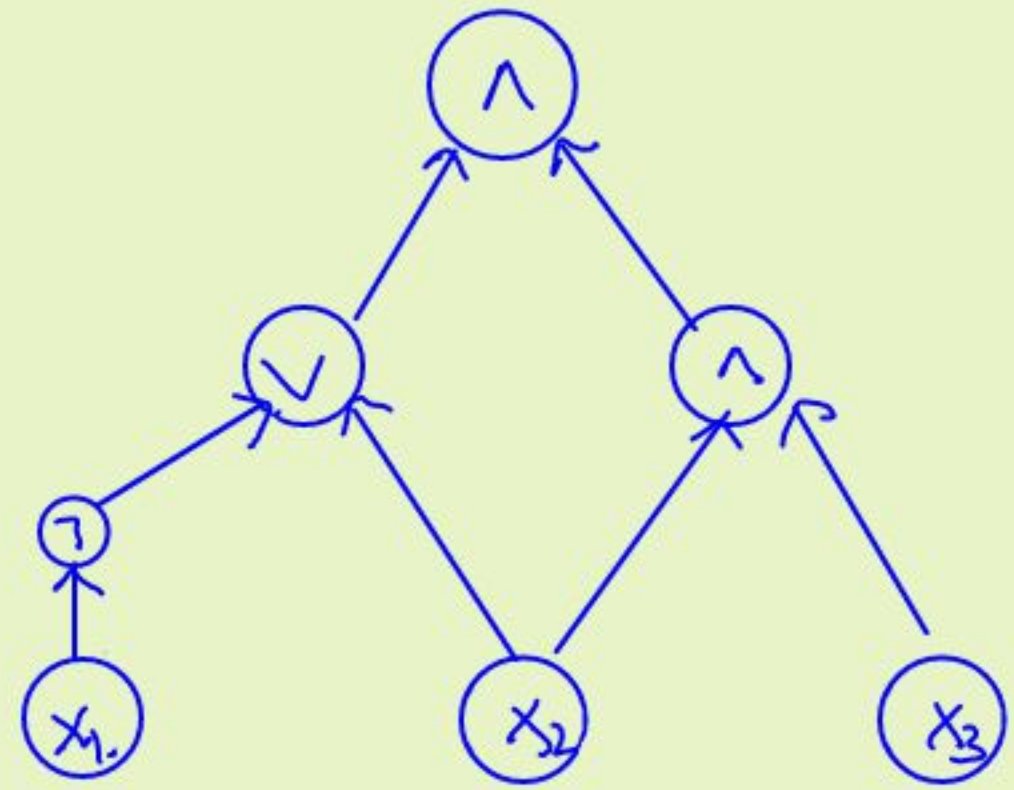
Depth = longest AND/OR path = 2.

Circuit Complexity

→ Boolean circuit

De Morgan basis

AND / OR / NOT



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

→ Any f has a circuit of size $O(2^n)$.

→ Most f need size $2^{\Omega(n)}$

→ Explicit f ?

Size = # of gates = 6

Depth = longest AND/OR path = 2.

Circuit Complexity

→ Boolean circuit

De Morgan basis

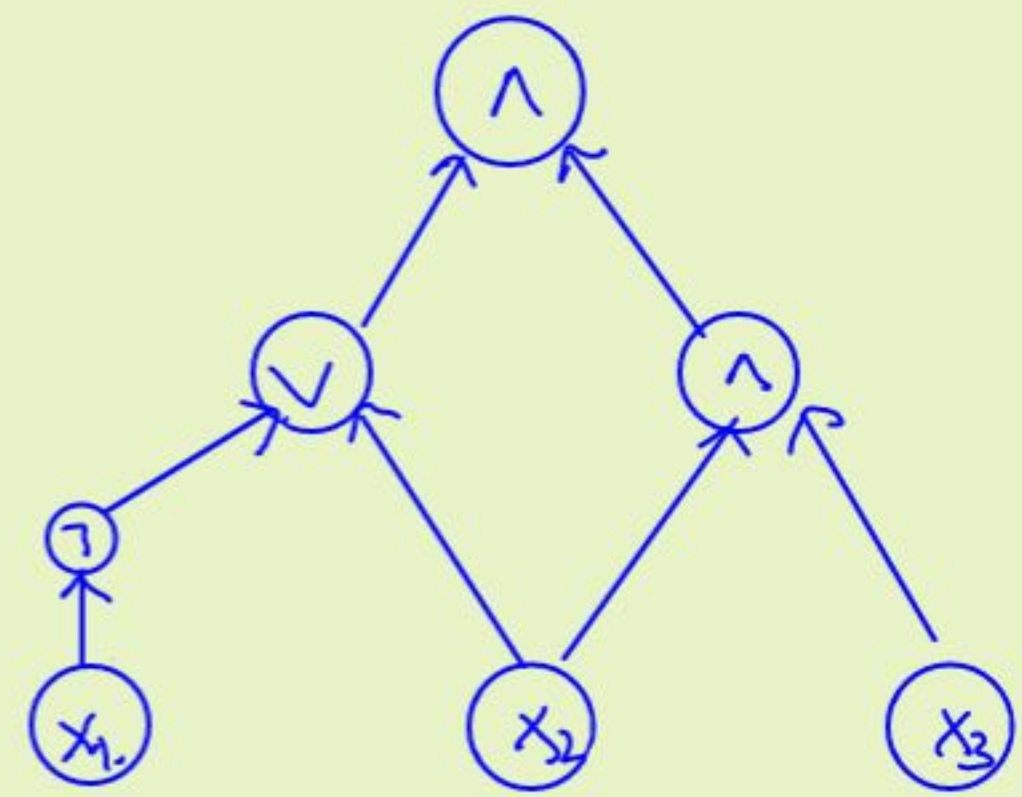
AND / OR / NOT

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

→ Any f has a circuit of size $O(2^n)$.

→ Most f need size $2^{\Omega(n)}$

→ Explicit f ?



Size = # of gates = 6

Depth = longest AND/OR path = 2.

By using De Morgan's laws, literals at leaves. Combine consecutive ANDs/ORs.

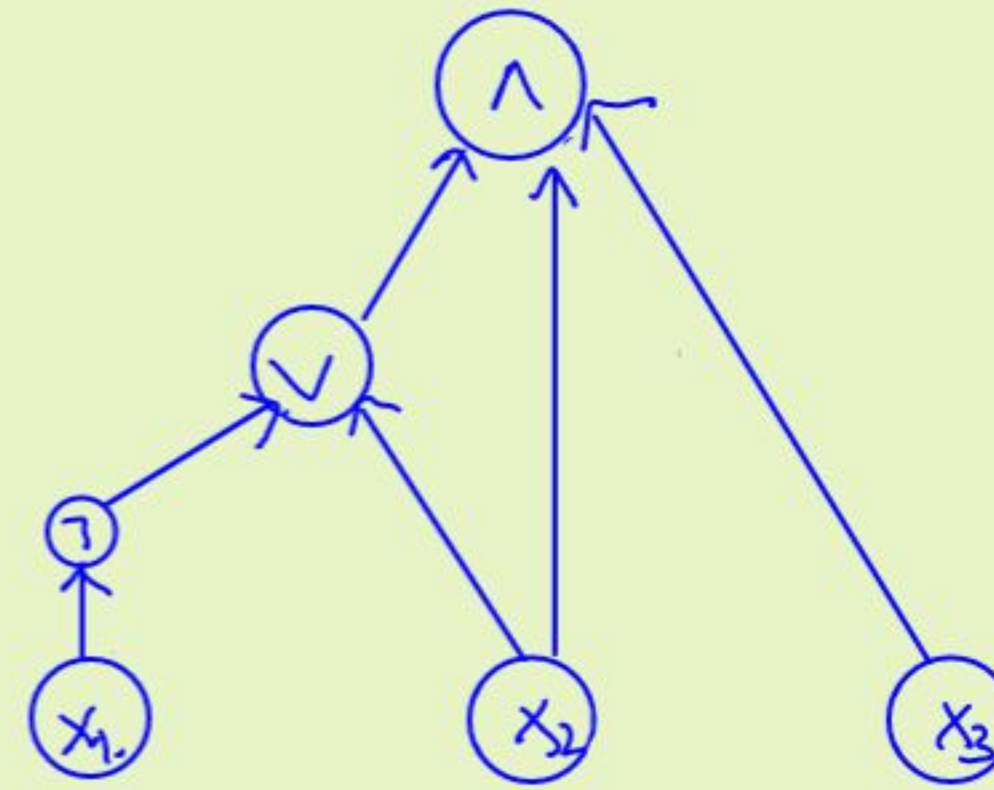
Circuit Complexity

→ Boolean circuit

De Morgan basis

AND / OR / NOT

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



→ Any f has a circuit of size $O(2^n)$.

→ Most f need size $2^{\Omega(n)}$

→ Explicit f ?

Size = # of gates = 6

Depth = longest AND/OR path = 2.

By using De Morgan's laws, literals at leaves. Combine consecutive ANDs/ORs.

Hard function: Parity

$\text{AND}(*, *, \ldots *, 0, *, \cdots *) = 0$

$\text{OR}(*, *, 1, * \cdots\ *) = 1$

Hard function: Parity

$$AND(*, *, \dots *, 0, *, \dots *) = 0$$

$$OR(*, *, 1, * \dots *) = 1$$

$$Parity_n = \oplus_n : \{0,1\}^n \to \{0,1\}$$

$$(x_1, \dots, x_n) \mapsto x_1 \oplus \dots \oplus x_n$$

Cannot fix to a constant without setting all inputs.

Hard function: Parity

$\mathrm{AND}(*, *, \ldots *, 0, *, \cdots *) = 0$

$\mathrm{OR}(*, *, 1, * \cdots *) = 1$

$\mathrm{Parity}_n = \oplus_n : \{0,1\}^n \to \{0,1\}$

$(x_1, \ldots, x_n) \mapsto x_1 \oplus \cdots \oplus x_n$

Sensitivity of $\oplus_n$

Cannot fix to a constant without setting all inputs.

Hard function: Parity

$\mathrm{AND}(*, *, \ldots *, 0, *, \ldots *) = 0$

$\mathrm{OR}(*, *, 1, * \cdots \; *) = 1$

$\mathrm{Parity}_n = \oplus_n : \{0,1\}^n \to \{0,1\}$

$(x_1, \ldots, x_n) \mapsto x_1 \oplus \cdots \oplus x_n$

Sensitivity of $\oplus_n$

Cannot fix to a constant without setting all inputs.

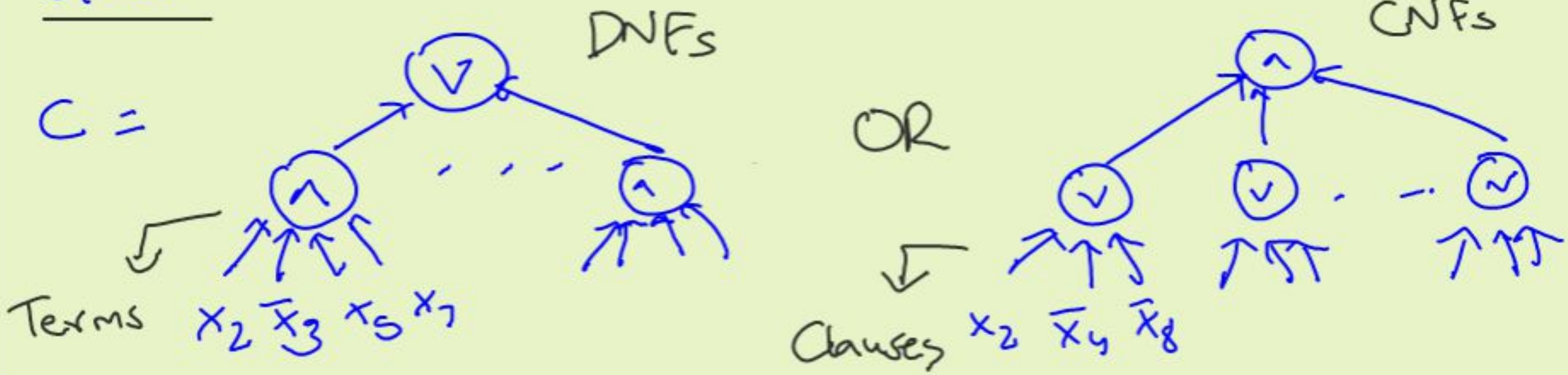
Thm: [FSS'81, Ajtai'83, ..., Håstad'86] Depth d circuits for $\oplus_n$ need size $\exp(\Omega(n^{1/d-1}))$.

2	n
3	$\sqrt{n}$
4	$n^{1/3}$

Ex: Tight!

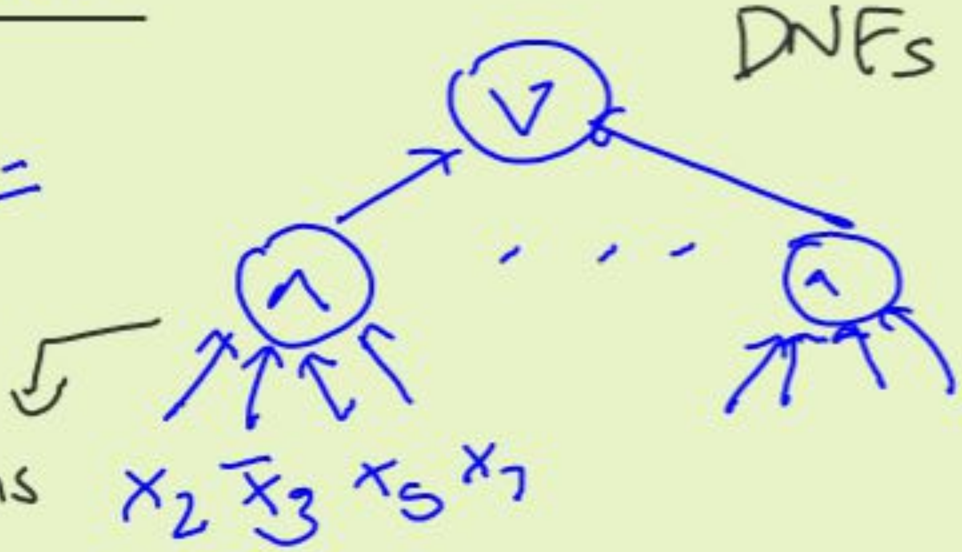
$\underline{d=2}$

$C =$

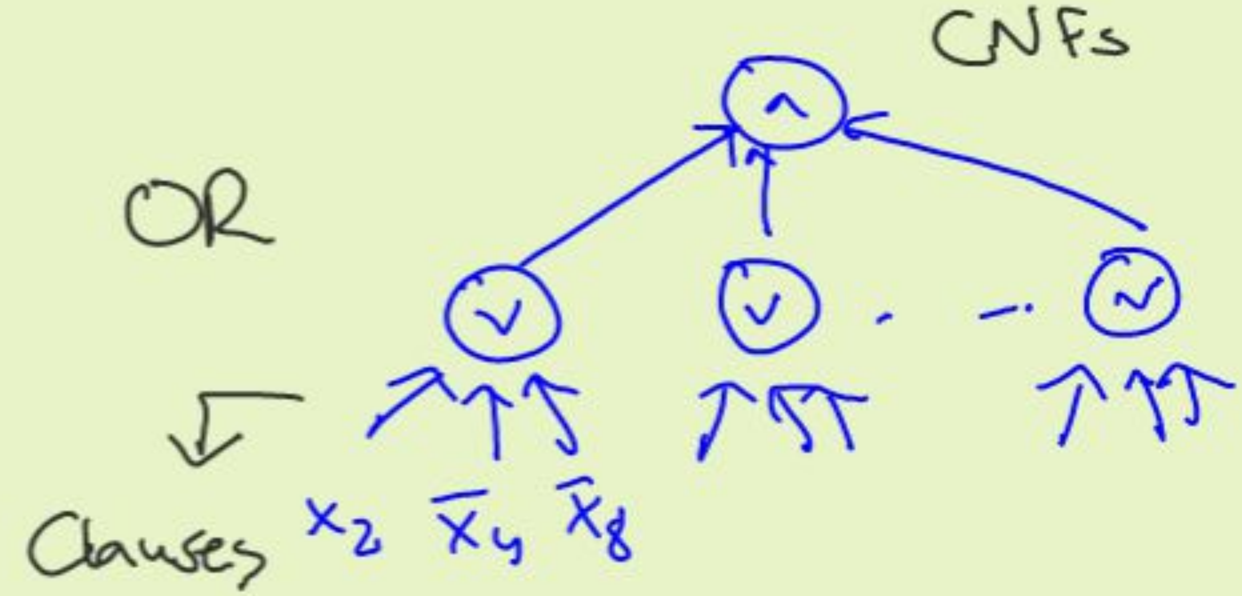


$d=2$

$C =$



OR

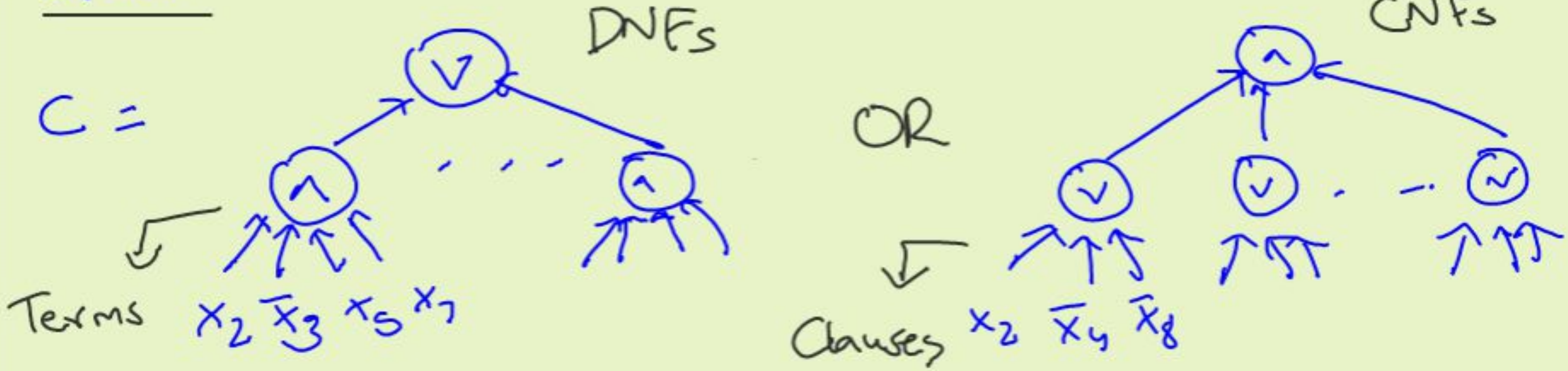


Clm: C a DNF for $\oplus_n \implies$ all terms have width n

Sensitivity of $\oplus_n$

$d=2$

$C =$



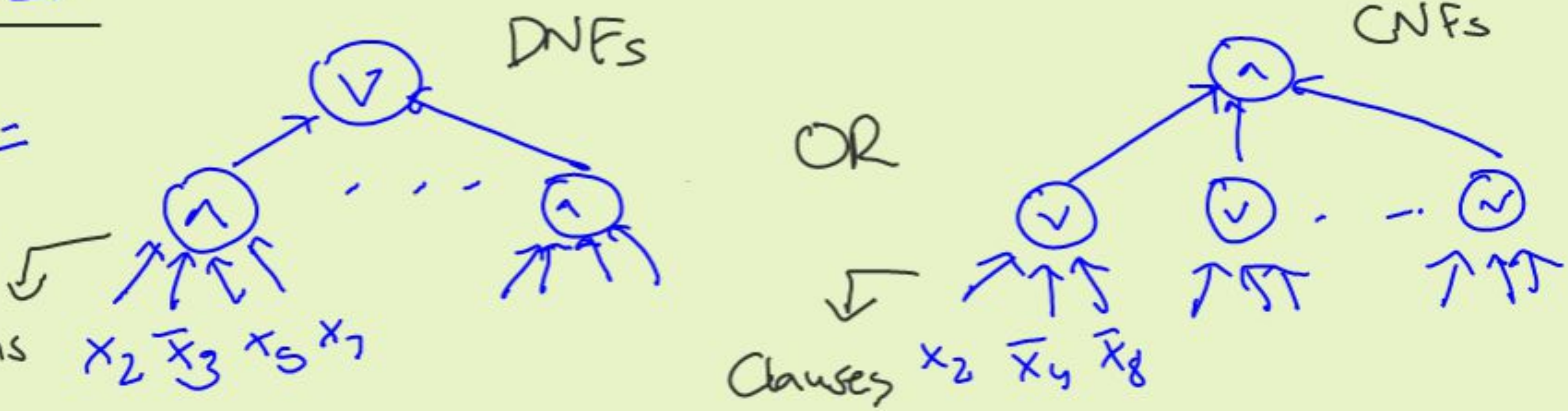
Clm: C a DNF for $\oplus_n \Longrightarrow$ all terms have width n

Sensitivity of $\oplus_n$

Obs: $\oplus_n^{-1}(1) = 2^{n-1} \Rightarrow 2^{n-1}$ terms needed.

$d=2$

$C =$



Clm: C a DNF for $\oplus_n \Longrightarrow$ all terms have width n

Sensitivity of $\oplus_n$

Obs: $\oplus_n^{-1}(1) = 2^{n-1} \Rightarrow 2^{n-1}$ terms needed.

[Analogous argument for CNFs]

Higher depths

Idea: Reduce to depth-2 iteratively via random restrictions.

Higher depths

Idea: Reduce to depth-2 iteratively via random restrictions.

Restriction $\rho : \{x_1, \ldots, x_n\} \to \{0, 1, *\}$

Higher depths

Idea: Reduce to depth-2 iteratively via random restrictions.

Restriction $\rho : \{x_1, \dots, x_n\} \to \{0, 1, *\}$

Random restriction with $*$-probability $q \in [0,1]$

→ Choose $S \subseteq [n]$, $|S| = qn$ u.a.r.

→ Set $\rho(x_i) = \begin{cases} * & i \in S \\ \text{uniformly random bit} & i \notin S \end{cases}$

Higher depths

Idea: Reduce to depth-2 iteratively via random restrictions.

Restriction $\rho : \{x_1, \dots, x_n\} \to \{0, 1, *\}$

Random restriction with $*$-probability $q \in [0,1]$

→ Choose $S \subseteq [n]$, $|S| = qn$ u.a.r.

→ Set $\rho(x_i) = \begin{cases} * & i \in S \\ \text{uniformly random bit} & i \notin S \end{cases}$

$\rho \sim R_{qn}$.

Informal Switching lemma

"Lemma": Any small-width DNF/CNF F simplifies whp under random restrictions.

$$\Pr_{\rho \sim R_{an}} [\underbrace{F\restriction_\rho}_{\text{restricted function}} \text{ "complicated"}] \leq \text{small}.$$

Informal Switching lemma

"Lemma": Any small-width DNF/CNF F simplifies whp under random restrictions.

$$\Pr\Big[\underbrace{F\restriction_\rho}_{\text{restricted function}} \text{ "complicated"}\Big] \leq \text{small.}$$

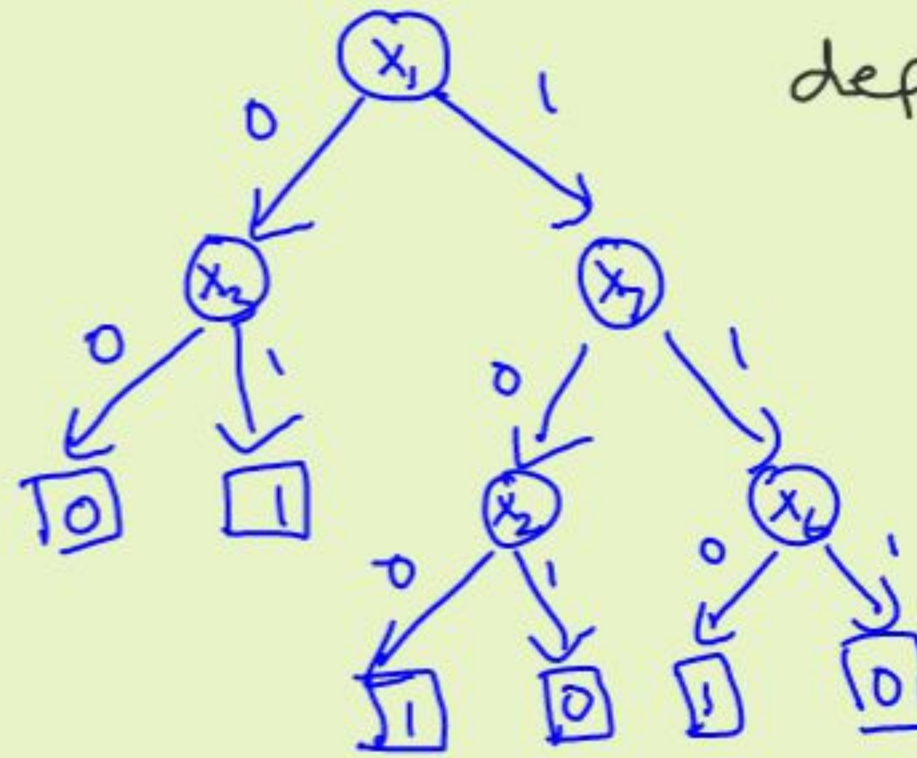
$\rho \sim R_{qn}$

→ Want: q not too small (E.g. $q > 1/n$)

General Switching Lemma

Decision trees

DTs of depth k



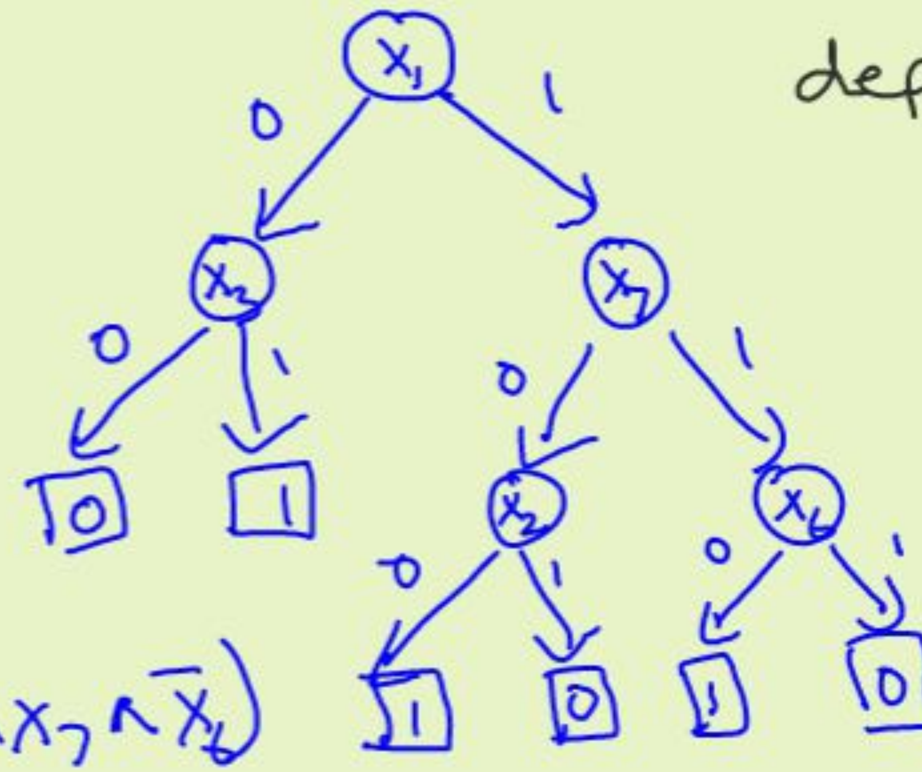
depth $= 3$

General Switching Lemma

Decision trees

DTs of depth k

k-DNFs $\qquad$ k-CNFs

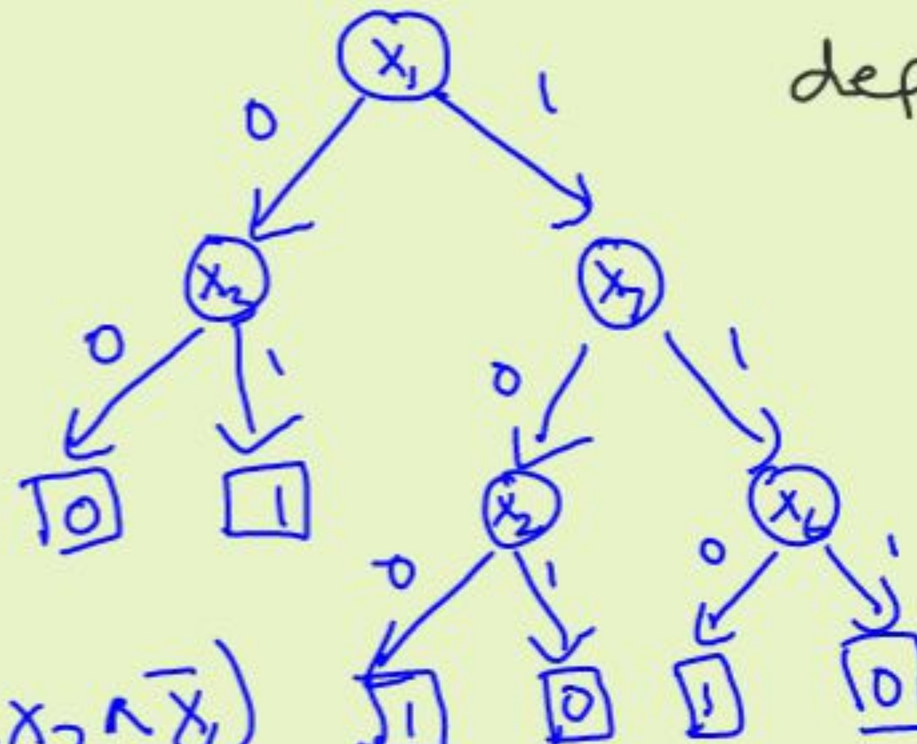


depth $= 3$

Eg: $(\bar{x}_1 \wedge x_3) \vee (x_1 \wedge \bar{x}_7 \wedge x_2) \vee (x_1 \wedge x_7 \wedge \bar{x}_6)$

General Switching Lemma

Decision trees



depth = 3

DTs of depth k

k-DNFs   k-CNFs

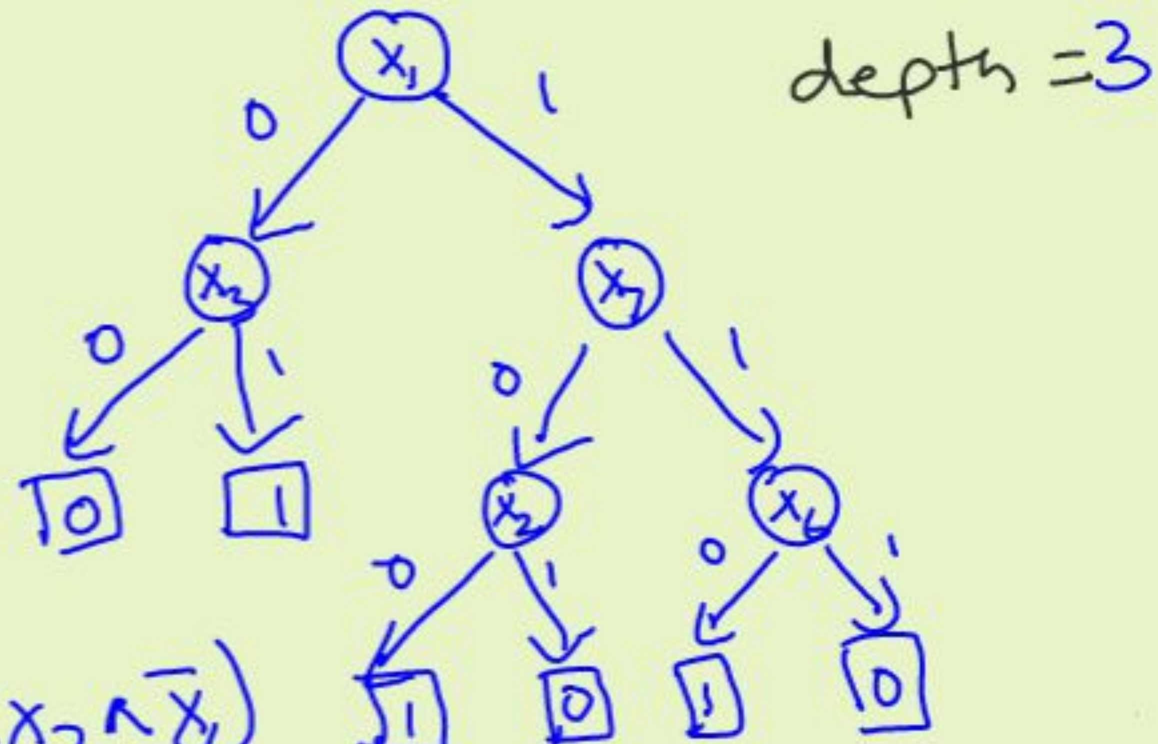
Eg: $(\bar{x}_1 \wedge x_3) \vee (x_1 \wedge \bar{x}_7 \wedge x_2) \vee (x_1 \wedge x_7 \wedge \bar{x}_6)$

Lemma: F a k-DNF or k-CNF.

[Håstad '86] $\Pr_{\rho \sim R_{q,n}} [\text{DT-depth}(F \restriction \rho) > \ell] \le O(qk)^{\ell}$.

General Switching Lemma

Decision trees



DTs of depth k

↙ ↘

k-DNFs $\quad$ k-CNFs

Eg: $(\bar{x}_1 \wedge x_3) \vee (x_1 \wedge \bar{x}_7 \wedge x_2) \vee (x_1 \wedge x_7 \wedge \bar{x}_6)$

Lemma: F a k-DNF or k-CNF.

[Håstad '86] $\quad \Pr_{\rho \sim R_{qn}} [\text{DT-depth}(F \upharpoonright \rho) > \ell] \leq O(qk)^{\ell}$.

Cor: F a k-DNF or k-CNF

$$\Pr_{\rho \sim R_{n/\alpha k}} [F \text{ not } \ell\text{-CNF or } \ell\text{-DNF}] \leq 2^{-\ell}.$$

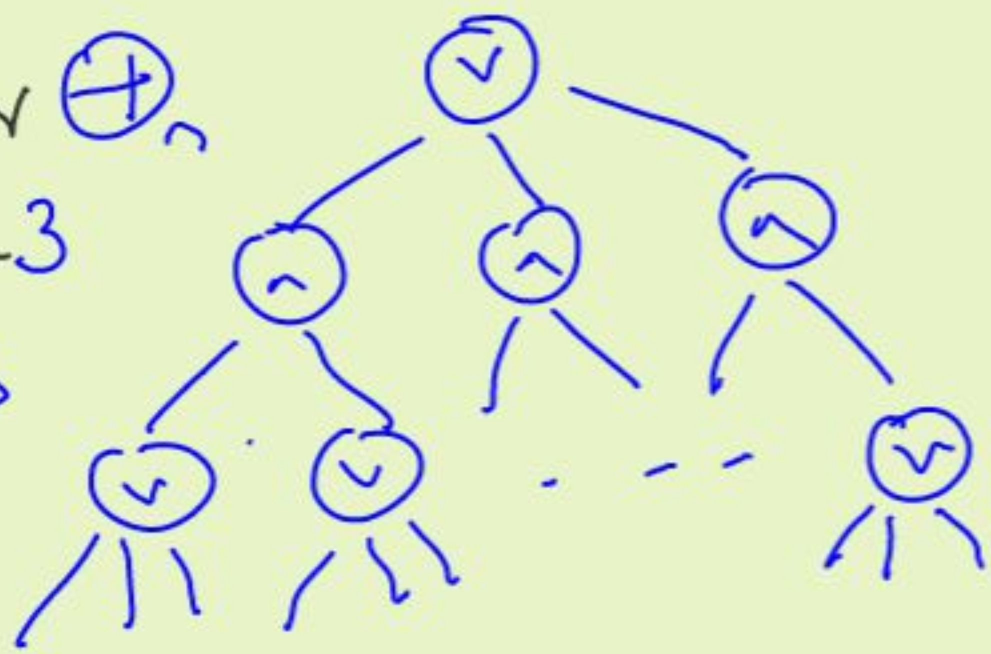
Switching lemma to lower bounds

Cor: F a k-DNF/CNF $\Pr_{\rho \sim R_{n/\alpha k}}[F \text{ not } \ell\text{-CNF/DNF}] \leq 2^{-\ell}$.

C for $\oplus_n$

depth-3

size s



Switching lemma to lower bounds

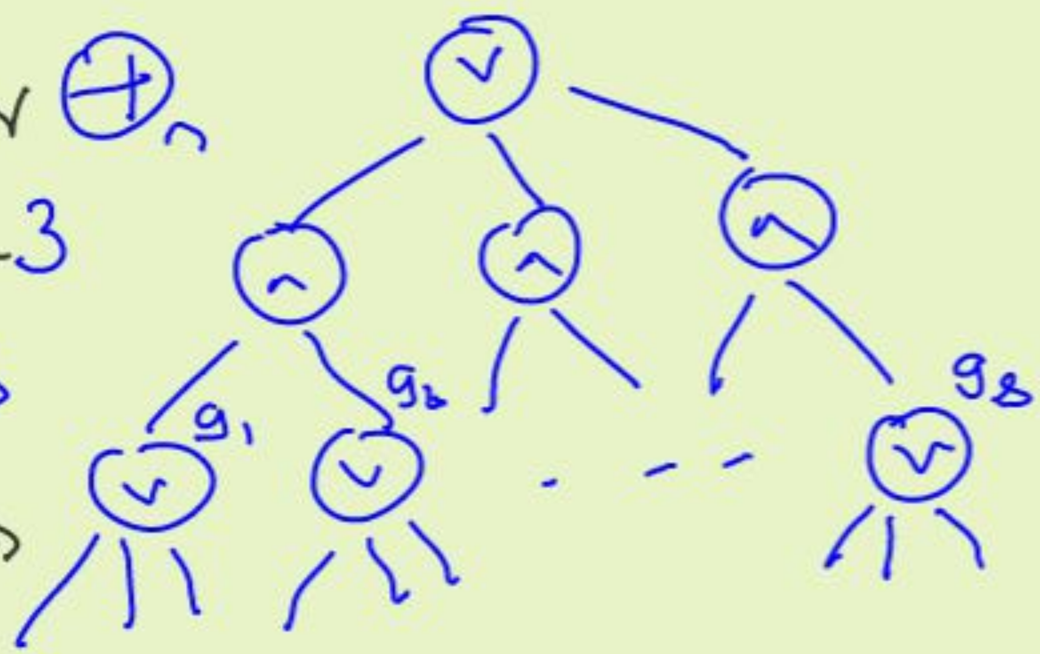
Cor: F a k-DNF/CNF $\quad \Pr_{\rho \sim R_{n/\alpha k}}[F \text{ not } \ell\text{-CNF/DNF}] \le 2^{-\ell}$.

C for $\oplus_n$

depth-3

size s

1-DNFs →



Switching lemma to lower bounds

Cor: F a k-DNF/CNF $\quad \Pr_{\rho \sim R_{n/\alpha k}}[F \text{ not } \ell\text{-CNF/DNF}] \le 2^{-\ell}.$

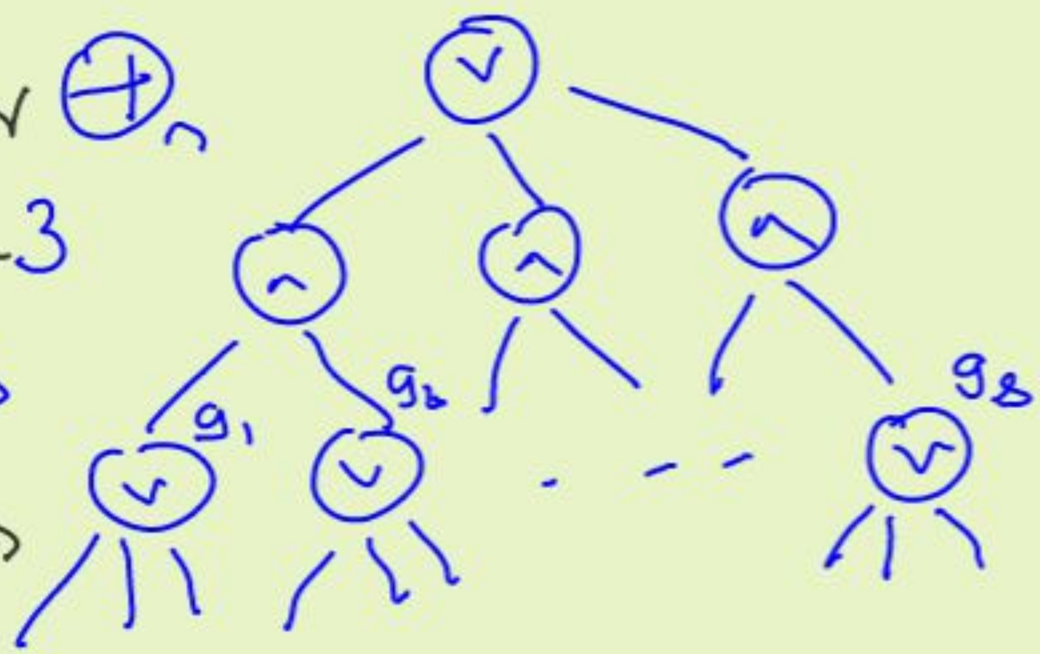
$\ell = 2 \log s$

C for $\oplus_n$

depth-3

size s

1-DNFs $\rightarrow$



$\Pr_{\rho_1 \sim R_{n/\alpha}}[g_i \text{ not } \ell\text{-CNF}] \le \frac{1}{s^2}$

$\Pr_{\rho_1 \sim R_{n/\alpha}}[\exists i : g_i \text{ not } \ell\text{-CNF}] \le \frac{1}{s}.$

Switching lemma to lower bounds

Cor: F a k-DNF/CNF $\quad \Pr_{\rho\sim R_{n/\alpha k}}[F \text{ not } \ell\text{-CNF/DNF}] \le 2^{-\ell}$.

$\ell = 2\log s$

$\Pr_{\rho_1\sim R_{n/\alpha}}[g_i \text{ not } \ell\text{-CNF}] \le \frac{1}{s^2}$

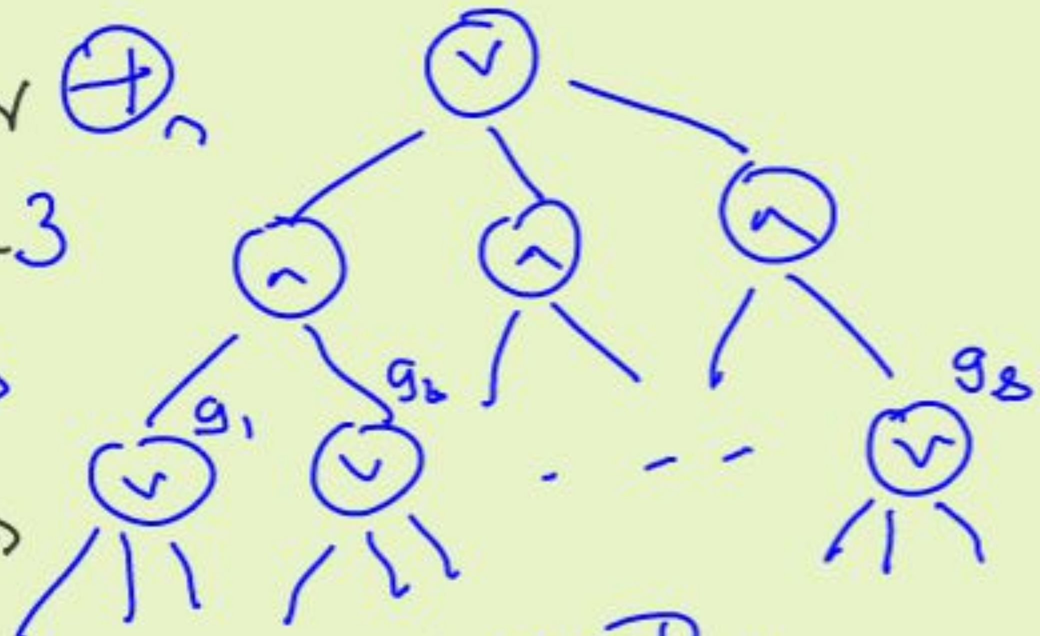
$\Pr_{\rho_1\sim R_{n/\alpha}}[\exists i : g_i \text{ not } \ell\text{-CNF}] \le \frac{1}{s}$.

C for $\oplus_n$

depth-3

size s

1-DNFs $\rightarrow$



$\downarrow \rho_1 \sim R_{n/\alpha}$

C' for $\oplus_{n/\alpha}$

ℓ-CNFs

Switching lemma to lower bounds

Cor: F a k-DNF/CNF $\quad \Pr_{\rho \sim R_{n/\alpha k}}[F \text{ not } \ell\text{-CNF/DNF}] \le 2^{-\ell}$.

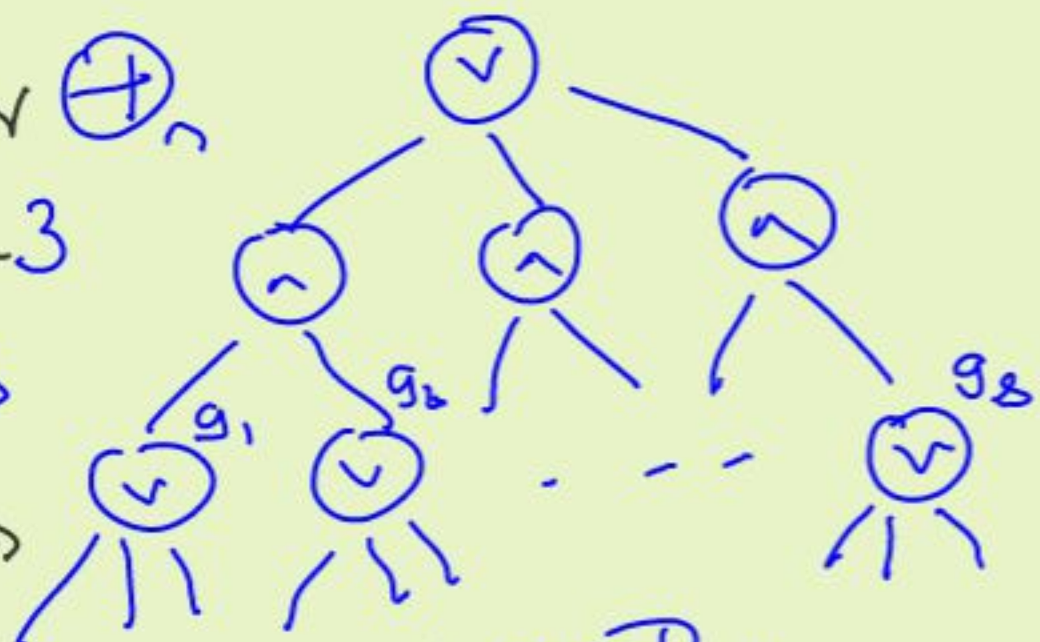
$\ell = 2\log s$

C for $\oplus_n$

depth-3

size s

1-DNFs $\to$



$\Pr_{\rho_1 \sim R_{n/\alpha}}[g_i \text{ not } \ell\text{-CNF}] \le \frac{1}{s^2}$

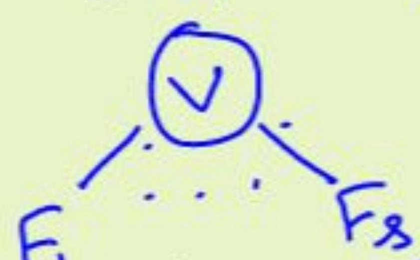
$\Pr_{\rho_1 \sim R_{n/\alpha}}[\exists i : g_i \text{ not } \ell\text{-CNF}] \le \frac{1}{s}$.

$\downarrow \rho_1 \sim R_{n/\alpha}$

$\Pr_{\rho_2 \sim R_{n/\alpha \cdot \alpha \cdot \ell}}[\exists i : F_i \text{ not } \ell\text{-DNF}] \le \frac{1}{s}$

C' for $\oplus_{n/\alpha}$

ℓ-CNFs



$\downarrow \rho_2 \sim R_{n/\alpha^2 \ell}$

C'' ℓ-DNF for $\oplus_{n/\alpha^2 \ell}$

Switching lemma to lower bounds

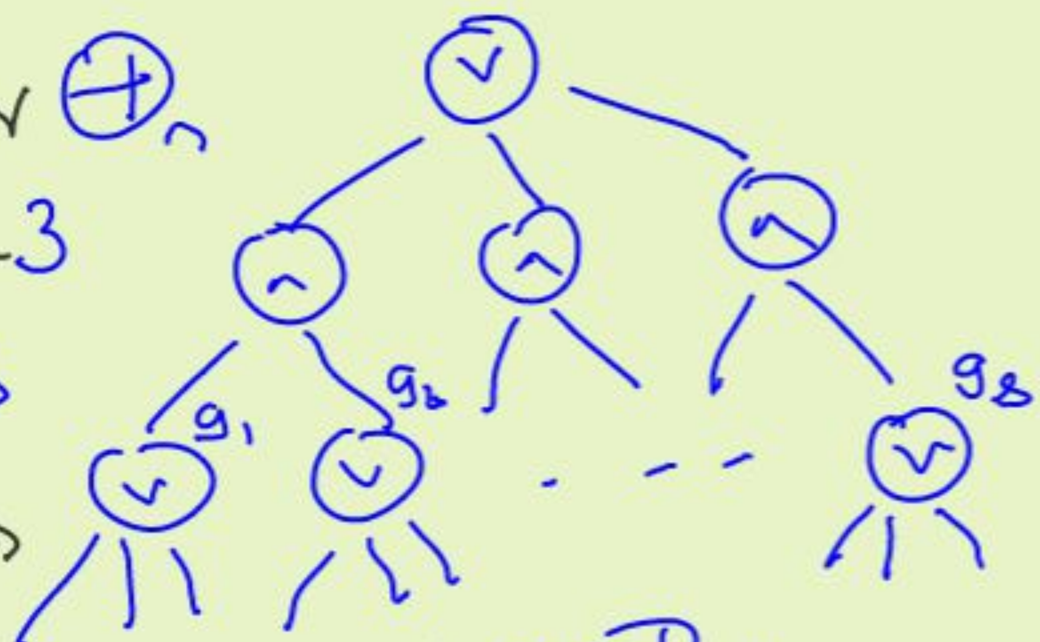
Cor: F a k-DNF/CNF $\quad \Pr_{\rho\sim R_{n/\alpha k}}[F \text{ not } \ell\text{-CNF/DNF}] \le 2^{-\ell}$.

C for $\oplus_n$

depth-3

size s

1-DNFs →



$\ell = 2\log s$

$\Pr_{\rho_1\sim R_{n/\alpha}}[g_i \text{ not } \ell\text{-CNF}] \le \frac{1}{s^2}$

$\Pr_{\rho_1\sim R_{n/\alpha}}[\exists i : g_i \text{ not } \ell\text{-CNF}] \le \frac{1}{s}$

$\Pr_{\rho_2\sim R_{n/\alpha\cdot\alpha\cdot\ell}}[\exists i : F_i \text{ not } \ell\text{-DNF}] \le \frac{1}{s}$

$\downarrow \rho_1 \sim R_{n/\alpha}$

C' for $\oplus_{n/\alpha}$

ℓ-CNFs

$\downarrow \rho_2 \sim R_{n/\alpha^2\ell}$

C'' ℓ-DNF for $\oplus_{n/\alpha^2\ell}$

$\Rightarrow \quad \ell \ge n/\alpha^2\ell$

$\log s = \Omega(\ell) = \Omega(\sqrt{n})$.

Switching lemma to lower bounds

Cor: F a k-DNF/CNF $\quad \Pr_{\rho \sim R_{n/\alpha k}} [F \text{ not } \ell\text{-CNF/DNF}] \leq 2^{-\ell}.$

$\ell = 2\log s$

$$C_d \xrightarrow{\rho_1 \sim R_{n/\alpha}} C_d' \xrightarrow{\rho_2 \sim R_{n/\alpha^2 \ell}} \cdots C_{d-1} \xrightarrow{\rho_3 \sim R_{n/\alpha^3 \ell^2}} C_{d-2} \cdots \xrightarrow{\rho_{d-1} \sim R_{n/O(\ell)^{d-2}}} C_2$$

depth-d	depth-d	depth $d-1$	depth 2
size s	bottom fanin ℓ	...	bottom fanin ℓ
	size s at ht. ≥ 2	...	

Switching lemma to lower bounds

Cor: F a k-DNF/CNF $\quad \Pr_{\rho\sim R_{n/\alpha k}}[F \text{ not } \ell\text{-CNF/DNF}] \le 2^{-\ell}$.

$\ell = 2\log s$

$$C_d \xrightarrow{\rho_1\sim R_{n/\alpha}} C'_d \xrightarrow{\rho_2\sim R_{n/\alpha^2\ell}} \cdots C_{d-1} \xrightarrow{\rho_3\sim R_{n/\alpha^3\ell^2}} C_{d-2} \cdots \xrightarrow{\rho_{d-1}\sim R_{n/O(\ell)^{d-2}}} C_2$$

C_d	C'_d	C_{d-1}	C_2
depth-d	depth-d	depth $d-1$	depth 2
size s	bottom fanin ℓ	...	bottom fanin ℓ
	size s at ht. ≥ 2	...	

$$\ell \ge \frac{n}{O(\ell)^{d-2}} \Rightarrow \log s = \Omega(\ell) = \Omega(n^{1/d-1})$$

Baby Switching lemma

Lemma: F a k-DNF (ie width k) or k-CNF

$$\Pr_{\rho \sim R_{qn}} [F \upharpoonright \rho \text{ not constant}] \leq O(qk)$$

Baby Switching lemma

no dependence on # terms/ clauses!

Lemma: F a k-DNF (ie width k) or k-CNF

$$\Pr_{\rho \sim R_{qn}} [F|_\rho \text{ not constant}] \le O(qk)$$

Baby Switching lemma

no dependence on # terms/clauses!

Lemma: F a k-DNF (ie width k) or k-CNF

$$\Pr_{\rho \sim R_{qn}} [F\restriction_\rho \text{ not constant}] \le O(qk)$$

$$\Updownarrow$$

$$BAD = \{\rho : F\restriction_\rho \text{ not constant}\} \qquad |BAD| \le O(qk) \cdot R_{qn}$$

Baby Switching lemma

no dependence on # terms/clauses!

Lemma: F a k-DNF (ie width k) or k-CNF

$$\Pr_{\rho \sim R_{qn}} [F \restriction_\rho \text{ not constant}] \leq O(qk)$$

$$\Updownarrow$$

$$BAD = \{\rho : F \restriction_\rho \text{ not constant}\} \qquad |BAD| \leq O(qk) \cdot R_{qn}$$

Pf: 1-1 map $\pi : BAD \to R_{qn-1} \times [k]$

$$\longrightarrow |R_{qn-1}| \leq O(q) \cdot |R_{qn}|$$

Baby Switching lemma

no dependence on # terms/clauses!

Lemma: F a k-DNF (i.e. width k) or k-CNF

$$\Pr_{\rho \sim R_{qn}} \left[F\restriction_\rho \text{ not constant} \right] \leq O(qk)$$

$$\Updownarrow$$

$$BAD = \left\{ \rho : F\restriction_\rho \text{ not constant} \right\} \qquad |BAD| \leq O(qk) \cdot R_{qn}$$

Pf: 1-1 map $\pi : BAD \to R_{qn-1} \times [k]$

$\longrightarrow |R_{qn-1}| \leq O(q) \cdot |R_{qn}|$

$$F\restriction_\rho = \vee$$

$$T_1\restriction_\rho \;\ldots\; T_i\restriction_\rho \;\ldots\; T_s\restriction_\rho$$

$$\neq 1 \qquad \neq 1 \qquad \neq 1$$

Baby Switching lemma

no dependence on # terms/clauses!

Lemma: F a k-DNF (i.e. width k) or k-CNF

$$\Pr_{\rho \sim R_{an}} [F\restriction\rho \text{ not constant}] \le O(ak)$$

$$\Updownarrow$$

$$BAD = \{\rho : F\restriction\rho \text{ not constant}\} \qquad |BAD| \le O(ak)\cdot R_{an}$$

Pf: 1-1 map $\pi : BAD \to R_{an-1} \times [k]$

$$|R_{an-1}| \le O(a)\cdot|R_{an}|$$

$$F\restriction\rho = \vee(T_1\restriction\rho \ldots T_i\restriction\rho \ldots T_s\restriction\rho)$$

$\not\equiv 1 \quad \not\equiv 1 \quad \not\equiv 1$

ρ': → Find $i^* = \min\{i \mid T_i\restriction\rho \not\equiv 0\}$

→ Set first unset literal L to 1.

$\pi(\rho) = (\rho', j)$ — j: Index of L in T_{i^*}.

Baby Switching lemma

no dependence on # terms/clauses!

Lemma: F a k-DNF (ie width k) or k-CNF

$$\Pr_{\rho \sim R_{qn}} [F\restriction_\rho \text{ not constant}] \le O(qk)$$

$$\Updownarrow$$

$$BAD = \left\{ \rho : F\restriction_\rho \begin{array}{c}\text{not}\\ \text{constant}\end{array} \right\} \qquad |BAD| \le O(qk)\cdot R_{qn}$$

Pf: 1-1 map $\pi : BAD \to R_{qn-1} \times [k]$

$\to |R_{qn-1}| \le O(q)\cdot |R_{qn}|$

$F\restriction_\rho = \vee(T_1\restriction_\rho, \dots, T_i\restriction_\rho, \dots, T_s\restriction_\rho)$

$\not\equiv 1 \qquad \not\equiv 1 \qquad \not\equiv 1$

ρ': $\to$ Find $i^* = \min\{i \mid T_i\restriction_\rho \not\equiv 0\}$

$\to$ Set first unset literal L to 1.

$\pi(\rho) = (\rho', j)$ — $j \to$ Index of L in T_{i^*}.

Decode (ρ', j): $i^* = \min\{i : T_i\restriction_{\rho'} \not\equiv 0\}$

↳ Unset jth literal get ρ.

Proof of Switching lemma [Razborov '93, Beame '94]

Lemma: F a k-DNF/CNF. $\Pr_{\rho \sim R_{q,n}} [\text{DT-depth}(F\restriction\rho) \geq l] \leq O(qk)^{l}$.

Proof of Switching Lemma [Razborov '93, Beame '94]

Lemma: F a k-DNF/CNF. $\Pr_{\rho \sim R_{q,n}} [\text{DT-depth}(F \upharpoonright \rho) \geq \ell] \leq O(qk)^\ell$.

Pf: $F \upharpoonright \rho$

$$\vee$$

$$T_1' = T_1 \upharpoonright \rho \quad \cdots \quad T_s \upharpoonright \rho$$

$\text{BAD} = \{\rho \mid \text{DT-depth}(F \upharpoonright \rho) \geq \ell\}$

$\pi : \text{BAD} \to R_{q,n-\ell} \times [k]^\ell \times \{0,1\}^\ell$

Proof of Switching lemma [Razborov '93, Beame '94]

Lemma: F a k-DNF/CNF. $\Pr_{\rho\sim R_{q,n}}[\text{DT-depth}(F\restriction\rho)\geq \ell] \leq O(qk)^{\ell}$.

Pf: $F\restriction\rho$

$$T_1' = T_1\restriction\rho \longrightarrow \vee \longleftarrow T_s\restriction\rho \qquad (T_1' = T_1\restriction\rho, \ \dots, \ T_s\restriction\rho)$$

$BAD = \{\rho \mid \text{DT-depth}(F\restriction\rho)\geq \ell\}$

$\pi : BAD \rightarrow R_{q,n-\ell} \times [k]^{\ell} \times \{0,1\}^{\ell}$

Canonical DT

→ If all $T_i' \equiv 0$, o/p 0

→ else

$i^* = \min\{i \mid T_i' \not\equiv 0\}$

Query all vars. in T_{i^*}'

& o/p 1 if satisfied

→ Substitute in F & repeat.

Proof of Switching Lemma [Razborov '93, Beame '94]

Lemma: F a k-DNF/CNF. $\Pr_{\rho \sim R_{q,n}} [\text{DT-depth}(F\restriction\rho) \geq \ell] \leq O(qk)^{\ell}$.

Pf: $F\restriction\rho$ $\qquad T_1' = T_1\restriction\rho \;\rightarrow\; \vee \;\leftarrow\; T_s\restriction\rho$ $\quad \cdots$

$\text{BAD} = \{\rho \mid \text{DT-depth}(F\restriction\rho) \geq \ell\}$

$\pi : \text{BAD} \rightarrow R_{qn-\ell} \times [k]^{\ell} \times \{0,1\}^{2\ell}$

Canonical DT

→ If all $T_i' \equiv 0$, o/p 0

→ else
$i^* = \min\{i \mid T_i' \not\equiv 0\}$

Query all vars. in T_{i^*}'
& o/p 1 if satisfied

→ Substitute in F & repeat.

SL-Encode$(\rho) = (\rho', u, v)$

→ $\rho' = \rho$

→ At each term T_{i^*}' queried by CDT, set literals to 1 in ρ'

→ $u \in [k]^{\ell} \times \{0,1\}^{\ell}$ – literals queried & "first bit" indicator

→ $v \in \{0,1\}^{\ell}$ – original assignment

$\text{CDT}(F\restriction\rho)$

Proof of Switching Lemma [Razborov '93, Beame '94]

Lemma: F a k-DNF/CNF. $\Pr_{\rho \sim R_{q,n}} [\text{DT-depth}(F\restriction\rho) \geq \ell] \leq O(qk)^{\ell}$.

Pf: $F\restriction\rho$ $\quad \vee$

$T_1' = T_1\restriction\rho \quad \cdots \quad T_s\restriction\rho$

$BAD = \{\rho \mid \text{DT-depth}(F\restriction\rho) \geq \ell\}$

$\pi : BAD \to R_{q,n-\ell} \times [k]^{\ell} \times \{0,1\}^{\ell}$

Canonical DT

→ If all $T_i' \equiv 0$, o/p 0

→ else

$i^* = \min\{i \mid T_i' \not\equiv 0\}$

Query all vars. in T_{i^*}' & o/p 1 if satisfied

→ Substitute in F & repeat.

SL-Encode$(\rho) = (\rho', u, v)$

→ $\rho' = \rho$

→ At each term T_{i^*}' queried by CDT, set literals to 1 in ρ'

→ $u \in [k]^{\ell} \times \{0,1\}^{\ell}$ – literals queried & "first bit" indicator

→ $v \in \{0,1\}^{\ell}$ – original assignment

SL-Decode(ρ', u, v)

→ $i^* = \min\{i : T_i\restriction\rho' \not\equiv 0\}$

→ Use u to find queried variables & v to reset.

→ Repeat.

Multi-Switching Lemma [Håstad'14]

→ Switching lemma for systems of DNFs / CNFs.

Multi-Switching Lemma [Håstad'14]

→ Switching lemma for systems of DNFs / CNFs.

→ $F_1, \ldots, F_s$ k-DNFs

→ $\Pr_{\rho \sim R_{n/\alpha k}} \left[\exists i : F_i \restriction \rho \text{ not } \ell\text{-CNF} \right] \leq s \cdot 2^{-\ell}$

Multi-Switching Lemma [Håstad'14]

→ Switching lemma for systems of DNFs / CNFs.

→ $F_1, \ldots, F_s$ k-DNFs

→ $\Pr_{\rho \sim R_{n/\alpha k}} [\exists i : F_i \restriction \rho \text{ not } \ell\text{-CNF}] \leq \underbrace{s \cdot 2^{-\ell}}$

can improve hugely
by setting few more vars.

Multi-Switching Lemma [Håstad'14]

→ Switching lemma for systems of DNFs / CNFs.

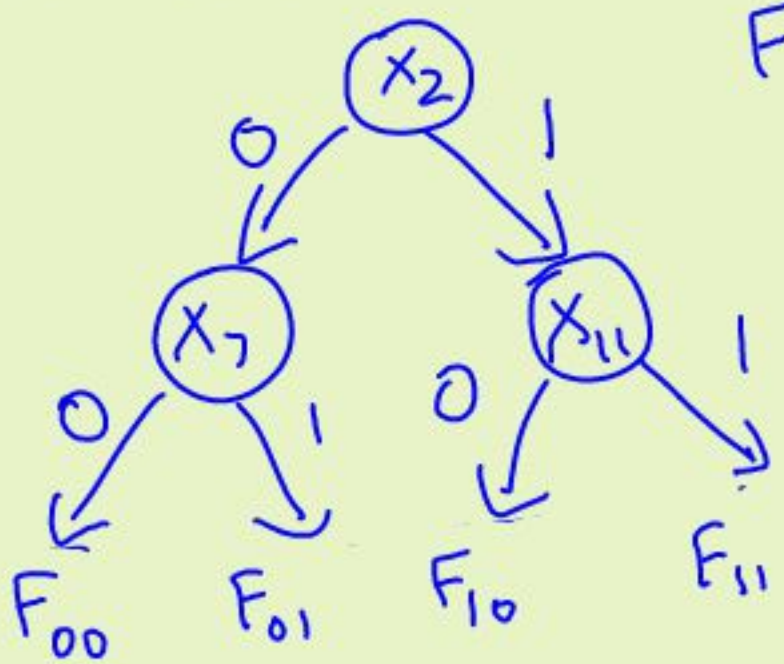
→ $F_1, \ldots, F_s$ k-DNFs

→ $\Pr_{\rho \sim R_{n/\alpha k}} [\exists i : F_i \restriction \rho \text{ not } \ell\text{-CNF}] \leq \underbrace{s \cdot 2^{-\ell}}$

can improve hugely by setting few more vars.

→ Restriction Tree (RT)

F a DNF/CNF



Multi-Switching Lemma [Håstad'14]

→ Switching lemma for systems of DNFs / CNFs.

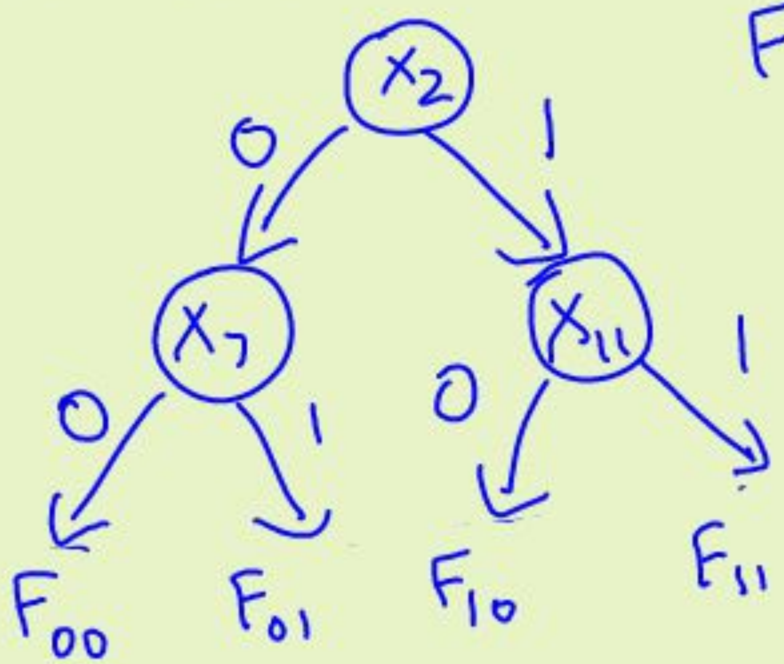
→ $F_1, \ldots, F_s$ k-DNFs

→ $\Pr_{\rho \sim R_{n/\alpha k}} [\exists i : F_i \restriction \rho \text{ not } \ell\text{-CNF}] \leq \underbrace{s \cdot 2^{-\ell}}$

can improve hugely by setting few more vars.

→ Restriction Tree (RT)

F a DNF/CNF



__Want:__ RT s.t. $(F_i \restriction \rho) \restriction \lambda$ a depth-ℓ DT $\forall i$ $\forall$ leaves λ

Multi-Switching Lemma [Håstad'14]

→ Switching lemma for systems of DNFs / CNFs.

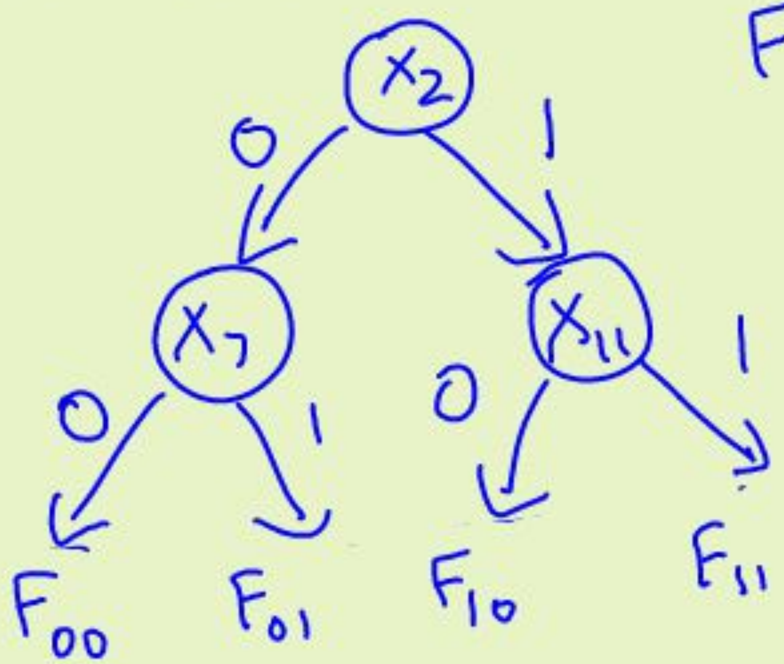
→ $F_1, \dots, F_s$ k-DNFs

→ $\Pr_{\rho \sim R_{n/\alpha k}} [\exists i : F_i \restriction \rho \text{ not } \ell\text{-CNF}] \le \underbrace{s \cdot 2^{-\ell}}$

can improve hugely by setting few more vars.

→ Restriction Tree (RT)

F a DNF/CNF



Want: RT s.t. $(F_i \restriction \rho) \restriction \lambda$ a

$\underbrace{\text{depth-}\ell \text{ DT } \forall i \; \forall \text{ leaves } \lambda}$

RT ℓ-depth$(F_1, \dots, F_s)$

Multi-Switching Lemma [Håstad'14]

→ Switching lemma for systems of DNFs / CNFs.

→ $F_1, \dots, F_s$ k-DNFs

→ $\Pr_{\rho \sim R_{n/\alpha k}} [\exists i : F_i \restriction \rho \text{ not } \ell\text{-CNF}] \leq \underbrace{s \cdot 2^{-\ell}}$

can improve hugely by setting few more vars.

→ Restriction Tree (RT)

Multi-Switching Lemma $F_1, \dots, F_s$ k-DNFs / CNFs, $\ell \geq \log s$

$$\Pr_{\rho \sim R_{2n}} [\ RT_\ell\text{-depth}(F_1, \dots, F_s) \geq D] \leq O(q, k)^D.$$

Proof of Multi-Switching lemma [Håstad'14, Servedio-Tan'19]

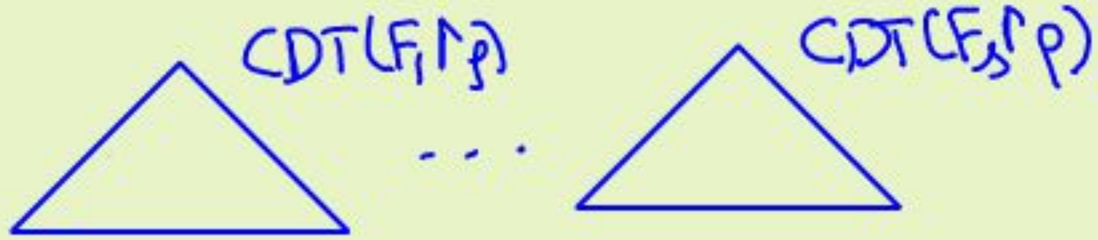
MSL: $F_1, \ldots, F_s$, $\ell \geq \log s$ $\quad \Pr_{\rho \sim R_{qn}} \left[RT_\ell\text{-depth}(F_1, \ldots, F_s) \geq D \right] \leq O(qk)^D$.

k-DNFs / CNFs

Proof of Multi-Switching lemma [Håstad'14, Servedio-Tan'19]

MSL: $F_1, \dots, F_s$, $\ell \geq \log s$ $\quad \Pr_{\rho \sim R_{qn}}\left[RT_\ell\text{-depth}(F_1, \dots, F_s) \geq D\right] \leq O(qk)^D$.

k-DNFs / CNFs



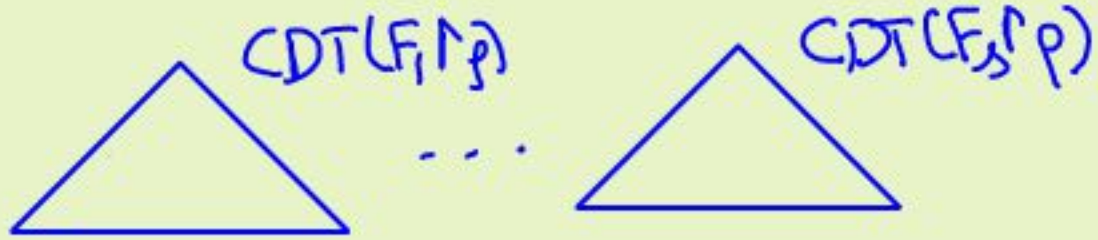
$BAD = \{\rho \mid RT_\ell\text{-depth}(F_1, \dots, F_s) \geq D\}$

$\pi : BAD \rightarrow R_{qn-D} \times \text{Advice}$

Proof of Multi-Switching lemma [Håstad'14, Servedio-Tan'19]

MSL: $F_1, \ldots, F_s$, $\ell \geq \log s$ $\quad \Pr_{\rho \sim R_{qn}}\left[RT_\ell\text{-depth}(F_1, \ldots, F_s) \geq D\right] \leq O(qk)^D$.

k-DNFs / CNFs



$BAD = \{\rho \mid RT_\ell\text{-depth}(F_1, \ldots, F_s) \geq D\}$

$\pi : BAD \to R_{qn-D} \times$ Advice

Canonical RT

→ If $\text{depth}(CDT(F_i\restriction\rho)) \leq \ell$ $\forall i$, stop.

→ else $i^* = \min\{i \mid \text{depth} > \ell\}$

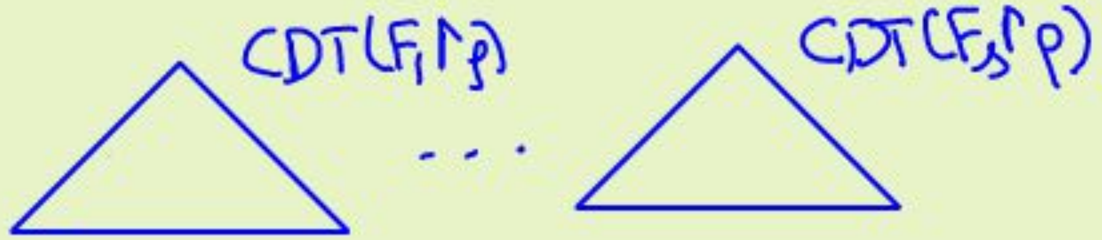
→ Find left-most path τ of length $> \ell$ & query all vars.

→ Substitute & repeat.

Proof of Multi-Switching lemma [Håstad'14, Servedio-Tan'19]

MSL: $F_1, \dots, F_s$, $\ell \geq \log s$ $\quad \Pr\left[RT_\ell\text{-depth}(F_1, \dots, F_s) \geq D\right] \leq O(qk)^D$.

k-DNFs / CNFs $\quad \rho \sim R_{qn}$



$BAD = \{\rho \mid RT_\ell\text{-depth}(F_1, \dots, F_s) \geq D\}$

$\pi : BAD \to R_{qn-D} \times \text{Advice}$

Canonical RT

→ If $\text{depth}(CDT(F_i \restriction \rho)) \leq \ell$ $\forall i$, stop.

→ else $i^* = \min\{i \mid \text{depth} > \ell\}$

→ Find left-most path τ of length $> \ell$ & query all vars.

→ Substitute & repeat.

MSL-Encode $(\rho) = (\rho', a_0, a_1)$

→ $\rho' = \rho$, $a_0 = a_1 =$ empty

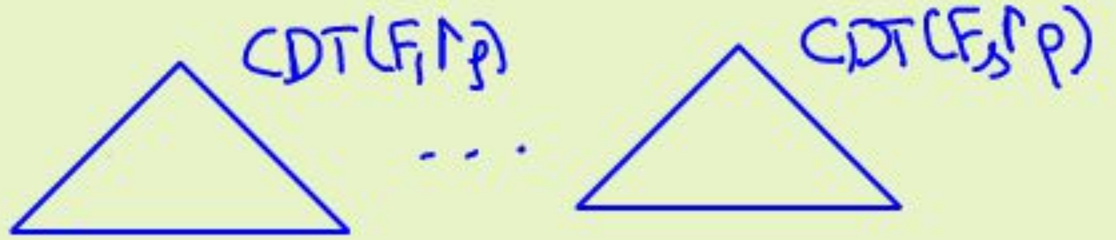
→ At each path τ queried by CRT, use SL-encoding to augment ρ', a_0

→ $a_1 = a_1 \circ (i^*$, CRT assignment to τ, firstbit indicator$)$

Proof of Multi-Switching lemma [Håstad'14, Servedio-Tan'19]

MSL: $F_1, \dots, F_s$, $\ell \geq \log s$ $\quad \Pr_{\rho \sim R_{an}} \left[RT_\ell\text{-depth}(F_1, \dots, F_s) \geq D \right] \leq O(qk)^D$.

k-DNFs / CNFs



$BAD = \{ \rho \mid RT_\ell\text{-depth}(F_1, \dots, F_s) \geq D \}$

$\pi : BAD \to R_{an-D} \times \text{Advice}$

Canonical RT

→ If $\text{depth}(CDT(F_i \upharpoonright \rho)) \leq \ell$ $\forall i$, stop.

→ else $i^* = \min\{ i \mid \text{depth} > \ell \}$

→ Find left-most path τ of length $> \ell$ & query all vars.

→ Substitute & repeat.

MSL-Encode$(\rho) = (\rho', a_0, a_1)$

→ $\rho' = \rho$, $a_0 = a_1 = \text{empty}$

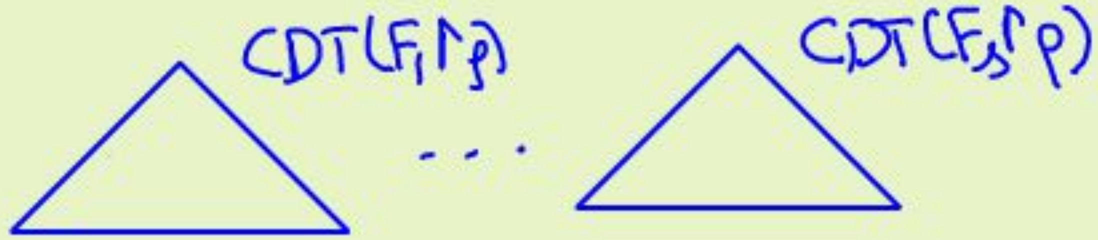
→ At each path τ queried by CRT, use SL-encoding to augment $\rho', a_0 \to \left| \{0,1\}^{2D} \times [k]^D \right| = O(k)^D$

→ $a_1 = a_1 \circ (i^*, \text{CRT assignment to } \tau, \text{firstbit indicator})$

Proof of Multi-Switching lemma [Håstad'14, Servedio-Tan'19]

MSL: $F_1, \ldots, F_s$, $\ell \geq \log s$ $\Pr_{\rho \sim R_{\alpha n}}\left[RT_\ell\text{-depth}(F_1, \ldots, F_s) \geq D\right] \leq O(\alpha k)^D$.

k-DNFs / CNFs



$BAD = \{\rho \mid RT_\ell\text{-depth}(F_1, \ldots, F_s) \geq D\}$

$\pi : BAD \to R_{\alpha n - D} \times \text{Advice}$

Canonical RT

$\to$ If $\text{depth}(CDT(F_i \restriction \rho)) \leq \ell$ $\forall i$, stop.

$\to$ else $i^* = \min\{i \mid \text{depth} > \ell\}$

$\to$ Find left-most path τ of length $> \ell$ & query all vars.

$\to$ Substitute & repeat.

MSL-Encode$(\rho) = (\rho', a_0, a_1)$

$\to$ $\rho' = \rho$, $a_0 = a_1 = $ empty

$\to$ At each path τ queried by CRT, use SL-encoding to augment $\rho', a_0 \to \left|\{0,1\}^{2D} \times [k]^D\right| = O(k)^D$

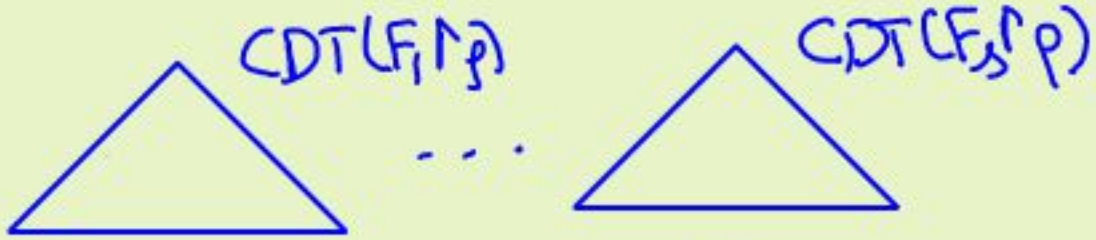
$\to$ $a_1 = a_1 \circ (i^*$, CRT assignment to τ, $\leftarrow$ firstbit indicator)

$\left|[s]^{D/\ell} \times \{0,1\}^{2D}\right| = O(1)^D$

Proof of Multi-Switching lemma [Håstad'14, Servedio-Tan'19]

MSL: $F_1, \ldots, F_s$, $\ell \geq \log s$ k-DNFs / CNFs

$\Pr_{\rho \sim R_{\alpha n}} \left[RT_\ell\text{-depth}(F_1, \ldots, F_s) \geq D \right] \leq O(qk)^D$.



$BAD = \{ \rho \mid RT_\ell\text{-depth}(F_1, \ldots, F_s) \geq D \}$

$\pi : BAD \to R_{\alpha n - D} \times \text{Advice}$

MSL-Decode (ρ', a_0, a_1)

→ Use a_1 to find first i^* & # vars read in first τ

→ Use SL-Decode to find vars & path in CRT.

→ Set & continue.

MSL-Encode $(\rho) = (\rho', a_0, a_1)$

→ $\rho' = \rho$, $a_0 = a_1 = \text{empty}$

→ At each path τ queried by CRT, use SL-encoding to augment ρ', a_0.

→ $a_1 = a_1 \circ (\text{length}(\tau), i^*)$