17/08/23

A certificate at $x \in \{0,1\}^n$ for f is a tuple

$$\left(S \subseteq [n],\ \alpha : S \to \{0,1\} \right)$$

s.t. $\forall\, y \in \{0,1\}^n$

s.t. $y_i = x_i = \alpha(i)$ $\forall\, i \in S$,

then $f(y) = f(x)$.

E.g:- OR_n at 0^n

$\{x_1 = 0, x_2 = 0, \dots, x_n = 0\}$

Certificate OR_n at 0110^{n-3}

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

$\{x_2 = 1, x_3 = 1\}$, $\{x_1 = 0, x_2 = 1\}$

- many certificates at an input

→ Size of a certificate

$:= |S|$

→ $C(f, x)$:= minimum size of a certificate for f at x.

→ Certificate complexity of f.

$$C(f) := \max_{x \in \{0,1\}^n} C(f,x).$$

Certificate complexity	Decision tree depth
$C(f)$	$D(f)$
"non-deterministic"	

Prop :- For all $x \in \{0,1\}^n$ $C(f,x) \leq D(f,x)$

$$\max_{x \in \{0,1\}^n} C(f,x) \leq \max_{x \in \{0,1\}^n} D(f,x)$$

$$\| \qquad\qquad \|$$

$$C(f) \qquad\qquad D(f)$$

~~Def~~ Define

$$C^1(f) := \max_{x \in f^{-1}(1)} C(f,x)$$

1-certificate complexity

$$C^0(f) := \max_{x \in f^{-1}(0)} C(f,x)$$

0-certificate complexity.

$\Rightarrow$ Obs :- $C(f) = \max(C^1(f), C^0(f))$

$\Rightarrow$ $C(f) \leq D(f)$.

$\Rightarrow$ low decision-tree depth
$D(f)$

$$\Downarrow$$

low $C^1(f)$ and $C^0(f)$

$\Rightarrow$ Does the reverse implication holds. ?

$D(f) \leq C(f)^{10}$?

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

$$D(f) = \Theta(n)$$

$$C(f) = \Theta(\sqrt{n})$$

$\{0,1\}^n$ = Domain.

set $= \{ (x_1, \ldots, x_n) \mid x_i \in \{0,1\} \ \forall i \}$

vector space.

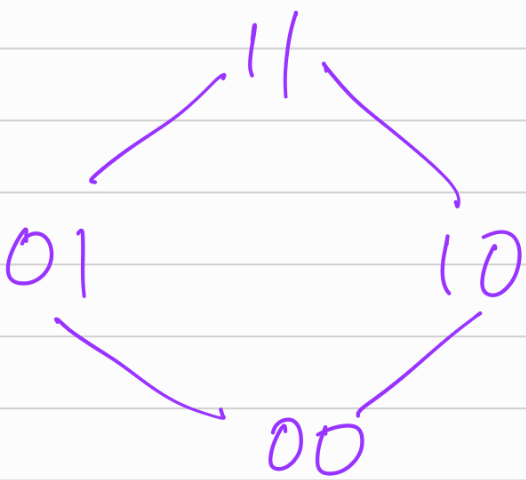
$\mathbb{F}_2^n \quad = \quad a + b = c$

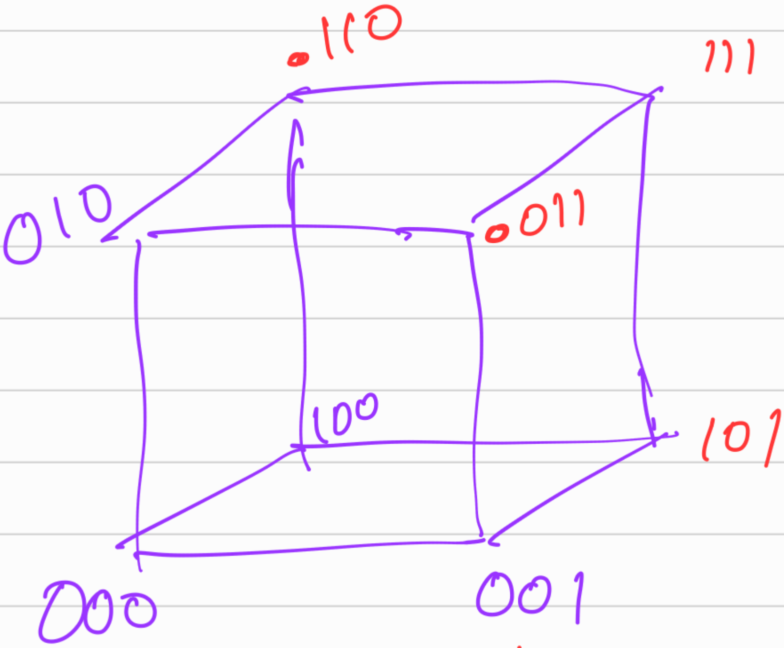
when $c_i = a_i \oplus b_i$

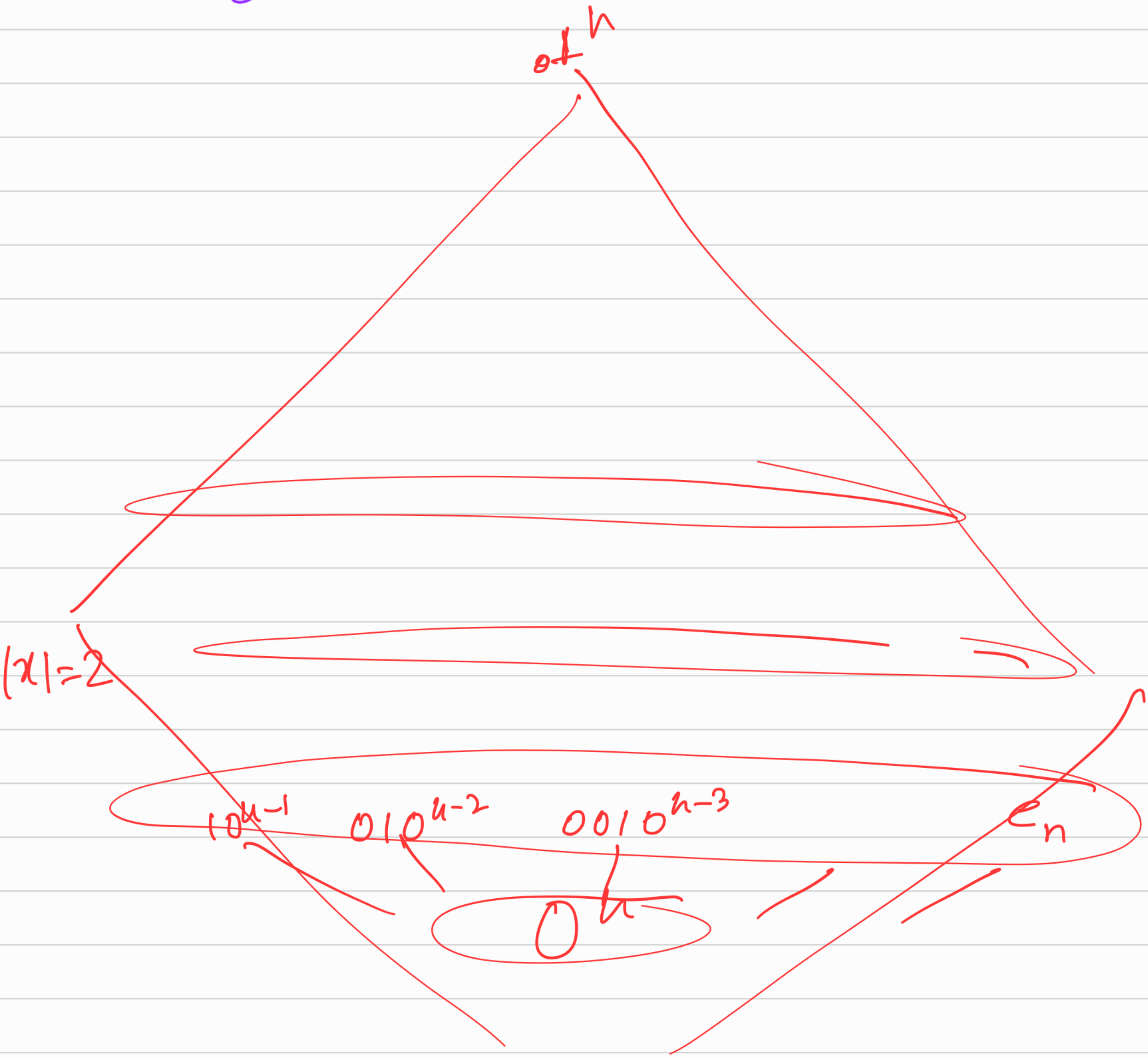
→ Hamming cube.

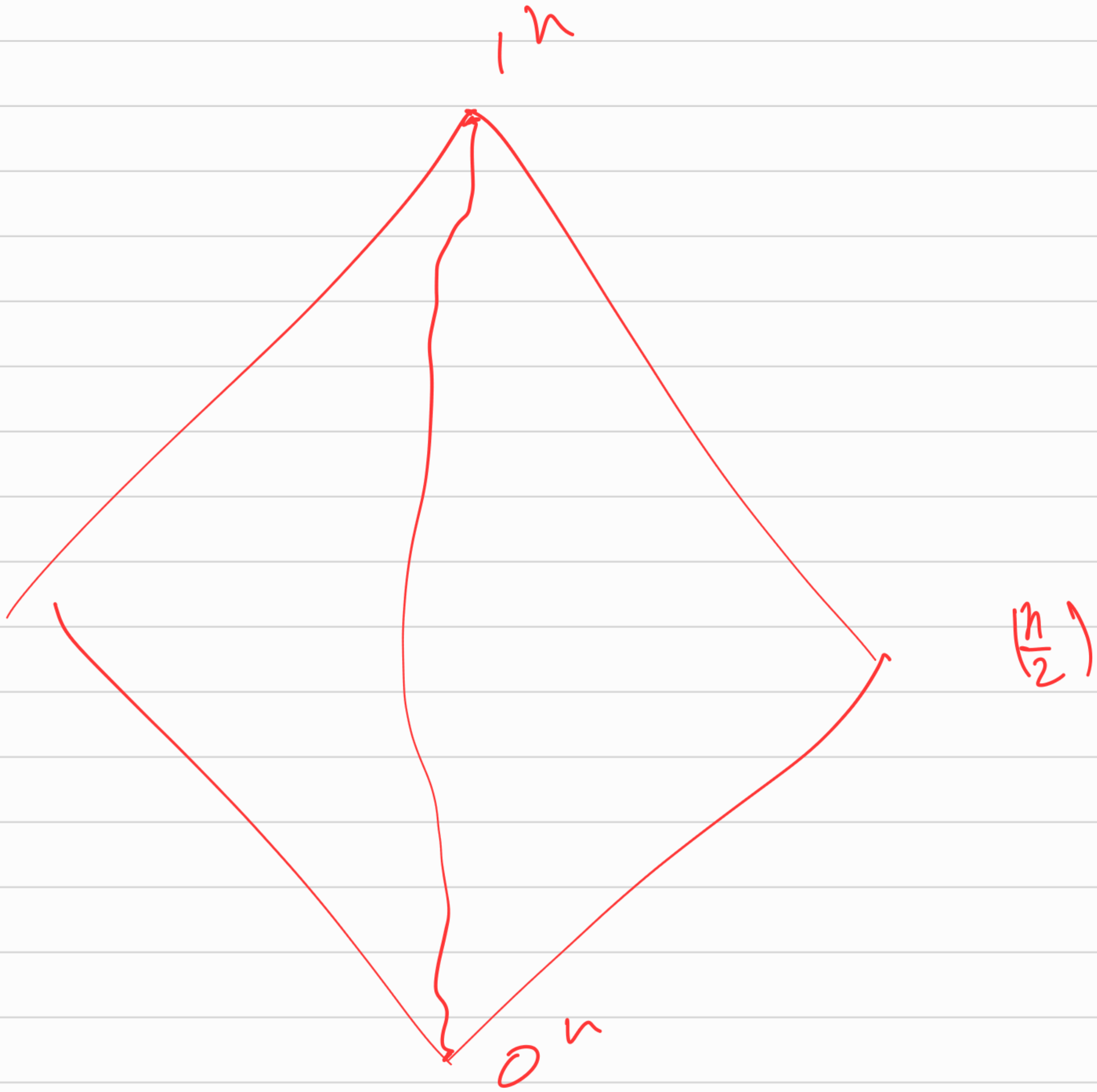
$$V = \{ x \in \{0,1\}^n \}$$

$E(x, y) = 1$ iff $\exists$ a unique $i \in [n]$ s.t. $x_i \neq y_i$




110
111
010
011
100
101
000
001


1^n
|x|=2
10^{n-1}
010^{n-2}
0010^{n-3}
e_n
0^n

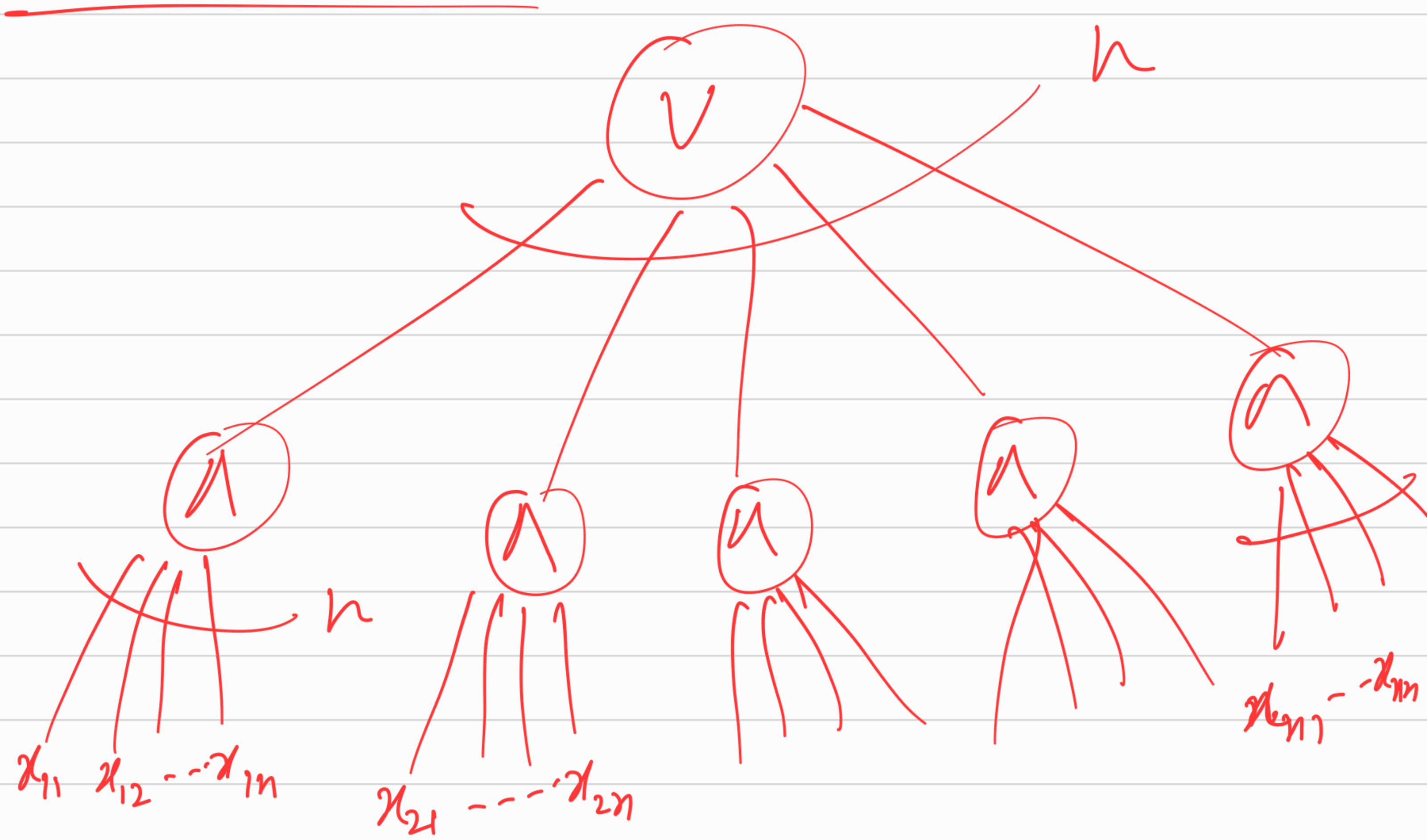


Certificate = monochromatic subcubes.

$$C(OR_n, 0^n) = \{x_1 = 0,\ x_2 = 0,\ \vdots,\ x_n = 0\}$$

$C(OR_{n},\ 1000\ldots) = \{x_1 = 1\}$

$\underline{\text{Tribes}_{n,n}}$:



$$\{0,1\}^{n^2} \rightarrow \{0,1\}$$

At any 1-input x,

$$C(\mathrm{Tribes}_{n,n}, x) \leq n$$

$$\Rightarrow \quad C^1(\mathrm{Tribes}_{n,n}) \leq n$$

At any 0-input y,

$$C(\mathrm{Tribes}_{n,n}, y) \leq n$$

$$\Rightarrow \quad C^0(\mathrm{Tribes}_{n,n}) \leq n$$

Lemma:- $D(\text{Tribes}_{n,n}) \geq n^2$

$\text{Tribes}_{n,n} : \{0,1\}^{n^2} \to \{0,1\}$

$$D(\text{Tribes}) = n^2$$

$C^1(\text{Tribes}) \leq n \; ; \; C^0(\text{Tribes}) \leq n$

Thm:- For all Boolean function

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

$$D(f) \leq C^0(f) \cdot C^1(f).$$

Question:-

Take a 1-certificate S_1

Take a 0-certificate S_2

Can $S_1 \cap S_2 = \phi$?

NO!

Prop:- $S_1 \cap S_2 \neq \phi$.

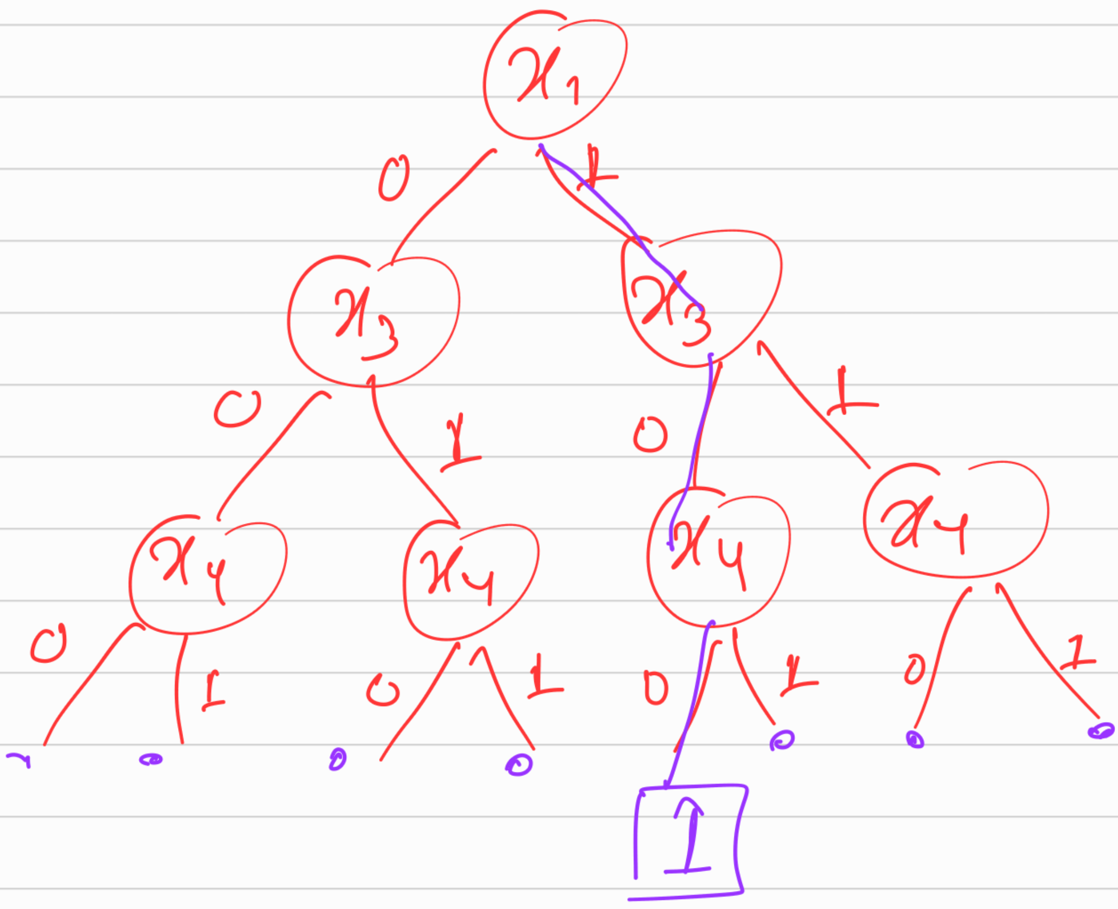
$$S_1 \cap S_2 = \{1, 2\}$$

$$\left.\begin{array}{l} x_1 = 1 \\ x_2 = 1 \end{array}\right\} \quad \begin{array}{l} y_1 = 1 \\ y_2 = 1 \end{array}$$

Prop:- 1-certificate and 0-certificate intersect in a contradictory way.

1-certificate

$$\{x_1 = 1,\ x_3 = 0,\ x_4 = 0\}$$



$$f\begin{pmatrix} x_1 = 1 \\ x_3 = 1 \\ x_4 = 1 \end{pmatrix}$$

$$D(f) \leq C^0(f) \cdot C^1(f).$$