04/09/23

Correctness :- $D(f) \leq C^1(f) \cdot bs(f)$

whenever the output is from Step 1, you are trivially correct.

Case 2: when the algo. outputs answer in Step 2.

For the sake of contradiction assume that in Step 2 the function is not constant on remaining inputs.

This implies $\exists$ x and y $\in \{0,1\}^n$, $x \neq y$ s.t.

$f(x) = 0$ and $f(y) = 1$.

⇒ x and y are both consistent with answers to the queries made until now.

⇒ Suppose, WLOG, that x is our input.

⇒ Let $c_1, c_2, \ldots, c_b$ be the 1-certificates that have been

queried. in step 1, where

$b = bs(f)$.

→ $x|_{C_i} = y|_{C_i} \neq C_i \quad \forall i \in [b]$

x/y disagrees with C_i on some variable.

→ Since $f(y) = 1$, y contains a 1-certificate distinct from C_1 to C_b. Let's call it C_{b+1}.

→ Let B_i be the set of

indices where x and C_i disagrees.

→ Claim:- $0 = f(x) \neq f(x^{B_i}) = 1$

$\forall\ i \in [b+1]$.

Pf:- flipping B_i makes it consistent with C_i.

→ Claim:- B_i's are disjoint for all $1 \leq i \leq b+1$.

Proof:- Let $C_1 = (S_1, \alpha)$.

Then S_1 is the first set of query.

In the next iteration we will be working with the subfunction

$$f|_{S=x|_S}$$

which is defined on Variables $[n] \setminus S$.

Therefore, B_i's are subset of disjoint sets and hence are disjoint themselves.

$\Rightarrow$ Hence, we obtain a contradiction

$\square$.

Thm:- $D(f) \leq C^1(f) \cdot bs(f)$

Thm:- $D(f) \leq C^0(f) \cdot bs(f)$.

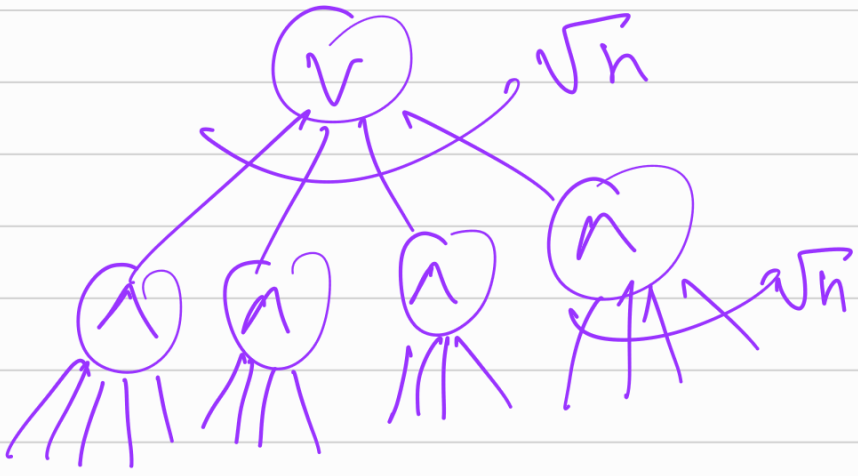
Thm:- $C(f) \leq s(f) \cdot bs(f) \leq bs^2(f)$

Thm:- $D(f) \leq s(f) \cdot bs(f) \cdot bs(f)$

$\leq bs^3(f)$.

Prop: $s(f) \leq bs(f) \leq C(f) \leq D(f)$

Tribes :-



$$s(\text{Tribes}) = bs(\text{Tribes}) = C(\text{Tribes}) = O(\sqrt{n}).$$

$$D(\text{Tribes}) \geq n.$$

$$\Rightarrow \exists f : D(f) = \Omega(bs^2(f)).$$

OPEN :- $\exists f : D(f) = \Omega(bs^3(f))$.

Or $\forall f : D(f) = O(bs^2(f))$

Polynomials.

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

$\Rightarrow$ multivariate polynomial

$p(x_1, \ldots, x_n)$ s.t.

$$p(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$$

$$\forall\ x \in \{0,1\}^n.$$

We say p represents the Boolean function f.

monomial: $x_1^2 x_2^3 x_3 x_5^4$

$2 \cdot x_1 x_2 + \frac{3}{2} \cdot x_1^2 x_3 - 5 \cdot x_2^3 \cdot x_4.$

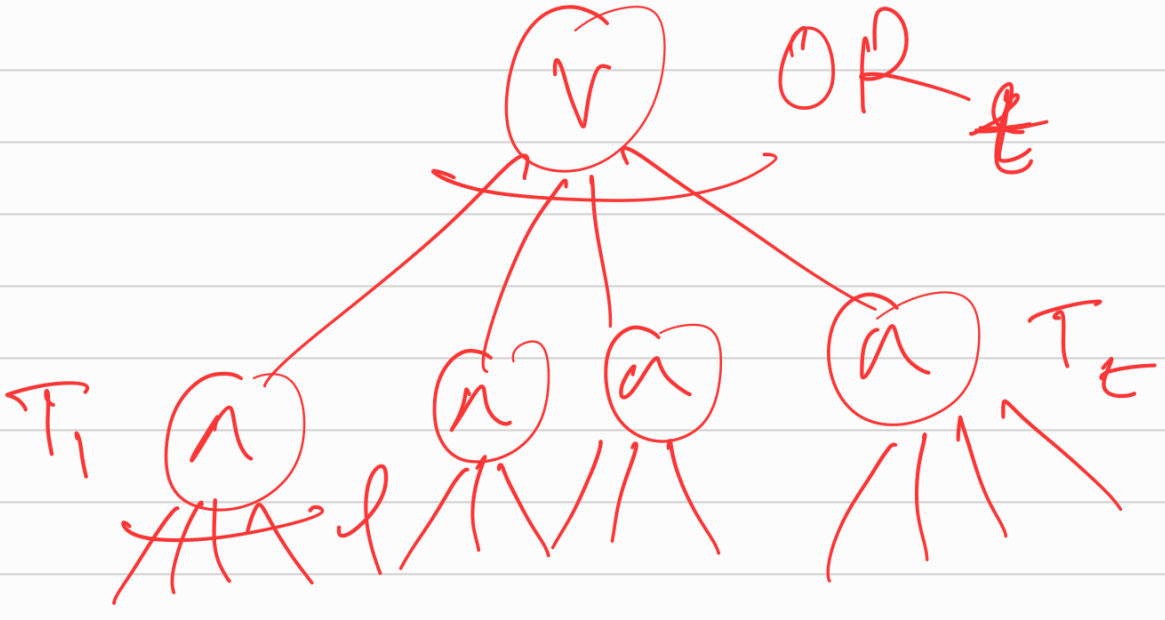
Q1 :- do we need individual degree of a variable to be ≥ 2 in such a polynomial representing f ?

⇒ De Morgan's Law.

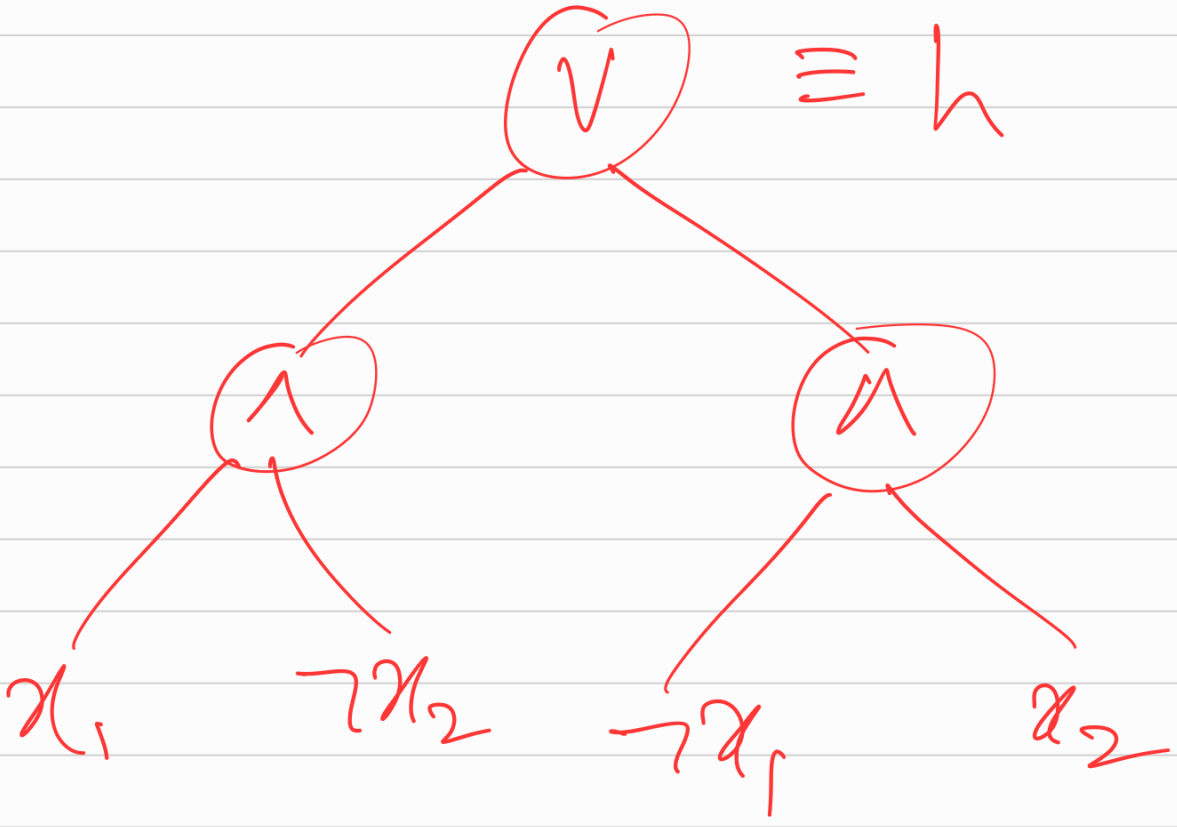
$$\neg(a \vee b) \equiv \neg a \wedge \neg b.$$

$$OR(x_1, \ldots, x_n) = 1 - \prod_{i=1}^{n} (1 - x_i)$$

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



$$f = OR_t(T_1, \ldots, T_t)$$



$$OR(y_1, y_2) \simeq 1 - (1-y_1)(1-y_2)$$

$$h \simeq 1 - (1 - x_1 \cdot (1-x_2))(1 - (1-x_1) \cdot x_2)$$

$$= 1 - (1 - x_1 + x_1 x_2)(1 - x_2 + x_1 x_2)$$

$$= 1 - (1 - x_2 + x_1 x_2 - x_1 + x_1 x_2 - x_1^2 x_2$$

Prop :- Every Boolean function is representable by a polynomial

For $x \in \{0,1\}$

$$x^k = x \quad \forall\, k \geq 1.$$

$\Rightarrow$ $\therefore$ we can assume WLOG that polynomials representing f are "multilinear."

$$\sum_{S \subseteq [n]} c_S \left(\prod_{i \in S} x_i \right) \in \mathbb{R}.$$

Q2:- Are there many distinct multilinear polynomials that represent a Boolean function? (Uniqueness problem).

Thm:- There exists a unique multilinear poly. that represents a given Boolean function f.

Pf:- Suppose not.

$\exists$ p and q polynomials

s.t. (a) $p(x) \neq q(x)$

(b) $p(a) = q(a) = f(a)$

$\forall\, a \in \{0,1\}^n$

Consider $r(x) = p(x) - q(x)$

(i) $r(x) \not\equiv 0$

r is not a zero polynomial

$p(x) \neq q(x)$.

(ii) $r(a) = 0 \quad \forall\, a \in \{0,1\}^n$

Monomial :- product of variable with repetition.

in our case :- multilinear monomials

$\prod_{i \in T} x_i$ for some $T \subseteq [n]$.

Consider a monomial with least degree.

Set every variable not present in this monomial to 0. and the ones present to 1.

At this input r evaluates to non-zero value.

which contradicts the second point that $r(a) = 0 \; \forall \; a \in \{0,1\}^n$.