Boolean Algebra

Algebraic system: The set of a set $\hat{}^{A}$ and relations and operations defined on the elements of this set $\hat{}^{A}$ is referred to as an algebraic system shown as

$$\{A, \text{relations}, \text{operations}\} \equiv \text{algebraic system}$$

Boolean Algebra: If an algebraic system defined on the set S with $|S| \geq 2$ and represented as $\{S, +, \cdot, '\}$ satisfy six independent axioms, then it is referred to as Boolean Algebra.

What is axiom?

- An axiom is a proposition that is not proved or demonstrated but considered to be either self-evident r subject to necessary decision

- serves as a starting point for deducing and nferring other (theory dependent) truths

What is theorem?

- A theorem is a statement that can be proved n the basis of axioms and logic rules

A short history

- The Boolean algebra was introduced by George Boole n 1854

- E.V. Huntington developed an independent axiomatic efinition for this algebraic system in 1904

- Finally, C. E. Shannon applied the Boolean algebra to the switching circuits

Axioms of Boolean Algebra

- we present six independent axioms

Axiom 1. Commutative property

$\forall a, b \in S$, we have

$$a + b = b + a$$

$$a \cdot b = b \cdot a$$

Axiom 2. Associative property

$\forall a, b, c \in S$, we have

$$a + (b + c) = (a + b) + c$$

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

Axiom 3. Distributive property

$\forall a, b, c \in S$, we have

$$a + b \cdot c = (a + b)(a + c)$$

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

Axiom 4. Identity element

$\exists$ a unique element of S denoted by $1 \in S$, s.t. $\forall a \in S$,

$$1 + a = a + 1 = 1$$

$$1 \cdot a = a \cdot 1 = a$$

- the uniqueness of the identity element can be proved

Axiom 5. Null element

$\exists$ a unique element of S denoted by $0 \in S$ such that $\forall a \in S$, we have

$$0 + a = a + 0 = a$$

$$0 \cdot a = a \cdot 0 = 0$$

Axiom 6. Complement element

$\forall a \in S$, $\exists$ a unique element of S denoted by $a' \in S$ such that

$$a + a' = a' + a = 1$$

$$a \cdot a' = a' \cdot a = 0$$

- then a' is referred to as the complement of a and vice versa

Duality property

- If we consider the replacements of $+ \leftrightarrow \cdot$ and $1 \leftrightarrow 0$ in an axiom and obtain another axiom, this feature is so called as "duality property"

e.g.

Axiom 4 : $1 \cdot a = a$

$1 \leftrightarrow 0$, $+ \leftrightarrow \cdot$ $\Rightarrow$ $0 + a = a$ Axiom 5

- the Boolean algebra possesses the duality property

- Now, let us consider the following theorems that can be proved

Theorem 1.

$\forall a \in S$ we have

$$a + a = a$$

$$a \cdot a = a$$

Proof.

$$a + a = a \cdot (1+1) = a \cdot 1 = a$$

$$a \cdot a = (a+0) \cdot (a+0) = a + 0 \cdot 0 = a + 0 = a$$

Theorem 2. De Morgan's Law

$\forall a, b \in S$, we have

$$(a+b)' = a' \cdot b'$$

$$(a \cdot b)' = a' + b'$$

Proof.

$$a + b + (a+b)' = a + b + a' \cdot b'$$

$$= a + (b+a') \cdot (b+b')$$

$$= a + (b+a') \cdot 1$$

$$= a + b + a' = b + 1 = 1$$

$$a \cdot b + (a \cdot b)' = a \cdot b + (a' + b')$$

$$= (a+a')(a'+b) + b'$$

$$= 1 \cdot (a'+b) + b' = a' + b + b' = a' + 1 = 1$$

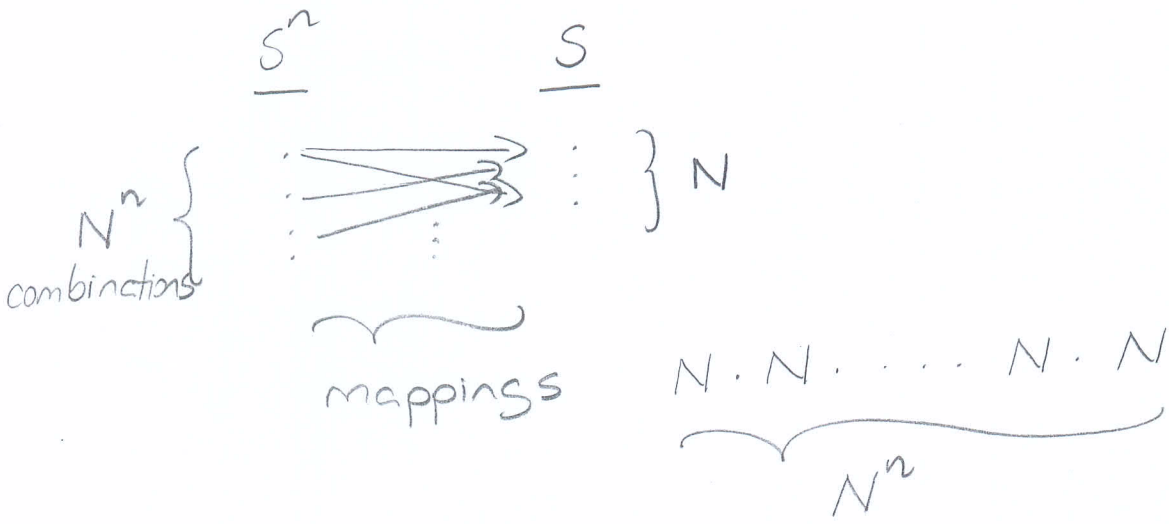
n-variable functions and Boolean functions

- Given a set S with $|S| = N$, let $f: S^n \to S$ be an n-variable function

- and consider $F = \{ f \mid f: S^n \to S \}$

so what is $|F| = ?$

- note that $|S^n| = N^n$, then



- therefore, the number of such fn.'s

$$|F| = N^{(N^n)}$$

Definition 1. The function $f: S^n \to S$ which is obtained by applying the operations $+, \cdot, '$ of Boolean algebra on the variables $x_1, \ldots, x_n$ and constants is referred to as a Boolean function.

e.g. Let $S = \{0, 1, 2, 3\}$ and consider three variable Boolean fn.

$$f(x_1, x_2, x_3) = (2x_1 + x_2)' + 2x_2x_3'$$
$$= (2' + x_1')x_2' + 2x_2x_3' = 2'x_2' + x_1'x_2' + 2x_2x_3' \quad 2.5$$

Theorem 3. Concensus theorem

$\forall a, b, c \in S$, we have

$$ab + a'c + bc = ab + a'c$$

Proof.

$$\begin{aligned} ab + a'c + bc &= ab + a'c + bc(a + a') \\ &= ab + a'c + abc + a'bc \\ &= ab(1 + c) + a'c(1 + b) \\ &= ab \cdot 1 + a'c \cdot 1 \\ &= ab + ac \end{aligned}$$

Theorem 4. Let $f: S^n \to S$ be a Boolean function, then

$$\begin{aligned} f(x_1, \ldots, x_n) &= f_i(1) x_i + f_i(0) x_i' \\ &= [f_i(1) + x_i'][f_i(0) + x_i] \end{aligned}$$

where

$$f_i(1) = f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n)$$

$$f_i(0) = f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n)$$

Proof.

- we can express f as follows

$$f(x_1, \ldots, x_n) = g x_i + h x_i' + k$$

where g, h, k are $(n-1)$ variable functions

-then

$$f(x_1, \ldots, x_n) = g x_i + h x_i' + k(x_i + x_i')$$

$$= g x_i + h x_i' + k x_i + k x_i'$$

$$= \underbrace{(g+k)}_{f_i(1)} x_i + \underbrace{(h+k)}_{f_i(0)} x_i' .$$

-for the 2nd half of the proof, we consider

$$[f_i(1) + x_i'][f_i(0) + x_i] = [g + k + x_i'][h + k + x_i]$$

$$= gh + gk + g x_i + kh + kk + k x_i$$
$$+ x_i' h + x_i' k + \cancel{x_i' x_i}^{\,0}$$

$$= gh + gk + g x_i + kh + k + k(x_i + x_i')$$
$$+ h x_i'$$

$$= g x_i + h x_i' + k + k + gh + gk + kh$$

$$k(1+g) + gh + kh$$

$$k + gh + kh$$

$$k(1+h) + gh$$

$$= g x_i + h x_i' + k + gh$$

-it follows from Concensus theorem that

$$g x_i + h x_i' + gh = g x_i + h x_i'$$

-then we set

$$[f_i(1)+x_i'][f_i(0)+x_i] = gx_i+hx_i'+k$$
$$\triangleq f(x_1,\dots,x_n)$$

-this completes the proof.

Recap

-Now we can employ Theorem 4 to express any Boolean function, $f_B: S^n \to S$ in one of the three canonical representations summarized with the following theorems

Theorem 5. An n-variable Boolean function $f: S^n \to S$ can be expressed in the following form

$$\begin{aligned} f(x_1,x_2,\dots,x_n) &= f(0,0,\dots,0)x_1'x_2'\cdots x_n' + f(0,0,\dots,1)x_1'x_2'\cdots x_n \\ &\quad + \dots + f(1,1,\dots,1)x_1x_2\cdots x_n \\ &= f(0)m_0 + f(1)m_1 + \dots + f(2^n-1)m_{2^n-1} \\ &= \sum_{i=0}^{2^n-1} f(i)m_i \end{aligned}$$

where $m_i = x_1^* x_2^* \cdots x_n^*$ is referred to as minterms with "*" denoting true or complement forms of the variable

Proof

-Note that, this canonical representation is so called as "sum of minterms" or "sum of products" in general.

Proof. It follows from Theorem 4 that we have

$$f(x_1,\dots,x_n) = f_i(1)x_i + f_i(0)x_i'$$

-now we can represent $f_i(1)$ and $f_i(0)$ in accordance with Theorem 4

-repeating this method for $i=1,2,\ldots,$ yields the sum of minterms expression for $f(x_1,\ldots,x_n)$

Example. Let $n=2$, then we have

$$f(x_1,x_2) = f(1,x_2)x_1 + f(0,x_2)x_1'$$

$$= [f(1,1)x_2 + f(1,0)x_2']x_1 + [f(0,1)x_2 + f(0,0)x_2']x_1'$$

$$= f(0,0)x_1'x_2' + f(0,1)x_1'x_2 + f(1,0)x_1x_2' + f(1,1)x_1x_2$$

$$= f(0)m_0 + f(1)m_1 + f(2)m_2 + f(3)m_3$$

$$= \sum_{i=0}^{3} f(i)m_i$$

Theorem 6. An n-variable Boolean function $f: S^n \to S$ can be expressed as follows

$$f(x_1,\ldots,x_n) = [f(0,0,\ldots,0) + x_1 + x_2 + \cdots + x_n]$$

$$\cdot [f(0,0,\ldots,1) + x_1 + x_2 + \cdots + x_n']$$

$$\cdots [f(1,1,\ldots,1) + x_1' + x_2' + \cdots + x_n']$$

$$= [f(0)+M_0][f(1)+M_1]\cdots[f(2^n-1)+M_{2^n-1}]$$

$$= \prod_{i=0}^{2^n-1} [f(i)+M_i]$$

where

$M_i = x_1^* + x_2^* + \cdots + x_n^*$ is referred to as maxterms with "$*$" denoting true or complement forms of the variable.

- Note that this canonical representation is so called as "Product of maxterms" or "product of sums"

Proof. In a similar manner as in the proof of Theorem 3 we have

$$f(x_1, x_2, \dots, x_n) = [f_i(1) + x_i'][f_i(0) + x_i]$$

- now we can rewrite $f_i(1)$ and $f_i(0)$ in accordance with Theorem 4
- repeating this method for $i = 1, 2, \dots, n$ gives the product of maxterms expression for $f(x_1, \dots, x_n)$

Example. Let $n = 2$, then we have

$$f(x_1, x_2) = [f(1, x_2) + x_1'][f(0, x_2) + x_1]$$

$$= \{[f(1,1) + x_2'][f(1,0) + x_2] + x_1'\}$$

$$\cdot \{[f(0,1) + x_2'][f(0,0) + x_2] + x_1\}$$

$$= [f(1,1) + x_2' + x_1'][f(1,0) + x_2 + x_1']$$

$$\cdot [f(0,1) + x_2' + x_1][f(0,0) + x_2 + x_1]$$

$$= [f(0) + x_1 + x_2][f(1) + x_1 + x_2'][f(2) + x_1' + x_2]$$

$$\cdot [f(3) + x_1' + x_2']$$

$$= [f(0) + M_0][f(1) + M_1][f(2) + M_2][f(3) + M_3]$$

$$= \prod_{i=0}^{3} [f(i) + M_i]$$

Remark. Note that

$$M_i = m_i' \quad \text{or} \quad m_i = M_i'$$

Exclusive OR (XOR) operation, $\oplus$

- We define a new type of operation, $\oplus$ as follows

$$a \oplus b = ab' + a'b$$

- thus, we have

$$a \oplus a = aa' + a'a = 0$$
$$1 \oplus a = 1 \cdot a' + 1' \cdot a = a'$$
$$a \oplus (b \oplus c) = (a \oplus b) \oplus c$$

Theorem 7. An n-variable Boolean function can be expressed as follows

$$f(x_1, x_2, \cdots, x_n) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_n x_n$$
$$+ a_{n+1} x_1 x_2 \oplus a_{n+2} x_1 x_3 \oplus \cdots$$
$$+ \cdots\cdots + a_m x_1 x_2 \cdots x_n$$

where

$$m = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n}$$
$$= \sum_{i=0}^{n} \binom{n}{i} = 2^n$$

- Note that this canonical representation is so called as Reed-Müller expansion

proof. Using the values of $f(0), f(1), \cdots, f(2^n - 1)$ leads to get a_i, i.e.

$$f(0, \ldots, 0) = a_0$$
$$f(1, 0, \ldots, 0) = a_0 \oplus a_1 \Rightarrow a_1 \text{ is solved}$$

- thus, at one time we obtain

$$a \oplus x = b$$

how to solve $a \oplus x = b$

- we can XOR both sides with a

$$a \oplus (a \oplus x) = a \oplus b$$

$$\Rightarrow (a \oplus a) \oplus x = 0 \oplus x = x = a \oplus b$$

Result of the whole story

- Now we can state the resulting theorem as follows

Theorem 8. It can be deduced or inferred from the three canonical representations that the function values, $f(0), f(1), \ldots, f(2^n - 1)$ are sufficient to specify a Boolean function in canonical form.

what does Theorem 8 imply?

- Assume that a Boolean function is expressed in terms of one of the canonical representations

Now;

- we wonder if the canonical representation is able to justify the same value as the function's values at a number of N^n points

But;

- we know that the canonical representation guarantee to generate the same values as the function's values at a number of $2^n - 1$ (only specific) points

So what about the remaining points "N-2" ?

- If the canonical representation gives the same values as the original function at the remaining $N^n - 2^n$ points too

  ↳ then it can be said that the Boolean function can be completely represented by one of the canonical forms

Otherwise;

- we say that such a Boolean function can NOT be expressed in one of the canonical representations

Remark. Note that we can show that if $N=2$, then $N^n - 2^n = 2^2 - 2^2 = 0$ implying that there exist NO remaining points other than $f(0), f(1), \ldots, f(2^n-1)$

Hence;

- A Boolean fn. defined for a Boolean algebra with $|S|=2$ and $\{S, +, \cdot, '\}$ can be represented in one of the canonical forms.

Recap

- this justifies why we consider Boolean algebra with a set of 2 elements, namely, denoted as 0 and 1 (this is INEVITABLE due to the existence of 1 and 0 in general Boolean algebra)

↳ in order to analyse logic circuits and digital systems

Example. Let us derive the canonical representations for a Boolean function defined as

$$f(x_1, x_2, x_3) = 3x_2' + x_1'x_2' + 2x_2x_3'$$

with

$x_1\ x_2\ x_3$	000	001	010	011	100	101	110	111
$f(x_1, x_2, x_3)$	1	1	2	0	3	3	2	0

- In sum of minterms form,

$$f(x_1, x_2, x_3) = 1 \cdot x_1'x_2'x_3' + 1 \cdot x_1'x_2'x_3 + 2 \cdot x_1'x_2x_3'$$
$$+ 0 \cdot x_1'x_2x_3 + 3 \cdot x_1x_2'x_3' + 3 \cdot x_1x_2'x_3'$$
$$+ 3 \cdot x_1x_2'x_3 + 2x_1x_2x_3' + 0 \cdot x_1x_2x_3$$

$$= x_1'x_2'x_3' + x_1'x_2'x_3 + 2x_1'x_2x_3' + 3x_1x_2'x_3'$$
$$+ 3x_1x_2'x_3' + 2x_1x_2x_3' + 3x_1x_2'x_3$$

- In product of maxterms form

$$f(x_1,x_2,x_3) = \overbrace{[1+x_1+x_2+x_3]}^{1}\cdot\overbrace{[1+x_1+x_2+x_3']}^{1}\cdot[2+x_1+x_2'+x_3]$$
$$\cdot[0+x_1+x_2'+x_3']\cdot[3+x_1'+x_2+x_3]\cdot[3+x_1'+x_2+x_3']$$
$$\cdot[2+x_1'+x_2'+x_3]\cdot[0+x_1'+x_2'+x_3']$$

$$= [2+x_1+x_2'+x_3]\cdot[x_1+x_2'+x_3']\cdot[3+x_1'+x_2+x_3]$$
$$\cdot[3+x_1'+x_2+x_3']\cdot[2+x_1'+x_2'+x_3]\cdot[x_1'+x_2'+x_3']$$

Finally;

- In Reed-Müller canonical form

$$f(x_1,x_2,x_3) = a_0 \oplus a_1x_1 \oplus a_2x_2 \oplus a_3x_3 \oplus a_4x_1x_2 \oplus a_5x_1x_3$$
$$\oplus a_6x_2x_3 \oplus a_7x_1x_2x_3$$

$f(0,0,0) = 1 = a_0$

$f(1,0,0) = 3 = a_0 \oplus a_1 = 1 \oplus a_1 \Rightarrow a_1 = 1 \oplus 3$
$= 1'\cdot 3 + 1\cdot 3'$
$= 0\cdot 3 + 3'$
$= 3'$

$f(0,1,0) = 2 = a_0 \oplus a_2 = 1 \oplus a_2 \Rightarrow a_2 = 1 \oplus 2 = 2'$

$f(0,0,1) = 1 = a_0 \oplus a_3 = 1 \oplus a_3 \Rightarrow a_3 = 1 \oplus 1 = 1' = 0$

$f(1,1,0) = 2 = a_0 \oplus a_1 \oplus a_2 \oplus a_4 = 1 \oplus 3' \oplus 2' \oplus a_4$

$\Rightarrow a_4 = 1 \oplus 3' \oplus 2' \oplus 2 = 3 \oplus (2'\cdot 2' + 2\cdot 2) = 3 \oplus 1 = 3'$

$f(1,0,1) = 3 = a_0 \oplus a_1 \oplus a_3 \oplus a_5 = 1 \oplus 3' \oplus 0 \oplus a_5$

$\Rightarrow a_5 = 1 \oplus 3' \oplus 3 = 3 \oplus 3 = 0$

$f(0,1,1) = 0 = a_0 \oplus a_2 \oplus a_3 \oplus a_6 = 1 \oplus 2' \oplus 0 \oplus a_6$

$\Rightarrow a_6 = 1 \oplus 2' \oplus 0 \oplus 0 = 2 \oplus 0 = 2$

$f(1,1,1) = a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_5 \oplus a_6 \oplus a_7 = 0$

$\Rightarrow a_7 = \underbrace{1 \oplus 3'} \oplus 2' \oplus 0 \oplus 3' \oplus 0 \oplus 2 \oplus 0$

$= 3 \oplus 2' \oplus 3' \oplus 2 = \underbrace{3 \oplus 3'}_{1} \oplus \underbrace{2' \oplus 2}_{1} = 0$

As a result;

$f(x_1, x_2, x_3) = 1 \oplus 3' x_1 \oplus 2' x_2 \oplus 3' x_1 x_2 \oplus 2 x_2 x_3$