Notes on Boolean Algebra

1 Boolean algebra

Definition 1 A **Boolean lattice** or **Boolean algebra** is a complemented, distributive lattice.

A Boolean algebra has the following properties:

(P1) Idempotent $x+x=x, \quad x\cdot x=x$

(P2) Commutative $x+y=y+x, \quad x\cdot y=y\cdot x$

(P3) Associative $x+(y+z)=(x+y)+z, \quad x\cdot(y\cdot z)=(x\cdot y)\cdot z$

(P4) Absortive $x\cdot(x+y)=x, \quad x+x\cdot y=x$

(P5) Distributive $x+y\cdot z=(x+y)\cdot(x+z), \quad x\cdot(y+z)=x\cdot y+x\cdot z$

(P6) Existence of the complement

It is possible to prove that an algebraic system $(B,+,\cdot)$ with the above properties is a Boolean algebra[1].

Theorem 1 *Complementation in a Boolean algebra is unique.*

Theorem 2 (Involution) *In a Boolean algebra,* $(x')'=x$.

Theorem 3 *In a Boolean algebra,*

$$\begin{aligned} x+x'y &= x+y, \\ x(x'+y) &= xy. \end{aligned}$$

Theorem 4 *In a Boolean algebra,*

$$\begin{aligned} x\le y &\Leftrightarrow xy'=0 \\ &\Leftrightarrow x'+y=1. \end{aligned}$$

Theorem 5 (DeMorgan's Laws) *In a Boolean algebra,*

$$\begin{aligned} (x+y)' &= x'y', \\ (xy)' &= x'+y'. \end{aligned}$$

Theorem 6 (Consensus) *In a Boolean algebra,*

$$\begin{aligned} xy+x'z+yz &= xy+x'z, \\ (x+y)(x'+z)(y+z) &= (x+y)(x'+z). \end{aligned}$$

[1] We can also define a Boolean algebra as an algebraic system $(B,+,\cdot)$ which satisfies the following properties:

(P1′) Commutative $x+y=y+x, \quad x\cdot y=y\cdot x$

(P2′) Distributive $x+y\cdot z=(x+y)\cdot(x+z), \quad x\cdot(y+z)=x\cdot y+x\cdot z$

(P3′) Identities $x+0=x, \quad x\cdot 1=x$

(P4′) Existence of the complement $x+x'=1, \quad x\cdot x'=0$

2 Boolean functions

Definition 2 Given a Boolean Algebra B, we can define **Boolean formula** inductively.

(1) an element of B is a Boolean formula,

(2) if g and h are Boolean formulas, then so are $(g)+(h)$, $(g)\cdot(h)$, and $(g)'$,

(3) no other expression is a Boolean formula unless it is compelled to be one by (1) and (2),

where an **expression** is a finite sequence of symbols.

A **symbol** is either a **logical symbol**, $+,\cdot,'$ or a **Boolean symbol** which is denoted by $x_1,\cdots,x_n$.

Definition 3 A **Boolean function** of n variables is also defined inductively:

(1) for any element $b\in B$, the **constant function**, defined by

$$f(x_1,\cdots,x_n)=b \quad \text{for all} \ (x_1,\cdots,x_n)\in B^n$$

is an n-variable Boolean function,

(2) for any x_i, the **projection function**, defined by

$$f(x_1,\cdots,x_n)=x_i \quad \text{for all} \ (x_1,\cdots,x_n)\in B^n$$

is an n-variable Boolean function,

(3) if g and h are n-variable Boolean functions, then the functions $g+h, g\cdot h$ and g' defined by

$$\begin{aligned} (g+h)(x_1,\cdots,x_n) &= g(x_1,\cdots,x_n)+h(x_1,\cdots,x_n), \\ (g\cdot h)(x_1,\cdots,x_n) &= g(x_1,\cdots,x_n)\cdot h(x_1,\cdots,x_n), \\ (g')(x_1,\cdots,x_n) &= (g(x_1,\cdots,x_n))', \end{aligned}$$

for all $(x_1,\cdots,x_n)\in B^n$ are n-variable Boolean functions,

(4) Only the functions that can be derived by above (1)–(3) are n-variable Boolean functions.

The functions defined as above are said to have **domain** B^n and **codomain** B and denoted by $f(x):B^n\mapsto B$ where $x=\vec{x}=(x_1,\cdots,x_n)$.

Definition 4 The **cofactor** of $f(x_1,\cdots,x_i,\cdots,x_n)$ with respect to x_i is defined to be $f_{x_i}=f(x_1,\cdots,1,\cdots,x_n)$. The **cofactor** of $f(x_1,\cdots,x_i,\cdots,x_n)$ with respect to x_i' is defined to be $f_{x_i'}=f(x_1,\cdots,0,\cdots,x_n)$.

Theorem 7 (Boole's Expansion Theorem) *If* $f:B^n\to B$ *is a Boolean function, then*

$$\begin{aligned} f(x_1,\cdots,x_n) &= x_1'\cdot f(0,x_2,\cdots,x_n)+x_1\cdot f(1,x_2,\cdots,x_n) \\ &= (x_1'+f(1,x_2,\cdots,x_n))\cdot(x_1+f(0,x_2,\cdots,x_n)), \end{aligned}$$

for all $(x_1,\cdots,x_n)\in B^n$.

If we recursively apply the Expansion Theorem to a n-variable Boolean function, we eventually get

$$\begin{aligned} f(x_1,\cdots,x_{n-1},x_n) = \quad & f(0,\cdots,0,0)\cdot x_1'\cdots x_{n-1}'x_n' \\ + \quad & f(0,\cdots,0,1)\cdot x_1'\cdots x_{n-1}'x_n \\ + \quad & f(0,\cdots,1,0)\cdot x_1'\cdots x_{n-1}x_n' \\ + \quad & \vdots \\ + \quad & f(1,\cdots,1,1)\cdot x_1\cdots x_{n-1}x_n. \end{aligned}$$

Definition 5 The values $f(0,\cdots,0,0)$ through $f(1,\cdots,1,1)$ are elements of B called the **discriminants** of the function f and the elementary products $x_1'\cdots x_{n-1}'x_n'$ through $x_1\cdots x_{n-1}x_n$ are called **minterms**.

Equivalently, a minterm is a cube in which every variable in the Boolean functions appear. A minterm m_1 is said to **dominate** m_2, denoted by $m_1 \succ m_2$, if for each position that m_2 has a 1, m_1 also has a 1. For example, *abc* dominates *ab*.

The Boolean functions of n variables form a Boolean algebra $(B,+,\cdot)$ where B is the set of Boolean functions, $+$ and $\cdot$ are functionals as previoiusly defined and 0 and 1 are adequately defined constant functions.

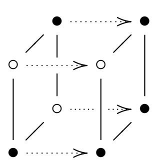
Definition 6 For single-output functions, the **distance** δ between a cube q and a cube r is defined as the cardinality of the set $\{l : (l \in q) \wedge (l' \in r)\}$, where l is a Boolean variable used in the given Boolean function.

For example, the distance between *abc* and *abc'* is 1 and the distance between *ab* and *abc* is 0.

Definition 7 A function $f(x_1,\cdots,x_i,\cdots,x_n)$ is (positive/negative) **unate in variable** x_i if $f_{x_i} \geq f_{x_i'}$ $(f_{x_i} \leq f_{x_i'})$. Otherwise it is **binate** (or mixed) in that variable. A function is (positive/negative) **unate** if it is (positive/negtive) unate in all support variables. Otherwise it is **binate** (or mixed).

2.1 Unateness of Boolean functions

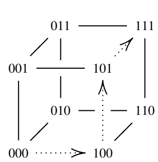
Unateness of Boolean functions w.r.t variables A function f is unate in variable x iff $f_{x'} \leq f_x$. Consider the following Boolean function f with three variables, which is unate in x.



Note, for any ON-vertex in the $x=0$ plane (the rectangle at the left side), the corresponding vertex in the $x=1$ plane is ON.

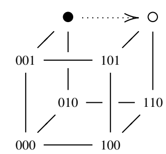
We can generalize this intuition to the multi-dimensional case.

Unateness of Boolean functions For example, consider a path from the min-vertex (000) to the max-vertex (111). Intuitively, when f is monotonic increasing, f values along this path never decrease.



In a three-dimensional hypercube, any path from the min-vertex to the max-vertex has length 3 and is a permutation of three length-1 move along the x, y, and z axis. Since unate function is unate in *every* variable, each of these three walks should be a "monotonically increasing" move.

Unateness of covers A cover F is unate in variable x if and only if x never appears complemented in the products of F. Thinking this pictorially, the fact that x' appears in a product of F means that the literal x' have not been removed through consensus. For example, if F contains $x'yz$, F must not have contained xyz as in the following figure:



Lemma 1 If a function f is unate in variable x, then there exists a cover F of f unate in x_1.

Theorem 8 If a function f is unate, then there exists a cover F of f which is unate.

Lemma 2 If a cover F is unate in variable x, then the function represented by F is also unate in x.

Theorem 9 If a cover F is unate, then the function represented by F is also unate.

2.2 Semantics of Boolean functions

Given a boolean function f and its corresponding Boolean expression e, the meaning of e is the set of minterms for which f

2.3 Multiple-valued functions

Definition 8 (Multiple-valued function) Let $p_i, i=1,\cdots,n$ be positive integers. Define $P_i = \{0,\cdots,p_i-1\}$ for $i=1,\cdots,n$, and $B=\{0,1,*\}$. A multiple-valued Boolean function, f, is a mapping

$$f : P_1 \times P_2 \times \cdots \times P_n \to B.$$

Definition 9 (Minterms) Each element in the domain of a Boolean function is called a **minterm** of the function.

An n-input, m-output switching function can be represented by a multiple-valued function of $n+1$ variables where $p_i = 2$ for $i=1,\cdots,n$, and $p_{n+1}=m$. Suppose that $\{f_i : i=0,\cdots,m-1\}$ is the set of output functions. Then we can have

$$f_i(x_1,\cdots,x_n) \equiv f(x_1,\cdots,x_n,i).$$

This special case is called a **multiple-output function**.

Definition 10 (ON-sets, OFF-sets, DC-sets) The **ON-set** of a function is the set of minterms for which the function value is 1. Likewise, the **OFF-set** of a function is the set of minterms for which the function value is 0 and the **OFF-set** of a function is the set of minterms for which the function value is unspecified.

In the case of multiple-output function f, the ON-set of f_i in f is defined to be the set of minterms for which $f_i(x)=1$. OFF-set and DC-set are defined likewise.

Definition 11 (Literals) Let X_i be a variable taking a value from P_i and let S_i be a subset of P_i. $X_i^{S_i}$ represents the Boolean function

$$X_i^{S_i} = \begin{cases} 0 & \text{if } X_i \notin S_i \\ 1 & \text{if } X_i \in S_i \end{cases}$$

$x_i^{S_i}$ is called a literal of variable X_i.

Formally, the meaning of $x_i^{S_i}$ is defined as follows:

$$[\![X_i^{S_i}]\!] = \{[x_1, \cdots, x_n] : x_1 \in P_1, \cdots, x_i \in S_i, \cdots, x_n \in P_n\}.$$

3 Boolean Algebra

Definition 12 An algebra, denoted by a quintuple $(\mathsf{B}, +, \cdot, 0, 1)$ where B is a set, $+, - : \mathsf{B} \times \mathsf{B} \rightarrow \mathsf{B}$ are binary operations on B, and 0 and 1 are distinct members of B, is a **Boolean algebra** if the following postulates are satisfied.

(a) Commutative laws

(b) Distributive laws

(c) Identities

(d) Complements

Definition 13 A **switching algebra** is a Boolean algebra $(\mathsf{B}, +, \cdot, 0, 1)$ with $|\mathsf{B}| = 2$. That is, $\mathsf{B} = \{0, 1\}$.

Theorem 10 (Stone's representation theorem) *Every finite Boolean algebra is isomorphic to the Boolean algebra of subsets of some finite set S.*

Theorem 11 *The number of prime implicants of a Boolean function with n input variables is at most $3^n/n$.*

References

[1] F. M. Brown. *Boolean Reasoning: The Logic of Boolean Equations*. Dover Publications, Inc., second edition, 2003.