Boolean Algebra

January 24, 1996

Sriram C. Krishnan*

*Thanks to Y. Kukimoto for the slides

Boolean Algebra

- Reference: Chapter 2, "Boolean Reasoning" by F.M.Brown

- Outline
  - Definition of Boolean algebra
  - Examples of Boolean algebra
  - Property of Boolean algebra
  - Boolean functions/Boolean formulas

Boolean Algebra

- Boolean algebra is an algebraic structure $(\mathbf{B}, +, \cdot, 0, 1)$
  - $\mathbf{B}$: a set called the *carrier*
  - $+, \cdot$: binary operations on $\mathbf{B}$
  - $0, 1$: distinct members of $\mathbf{B}$

  satisfying a certain set of postulates.

Postulates for Boolean Algebra

$(\mathbf{B}, +, \cdot, 0, 1)$

B is closed under + and $\cdot$:

$$\forall a, b \in \mathbf{B}, a + b \in \mathbf{B} \text{ and } a \cdot b \in \mathbf{B}$$

Commutative Laws: $\forall a, b \in \mathbf{B}$,

$$\begin{aligned} a + b &= b + a \\ a \cdot b &= b \cdot a \end{aligned}$$

Distributive Laws: $\forall a, b, c \in \mathbf{B}$,

$$\begin{aligned} a + (b \cdot c) &= (a + b) \cdot (a + c) \\ a \cdot (b + c) &= (a \cdot b) + (a \cdot c) \end{aligned}$$

Identities: $\forall a \in \mathbf{B}$,

$$\begin{aligned} 0 + a &= a \\ 1 \cdot a &= a \end{aligned}$$

Complements: $\forall a \in \mathbf{B}, \exists a' \in \mathbf{B}$ s.t.

$$\begin{aligned} a + a' &= 1 \\ a \cdot a' &= 0 \end{aligned}$$

Examples of Boolean Algebra

- Switching algebra
- The algebra of classes(Subsets of a set)
- Arithmetic Boolean algebra
- The Boolean algebra of Boolean functions

Switching Algebra (Two-element Boolean Algebra)

The switching algebra is an algebraic system consisting of

- the set $\{0, 1\}$
- two binary operations AND($\cdot$) and OR($+$)
- one unary operation NOT($'$)

where

$$\begin{array}{rclcrclcrcl} 0+0 &=& 0 & & 0\cdot 0 &=& 0 & & & & \\ 0+1 &=& 1 & & 0\cdot 1 &=& 0 & & 0' &=& 1 \\ 1+0 &=& 1 & & 1\cdot 0 &=& 0 & & 1' &=& 0 \\ 1+1 &=& 1 & & 1\cdot 1 &=& 1 & & & & \end{array}$$

Switching Algebra — revisited

$$(\{0, 1\}, +, \cdot, 0, 1)$$

$+$	0	1
0	0	1
1	1	1

$\cdot$	0	1
0	0	0
1	0	1

- One of many Boolean algebras (Ex: verify that the algebra satisfies all the postulates.)

- Special case! $\Longrightarrow$ Exclusive Property: Not found in postulates of Boolean algebras

$$x + y = 1 \text{ iff } x = 1 \text{ or } y = 1$$
$$x \cdot y = 0 \text{ iff } x = 0 \text{ or } y = 0$$

The Algebra of Classes(Subsets of a Set)

$$\begin{aligned}
\mathbf{B} &\longleftrightarrow 2^S \\
+ &\longleftrightarrow \cup \\
\cdot &\longleftrightarrow \cap \\
\mathbf{0} &\longleftrightarrow \emptyset \\
\mathbf{1} &\longleftrightarrow S
\end{aligned}$$

- S is a universal set($S \neq \emptyset$). Each subset of S is called a class of S.
- If $S = \{a, b\}$, then $\mathbf{B} = 2^S = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.
- Stone Representation Theorem:

  Every finite Boolean algebra is isomorphic to the Boolean algebra of subsets of some finite set S.

The Algebra of Classes (cont'd)

$(\mathbf{B}, +, \cdot, 0, 1) = (2^S, \cup, \cap, \emptyset, S)$

- $\mathbf{B}$ is closed under $\cup$ and $\cap$.

- Commutative Laws: $\forall S_1, S_2 \in 2^S$,

$$\begin{aligned} S_1 \cup S_2 &= S_2 \cup S_1 \\ S_1 \cap S_2 &= S_2 \cap S_1 \end{aligned}$$

- Distributive Laws: $\forall S_1, S_2, S_3 \in 2^S$,

$$\begin{aligned} S_1 \cup (S_2 \cap S_3) &= (S_1 \cup S_2) \cap (S_1 \cup S_3) \\ S_1 \cap (S_2 \cup S_3) &= (S_1 \cap S_2) \cup (S_1 \cap S_3) \end{aligned}$$

- Identities: $\forall S_1 \in 2^S$,

$$\begin{aligned} \emptyset \cup S_1 &= S_1 \\ S \cap S_1 &= S_1 \end{aligned}$$

- Complements: $\forall S_1 \in 2^S, \exists S_1' = S \backslash S_1 \in 2^S$,

$$\begin{aligned} S_1 \cup S_1' &= S \\ S_1 \cap S_1' &= \emptyset \end{aligned}$$

Arithmetic Boolean Algebra

- $(D_n, \mathit{lcm}, \mathit{gcd}, \underline{1}, n)$
  - n: product of distinct prime numbers
  - D_n: set of all divisors of n
  - *lcm*: least common multiple
  - *gcd*: greatest common divisor
  - $\underline{1}$: integer 1 (not the Boolean 1-element)

Arithmetic Boolean Algebra (cont'd)

$(\mathbf{B}, +, \cdot, 0, 1) = (D_n, \mathrm{lcm}, \mathrm{gcd}, \underline{1}, n)$

- $n = 30 = 2 \times 3 \times 5$

- $D_n = \{1, 2, 3, 5, 6, 10, 15, 30\}$

- If we look at D_n as $\{\emptyset, \{2\}, \{3\}, \{5\}, \{2,3\}, \{2,5\}, \{3,5\}, \{2,3,5\}\}$, it is easy to see that arithmetic Boolean algebra is isomorphic to the algebra of classes. (See Stone Representation Theorem)

Boolean algebra of Boolean functions

- $(F_n(\mathbf{B}), +, \cdot, 0, 1)$ where
  - $F_n(\mathbf{B})$: the set of n-variable Boolean functions on **B**
  - $+$: addition of functions
  - $\cdot$: multiplication of functions
  - 0: the zero function
  - 1: the one function

Properties of Boolean Algebras

1. Associativity

$$\begin{aligned} a + (b + c) &= (a + b) + c \\ a(bc) &= (ab)c \end{aligned}$$

2. Idempotence

$$\begin{aligned} a + a &= a \\ aa &= a \end{aligned}$$

3.

$$\begin{aligned} a + 1 &= 1 \\ a \cdot 0 &= 0 \end{aligned}$$

4. Absorption

$$\begin{aligned} a + (ab) &= a \\ a(a+b) &= a \end{aligned}$$

5. Involution $\quad (a')' = a$

6. De Morgan's Laws

$$\begin{aligned} (a+b)' &= a'b' \\ (ab)' &= a' + b' \end{aligned}$$

7.

$$\begin{aligned} a + a'b &= a + b \\ a(a'+b) &= ab \end{aligned}$$

8. Consensus

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

The Principle of Duality

Every identity on Boolean algebra is transformed into another identity if the following is interchanged

1. the operations $+$ and $\cdot$,
2. the elements 0 and 1

- Example:

$$\begin{aligned} a + 1 &= 1 \\ a \cdot 0 &= 0 \end{aligned}$$

Boolean Formulas and Boolean Functions

- A Boolean function is a mapping that can be described by a Boolean formula.
- Outline:
  - Definition of Boolean formulas
  - Definition of Boolean functions
  - Boole's expansion theorem
  - The minterm canonical form

n-Variable Boolean Formulas

- Given a Boolean algebra **B** and n symbols $x_1, \ldots, x_n$, the set of all Boolean formulas on the n symbols is defined by:

  1. The elements of **B** are Boolean formulas.

  2. The symbols $x_1, \ldots, x_n$ are Boolean formulas.

  3. If g and h are Boolean formulas, then so are

     (a) $(g) + (h)$

     (b) $(g)(h)$

     (c) $(g)'$

4. A string is a Boolean formula iff it is obtained by finitely many applications of rules 1, 2 and 3.

- The number of n-variable Boolean formulas is *infinite*.

n-Variable Boolean Functions

- Given an n-variable Boolean formula F, the corresponding n-variable function $f : \mathbf{B}^n \to \mathbf{B}$ is defined as follows.

  1. If $F = b \in \mathbf{B}$, then the formula represents the *constant function* defined by

  $$f(x_1, \ldots, x_n) = b \qquad \forall (x_1, \ldots, x_n) \in \mathbf{B}^n$$

  2. If $F = x_i$, then the formula represents the *projection function* defined by

  $$f(x_1, \ldots, x_n) = x_i \qquad \forall (x_1, \ldots, x_n) \in \mathbf{B}^n$$

3. If the formula is of type either $G + H$, GH or G', then the corresponding n-variable function is defined as follows.

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

for $\forall(x_1,\ldots,x_n) \in \mathbf{B}^n$

- The number of n-variable Boolean functions over a finite Boolean algebra **B** is *finite*.

Example

- $\mathbf{B} = \{0, 1, a', a\}$
- symbols: $\{x, y\}$
- 2-variable Boolean formula: e.g. $a'x + ay'$
- 2-variable Boolean function: $f : \mathbf{B}^2 \to \mathbf{B}$
- Domain: $\mathbf{B}^2 = \{(0,0), (0,1), \ldots, (a,a)\}$

x	y	$f(x,y)$
0	0	a
0	1	0
0	a'	a
0	a	0
$\vdots$	$\vdots$	$\vdots$

Boole's Expansion Theorem

- Shannon expansion holds in Boolean algebras even if $\mathbf{B} \neq \{0, 1\}$.

Theorem 1 *If* $f : \mathbf{B}^n \to \mathbf{B}$ *is a Boolean function, then*

$$f(x_1, x_2, \ldots, x_n) = x_1' \cdot f(0, x_2, \ldots, x_n) + x_1 \cdot f(1, x_2, \ldots, x_n)$$

for $\forall (x_1, \ldots, x_n) \in \mathbf{B}^n$.

Proof. Follows from the definition of Boolean functions. $\square$

The Minterm Canonical Form

Theorem 2 *A function $f : \mathbf{B}^n \to \mathbf{B}$ is* <u>*Boolean*</u> *iff it can be expressed in the minterm canonical form*

$$f(X) = \sum_{A \in \{0,1\}^n} f(A) X^A$$

where $X = (x_1, \ldots, x_n)$, $A = (a_1, \ldots, a_n) \in \{0, 1\}^n$, *and* $X^A = x_1^{a_1} \ldots x_n^{a_n}$.

Proof. Follows from Boole's expansion theorem. $\square$

Example($n = 3$):

$$\begin{aligned} f(x_1, x_2, x_3) = {} & f(0,0,0)x_1'x_2'x_3' + f(0,0,1)x_1'x_2'x_3 \\ & + f(0,1,0)x_1'x_2x_3' + f(0,1,1)x_1'x_2x_3 \\ & + f(1,0,0)x_1x_2'x_3' + f(1,0,1)x_1x_2'x_3 \\ & + f(1,1,0)x_1x_2x_3' + f(1,1,1)x_1x_2x_3 \end{aligned}$$

Example

x	y	$f(x,y)$
0	0	a
0	1	0
1	0	1
1	1	a'

- $f(x,y) = a'x + ay' = ax'y' + 0x'y + 1xy' + a'xy$ over $\{0, 1, a', a\}$

- f is Boolean (don't have to specify outputs for 16 input patterns)

Example(cont'd)

x	$f(x)$
0	a
1	1
a'	a'
a	1

- NOT Boolean

Proof. If f is Boolean, f can be expressed by

$$f(x) = x' \cdot f(0) + x \cdot f(1) = x' \cdot a + x \cdot 1$$

from the minterm canonical form theorem. Substituting $x = a$ yields, however,

$$f(a) = a' \cdot a + a \cdot 1 = a \neq 1$$

Contradiction. $\square$

Boolean Algebras of Boolean Functions

- $(F_n(\mathbf{B}), +, \cdot, 0, 1)$
  - $F_n(\mathbf{B})$: the set of n-variable Boolean functions on $\mathbf{B}$.
  - $+$: addition of functions
  - $\cdot$: multiplication of functions
  - 0: the zero function
  - 1: the one function

- Let $\mathbf{B} = \{0, 1\}$. $F_1(\mathbf{B}) = \{0, 1, x, x'\}$. $F_2(\mathbf{B}) = \{0, 1, x, x', y, y', x+y, x+y', x'+y, x'+y', xy, xy', x'y, x'y', xy + x'y', xy' + x'y\}$.

Why Do We Need "Big" Boolean Algebras?

- Big algebras can't be avoided

$$f = xy + xz' + x'z$$

  - Two-element view: $x, y, z \in \{0, 1\}$ and $f \in \{0, 1\}$

  - Big-algebra view: f as a member of the Boolean algebra of 3-variable Boolean functions

- Big algebras are useful
  - Two-element view: Truth tables include only 0 and 1.
  - Big-algebra view: Truth tables contain any elements of **B**.

J	K	Q	$Q^+(J,K,Q)$
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	0

$\mathbf{B} = \{0, 1\}$

J	K	$Q^+(J,K)$
0	0	Q
0	1	0
1	0	1
1	1	Q'

$\mathbf{B} = \{0, Q, Q', 1\}$

Alternative Characterization of Boolean Algebra

Definition 1 $a \leq b$ *iff* $ab' = 0$, *where* $a, b \in \mathbf{B}$

- $\leq$ defines a *partial order* in $\mathbf{B}$, i.e.

  1. Reflexive: $a \leq a$
  2. Antisymmetric:
     $a \leq b$ and $b \leq a \Rightarrow a = b$
  3. Transitive: $a \leq b$ and $b \leq c \Rightarrow a \leq c$

Alternative Characterization of Boolean Algebra–Contd.

In addition it can be shown that:

- For each $x, y \in \mathbf{B}$, there exists
  - Greatest lower bound $z \in \mathbf{B}$, written $z = a \wedge b$, AND
  - Least upper bound $w \in \mathbf{B}$, written $w = a \vee b$
- $\vee$ distributes over $\wedge$, and $\wedge$ distributes over $\vee$
- For each $x \in \mathbf{B}$, there exists $x' \in \mathbf{B}$ such that

- $x \vee x' = 1$, where 1 is the greatest element, AND

- $x \wedge x' = 0$, where 0 is the least element

Thus a Boolean Algebra is a distributive lattice with complements.

A Note on Proofs

"Even if we do not understand exactly what proof is, we can, in ordinary analsysis at any rate, recognise a proof when we see one. Secondly, there are two different motives in any presentation of a proof. The first motive is to secure conviction. The second is to exhibit the conclusion as the climax of a conventional pattern of propositions whose truth is admitted and which are arranged in accordance with rules. These are the two ideals, and experience shows that, except in the simplest mathematics, we can hardly ever satisfy the first ideal without also satisfying the second. "