

# Logic Synthesis and Verification

Jie-Hong Roland Jiang  
江介宏

Department of Electrical Engineering  
National Taiwan University



Fall 2024

# Boolean Algebra



# Boolean Algebra

---

## □ Reading

F. M. Brown. *Boolean Reasoning: The Logic of Boolean Equations*. Dover, 2003.  
(Chapters 1-3)

# Boolean Algebra

---

## □ Outline

- Definitions
- Examples
- Properties
- Boolean formulae and Boolean functions

# Boolean Algebra

---

□ A Boolean algebra is an algebraic structure  $(\mathbf{B}, +, \cdot, \underline{0}, \underline{1})$

- $\mathbf{B}$  is a set, called the *carrier*
- $+$  and  $\cdot$  are binary operations defined on  $\mathbf{B}$
- $\underline{0}$  and  $\underline{1}$  are distinct members of  $\mathbf{B}$

that satisfies the following postulates (axioms):

1. *Commutative laws*
2. *Distributive laws*
3. *Identities*
4. *Complements*

# Postulates of Boolean Algebra

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

1.  $\mathbf{B}$  is **closed** under  $+$  and  $\cdot$ .  
 $\forall a, b \in \mathbf{B}, a + b \in \mathbf{B}$  and  $a \cdot b \in \mathbf{B}$
2. **Commutative laws**:  $\forall a, b \in \mathbf{B}$   
 $a + b = b + a$   
 $a \cdot b = b \cdot a$
3. **Distributive laws**:  $\forall a, b, c \in \mathbf{B}$   
 $a + (b \cdot c) = (a + b) \cdot (a + c)$   
 $a \cdot (b + c) = a \cdot b + a \cdot c$
4. **Identities**:  $\forall a \in \mathbf{B}$   
 $\underline{0} + a = a$   
 $\underline{1} \cdot a = a$
5. **Complements**:  $\forall a \in \mathbf{B}, \exists a' \in \mathbf{B}$  s.t.  
 $a + a' = \underline{1}$   
 $a \cdot a' = \underline{0}$   
Verify that  $a'$  is unique in  $(\mathbf{B}, +, \cdot, \underline{0}, \underline{1})$ .

# Instances of Boolean Algebra

---

- Switching algebra (two-element Boolean algebra)
- The algebra of classes (subsets of a set)
- Arithmetic Boolean algebra
- The algebra of propositional functions

# Instance 1: Switching Algebra

□ A switching algebra is a two-element Boolean Algebra  $(\{0,1\}, +, \cdot, 0, 1)$  consisting of:

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

where

OR	0	1
0	0	1
1	1	1

AND	0	1
0	0	0
1	0	1

NOT	-
0	1
1	0



# Switching Algebra

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

- An exclusive property (not hold for all Boolean algebras) for two-element Boolean algebra:

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

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

OR	0	1
0	0	1
1	1	1

AND	0	1
0	0	0
1	0	1

NOT	-
0	1
1	0

# Instance 2: Algebra of Classes

## □ Subsets of a set

$$\mathbf{B} \leftrightarrow 2^S$$

$$+ \leftrightarrow \cup$$

$$\cdot \leftrightarrow \cap$$

$$\underline{0} \leftrightarrow \phi$$

$$\underline{1} \leftrightarrow S$$

□  $S$  is a universal set ( $S \neq \phi$ ). Each subset of  $S$  is called a *class* of  $S$ .

□ If  $S = \{a, b\}$ , then  $\mathbf{B} = \{\phi, \{a\}, \{b\}, \{a, b\}\}$

□  $\mathbf{B}$  ( $= 2^S$ ) is **closed** under  $\cup$  and  $\cap$

# Algebra of Classes

## □ Commutative laws: $\forall S_1, S_2 \in 2^S$

$$S_1 \cup S_2 = S_2 \cup S_1$$

$$S_1 \cap S_2 = S_2 \cap S_1$$

## □ Distributive laws: $\forall S_1, S_2, S_3 \in 2^S$

$$S_1 \cup (S_2 \cap S_3) = (S_1 \cup S_2) \cap (S_1 \cup S_3)$$

$$S_1 \cap (S_2 \cup S_3) = (S_1 \cap S_2) \cup (S_1 \cap S_3)$$

## □ Identities: $\forall S_1 \in 2^S$

$$S_1 \cup \phi = S_1$$

$$S_1 \cap S = S_1$$

## □ Complements: $\forall S_1 \in 2^S, \exists S_1' \in 2^S, S_1' = S \setminus S_1$ s.t.

$$S_1 \cup S_1' = S$$

$$S_1 \cap S_1' = \phi$$

# Algebra of Classes

## □ *Stone Representation Theorem:*

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

Therefore, for all finite Boolean algebra,  $|\mathbf{B}|$  can only be  $2^k$  for some  $k \geq 1$ .

□ The theorem proves that finite class algebras are not specialized (i.e. no exclusive properties, e.g.  $x + y = 1$  iff  $x=1$  or  $y=1$  in two-element Boolean algebra)

■ Can reason in terms of specific and easily “visualizable” concepts (union, intersection, empty set, universal set) rather than abstract operations ( $+$ ,  $\cdot$ ,  $\underline{0}$ ,  $\underline{1}$ )

# Instance 3: Arithmetic Boolean Algebra

□  $(D_n, lcm, gcd, 1, n)$

$n$ : product of distinct prime numbers

$D_n$ : set of all divisors of  $n$

$lcm$ : least common multiple

$gcd$ : greatest common divisor

1: integer 1 (not the Boolean 1-element)

□  $n = 30 = 2 \times 3 \times 5$

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

□ 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

# Instance 4: Algebra of Propositional Functions

---

□ ( $P$ ,  $\vee$ ,  $\wedge$ , □, ■)

$P$ : the set of propositional functions of  $n$  given variables

$\vee$ : disjunction symbol (OR)

$\wedge$ : conjunction symbol (AND)

□: formula that is always false (contradiction)

■: formula that is always true (tautology)

# Lessons from Abstraction

---

- Abstract mathematical objects in terms of simple rules
- A systematic way of characterizing various seemingly unrelated mathematical objects
- Abstraction trims off immaterial details and simplifies problem formulation

# Properties of Boolean Algebras

□ For arbitrary elements  $a$ ,  $b$ , and  $c$  in Boolean algebra

## 1. Associativity

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

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

## 2. Idempotence

$$a + a = a$$

$$a \cdot a = a$$

## 3.

$$a + \underline{1} = \underline{1}$$

$$a \cdot \underline{0} = \underline{0}$$

## 4. Absorption

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

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

## 5. Involution

$$(a')' = a$$

## 6. De Morgan's Laws

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

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

## 7.

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

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

## 8. Consensus

$$a \cdot b + a' \cdot c + b \cdot c =$$

$$a \cdot b + a' \cdot c$$

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

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



# Principle of Duality

---

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

- the operations  $+$  and  $\cdot$ ,
- the elements 0 and 1

□ Example:

- $a + \underline{1} = \underline{1}$
- $a \cdot \underline{0} = \underline{0}$

# Postulates for Boolean Algebra (Revisited in View of Duality)

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

1. **B** is **closed** under  $+$  and  $\cdot$ .  
 $\forall a, b \in \mathbf{B}, a + b \in \mathbf{B}$  and  $a \cdot b \in \mathbf{B}$
2. **Commutative Laws:**  $\forall a, b \in \mathbf{B}$   
 $a + b = b + a$   
 $a \cdot b = b \cdot a$
3. **Distributive laws:**  $\forall a, b, c \in \mathbf{B}$   
 $a + (b \cdot c) = (a + b) \cdot (a + c)$   
 $a \cdot (b + c) = a \cdot b + a \cdot c$
4. **Identities:**  $\forall a \in \mathbf{B}$   
 $\underline{0} + a = a$   
 $\underline{1} \cdot a = a$
5. **Complements:**  $\forall a \in \mathbf{B}, \exists a' \in \mathbf{B}$  s.t.  
 $a + a' = \underline{1}$   
 $a \cdot a' = \underline{0}$

# Two Propositions

1. Let  $a$  and  $b$  be members of a Boolean algebra. Then
- $$\begin{aligned} a = \underline{0} \text{ and } b = \underline{0} &\quad \text{iff} \quad a + b = \underline{0} \\ a = \underline{1} \text{ and } b = \underline{1} &\quad \text{iff} \quad ab = \underline{1} \end{aligned}$$

c.f. The following two propositions are only true for two-element Boolean algebra (not other Boolean algebra)

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

$$xy=0 \text{ iff } x=0 \text{ or } y=0$$

Why?

2. Let  $a$  and  $b$  be members of a Boolean algebra. Then
- $$a = b \quad \text{iff} \quad a'b + ab' = \underline{0}$$

# Boolean Formulas and Boolean Functions



# Boolean Formulas and Boolean Functions

---

## □ 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  $x_1, \dots, x_n$  the set of all Boolean formulas on the  $n$  symbols is defined by:
  1. The elements of **B** are Boolean formulas.
  2. The variable symbols  $x_1, \dots, x_n$  are Boolean formulas.
  3. If  $g$  and  $h$  are Boolean formulas, then so are
    - $(g) + (h)$
    - $(g) \cdot (h)$
    - $(g)'$
  4. A string is a Boolean formula if and only if it is obtained by finitely many applications of rules 1, 2, and 3.
- There are infinitely many  $n$ -variable Boolean formulas.

# $n$ -variable Boolean Functions

- A Boolean function is a mapping that can be described by a Boolean formula.
- Given an  $n$ -variable Boolean formula  $F$ , the corresponding  $n$ -variable function  $f : \mathbf{B}^n \rightarrow \mathbf{B}$  is defined as follows:
  1. If  $F = b \in \mathbf{B}$ , then the formula represents the **constant** function defined by
$$f(x_1, \dots, x_n) = b \quad \forall ([x_1], \dots, [x_n]) \in \mathbf{B}^n$$
  2. If  $F = x_i$ , then the formula represents the **projection** function defined by
$$f(x_1, \dots, x_n) = x_i \quad \forall ([x_1], \dots, [x_n]) \in \mathbf{B}^n$$
where  $[x_k]$  denotes a valuation of variable  $x_k$

# $n$ -variable Boolean Functions

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

$$(g + h)(x_1, \dots, x_n) = g(x_1, \dots, x_n) + h(x_1, \dots, x_n)$$

$$(g \cdot h)(x_1, \dots, x_n) = g(x_1, \dots, x_n) \cdot h(x_1, \dots, x_n)$$

$$(g')(x_1, \dots, x_n) = g(x_1, \dots, x_n)'$$

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

- The number of  $n$ -variable Boolean functions over a finite Boolean algebra  $\mathbf{B}$  is *finite*.



# Example

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

$x$	$y$	$f$
<u>0</u>	<u>0</u>	$a$
<u>0</u>	<u>1</u>	<u>0</u>
<u>0</u>	$a'$	$a$
<u>0</u>	$a$	<u>0</u>
<u>1</u>	<u>0</u>	<u>1</u>
<u>1</u>	<u>1</u>	$a'$
<u>1</u>	$a'$	<u>1</u>
<u>1</u>	$a$	$a'$
$a$	<u>0</u>	$a$
$a$	<u>1</u>	<u>0</u>
$a$	$a'$	$a$
$a$	$a$	<u>0</u>
$a'$	<u>0</u>	<u>1</u>
$a'$	<u>1</u>	$a'$
$a'$	$a'$	<u>1</u>
$a'$	$a$	$a'$

# Boole's Expansion Theorem

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

$$f(x_1, \dots, x_n) = x'_1 f(\underline{0}, \dots, x_n) + x_1 f(\underline{1}, \dots, x_n) \\ \text{for } \forall ([x_1], \dots, [x_n]) \in \mathbf{B}^n$$

*Proof.* Case analysis of Boolean functions under the construction rules. Apply postulates of Boolean algebra.

□ The theorem holds not only for two-element Boolean algebra (c.f. Shannon expansion)

# Minterm Canonical Form

**Theorem 2** A function  $f : \mathbf{B}^n \rightarrow \mathbf{B}$  is Boolean if and only if it can be expressed in the minterm canonical form

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

where  $X = (x_1, \dots, x_n) \in \mathbf{B}^n$ ,  $A = (a_1, \dots, a_n) \in \{0,1\}^n$ , and  $X^A \equiv x_1^{a_1} \cdot x_2^{a_2} \dots x_n^{a_n}$  (with  $x^0 \equiv x'$  and  $x^1 \equiv x$ )

*Proof.*

( $\Rightarrow$ ) Follows from Boole's expansion theorem.

( $\Leftarrow$ ) Examine the construction rules of Boolean functions.

# Example

$f$  is **not** Boolean!

*Proof.* If  $f$  is Boolean,  $f$  can be expressed by  $f(x) = x f(1) + x' f(0) = x + a x'$  from the minterm canonical form. However, substituting  $x = a$  in the previous expression yields:  $f(a) = a + a a' = a \neq 1$

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

# Why Study General Boolean Algebra?

---

- General algebras can't be avoided

$$f = x y + x z' + x' z$$

- Two-element view:  $x, y, z \in \{0,1\}$  and  $f \in \{0,1\}$
- General algebra view:  $f$  as a member of the Boolean algebra of 3-variable Boolean functions

# Why Study General Boolean Algebra?

## □ General algebras are useful

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

J	K	Q	Q+
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
..	..	..	..

J	K	Q+
0	0	Q
0	1	0
1	0	1
1	1	Q'