Boolean Algebra

Reference:
Introduction to Digital Systems
Miloš Ercegovac, Tomás Lang, Jaime H. Moreno
Pages: 480-487
A **Boolean Algebra** is a 3-tuple \( \{ B, +, \cdot \} \), where

- \( B \) is a set of at least 2 elements
- \(( + )\) and \(( \cdot )\) are binary operations (i.e. functions \( B \times B \to B \))

satisfying the following axioms:

**A1. Commutative laws:** For every \( a, b \in B \)

I. \( a + b = b + a \)

II. \( a \cdot b = b \cdot a \)

**A2. Distributive laws:** For every \( a, b, c \in B \)

I. \( a + (b \cdot c) = (a+ b) \cdot (a + c) \)

II. \( a \cdot (b + c) = (a \cdot b) + (a \cdot c) \)
**A3.** Existence of identity elements: The set $B$ has two distinct identity elements, denoted as 0 and 1, such that for every element $a \in B$

I. $a + 0 = 0 + a = a$

II. $a \cdot 1 = 1 \cdot a = a$

**A4.** Existence of a complement: For every element $a \in B$ there exists an element $a'$ such that

I. $a + a' = 1$

II. $a \cdot a' = 0$

**Precedence ordering:**

$\cdot$ before $+$

For example:

$$a + (b \cdot c) = a + bc$$
Switching Algebra

\[ B = \{ 0 , 1 \} \]

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

**Theorem 1:** The switching algebra is a Boolean algebra.
Proof:

By satisfying the axioms of Boolean algebra:

• $B$ is a set of at least two elements

$$B = \{0, 1\}, \quad 0 \neq 1 \text{ and } |B| \geq 2.$$  

• Closure of (+) and (·) over $B$ (functions $B \times B \to B$).

<table>
<thead>
<tr>
<th>AND</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OR</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

closure
A1. Commutativity of (+) and (·).

<table>
<thead>
<tr>
<th>AND</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OR</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Symmetric about the main diagonal

A2. Distributivity of (+) and (·).

<table>
<thead>
<tr>
<th>abc</th>
<th>a + bc</th>
<th>(a + b)(a + c)</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>010</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>011</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>100</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>101</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>110</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>111</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>abc</th>
<th>a(b + c)</th>
<th>ab + ac</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>010</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>011</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>100</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>101</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>110</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>111</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
* Alternative proof of the distributive laws:

**Claim:** (follow directly from operators table)

- \( \text{AND}(0, x) = 0 \) \hspace{1cm} \( \text{AND}(1, x) = x \)
- \( \text{OR}(1, x) = 1 \) \hspace{1cm} \( \text{OR}(0, x) = x \)

Consider the distributive law of (·):

\[
\text{AND}(a, \text{OR}(b, c)) = \text{OR}(\text{AND}(a, b), \text{AND}(a, c))
\]

\(a = 0:\)

\[
\text{AND}(0, \text{OR}(b, c)) = \text{OR}(\text{AND}(0, b), \text{AND}(0, c))
\]

\(\underbrace{0}_{0} \hspace{1cm} \underbrace{0}_{0} \underbrace{0}_{0}\)

\(a = 1:\)

\[
\text{AND}(1, \text{OR}(b, c)) = \text{OR}(\text{AND}(1, b), \text{AND}(1, c))
\]

\(\underbrace{\text{OR}(b, c)}_{b} \hspace{1cm} \underbrace{c}_{c} \underbrace{\text{OR}(b, c)}_{\text{OR}(b, c)}\)
Consider the distributive law of (+):

\[ \text{OR}( a , \text{AND}( b , c )) = \text{AND}( \text{OR}( a , b ) , \text{OR}( a , c )) \]

\[ a = 0 : \quad \text{OR}( 0 , \text{AND}( b , c )) = \text{AND}( \text{OR}( 0 , b ) , \text{OR}( 0 , c )) \]

\[ a = 0 : \quad \text{AND}( b , c ) \quad b \quad c \quad \text{AND}( b , c ) \]

\[ a = 1 : \quad \text{OR}( 1 , \text{AND}( b , c )) = \text{AND}( \text{OR}( 1 , b ) , \text{OR}( 1 , c )) \]

\[ a = 1 : \quad 1 \quad \text{AND}( b , c ) \quad 1 \quad 1 \quad \text{AND}( b , c ) \quad 1 \]

Why have we done that?!

For complex expressions truth tables are not an option.

\[ 0 + 1 = 1 + 0 = 1 \quad \text{(0 – additive identity)} \]

\[ 0 \cdot 1 = 1 \cdot 0 = 0 \quad \text{(1 – multiplicative identity)} \]

A4. Existence of the complement.

<table>
<thead>
<tr>
<th>( a )</th>
<th>( a' )</th>
<th>( a + a' )</th>
<th>( a \cdot a' )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

All axioms are satisfied \( \Rightarrow \) Switching algebra is Boolean algebra.
Theorems in Boolean Algebra

Theorem 2:

Every element in $B$ has a **unique** complement.

Proof:

Let $a \in B$. Assume that $a_1'$ and $a_2'$ are both complements of $a$, (i.e. $a_i' + a = 1$ & $a_i' \cdot a = 0$), we show that $a_1' = a_2'$.

\[
\begin{align*}
    a_1' &= a_1' \cdot 1 \\
    &= a_1' \cdot (a + a_2') \\
    &= a_1' \cdot a + a_1' \cdot a_2' \\
    &= a \cdot a_1' + a_1' \cdot a_2' \\
    &= 0 + a_1' \cdot a_2' \\
    &= a_1' \cdot a_2'
\end{align*}
\]
We swap $a_1'$ and $a_2'$ to obtain,

\[
a'_2 = a'_2 \cdot a'_1 \\
= a'_1 \cdot a'_2
\]

\[a'_1 = a'_2\]

\[\text{Complement uniqueness}
\]

\[\text{can be considered as a unary operation}
\]

\[B \rightarrow B \text{ called complementation}\]
**Boolean expression** - Recursive definition:

**base:** 0, 1, \( a \in B \) – expressions.

**recursion step:** Let \( E_1 \) and \( E_2 \) be Boolean expressions.

Then,

\[
E_1', \\
( E_1 + E_2 ), \\
( E_1 \cdot E_2 )
\]

**Example:**

\[
(((a' + 0) \cdot c) + (b + a)'),
\]

\[
\begin{array}{c}
((a' + 0) \cdot c) \\
(a' + 0) \\
a'
\end{array}
\quad
\begin{array}{c}
(b + a)' \\
c \\
0
\end{array}
\]

\[
\begin{array}{c}
(b + a) \\
b \\
\end{array}
\quad
\begin{array}{c}
a \\
a
\end{array}
\]
Dual transformation - Recursive definition:

Dual: expressions → expressions

- **base:**
  - 0 → 1
  - 1 → 0
  - \( a \rightarrow a', a \in B \)

- **recursion step:** Let \( E_1 \) and \( E_2 \) be Boolean expressions.
  Then,
  \[
  E_1' \rightarrow [\text{dual}(E_1)]'
  \]
  \[
  (E_1 + E_2) \rightarrow [\text{dual}(E_1) \cdot \text{dual}(E_2)]
  \]
  \[
  (E_1 \cdot E_2) \rightarrow [\text{dual}(E_1) + \text{dual}(E_2)]
  \]

Example:

\[
( (a + b) + (a' \cdot b') ) \cdot 1
\]

\[
( (a \cdot b) \cdot (a' + b') ) + 0
\]
The axioms of Boolean algebra are in dual pairs.

**A1. Commutative laws:** For every \( a, b \in B \)

I. \( a + b = b + a \)

II. \( a \cdot b = b \cdot a \)

**A2. Distributive laws:** For every \( a, b, c \in B \)

I. \( a + (b \cdot c) = (a + b) \cdot (a + c) \)

II. \( a \cdot (b + c) = (a \cdot b) + (a \cdot c) \)

**A3. Existence of identity elements:** The set \( B \) has two distinct identity elements, denoted as 0 and 1, such that for every element \( a \in B \)

I. \( a + 0 = 0 + a = a \)

II. \( a \cdot 1 = 1 \cdot a = a \)

**A4. Existence of a complement:** For every element \( a \in B \) there exists an element \( a' \) such that

I. \( a + a' = 1 \)

II. \( a \cdot a' = 0 \)
Theorem 3:

For every $a \in B$:

1. $a + 1 = 1$
2. $a \cdot 0 = 0$

Proof:

(1)

$\begin{align*}
\text{Identity} & \quad a + 1 = 1 \cdot (a + 1) \\
\text{a’ is the complement of a} & \quad = (a + a’) \cdot (a + 1) \\
\text{distributivity} & \quad = a + (a’ \cdot 1) \\
\text{Identity} & \quad = a + a’ \\
\text{a’ is the complement of a} & \quad = 1
\end{align*}$
(2) we can do the same way:

\[ a \cdot 0 = 0 + (a \cdot 0) \]

\[ = (a \cdot a') + (a \cdot 0) \]

\[ = a \cdot (a' + 0) \]

\[ = a \cdot a' \]

\[ = 0 \]

Note that:

- \( a \cdot 0 , 0 \) are the dual of \( a + 1 , 1 \) respectively.
- The proof of (2) follows the same steps exactly as the proof of (1) with the same arguments, but applying the dual axiom in each step.
Theorem 4: Principle of Duality

Every algebraic identity deducible from the axioms of a Boolean algebra attains:

\[ E_1 = E_2 \Rightarrow \text{dual}(E_1) = \text{dual}(E_2) \]

For example:

\[ (a + b) + a' \cdot b' = 1 \]

\[ (a \cdot b) \cdot (a' + b') = 0 \]

Correctness by the fact that each axiom has a dual axiom as shown

Every theorem has its dual for “free”
Theorem 5:
The complement of the element 1 is 0, and vice versa:

1. \(0' = 1\)
2. \(1' = 0\)

Proof:

By Theorem 3,

\[
0 + 1 = 1 \quad \text{and} \quad 0 \cdot 1 = 0
\]

By the uniqueness of the complement, the Theorem follows.
Theorem 6: Idempotent Law

For every $a \in B$

1. $a + a = a$
2. $a \cdot a = a$

Proof:

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

- Identity
- $a'$ is the complement of $a$
- Distributivity

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

- $a'$ is the complement of $a$

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

- Identity

$= a + 0$

$= a$

(2) duality.
**Theorem 7: Involution Law**

For every \( a \in B \)

\[
( a' )' = a
\]

Proof:

\( ( a' )' \) and \( a \) are both complements of \( a' \).

Uniqueness of the complement \( \rightarrow ( a' )' = a \).

**Theorem 8: Absorption Law**

For every pair of elements \( a, b \in B \),

1. \( a + a \cdot b = a \)
2. \( a \cdot ( a + b ) = a \)

Proof: home assignment.
**Theorem 9:**

For every pair of elements \( a, b \in B \),

1. \( a + a' \cdot b = a + b \)
2. \( a \cdot (a' + b) = a \cdot b \)

**Proof:**

(1) \[ a + a'b = (a + a')(a + b) \]

- Distributivity
- \( a' \) is the complement of \( a \)

\[ = 1(a + b) \]

- Identity

\[ = a + b \]

(2) Duality.
**Theorem 10:**

In a Boolean algebra, each of the binary operations (+) and (·) is associative. That is, for every $a, b, c \in B$,

1. $a + (b + c) = (a + b) + c$
2. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

**Proof:** home assignment (hint: prove that both sides in (1) equal $[(a + b) + c] \cdot [a + (b + c)]$.)

**Theorem 11:** DeMorgan’s Law

For every pair of elements $a, b \in B$,

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

**Proof:** home assignment.
Theorem 12: Generalized DeMorgan’s Law

Let \( \{a, b, \ldots, c, d\} \) be a set of elements in a Boolean algebra. Then, the following identities hold:

1. \((a + b + \ldots + c + d)' = a' b' \ldots c' d'\)
2. \((a \cdot b \cdot \ldots \cdot c \cdot d)' = a' + b' + \ldots + c' + d'\)
Proof: By induction.

Induction basis: follows from DeMorgan’s Law

\[(a + b)' = a' \cdot b'.\]

Induction hypothesis: DeMorgan’s law is true for \(n\) elements.

Induction step: show that it is true for \(n+1\) elements.

Let \(a, b, \ldots, c\) be the \(n\) elements, and \(d\) be the \((n+1)st\) element.

\[
(a + b + \ldots + c + d)' = [(a + b + \ldots + c) + d]' \\
\text{Associativity} \\
\text{DeMorgan’s Law} \\
\text{Induction assumption } (a + b + \ldots + c)' = a'b' \ldots c' \\
= (a + b + \ldots + c)' d' \\
= a'b' \ldots c'd'
\]
The symbols $a, b, c, \ldots$ appearing in theorems and axioms are **generic variables**.

Can be substituted by complemented variables or expressions (formulas). For example:

For example:

\[
(a + b)' = a' b'
\]

De Morgan’s Law

\[
\begin{align*}
(a' + b')' &= ab \\
(a + b)' &= (a + b)' c
\end{align*}
\]

etc.
Other Examples of Boolean Algebras

Algebra of Sets

Consider a set $S$.

$B = \text{all the subsets of } S$ (denoted by $P(S)$).

“plus” $\rightarrow$ set-union $\cup$

“times” $\rightarrow$ set-intersection $\cap$

$$M = (P(S), \cup, \cap)$$

Additive identity element – empty set $\emptyset$

Multiplicative identity element – the set $S$.

$P(S)$ has $2^{|S|}$ elements, where $|S|$ is the number of elements of $S$. 
Elements of $B$ are $T$ and $F$ (true and false).

“plus” $\rightarrow$ Logical OR $\lor$

“times” $\rightarrow$ Logical AND $\land$

$$M = (\{T, F\}, \lor, \land)$$

Additive identity element – $F$

Multiplicative identity element – $T$