מבנה המחשב + מבוא למחשבים ספרתיים

תרגול #1

Boolean Algebra

Reference:

Introduction to Digital Systems

Miloš Ercegovac, Tomás Lang, Jaime H. Moreno

Pages: 480-487

“plus” / ”OR”

“times” / ”AND”

A **Boolean Algebra** is a 3-tuple $\{B, +, \cdot\}$, where

- B is a set of at least 2 elements
- (+) and (·) 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 $a \in B$

additive identity element

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

multiplicative identity element

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. $a \cdot a' = 0$

the complement of *a*

Precedence ordering: $\cdot$ **before** +

For example:

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

Switching Algebra

$B = \{ 0 , 1 \}$

AND	0	1
0	0	0
1	0	1

OR	0	1
0	0	1
1	1	1

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

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

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

AND	0	1
0	0	0
1	0	1

OR	0	1
0	0	1
1	1	1

closure

A1. Cummutativity of (+) and (·).

AND	0	1
0	0	0
1	0	1

OR	0	1
0	0	1
1	1	1

Symmetric about the main diagonal

A2. Distributivity of (+) and (·).

abc	a + bc	(a + b)(a + c)
000	0	0
001	0	0
010	0	0
011	1	1
100	1	1
101	1	1
110	1	1
111	1	1

abc	a(b + c)	ab + ac
000	0	0
001	0	0
010	0	0
011	0	0
100	0	0
101	1	1
110	1	1
111	1	1

* Alternative proof of the distributive laws:

$$\left\{\begin{array}{ll} \underline{\text{Claim:}}\ \text{(follow directly from operators table)} & \\ \bullet\ \mathrm{AND}(\,0\,,\,\mathrm{x}\,) = 0 & \mathrm{AND}(\,1\,,\,\mathrm{x}\,) = \mathrm{x} \\ \bullet\ \mathrm{OR}(\,1\,,\,\mathrm{x}\,) = 1 & \mathrm{OR}(\,0\,,\,\mathrm{x}\,) = \mathrm{x} \end{array}\right\}$$

Consider the distributive law of (·):

$$\mathrm{AND}(\,a\,,\,\mathrm{OR}(\,b\,,\,c\,)\,) = \mathrm{OR}(\,\mathrm{AND}(\,a\,,\,b\,)\,,\,\mathrm{AND}(\,a\,,\,c\,)\,)$$

$$\underline{\mathrm{a} = 0}:\ \underbrace{\mathrm{AND}(\,0\,,\,\mathrm{OR}(\,b\,,\,c\,)\,)}_{0} = \underbrace{\mathrm{OR}(\,\underbrace{\mathrm{AND}(\,0\,,\,b\,)}_{0}\,,\,\underbrace{\mathrm{AND}(\,0\,,\,c\,)}_{0}\,)}_{0}$$

$$\underline{\mathrm{a} = 1}:\ \underbrace{\mathrm{AND}(\,1\,,\,\mathrm{OR}(\,b\,,\,c\,)\,)}_{\mathrm{OR}(\,b\,,\,c\,)} = \underbrace{\mathrm{OR}(\,\underbrace{\mathrm{AND}(\,1\,,\,b\,)}_{b}\,,\,\underbrace{\mathrm{AND}(\,1\,,\,c\,)}_{c}\,)}_{\mathrm{OR}(\,b\,,\,c\,)}$$

Consider the distributive law of (+):

$$\mathrm{OR}(\, a\,,\ \mathrm{AND}(\, b\,,\, c\,)\,) = \mathrm{AND}(\, \mathrm{OR}(\, a\,,\, b\,)\,,\ \mathrm{OR}(\, a\,,\, c\,)\,)$$

$\underline{a = 0}$:

$$\underbrace{\mathrm{OR}(\, 0\,,\ \mathrm{AND}(\, b\,,\, c\,)\,)}_{\mathrm{AND}(\, b\,,\, c\,)} = \mathrm{AND}(\, \underbrace{\underbrace{\mathrm{OR}(\, 0\,,\, b\,)}_{b}\,,\ \underbrace{\mathrm{OR}(\, 0\,,\, c\,)}_{c}}_{\mathrm{AND}(\, b\,,\, c\,)}\,)$$

$\underline{a = 1}$:

$$\underbrace{\mathrm{OR}(\, 1\,,\ \mathrm{AND}(\, b\,,\, c\,)\,)}_{1} = \mathrm{AND}(\, \underbrace{\underbrace{\mathrm{OR}(\, 1\,,\, b\,)}_{1}\,,\ \underbrace{\mathrm{OR}(\, 1\,,\, c\,)}_{1}}_{1}\,)$$

Why have we done that?!

For complex expressions truth tables are not an option.

A3. Existence of additive and multiplicative identity element.

$0 + 1 = 1 + 0 = 1$ $\Rightarrow$ 0 – additive identity

$0 \cdot 1 = 1 \cdot 0 = 0$ $\Rightarrow$ 1 – multiplicative identity

A4. Existence of the complement.

a	a'	$a + a'$	$a \cdot a'$
1	0	1	0
0	1	1	0

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’ · a = 0), we show that a_1’ = a_2’ .

Identity
$$a_1' = a_1' \cdot 1$$

a_2’ is the complement of a
$$= a_1' \cdot (a + a_2')$$

distributivity
$$= a_1' \cdot a + a_1' \cdot a_2'$$

commutativity
$$= a \cdot a_1' + a_1' \cdot a_2'$$

a_1’ is the complement of a
$$= 0 + a_1' \cdot a_2'$$

Identity
$$= a_1' \cdot a_2'$$

We swap a_1' and a_2' to obtain,

$$\begin{aligned} a_2' &= a_2' \cdot a_1' \\ &= a_1' \cdot a_2' \end{aligned}$$

$$\Rightarrow \quad a_1' = a_2'$$

$\blacksquare$

★ Complement uniqueness

' can be considered as a unary operation

$B \to B$ called **complementation**

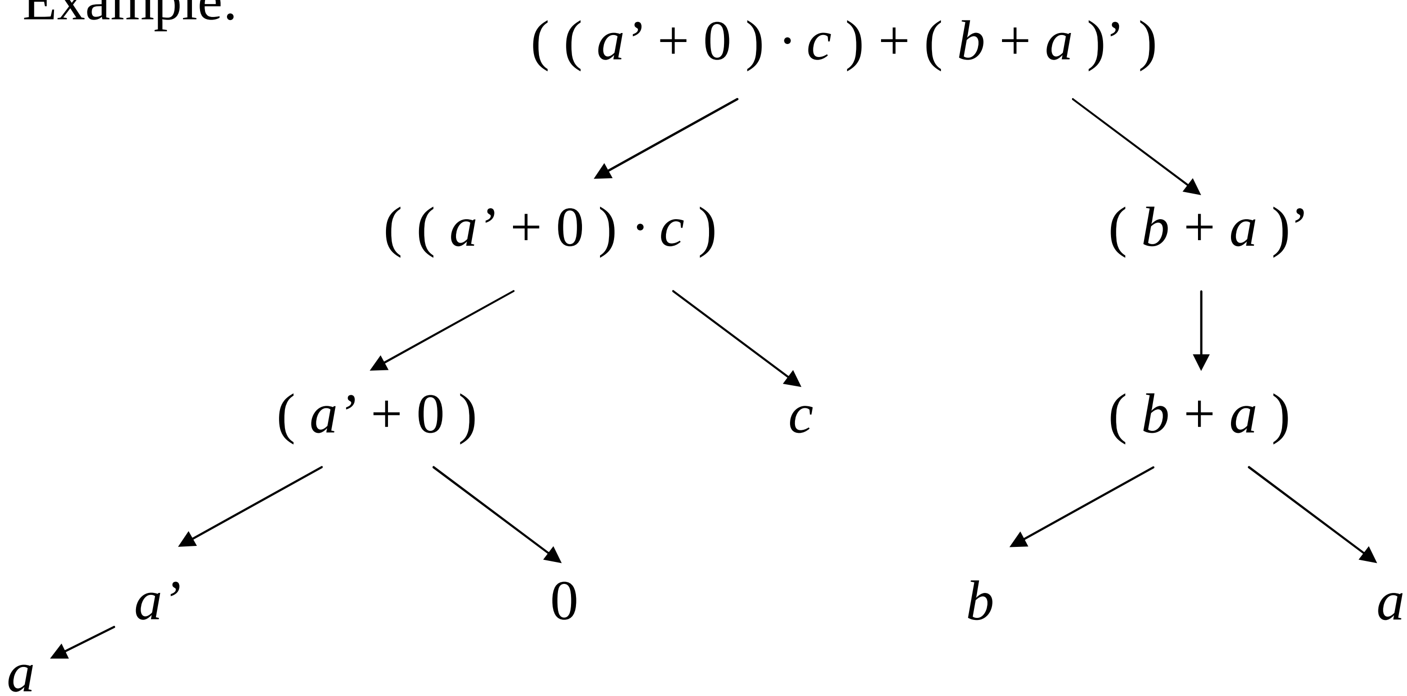
Boolean expression - Recursive definition:

base: 0 , 1 , $a \in B$ – expressions.

recursion step: Let E_1 and E_2 be Boolean expressions.
Then,

$$\left.\begin{array}{l} E_1' \\ (E_1 + E_2) \\ (E_1 \cdot E_2) \end{array}\right\} \text{expressions}$$

Example:



Dual transformation - Recursive definition:

Dual: expressions $\longrightarrow$ expressions

base: $0 \longrightarrow 1$

$1 \longrightarrow 0$

$a \longrightarrow a \quad , a \in B$

recursion step: Let E_1 and E_2 be Boolean expressions.
Then,

$$E_1' \longrightarrow [\text{dual}(E_1)]'$$
$$(E_1 + E_2) \longrightarrow [\text{dual}(E_1) \cdot \text{dual}(E_2)]$$
$$(E_1 \cdot E_2) \longrightarrow [\text{dual}(E_1) + \text{dual}(E_2)]$$

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)

Identity	$a + 1 = 1 \cdot (a + 1)$
a' is the complement of *a*	$= (a + a') \cdot (a + 1)$
distributivity	$= a + (a' \cdot 1)$
Identity	$= a + a'$
a' is the complement of *a*	$= 1$

(2) we can do the same way:

Identity	$a \cdot 0 = 0 + (a \cdot 0)$
a' is the complement of *a*	$= (a \cdot a') + (a \cdot 0)$
distributivity	$= a \cdot (a' + 0)$
Identity	$= a \cdot a'$
a' is the complement of *a*	$= 0$

$\blacksquare$

Note that:

- $\boldsymbol{a \cdot 0}$ **,** $\mathbf{0}$ are the dual of $\boldsymbol{a + 1}$ **,** $\mathbf{1}$ 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:

$$E_1 = E_2 \Rightarrow dual(E_1) = dual(E_2)$$

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

For example:

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

$$\Downarrow$$

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

★ 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,

$$0 + 1 = 1 \qquad \text{and}$$

$$0 \cdot 1 = 0$$

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)

Identity	$a + a = (a + a) \cdot 1$
a' is the complement of a	$= (a + a) \cdot (a + a')$
distributivity	$= (a + (a \cdot a'))$
a' is the complement of a	$= a + 0$
Identity	$= a$

(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)

distributivity

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

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 , … , c , d} be a set of elements in a Boolean algebra. Then, the following identities hold:

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

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* , . . . , *c* be the *n* elements, and *d* be the *(n+1)*st element.

$$(a+b+\ldots+c+d)' = [(a+b+\ldots+c)+d]'$$

$$= (a+b+\ldots+c)' d'$$

$$= a'b'\ldots c'd'$$

Associativity

DeMorgan's Law

Induction assumption $(a+b+\ldots+c)' = a'b'\ldots c'$

■

The symbols *a*, *b*, *c*, . . . appearing in theorems and axioms are **generic variables**

Can be substituted by complemented variables or expressions (formulas)

For example:

$$(a+b)' = a'b' \xrightarrow{\substack{a \leftarrow a' \\ b \leftarrow b'}} (a'+b')' = ab$$

DeMorgan's Law

$$(a+b)' = a'b' \xrightarrow[\substack{a \leftarrow (a+b) \\ b \leftarrow c'}]{} [(a+b)+c']' = (a+b)'c$$

etc.

Other Examples of Boolean Algebras

Algebra of Sets

Consider a set S.

B = all the subsets of *S* (denoted by *P(S)*).

“plus” → set-union U

“times” → set-intersection ∩

$$M = \left(P(S),\quad \cup,\quad \cap\right)$$

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*

Algebra of Logic (Propositional Calculus)

Elements of B are T and F (true and false).

“plus” → Logical OR $\vee$

“times” → Logical AND $\wedge$

$$M = \left(\{T, F\}, \quad \vee, \quad \wedge\right)$$

Additive identity element – F

Multiplicative identity element – T