

## CHAPTER 4

# BOOLEAN ALGEBRAS

In the middle of the nineteenth century the English mathematician George Boole introduced the algebras which are now named after him. These algebras give a mathematical basis to logical reasoning (see Chapter 5); they are also the basis of electronic computer design via the physical implementation of Boolean operations.

In this chapter we introduce Boolean algebras and their operations, and we define Boolean functions which specify the operation performed by a Boolean circuit, or the truth value of a logical formula. Finally, we show how to represent a Boolean function by a polynomial expression built up using the basic operations of Boolean algebras.

We recommend the following textbooks:

Garrett Birkhoff, Thomas Bartee, *Modern Applied Algebra*, McGraw Hill, New York (1970).

Kenneth Ross, Charles Wright, *Discrete Mathematics*, Prentice Hall, London (1988).

### 4.1 Boolean algebras

A Boolean algebra is a distributive and complemented lattice having at least two elements.

**EXAMPLE 4.1** If  $E$  is a non-empty set,  $\mathcal{P}(E)$ , ordered by inclusion, is a Boolean algebra. The condition  $E \neq \emptyset$  ensures that  $\mathcal{P}(E)$  has at least two elements.

#### 4.1.1 Algebraic definition

A Boolean algebra can also be viewed as an algebraic structure, and this yields the following definition.

**Definition 4.2** A Boolean algebra  $B$  consists of

- a set  $E$ ,
- two distinct elements of  $E$ , denoted by  $\perp$  and  $\top$ ,
- two binary operations on  $E$ , denoted by  $\sqcap$  and  $\sqcup$ ,
- a unary operation on  $E$ , denoted by  $\bar{\phantom{x}}$ ,

satisfying the following conditions:

- the operations  $\sqcap$  and  $\sqcup$  are idempotent, associative, commutative and distributive,
- $x \sqcap (x \sqcup y) = x = (y \sqcap x) \sqcup x$ ,
- $x \sqcap \perp = \perp$ ,  $x \sqcup \perp = x$ ,  $x \sqcap \top = x$ ,  $x \sqcup \top = \top$ ,
- $x \sqcap \bar{x} = \perp$ ,  $x \sqcup \bar{x} = \top$ .

Of course this list of properties is redundant: some of them are consequences of the others. This will be shown in Exercise 4.1.

If  $B = (E, \sqcap, \sqcup, \bar{\phantom{x}}, \perp, \top)$  is a Boolean algebra, then  $\tilde{B} = (E, \sqcup, \sqcap, \bar{\phantom{x}}, \top, \perp)$  is also a Boolean algebra, called the *dual* Boolean algebra of  $B$ . This algebra is obtained by interchanging  $\sqcup$  and  $\sqcap$ , as well as  $\perp$  and  $\top$ . The result of this operation is a Boolean algebra because the interchanged elements play symmetric roles in the definition. Considering  $B$  as an ordered set,  $\tilde{B}$  is the set ordered by the inverse ordering.

**EXERCISE 4.1** The purpose of this exercise is to prove that the following conditions ensure that  $B = (E, \sqcap, \sqcup, \bar{\phantom{x}}, \perp, \top)$  is a Boolean algebra:

- $N_0$  :  $x \sqcup x = x$ ,
- $N_1$  :  $x \sqcap (y \sqcup z) = (x \sqcap y) \sqcup (x \sqcap z)$ ,
- $N'_1$  :  $(x \sqcup y) \sqcap z = (x \sqcap z) \sqcup (y \sqcap z)$ ,
- $N_{2a}$  :  $x \sqcap \top = x$ ,
- $N_3$  :  $x \sqcup \perp = x = \perp \sqcup x$ ,
- $N_4$  :  $x \sqcap \bar{x} = \perp$  and  $x \sqcup \bar{x} = \top$ .

Note that  $\sqcap$  and  $\sqcup$  should not be assumed to be associative or commutative, and that  $\sqcap$  should not be assumed to be idempotent; associativity, commutativity and idempotence will be shown to be consequences of the hypotheses.

1. First show the following equalities:

- $N'_0$  :  $x \sqcap x = x$ ,
- $N_{2b}$  :  $\top \sqcap x = x$ ,
- $N'_2$  :  $x \sqcup \top = \top = \top \sqcup x$ .

2. Show that  $y \sqcap x = \perp$  and  $y \sqcup x = \top$  imply that  $y = \bar{x}$ . Infer that  $N_6$  :  $\bar{\bar{x}} = x$ .
3. Show that  $N'_3$  :  $x \sqcap \perp = \perp = \perp \sqcap x$ .
4. Next show that  $N_5$  :  $x = x \sqcup (x \sqcap y) = x \sqcup (y \sqcap x) = (x \sqcap y) \sqcup x = (y \sqcap x) \sqcup x$ . Infer the associativity and commutativity of  $\sqcup$ . Show that  $N''_1$  :  $x \sqcup (y \sqcap z) = (x \sqcup y) \sqcap (x \sqcup z)$ .
5. Finally, show that  $N_7$  :  $\overline{x \sqcap y} = \bar{x} \sqcup \bar{y}$ , and  $N'_7$  :  $\overline{x \sqcup y} = \bar{x} \sqcap \bar{y}$ . Infer the associativity and commutativity of  $\sqcap$ .  $\diamond$

In the rest of the present chapter we will sometimes use more algebraic and more familiar notations, denoting lattice operations by sum and product. (We have avoided their use until now, because such well-known symbols might have misled the reader into believing that the operations  $\sqcup$  and  $\sqcap$  are exactly identical to sum and product.)

We will therefore denote  $\sqcup$  by the addition symbol  $+$ , and  $\sqcap$  will be denoted as a product, by simply concatenating its arguments. We will thus write  $(x + y)z$  instead of  $(x \sqcup y) \sqcap z$ . As is usual, we will also assume that products take precedence over sums; this will allow us to denote  $(x \sqcap y) \sqcup z$  by  $xy + z$ , instead of  $(xy) + z$ . Finally,  $\perp$  will be denoted by  $0$  and  $\top$  will be denoted by  $1$ .

Sum and product operations being associative and commutative, and product being distributive over sum, this notation is quite natural. In a Boolean algebra, the usual equalities also hold:  $x + 0 = x$ ,  $x0 = 0$ , and  $x1 = x$ . But the following equalities, which are particular to Boolean algebras, also hold:

- $x + x = x = xx$ ,
- $x + 1 = 1$ ,
- $(x + y)(x + z) = x + yz$ ,
- $x + xy = x$ .

EXERCISE 4.2

1. Show that  $x = ax + b\bar{x} \iff b \leq x \leq a$  (Poretsky's formula).
2. Show that  $ax + b\bar{x} = 0 \iff b \leq x \leq \bar{a}$  (Schröder's formula).
3. Show that
  - (i) if  $b \leq a$ , then  $\exists u : x = au + b\bar{u} \implies b \leq x \leq a$ ,
  - (ii) if  $b \leq x \leq a$ , then  $\forall u : \bar{b}x \leq u \leq \bar{a} + x, \quad x = au + b\bar{u}$ . (Hint: first show that with these hypotheses,  $u$  can be written  $\bar{b}x + by + \bar{a}z$ .)  $\diamond$

4.1.2 Homomorphisms

Let  $B = (E, \sqcap, \sqcup, \bar{\phantom{x}}, \perp, \top)$  and  $B' = (E', \sqcap', \sqcup', \hat{\phantom{x}}, \perp', \top')$  be two Boolean algebras. A *homomorphism* from  $B$  to  $B'$  is a mapping  $h$  from  $E$  to  $E'$  satisfying

- $h(x \sqcup y) = h(x) \sqcup' h(y)$ ,
- $h(x \sqcap y) = h(x) \sqcap' h(y)$ ,
- $h(\bar{x}) = \widehat{h(x)}$ ,
- $h(\perp) = \perp'$ ,
- $h(\top) = \top'$ .

An *antihomomorphism* from  $B$  to  $B'$  is a homomorphism from  $B$  to the dual  $\widetilde{B'}$  of  $B'$ .

EXERCISE 4.3 Show that a homomorphism is a monotone mapping with respect to the order relation defining the Boolean algebra.

Show that not all monotone mappings are homomorphisms.  $\diamond$

EXERCISE 4.4 Let  $B = (E, \cdot, +, \bar{\phantom{x}}, 0, 1)$  be a Boolean algebra and  $e$  an element of  $E$  different from 0. Let  $E' = \{x \in E / xe = x\}$ . Show that  $B' = (E', \cdot, +, \bar{\phantom{x}}, 0, e)$ , where  $\hat{x} = \bar{x}e$  is a Boolean algebra and that the mapping  $h$  from  $E$  to  $E'$  defined by  $h(x) = xe$  is a homomorphism.  $\diamond$

**Proposition 4.3** Let  $B = (E, \cdot, +, \bar{\phantom{x}}, 0, 1)$  be a Boolean algebra. The mapping  $h$  from  $E$  to  $E$  defined by  $h(x) = \bar{x}$  is an antihomomorphism.

*Proof.*  $\bar{\bar{1}} = 0$  and  $\bar{\bar{0}} = 1$  hold. By the De Morgan laws,  $\overline{x + y} = \bar{x} \bar{y}$  and  $\overline{xy} = \bar{x} + \bar{y}$ . Finally,  $h(\bar{x}) = \overline{\bar{x}} = x$ .  $\square$

EXERCISE 4.5 Let  $F$  be a finite set. Let  $\mathcal{F} = \mathcal{P}(\mathcal{P}(F))$ . This is a Boolean algebra if  $\mathcal{F}$  is ordered by inclusion, namely,

$$\mathcal{X} = \{X_1, \dots, X_n\} \subseteq \mathcal{Y} = \{Y_1, \dots, Y_m\}$$

if and only if  $\forall X \in \mathcal{X}, \exists Y \in \mathcal{Y}: X = Y$  (see Exercise 1.29).

We consider the mapping  $i$  from  $f$  to  $\mathcal{F}$  defined by  $i(x) = \{X \subseteq F / x \in X\}$ .

Let  $B = (E, \cdot, +, \bar{\phantom{x}}, 0, 1)$  be a Boolean algebra, and  $g$  a mapping from  $F$  to  $E$ . Show that there exists a unique homomorphism  $h$  from  $\mathcal{F}$  to  $B$  such that  $\forall x \in F, h(i(x)) = g(x)$ .  $\diamond$

### 4.1.3 The minimal Boolean algebra

A very special Boolean algebra, denoted by  $\mathbb{B}$ , is the Boolean algebra containing only the two elements 0 and 1. (It is usually referred to as *The* Boolean algebra.) The sum, product and complement operations on this two element algebra are described in the following table:

$x$	$y$	$x + y$	$xy$	$\bar{x}$
0	0	0	0	1
0	1	1	0	1
1	0	1	0	0
1	1	1	1	0

The two values of this Boolean algebra can be given various special interpretations:

- 0 and 1, not forgetting that  $1 + 1 = 1$ !
- if  $E$  is a set, 0 is its empty subset and 1 its full subset. Unions, intersections and complements will be performed only on these two subsets.
- ‘true’ and ‘false’. Sum is then logical disjunction (read ‘or’) and product is logical conjunction (read ‘and’). This will be studied in more detail in Chapter 5.

## 4.2 Boolean rings

### 4.2.1 Exclusive ‘or’

Let  $(E, \cdot, +, \bar{\phantom{x}}, 0, 1)$  be a Boolean algebra. We define a new binary operation denoted by  $\oplus$  and called ‘exclusive or’ by

$$x \oplus y = x\bar{y} + \bar{x}y.$$

Note that  $x\bar{y} + \bar{x}y$  is also equal to  $(x + y)\bar{xy}$ .

EXAMPLE 4.4 Considering the Boolean algebra consisting of the subsets of a set, this operation coincides exactly with the symmetrical difference (see Section 1.1.2).

The following properties arise from the definition of this operation.

#### Proposition 4.5

- $\oplus$  is associative and commutative,
- $x \oplus x = 0$ ,
- $x \oplus 0 = x$ ,
- $x \oplus 1 = \bar{x}$ ,
- $(x \oplus y)z = xz \oplus yz$ ,
- $x + y = x \oplus y \oplus xy$ .

*Proof.* Let us merely show the associativity of  $\oplus$  and the last two points (the rest is straightforward).

1. 
$$\begin{aligned} (x \oplus y) \oplus z &= (x\bar{y} + \bar{x}y) \oplus z = (x\bar{y} + \bar{x}y)\bar{z} + \overline{(x\bar{y} + \bar{x}y)}z \\ &= (x\bar{y} + \bar{x}y)\bar{z} + (\bar{x} + y)(x + \bar{y})z = x\bar{y}\bar{z} + \bar{x}y\bar{z} + \bar{x}\bar{y}z + xyz, \\ x \oplus (y \oplus z) &= x \oplus (y\bar{z} + \bar{y}z) = x(\bar{y} + z)(\bar{y} + \bar{z}) + \bar{x}(y\bar{z} + \bar{y}z) \\ &= x\bar{y}\bar{z} + xyz + \bar{x}y\bar{z} + \bar{x}\bar{y}z. \end{aligned}$$
2. 
$$\begin{aligned} xz \oplus yz &= xz\bar{y}\bar{z} + \bar{x}\bar{z}yz = xz(\bar{y} + \bar{z}) + (\bar{x} + \bar{z})yz \\ &= xz\bar{y} + \bar{x}yz = (x\bar{y} + \bar{x}y)z = (x \oplus y)z. \end{aligned}$$
3. 
$$\begin{aligned} (x \oplus y) \oplus xy &= (x\bar{y} + \bar{x}y) \oplus xy = (x\bar{y} + \bar{x}y)(\bar{x} + \bar{y}) + (\bar{x} + y)(x + \bar{y})xy \\ &= \bar{x}y + x\bar{y} + xy = (x + \bar{x})y + x(y + \bar{y}) = x + y. \end{aligned} \quad \square$$

### 4.2.2 Boolean rings

It can be seen that the ‘exclusive or’ has the properties of an addition operation in an additive group where each element is its own inverse, since  $x \oplus x = 0$ . By also taking into account the product, we obtain a ring structure. Thus the following definition holds: a *Boolean ring* is a structure  $A = (E, \pm, \cdot, 0, 1)$  satisfying the following conditions:

- sum and product are associative and commutative,
- product is distributive over sum,
- 0 is the unit (or identity element) for sum and 1 is the identity element for product,
- $x0 = 0$ ,

and, moreover,

- $xx = x$ ,
- $x \pm x = 0$ .

The notation  $\pm$  for addition is designed to remind us that this addition could also be thought of as a subtraction!

**EXAMPLE 4.6** The ring  $\mathbb{Z}/2\mathbb{Z}$  of the integers modulo 2 is a Boolean ring.

Here again some of the hypotheses are redundant. For instance, we can substitute for the condition  $x \pm x = 0$  the weaker condition  $x \pm y = x \implies y = 0$ , and not assume commutativity of the product. Then  $x \pm y = (x \pm y)(x \pm y) = x \pm y \pm xy \pm yx$ , whence  $\forall x, y, xy \pm yx = 0$ . Letting  $x = y$ , we have  $x \pm x = 0$ , and adding  $xy$  to  $xy \pm yx = 0$  we obtain  $xy = yx$ .

**Proposition 4.7** *If  $B = (E, \cdot, +, \bar{\cdot}, 0, 1)$  is a Boolean algebra then  $A = (E, \oplus, \cdot, 0, 1)$  is a Boolean ring.*

Proposition 4.5 shows that sum and complement can be retrieved from  $\oplus$ . The converse of this result also holds: let  $A = (E, \pm, \cdot, 0, 1)$  be a Boolean ring. Let us define the two operations

- $x + y = x \pm y \pm xy$ ,
- $\bar{x} = 1 \pm x$ .

**Proposition 4.8**  *$B = (E, \cdot, +, \bar{\cdot}, 0, 1)$  is a Boolean algebra.*

*Proof.* Let us first show that the operation  $+$  is associative, commutative, idempotent and has 0 as unit. It clearly is commutative since  $\pm$  and the product

are commutative. Moreover,  $x + x = x \pm x \pm xx = 0 \pm xx = xx = x$ , and  $0 + x = 0 \pm x \pm x0 = x$ . Finally,

$$\begin{aligned}(x + y) + z &= (x \pm y \pm xy) + z = x \pm y \pm xy \pm z \pm (x \pm y \pm xy)z \\ &= x \pm y \pm xy \pm xz \pm yz \pm xyz,\end{aligned}$$

$$\begin{aligned}x + (y + z) &= x + (y \pm z \pm yz) = x \pm y \pm z \pm yz \pm x(y \pm z \pm yz) \\ &= x \pm y \pm xy \pm xz \pm yz \pm xyz.\end{aligned}$$

We also have  $1 + x = 1 \pm x \pm 1x = 1 \pm 0 = 1$ .

Next, let us show distributivity:

$$(x + y)z = (x \pm y \pm xy)z = (xz \pm yz \pm xzyz) = xz + yz,$$

$$\begin{aligned}(x + y)(x + z) &= (x \pm y \pm xy)(x \pm z \pm xz) \\ &= xx \pm xz \pm xxz \pm xy \pm yz \pm xyz \pm xxy \pm xyz \pm xxyz \\ &= x \pm yz \pm xyz = x + yz,\end{aligned}$$

and absorption:

$$x + xy = x \pm xy \pm xxy = x \quad , \quad x(x + y) = x(x \pm y \pm xy) = x \pm xy \pm xy = x.$$

Let us now have a look at the properties of negation:

$$\bar{0} = 1 \pm 0 = 1, \quad \bar{1} = 1 \pm 1 = 0,$$

$$x\bar{x} = x(1 \pm x) = x \pm xx = x \pm x = 0,$$

$$x + \bar{x} = x \pm (1 \pm x) \pm x(1 \pm x) = x \pm (1 \pm x)(1 \pm x) = x \pm 1 \pm x = 1,$$

$$\bar{x} + \bar{y} = 1 \pm x \pm 1 \pm y \pm (1 \pm x)(1 \pm y) = x \pm y \pm (1 \pm x \pm y \pm xy) = 1 \pm xy = \overline{xy},$$

$$\bar{x}\bar{y} = (1 \pm x)(1 \pm y) = 1 \pm x \pm y \pm xy = 1 \pm (x + y) = \overline{x + y}. \quad \square$$

### 4.3 The Boolean functions

Let  $\mathbb{B}$  be the two-element Boolean algebra. A *Boolean function* (with  $n$  arguments) is a mapping from  $\mathbb{B}^n$  to  $\mathbb{B}$ .

A Boolean function  $f$  with  $n$  arguments is completely defined by the  $n$ -tuples of  $\mathbb{B}^n$  for which it takes the value 1. Since there are  $2^n$   $n$ -tuples in  $\mathbb{B}^n$  and since a set with  $k$  elements has  $2^k$  different subsets, there are  $2^{2^n}$  Boolean functions with  $n$  arguments.

- If  $n = 0$ , then  $2^n = 1$  and  $2^1 = 2$ ; there are two Boolean functions with 0 arguments and these are the two constants 0 and 1.
- If  $n = 1$ , then  $2^n = 2$  and  $2^2 = 4$ ; there are four Boolean functions with 1 argument: the two constant functions, the identity function and the complement function.
- If  $n = 2$ , then  $2^n = 4$  and  $2^4 = 16$ ; see Exercise 4.6.

#### 4.3.1 Polynomial form of the Boolean functions

A Boolean function is said to be *polynomial* if it can be written as a combination of its arguments via the sum, product and complement operations, or if it is the zero function.

**EXAMPLE 4.9** The function  $f(x, y) = \bar{x}y + \bar{y}$  is a polynomial function. Its values are given by the following table:

$x$	$y$	$\bar{x}$	$\bar{x}y$	$\bar{y}$	$\bar{x}y + \bar{y}$
0	0	1	0	1	1
0	1	1	1	0	1
1	0	0	0	1	1
1	1	0	0	0	0

We next show that every Boolean function is polynomial.

**Lemma 4.10** *Let  $f$  be a function with  $k + 1$  arguments. Then*

$$f(x_0, x_1, \dots, x_k) = \bar{x}_0 f(0, x_1, \dots, x_k) + x_0 f(1, x_1, \dots, x_k).$$

*Proof.* Let

$$g(x_0, x_1, \dots, x_k) = \bar{x}_0 f(0, x_1, \dots, x_k) + x_0 f(1, x_1, \dots, x_k)$$

and let  $(b_0, b_1, \dots, b_k)$  denote an arbitrary  $(k + 1)$ -tuple in  $\mathbb{B}^{k+1}$ . Then

$$g(b_0, b_1, \dots, b_k) = \bar{b}_0 f(0, b_1, \dots, b_k) + b_0 f(1, b_1, \dots, b_k).$$



If  $b_0 = 0$  then  $b_0 f(1, b_1, \dots, b_k) = 0 f(1, b_1, \dots, b_k) = 0$  and

$$\begin{aligned} g(b_0, b_1, \dots, b_k) &= \overline{b_0} f(0, b_1, \dots, b_k) = 1 f(0, b_1, \dots, b_k) \\ &= f(0, b_1, \dots, b_k) = f(b_0, b_1, \dots, b_k). \end{aligned}$$

Similarly, if  $b_0 = 1$  then

$$g(b_0, b_1, \dots, b_k) = b_0 f(1, b_1, \dots, b_k) = f(b_0, b_1, \dots, b_k). \quad \square$$

**Theorem 4.11** *Every Boolean function is polynomial.*

*Proof.* By induction on the number of arguments of  $f$ . A function  $f(x)$  with one argument can be written, by the lemma,  $\overline{x}f(0) + xf(1)$ .

If  $f(0)$  and  $f(1)$  are both equal to 0, the function  $f$  is the zero function. If they are both equal to 1 we obtain  $x + \overline{x}$ . If only one of the two is 0, we obtain  $f(x) = x$  or  $f(x) = \overline{x}$ .

Let us now assume that every Boolean function with  $k$  arguments is polynomial. A Boolean function with  $k + 1$  arguments can be written  $\overline{x_0}f(0, x_1, \dots, x_k) + x_0 f(1, x_1, \dots, x_k)$ . The Boolean functions  $g(x_1, \dots, x_k) = f(0, x_1, \dots, x_k)$  and  $g'(x_1, \dots, x_k) = f(1, x_1, \dots, x_k)$  are functions with  $k$  arguments; hence they are polynomial, and  $f$  is polynomial, too.  $\square$

EXAMPLE 4.12 Let us come back to the function  $f$  of the preceding example, as given by its table. We have

$$\begin{aligned} f(x, y) &= \overline{x}f(0, y) + xf(1, y), \\ f(0, y) &= \overline{y}f(0, 0) + yf(0, 1) = \overline{y} + y, \\ f(1, y) &= \overline{y}f(1, 0) + yf(1, 1) = \overline{y}, \end{aligned}$$

whence

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

The polynomial form of a Boolean function given by its table can be found very easily. Let  $f$  be a function with  $n$  arguments. Let  $D_f = \{(b_1, \dots, b_n) \in \mathbb{B}^n / f(b_1, \dots, b_n) = 1\}$ . If  $D_f$  is empty then  $f$  is the zero function. Otherwise, to each element  $\vec{b} = (b_1, \dots, b_n)$  of  $D_f$  we associate the Boolean function  $M_{\vec{b}}(x_1, \dots, x_n)$  whose polynomial form is

$$x'_1 \cdots x'_n \text{ with } x'_i = \begin{cases} x_i & \text{if } b_i = 1, \\ \overline{x_i} & \text{if } b_i = 0. \end{cases}$$

We then have  $f(x_1, \dots, x_n) = \sum_{\vec{b} \in D_f} M_{\vec{b}}(x_1, \dots, x_n)$ . Indeed, since a product of elements of  $\mathbb{B}$  can take the value 1 only when all its factors are 1,  $M_{\vec{b}}(\vec{c}) = 1$  if and only if  $\vec{b} = \vec{c}$  and, since a sum of elements of  $\mathbb{B}$  takes the value 1 as soon as one of its elements is 1,  $(\sum_{\vec{b} \in D_f} M_{\vec{b}})(\vec{c}) = 1$  if and only if  $\vec{c} \in D_f$ , and therefore if and only if  $f(\vec{c}) = 1$ .

### 4.3.2 Dual functions

Let  $f$  be a Boolean function with  $n$  arguments. Its *dual*, denoted by  $\tilde{f}$ , is the Boolean function with  $n$  arguments defined by

$$\tilde{f}(x_1, \dots, x_n) = \overline{f(\overline{x_1}, \dots, \overline{x_n})}.$$

EXAMPLE 4.13 Letting  $f(x, y) = x + y$ , its dual  $\tilde{f}$  is defined by

$$\tilde{f}(x, y) = \overline{\overline{x} + \overline{y}} = xy.$$

Let  $f(x) = \overline{x}$ , its dual is  $\tilde{\tilde{x}} = \overline{\overline{\overline{x}}} = \overline{\overline{x}}$ .

#### Proposition 4.14

1.  $\tilde{\tilde{f}} = g \implies \tilde{g} = f$ ,
2. If  $g(x_1, \dots, x_n) = f(f_1(x_1, \dots, x_n), \dots, f_k(x_1, \dots, x_n))$  then

$$\tilde{g}(x_1, \dots, x_n) = \tilde{f}(\tilde{f}_1(x_1, \dots, x_n), \dots, \tilde{f}_k(x_1, \dots, x_n)).$$

*Proof.*

1. If  $\tilde{\tilde{f}} = g$  then

$$g(x_1, \dots, x_n) = \tilde{\tilde{f}}(x_1, \dots, x_n) = \overline{\overline{f(\overline{x_1}, \dots, \overline{x_n})}}$$

and

$$\tilde{g}(x_1, \dots, x_n) = \overline{\overline{\overline{f(\overline{x_1}, \dots, \overline{x_n})}}} = \overline{\overline{f(\overline{x_1}, \dots, \overline{x_n})}} = f(x_1, \dots, x_n).$$

2. If  $g(x_1, \dots, x_k) = f(f_1(x_1, \dots, x_n), \dots, f_k(x_1, \dots, x_n))$  then

$$\tilde{g}(x_1, \dots, x_n) = \overline{\overline{f(f_1(\overline{x_1}, \dots, \overline{x_n}), \dots, f_k(\overline{x_1}, \dots, \overline{x_n}))}},$$

but  $f_i(\overline{x_1}, \dots, \overline{x_n}) = \tilde{\tilde{f}}_i(x_1, \dots, x_n)$ , whence

$$\begin{aligned} \tilde{g}(x_1, \dots, x_n) &= \overline{\overline{f(\tilde{\tilde{f}}_1(x_1, \dots, x_n), \dots, \tilde{\tilde{f}}_k(x_1, \dots, x_n))}}} \\ &= \tilde{f}(\tilde{f}_1(x_1, \dots, x_n), \dots, \tilde{f}_k(x_1, \dots, x_n)). \quad \square \end{aligned}$$

Given a function in polynomial form, to find its dual we simply have to substitute sums for products and products for sums.

EXAMPLE 4.15 The dual of  $xy + \overline{y}$  is  $(x + y)\overline{y}$  which can be simplified into  $x\overline{y}$ .

EXERCISE 4.6 Give the sixteen Boolean functions with two arguments in polynomial form. For each one of them, give the dual function.  $\diamond$