Lesson 3. Boolean lattices and algebras

(Computer Science Engineering Degree)
Departamento de Matemática Aplicada
ETS Ingeniería Informática
Universitat Politècnica de València

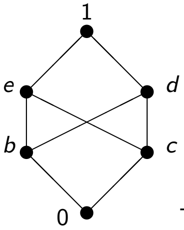
Contents

Boolean lattices (or Boolean lattices)

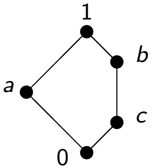
Definition (Boolean lattices (or Boolean lattices))

- An ordered set $(A, \leq)$ is a **lattice**, if every subset of two elements of A has supremum and infimimum.
- If A is lattice and $a, b \in A$, we will use the symbols $+$ and $\cdot$ to denote **the supremum and the infimum in** A of the subset $\{a, b\}$:
$$a + b = \sup_A(\{a, b\}), \qquad a \cdot b = \inf_A(\{a, b\}).$$
- A lattice $(A, \leq)$ is said to be **distributive** if $\forall a,\ b,\ c \in A$ we have
$$a + (b \cdot c) = (a + b) \cdot (a + c), \qquad a \cdot (b + c) = (a \cdot b) + (a \cdot c).$$
- A lattice is **bounded** if it has maximum (usually denoted by 1) and minimum (usually denoted by 0).
- A lattice is said to be **complemented** if it is bounded and for all $a \in A$, there exists a unique elemente $\overline{a} \in A$ (called **complement** of a) such that $a + \overline{a} = 1$ and $a \cdot \overline{a} = 0$.
- A lattice is said to be **Boolean lattice** (or a **Boolean lattice**) if it is distributive and complemented.

Examples

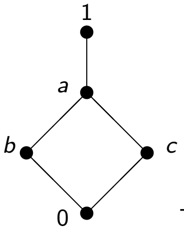
1. 

This is a not a lattice since $\{b, c\}$ does not have supremum.

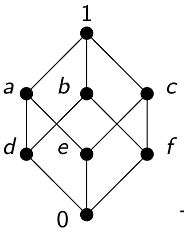
2. 

It is a bounded lattice. However, it is not a Boolean lattice since it is not distributive, and a thas two complements, not only one.

Examples

1. 

This is a bounded and distributive lattice, but a, b, and c have no complements.

2. 

This is a Boolean lattice.

Properties

If A is a Boolean lattice, the operations $+$ (supremum) and $\cdot$ (infimum) satisfy the following properties $\forall\, a, b, c \in A$:

Commutative	$a+b=b+a$	$a\cdot b=b\cdot a$
Distributive	$a+(b\cdot c)=(a+b)\cdot(a+c)$	$a\cdot(b+c)=(a\cdot b)+(a\cdot c)$
Identity element	$a+0=a$	$a\cdot 1=a$
Complement	$a+\overline{a}=1$	$a\cdot\overline{a}=0$
Associative	$a+(b+c)=(a+b)+c$	$a\cdot(b\cdot c)=(a\cdot b)\cdot c$
Absorption law	$a+(a\cdot b)=a$	$a\cdot(a+b)=a$
Idempotency	$a+a=a$	$a\cdot a=a$
Absorbent element	$a+1=1$	$a\cdot 0=0$
Identity comlements	$0+1=1$	$0\cdot 1=0$

The complement is unique.

Involution (or double complement): $\overline{\overline{a}}=a$

If A is non trivial, then $0\neq 1$ and $a\neq\overline{a}$

De Morgan's law	$\overline{(a+b)}=\overline{a}\cdot\overline{b}$	$\overline{(a\cdot b)}=\overline{a}+\overline{b}$

Examples

Examples of Boolean lattices

1. The set $A = \{0, 1\}$ with the order relation *"less or equal than"* is a Boolean lattice called binary. The supremum and infimum operations coincide with the logical operations $\vee$ and $\wedge$.
2. The quotient set of the propositional forms respect to the logical equivalence relation is an equivalence binary relation. This is a Boolean lattice with the operations $\vee$ and $\wedge$.
3. Given a set E, the power set of E, $\mathscr{P}(E)$, is a Boolean lattice with the relation of set inclusion (which is an order relation). In this case, if X and Y are two subsets of E, we have that

$$\sup_{\mathscr{P}(E)} (\{X, Y\}) = X \cup Y, \qquad \inf_{\mathscr{P}(E)} (\{X, Y\}) = X \cap Y.$$

4. The set $\mathbb{N}$ with the divisibility relation is a Boolean lattice (it is not bounded because it has no maximum). In this case, if $a, b \in \mathbb{N}$

$$\sup_{\mathbb{N}}(\{a, b\}) = \operatorname{lcm}(a, b), \qquad \inf_{\mathbb{N}}(\{a, b\}) = \gcd(a, b)$$

Examples

The Boolean lattice of divisors

If n is a natural number, we denote by D_n to **the set of natural divisors of** n. In D_n we can consider the divisibility relation: if $a, b \in D_n$, a is related with b if $a \mid b$ (which is an ordered relation).

Properties

- D_n is a distributive lattice with the operations

$$\sup_{D_n}(\{a,b\}) = \operatorname{lcm}(a,b) \quad \text{and} \quad \inf_{D_n}(\{a,b\}) = \gcd(a,b).$$

- D_n has maximum (which is n) and minimum (which is 1).
- Therefore, D_n is a Boolean lattice if and only if every element $a \in D_n$ admits a **complement**, that is, if there exists $\overline{a} \in D_n$ such that $\operatorname{lcm}(a,\overline{a}) = n$ and $\gcd(a,\overline{a}) = 1$.

It is clear that D_6 is a Boolean lattice. Is D_{12} a Boolean lattice?

For which natural numbers $n \in \mathbb{N}$ is D_n a Boolean lattice?

Boolean functions

Definition (Boolean function)

If A is a Boolean lattice, then we called a **Boolean function of order** n on A to any map $f\colon A^n \longrightarrow A$ such that the image of an n-tuple, $f(x_1, x_2, \ldots, x_n)$, is obtained applying a finite number of times the Boolean lattice operations of sum, product, and taking complements to the elements x_1, $x_2, \ldots,$ x_n.

Example (of a Boolean function)

If A is a Boolean lattice, the map $f : A^3 \rightarrow A$ given by:
$f(x,y,z) = x + x \cdot y + \overline{y} \cdot z$ is a Boolean function of 3rd order.

- If A is the Boolean lattice of the power set of E, that is $\mathscr{P}(E)$, the previous function corresponds to the operation:

$$X \cup (X \cap Y) \cup (Y^c \cap Z)$$

- If A is the Boolean lattice of propositional forms, this function corresponds to the propositional form:

$$P \vee (P \wedge Q) \vee (\rceil Q \wedge R).$$

Representation of Boolean functions

Any Boolean function can admit different expressions.

Example (Example)

Applying the absorption law to the function of the previous example, $f(x,y,z) = x + x \cdot y + \overline{y} \cdot z$, we obtain $f(x,y,z) = x + \overline{y} \cdot z$.

Having in mind these situation, two natural questions arise:

Questions

- How to find if two different expressions **correspond to the same** Boolean function?
- How to obtain the **simplest** expression that correspond to a Boolean function?

To solve the first question we will see that a Boolean function admits two expresssions (called **normal forms**) that characterize a function. In addition, this way of writing Boolean functions will let us to simplify them, which will answer to the second question.

Minimal and maximal terms

Definition (Minimal terms)

A minimal term of n-th order n (or **minterm of n-th order**) is a Boolean function of the form $m(x_1, x_2, \dots, x_n) = b_1 \cdot b_2 \cdots b_n$, where $b_i = x_i$ or $b_i = \overline{x}_i$ for all $i = 1, 2, \dots, n$.

Example (Examples of minimal terms)

1. $m(x, y, z) = \overline{x} \cdot y \cdot z$ is a minimal term of third order.
2. $m(x, y, z, t) = x \cdot \overline{y} \cdot \overline{z} \cdot t$ is a minimal term of fourth order.

Definition (Maximal terms)

A **maximal term of n-th order** (or **maxterm of n-th order**) is a Boolean function of the form $M(x_1, x_2, \dots, x_n) = b_1 + b_2 + \dots + b_n$, where $b_i = x_i$ or $b_i = \overline{x}_i$ for all $i = 1, 2, \dots, n$.

Example (Examples of maximal terms)

- $M(x, y, z) = \overline{x} + y + z$ is a maximal term of third order.
- $M(x, y, z, t) = x + \overline{y} + \overline{z} + t$ is a maximal term of fourth order.

Minimal terms and binary expressions

Proposition

If m is a **minimal term of** n**-th order** *in a Boolean lattice, then* **there exists a unique** n**-tuple of zeros and ones such that** m **takes the value** 1*. (m takes the value* 0 *in the others n binary tuples).*

Example

The minterm of 3rd order $m(x,y,z) = x \cdot \overline{y} \cdot z$ only takes the value 1 for the 3-tuple $(1,0,1)$: $m(1,0,1) = 1 \cdot \overline{0} \cdot 1 = 1 \cdot 1 \cdot 1 = 1$, If we replace the variables for any other combination of $0's$ and $1's$, the result will be always 0.

How to call the minterms?

It is usual to denote this minimal term as m_{101}, or m_5, since 5 in base 10 is equivalent to 101 in base 2.

To find the binary n-tuple associated to a minimal term it is enough to realise that the product will only be 1 if all the factors are 1. Therefore, if a variable is not complemented, then it takes the value 1, and if it is complemented, then it takes the value 0.

Maximal terms and binary expressions

Theorem

If M is **a maximal term of order** *n on a Boolean lattice Boole, then* **there exists a unique** *n***-tuple of zeros and ones with whom** *M* **is 0** *(M is 1 for the rest of binary n-tuples).*

Example

The maxterm of 3rd order, $M(x,y,z) = \overline{x} + \overline{y} + z$ takes the value 0 for the 3-tuple $(1,1,0)$: $M(1,1,0) = \overline{1} + \overline{1} + 0 = 0 + 0 + 0 = 0$, but if we replace the variables for any other combination of 0's and 1's, the result wil be always 1.

How to call the minterms?

It is usual to denote this maximal term as m_{110}, or M_6, since 6 in base 10 is equivalent to 110 in base 2.

To find the binary n-tuple associated to a maximal term it is enough to see that it would only be if all the summands are 0. Therefore the complemented variables must take the value 1, and the others the value 0.

Disjunctive normal form

Theorem

Every non null Boolean function f can only expressed in a unique way, except by the order as a **sum of different minimal terms**. *This expression is known as the* **disjunctive normal form** *of the function f.*

Remark

In particular, the minimal terms that belong to the disjunctive normal form of the boolean function f of n-th order are the ones **associated to those binary n-tuples where f takes the value 1**.

Therefore, to obtain the disjunctive normal form of a function f of orden n on a Boolean lattice A, it will be enough to compute the values of f over the elements of $\{0,1\}^n \subseteq A^n$ (that is, over the n-tuples of 0's and 1's). That is, to compute the **table of truth** of f.

Computing the disjunctive normal form

Example (Example of a disjunctive normal form)

Let $f(x, y) = x \cdot y + \overline{x}$ be a Boolean function of 2nd order. Consider its **table of truth**:

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

The normal disjunctive form of f would be:

$$f(x, y) = m_{00}(x, y) + m_{01}(x, y) + m_{11}(x, y)$$
$$= \overline{x} \cdot \overline{y} + \overline{x} \cdot y + x \cdot y$$

Conjunctive normal form

Theorem

Every Boolean function f different from the constant function 1 can be expressed in a unique way (except by the order) as the **product of different maximal terms***. This expression is known as the* **conjunctive normal form** *of the function f.*

Remark

In particular, the maximal terms that appear in a conjunctive normal form of an n-th order Boolean function f, that is **the ones which are associated to the binary n-tuples where f takes the value 0**.

Calculation of the normal conjuntive form

Example (Example of a conjunctive normal form)

Consider the Boolean function of the previous example. Its table of truth is the following one:

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

The conjunctive normal form of f will be:

$$f(x,y) = M_{10}(x,y) = \overline{x} + y$$

Quine-McCluskey algorithm

This is a method to simplify Boolean functions of **any order**.

The Quine-McCluskey algorithm has two part:

1. In the **first part** it is considered the normal disjunctive form of f, and then we find the so called **prime implicants** of the Boolean functions. **They are the Boolean expressions obtained when we remove as much variables as possible in the minimal terms of the function.**
   This part is based on the use of the distributive, complementary, and idempotent law.
2. In the **second part**, we calculate one (or more) set(s) of prime implicants whose sum gives the initial function.

Description of the 1st part (1st step)

Example (Consider the following Boolean function of 4th order, expressed in its normal disjunctive form as follows:)

$$f(x,y,z,t) = \overline{x}\cdot\overline{y}\cdot\overline{z}\cdot\overline{t} + \overline{x}\cdot\overline{y}\cdot z\cdot\overline{t} + \overline{x}\cdot\overline{y}\cdot z\cdot t + \overline{x}\cdot y\cdot z\cdot\overline{t} + \overline{x}\cdot y\cdot z\cdot t +$$

$$x\cdot\overline{y}\cdot\overline{z}\cdot\overline{t} + x\cdot\overline{y}\cdot\overline{z}\cdot t + x\cdot y\cdot\overline{z}\cdot\overline{t} + x\cdot y\cdot\overline{z}\cdot t + x\cdot y\cdot z\cdot\overline{t} + x\cdot y\cdot z\cdot t$$

Using the minterms notation with binary subindex we have

$$f(x,y,z,t) = m_{0000} + m_{0010} + m_{0011} + m_{0110} + m_{0111} +$$

$$m_{1000} + m_{1001} + m_{1100} + m_{1101} + m_{1110} + m_{1111}$$

Description of the 1st part (2nd step)

0000
0010
1000
0011
0110
1001
1100
0111
1101
1110
1111

We write in a column on the left, the binary subindex of the minimal terms of f. They will be separated by **blocks** so that the numbers in the first block do not contain any 1, the numbers in the second one contain exactly one 1, the ones in third block contain two 1's, and so on.

Description of the 1st part (3rd step)

0000 *	00-0
0010 *	-000
1000 *	001-
0011 *	0-10
0110 *	100-
1001 *	1-00
1100 *	0-11
0111 *	011-
1101 *	-110
1110 *	1-01
1111 *	110-
	11-0
	-111
	11-1
	111-

We consider all the pairs of binary numbers that belong to **contiguous** blocks that differ only in **one digit**. We mark them with an $*$ and we write, in another column to the right, the expression obtained by replacing the digit that is different by a dash $-$. For example, the term 0000 (that belongs to the first block) and the term 0010 (that belongs to the second one) only differ in the digit at third position; therefore we should mark them and we have to add the term with the dash to the right column.

This is the reason: the minterms corresponding to 0000 and 0010 are $\overline{x}\cdot\overline{y}\cdot\overline{z}\cdot\overline{t}$ and $\overline{x}\cdot\overline{y}\cdot z\cdot\overline{t}$. Applying the **distributive and complementing** laws, their sum can be "simplified" to:

$$\overline{x}\cdot\overline{y}\cdot\overline{t}\cdot(\overline{z}+z)=\overline{x}\cdot\overline{y}\cdot\overline{t}=:m_{00-0}$$

Now, we can substitute in the expression of the disjunctive normal form of f, the sum $m_{0000}+m_{0010}$ by m_{00-0}. We observe that 0000 can be also combined with 1000 giving -000. This can be done because the minterm m_{0000} can be considered that it is "repeated" as a summand in the expression of f as many times as we want using the **idempotent law**.

Description of the 1st part (3rd step)

0000 *	00-0	0-1-
0010 *	-000	1-0-
1000 *	001- *	-11-
0011 *	0-10 *	11--
0110 *	100- *	
1001 *	1-00 *	
1100 *	0-11 *	
0111 *	011- *	
1101 *	-110*	
1110 *	1-01 *	
1111 *	110- *	
	11-0 *	
	-111*	
	11-1 *	
	111- *	

We proceed as before with the new blocks (of the second column), "combining" the terms corresponding to contiguous blocks with **exactly** one different digit (and the dash in the same position). These new terms will be added to a third column on the left.

We observe that we cannot combine any element of the first block with elements of the second block. However, the term $001-$ (of the second block) can be combined with $011-$ (of the third block) giving $0-1-$ (that is introduced in a new column on the right). That is:

$$m_{001-} + m_{011-} = \overline{x}\cdot\overline{y}\cdot z + \overline{x}\cdot y\cdot z = \overline{x}\cdot z\cdot(\overline{y}+y) =$$

$$\overline{x}\cdot z =: m_{0-1-}$$

We repeat this procedure until we cannot combine any other pair of terms.

We called **prime implicants** to the terms that are still without being marked. In our case they are: $m_{00-0} = \overline{x}\cdot\overline{y}\cdot\overline{t}$, $m_{-000} = \overline{y}\cdot\overline{z}\cdot\overline{t}$, $m_{0-1-} = \overline{x}\cdot z$, $m_{1-0-} = x\cdot\overline{z}$, $m_{-11-} = y\cdot z$, and $m_{11--} = x\cdot y$.

We repeat this process until no new columns can be added

Description of the first part (4th step)

We have deduced that the initial function can be expressed as a **sum of the following prime implicants**:

$$f(x,y,z,t) = m_{00-0} + m_{-000} + m_{0-1-} + m_{1-0-} + m_{-11-} + m_{11--} =$$

$$= \overline{x}\cdot\overline{y}\cdot\overline{t} + \overline{y}\cdot\overline{z}\cdot\overline{t} + \overline{x}\cdot z + x\cdot\overline{z} + y\cdot z + x\cdot y$$

We have arrived to the **simplest expression** of the function f.

In the second step we will see how to obtain some even simpler expressions, removing some “repeated” prime implicants.

Description of the 2nd part (1st step)

Definition

We say that a term r **covers** certain minterm m if all the variables (complemented or not) that appear in r also appear in m.

Example

The term $\overline{y} \cdot t$ covers the minterm $x \cdot \overline{y} \cdot \overline{z} \cdot t$.

The first step of the 2nd part of the Quine-McCluskey consists on finding which minterms of the disjunctive normal form of f cover each one of the prime implicants that appear in the simplified expression of f that we have already obtained in the first part.

Description of the 2nd part (1st step)

We construct a table such that every row corresponds a prime implicant and every column corresponds to a minterm of the disjunctive normal form of f. We mark with X all the cells that correspond to a prime implicant (row) that cover a minterm (colum).

	0000	0010	0011	0110	0111	1000	1001	1100	1101	1110	1111
$00-0$	X	X									
-000	X					X					
$0-1-$		X	X	X	X						
$1-0-$						X	X	X	X		
$-11-$				X	X					X	X
$11--$								X	X	X	X

Description of the 2nd part (2nd step)

We look for the columns **that only contain one** X and we mark these X with a circle. This means that the corresponding minterms are covered by a unique prime implicant.
These are the essential prime implicants (marked with green). They necessarily have to appear in every minimal expression of f (because, on the contrary, there will be minterms that will not be covered):

$$f(x,y,z,t) = m_{0-1-} + m_{1-0-} + \cdots = \overline{x}\cdot z + x\cdot\overline{z} + \cdots$$

	0000	0010	0011	0110	0111	1000	1001	1100	1101	1110	1111
$00-0$	X	X									
-000	X					X					
$0-1-$		X	$\otimes$	X	X						
$1-0-$						X	$\otimes$	X	X		
$-11-$				X	X					X	X
$11--$								X	X	X	X

Description of 2nd part (3rd step)

We also mark all the minterms that are covered by the essential prime implicants (the ones written in red, in the table). Now, the expression:

$$m_{0-1-} + m_{1-0-} = \overline{x} \cdot z + x \cdot \overline{z}$$

"covers" to all minterms written in red. We have only to cover the minterms that are written in blue.

	0000	0010	0011	0110	0111	1000	1001	1100	1101	1110	1111
$00-0$	X	X									
-000	X					X					
$0-1-$		X	$\otimes$	X	X						
$1-0-$						X	$\otimes$	X	X		
$-11-$				X	X					X	X
$11--$								X	X	X	X

Description of 2nd part (4th step)

The minterms that are still **uncovered** have to be covered by the prime implicants marked with blue. Therefore:

	0000	0010	0011	0110	0111	1000	1001	1100	1101	1110	1111
$00-0$	X	X									
-000	X					X					
$0-1-$		X	$\otimes$	X	X						
$1-0-$						X	$\otimes$	X	X		
$-11-$				X	X					X	X
$11--$								X	X	X	X

The simplified expression of f obtained in this second part will be obtained **adding**, to the **essential prime implicants** (that must necessarily appear in **all** the simplified expressions), a **minimum amount of non essential prime implicants** in order to cover all the minterms.

Description of the second part (5th step)

	0000	0010	0011	0110	0111	1000	1001	1100	1101	1110	1111
$00-0$	X	X									
-000	X					X					
$0-1-$		X	⊗	X	X						
$1-0-$						X	⊗	X	X		
$-11-$				X	X					X	X
$11--$								X	X	X	X

In our case we can obtain 4 simplified expressions of f ("playing" with the 4 non-essential prime implicants):

$$f(x,y,z,t) = m_{0-1-} + m_{1-0-} + m_{00-0} + m_{-11-} = \\ = \overline{x}\cdot z + x\cdot\overline{z} + \overline{x}\cdot\overline{y}\cdot\overline{t} + y\cdot z$$

$$f(x,y,z,t) = m_{0-1-} + m_{1-0-} + m_{00-0} + m_{11--} = \\ = \overline{x}\cdot z + x\cdot\overline{z} + \overline{x}\cdot\overline{y}\cdot\overline{t} + x\cdot y$$

$$f(x,y,z,t) = m_{0-1-} + m_{1-0-} + m_{-000} + m_{-11-} = \\ = \overline{x}\cdot z + x\cdot\overline{z} + \overline{y}\cdot\overline{z}\cdot\overline{t} + y\cdot z$$

$$f(x,y,z,t) = m_{0-1-} + m_{1-0-} + m_{-000} + m_{11--} = \\ = \overline{x}\cdot z + x\cdot\overline{z} + \overline{y}\cdot\overline{z}\cdot\overline{t} + x\cdot y$$