### **BOOLEAN ALGEBRA**

Department of Mathematics
Manipal Institute of Technology
Manipal Academy of Higher Education Manipal
Manipal



# Contents

- Binary relations
- 2 Lattice
- 3 Distributive and complemented lattice
- Boolean lattice and boolean algebra
- 5 Boolean functions and boolean expressions
- 6 Reference

- A binary relation R from a set A to B is a subset of  $A \times B$ . That is,  $R = \{(a,b)|a \in A, b \in B\} \subseteq A \times B$ . If  $(a,b) \in R$ , then we say that the element 'a is related to b' and write aRb.
- A binary relation a set A to A is said to be a binary relation on A.

# Types of relations:

- Reflexive relation: A binary relation R on a A is said to be a reflexive relation if (a, a) ∈ R for all a ∈ A.
  Ex: Let A be the set of positive integers and R be the binary relation on A defined by (a, b) ∈ R if and only if a divides b. Then R is reflexive as every integer divides itself.
- Symmetric relation: A binary relation R on a A is said to be symmetric if (a, b) ∈ R ⇒ (b, a) ∈ R for all a, b ∈ A.
  Ex: The relations "is parallel to "and "is perpendicular to "are symmetric relations on the set of all straight lines.

- **3** Antisymmetric relation: A binary relation R on a set A is said to be antisymmetric if  $(a,b) \in R \implies (a,b) \notin R$  unless a=b. Ex: The binary relation R defined by  $(a,b) \in R$  if and only if  $a \ge b$  is antisymmetric on the set of positive integers.
- Transitive relation: A binary relation R on a A is said to be transitive if (a, c) ∈ R whenever both (a, b) ∈ R and (b, c) ∈ R. Ex: The relation "is parallel to "is transitive, but the relation "is perpendicular to "is not transitive on the set of straight lines.
- **5 Equivalence relation:** A binary relation on a set is said to be an equivalence relation if it is reflexive, symmetric and transitive.

**3** Partial ordering relation: A binary relation on a set is said to be an equivalence relation if it is reflexive, antisymmetric and transitive. A nonempty set A with a partial ordering relation R is a partially ordered set (abbreviated as poset). For each ordered pair  $(a,b) \in R$ , we write  $a \le b$  instead of aRb where  $\le$  is a generic symbol and commonly read as "less than or equal to". It is often denoted as (A,R) or (A,R) or  $(A,\le)$ .

Ex: Let A be the set of positive integers and R be the binary relation on A defined by  $a \le b$  if and only if a divides b. Then  $(A, \le)$  is a poset.

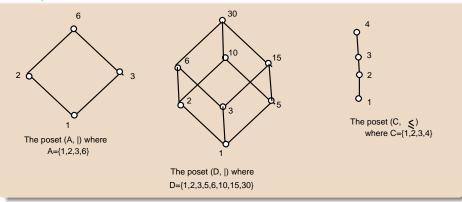
- Comparable elements: Let  $(A, \leq)$  is a poset. Two elements  $a, b \in A$  are said to be comparable if either  $a \leq b$  or  $b \leq a$ .
- Chain: Let  $(A, \leq)$  is a poset. A subset of A is called a chain if every two elements in the subset are comparable. The number of elements in a chain is known as the length of the chain.
- Antihain: Let  $(A, \leq)$  is a poset. A subset of A is called an antichain if no two distinct elements in the subset are comparable.
- Totally ordered set: A poset (A, ≤) is called a totally ordered set if A is a chain. In this case, the binary relation ≤ is called a total ordering relation.
- Cover of an element: Let  $(A, \leq)$  is a poset. An element  $b \in A$  is said to cover an element  $a \in A$  if  $a \leq b$  and there is no element  $c \in A$  such that  $a \leq c \leq b$ .

# Hasse diagram

A poset  $(A, \leq)$  is graphically represented by Hasse diagram. The following steps are to be followed to draw Hasse diagram corresonding to a given poset  $(A, \leq)$ .

- Each element of A is represented by a small circle or a dot.
- The circle for  $x \in A$  is drawn below the circle for  $y \in A$  if  $x \le y$ . A line is drawn if y covers x.
- If x ≤ y but y doesn't cover x, then x and y are not connected directly by a single line.

# Example 1.1.



Here  $\mid$  is the relation "divides " and  $\leq$  is the relation "less than or equal to " .

We note the following terminologies for a given poset  $(A, \leq)$ .

- Maximal element: An element  $a \in A$  is said to be a maximal element of A if there is no  $b \in A$  such that  $a \neq b$  and  $a \leq b$ . We note that 6,30 and 4 are the maximal elements of (A, |), (D, |) and  $(C, \leq)$  respectively.
- **Minimal element:** An element  $a \in A$  is said to be a minimal element of A if there is no  $b \in A$  such that  $a \neq b$  and  $b \leq a.1$  is the minimal element of (A, |), (D, |) and  $(C, \leq)$ .
- **Upper bound:** Let  $a, b \in A$ . An element  $c \in A$  is said to be an upper bound of a and b if  $a \le c$  and  $b \le c$ .
- **Lower bound:** An element  $c \in A$  is said to be an lower bound of a and b if  $c \le a$  and  $c \le b$ .

- Least upper bound (lub): An element c∈ A is said to be a least upper bound of a and b if c is an upper bound for a and b, and there is no upper bound d of a and b such that d ≤ c.
  In (D, |) of example 1.1, the element 30 is an upper bound of 2 and 3, but it is not the least upper bound. The lub for 2 and 3 is 6.
- Greatest lower bound (glb): An element  $c \in A$  is said to be an greatest lower bound of a and b if c is a lower bound for a and b, and there is no lower bound d of a and b such that c < d.

#### Lattice:

A partially ordered set is said to be a lattice if every two elements in the set have a unique glb and unique lub. Let  $(L, \leq)$  be a lattice. For any two elements a, b, let

 $a \lor b$ : **lub of** a **and** b and  $a \land b$ : **glb of** a **and** b.

Then  $(L, \leq, \vee, \wedge)$  is an algebraic system defined by the lattice  $(L, \leq)$ .

# Example 2.1.

Let P(S) be the power set of a nonempty set S. Then  $(P(S), \subseteq)$  is a lattice where  $A \vee B = A \cup B$  and  $A \wedge B = A \cap B$ . This defines the algebraic system  $(P(S), \subseteq, \cup, \cap)$ .

# Example 2.2.

Let  $N^+$  be the set of all positive integers. Then  $(N^+, |)$  (a|b if a divides b) is a lattice where  $a \lor b = lcm(a, b)$  and  $a \land b = gcd(a, b)$ .

# Theorem 2.3.

For any elements a, b in a lattice  $(A, \leq)$ ,

- $a \le a \lor b$  and  $b \le a \lor b$
- $a \wedge b \leq a$  and  $a \wedge b \leq b$

### Theorem 2.4.

For any elements a,b,c,d in a lattice  $(A,\leq)$ , if  $a\leq b$  and  $c\leq d$ 

- $a \lor c \le b \lor d$
- $a \wedge c \leq b \wedge c$

# **Duality Principle**

Let  $(A, \leq)$  be a poset. Let  $\geq$  be a binary relation on A such that for any a, b in A,  $a \geq b$  if and only if  $b \leq a$ . We note that  $(A, \geq)$  is a poset.

- If  $(A, \leq)$  is a lattice, then so is  $(A, \geq)$
- The join operation of the algebraic system defined by the lattice  $(A, \leq)$  is the meet operation of the algebraic system defined by  $(A, \geq)$  and vice versa.
- Consequently, given any valid statement concerning the general properties of the lattices, we can obtain another valid statement by replacing the relation ≤ with ≥, the meet operation with the join operation and the join operation with the meet operation. This is known as principle of duality for lattices.
- If the statement remains the same after dualism, then such a statement is called self dual.

# Properties of aglebraic systems defined by lattices:

Let  $(A, \leq, \vee, \wedge)$  be the algebraic system defined by the lattice  $(A, \leq)$ . For any elements  $a, b, c \in A$ ,

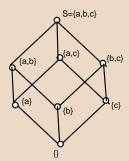
- Commutative property:
  - $a \lor b = b \lor a$
  - $a \wedge b = b \wedge a$
- Associative property:
  - $(a \lor b) \lor c = a \lor (b \lor c)$
  - $(a \wedge b) \wedge c = a \wedge (b \wedge c)$
- Idempotent property:
  - $a \lor a = a$
  - $a \wedge a = a$
- 4 Absorption property:
  - $a \wedge (a \vee b) = a$
  - $a \lor (a \land b) = a$

**Distributive lattice:** A lattice is said to be a distributive lattice if the meet operation is distributes over the join operation and the join operation s distributes over the meet operation. For any a,b,c

- $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$
- $a \lor (b \land c) = (a \lor b) \land (a \lor c)$

# Example 3.1.

Let  $S = \{a, b, c\}$ . Then  $(P(S), \subseteq)$  is a distributive lattice.



#### Theorem 3.2.

If the meet operation is distributive over the join operation in a lattice, then the join operation is also distributive over the meet operation. If the join operation is distributive over the meet operation in a lattice, then the meet operation is also distributive over the join operation.

### Proof.

#### **Problems:**

**Q1.** Let a and b be two elements in a lattice  $(A, \leq)$ . Show that  $a \wedge b = b$  if and only if  $a \vee b = a$ .

Sol.

**Q2.** Let a, b, c be elements in a lattice  $(A, \leq)$ . Show that

- i.  $a \lor (b \land c) \le (a \lor b) \land (a \lor c)$
- ii.  $(a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c)$

#### Sol.

- **Q3.** Let a, b, c be elements in a lattice  $(A, \leq)$ . Show that if  $a \leq b$ , then  $a \vee (b \wedge c) \leq b \wedge (a \vee c)$ .
- **Q4.** Let  $(A, \leq, \vee, \wedge)$  be an algebraic system where  $\vee, \wedge$  are binary operations satisfying absorption law. Show that  $\vee$  and  $\wedge$  also satisfy idempotent law.

- **Q5.** Let  $(A, \vee, \wedge)$  be an algebraic system where  $\vee, \wedge$  are binary operations satisfying commutative, associative and absorption laws. Define a binary operation  $\leq$  as follows: for all  $a, b \in A, a \leq b$  if and only if  $a \wedge b = a$ . Show that  $\leq$  is a poset. Also show that  $a \vee b$  is lub of a and b and  $a \wedge b$  is glb of a and b in  $(A, \leq)$ .
- **Q6.(Cancellation laws)** Let  $(A, \leq)$  be a distributive lattice. Show that if  $a \wedge x = a \wedge y$  and  $a \vee x = a \vee y$  for some a, then x = y.
- **Q7.** Show that a lattice is distributive if and only if for any elements a, b, c in lattice  $(a \lor b) \land c \le a \lor (b \land c)$ .

**Universal lower and upper bounds:** An element a in a lattice  $(A, \leq)$  is called a universal lower bound if for every element  $b \in A$ ,  $a \leq b$ . We use '0'to denote universal lower bound. An element a in a lattice  $(A, \leq)$  is called a universal upper bound if for every element  $b \in A$ ,  $b \leq a$ . We use '1' to denote universal upper bound. If a lattice has a universal lower (upper) bound, then it is unique. In the lattice  $(P(S), \subseteq)$ , the nullset  $\phi$  and the set S are the universal lower and upper bounds respectively.

### Theorem 3.3.

Let  $(A, \leq)$  be a lattice with universal upper and lower bounds 1 and 0. For any elements  $a \in A$ 

 $\bullet a \lor 1 = 1$ 

 $\bullet a \wedge 1 = a$ 

 $\bullet a \lor 0 = a$ 

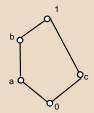
 $\bullet a \wedge 0 = 0$ 

**Complement of an element:** Let  $(A, \leq)$  be a lattice with universal upper and lower bounds 1 and 0. For any element  $a \in A$ , an element b is said to be a complement of a if  $a \lor b = 1$  and  $a \land b = 0$ 

An element in a lattice may have more than one complement. Not all the elements in a lattice have complements. It's evident that '0' is the unque complement of '0' and vice versa.

**Complemented lattice:** A lattice is said to be a complemented lattice if every element in the lattice has a complement. Clearly, a complemented lattice has a universal lower and upper bounds.

# Example 3.4.



Complement of a and b is c. Complement of c are a, b.

#### Theorem 3.5.

In a distributive lattice, if an element has a complement, it is unique.

#### Proof.

Suppose an element a has two complements b and c. i.e.

$$a \lor b = a \lor c = 1$$
 and  $a \land b = a \land c = 0$ .

Consider 
$$b = b \land 1$$
  
 $= b \land (a \lor c)$   
 $= (b \land a) \lor (b \lor c)$   
 $= 0 \lor (b \lor c)$   
 $= (a \land c) \lor (b \lor c)$   
 $= c \land (a \lor b)$   
 $= c \land 1$   
 $= c$ 

Thus 
$$b = c$$



**Boolean lattice:** A complemented and distributive lattice is called a boolean lattice.

# Example 4.1.

 $(P(S), \subseteq)$  is a boolean lattice.

Let  $(A, \leq)$  be a boolean lattice. Since every element a has a unique complement  $\bar{a}$ , we have another unary operation known as complementation and denoted by  $\bar{a}$ . Thus we can say that the lattice  $(A, \leq)$  defines an algebraic system  $(A, \leq, \vee, \wedge)$  where  $\vee$  and  $\wedge$  are the join and meet operations respectively. The algebraic system defined by a boolean lattice is known as **boolean algebra**.

#### Theorem 4.2.

DeMorgan's laws: For any elements a, b in a boolean algebra  $(A, \leq, \vee, \wedge)$ ,

• 
$$\overline{a \vee b} = \bar{a} \wedge \bar{b}$$

$$a \wedge \overline{a \wedge b} = \overline{a} \vee \overline{b}$$

The second part follows from principle of duality.

#### Proof.

We have to prove that 
$$(a \lor b) \lor (\bar{a} \land \bar{b}) = 1$$
 and  $(a \lor b) \land (\bar{a} \land \bar{b}) = 0$ . Consider  $(a \lor b) \lor (\bar{a} \land \bar{b}) = [(a \lor b) \lor \bar{a}] \land [(a \lor b) \lor \bar{b}]$  (distributive law) 
$$= [\bar{a} \lor (a \lor b)] \land [a \lor (b \lor \bar{b})] \text{ (associative law)}$$
$$= [(\bar{a} \lor a) \lor b] \land [a \lor 1] \text{ (associative law)}$$
$$= [1 \lor b] \land [a \lor 1]$$
$$= 1 \land 1 = 1$$
Similarly,  $(a \lor b) \land (\bar{a} \land \bar{b}) = (\bar{a} \land \bar{b}) \land (a \lor b) \text{ (commutative law)}$ 
$$= [(\bar{a} \land \bar{b}) \land a] \lor [(\bar{a} \land \bar{b}) \land b] \text{ (distributive law)}$$
$$= [a \land (\bar{a} \land \bar{b})] \lor [(\bar{a} \lor \bar{b}) \land b] \text{ (commutative law)}$$
$$= [(a \land \bar{a}) \land \bar{b}] \lor [\bar{a} \lor (\bar{b} \land b)] \text{ (associative law)}$$
$$= [0 \land \bar{b}] \lor [(\bar{a} \land 0]$$
$$= 0 \lor 0 = 0$$

25 / 36

**Uniqueness of finite boolean algebras:** We show that a finite boolean algebra has  $2^n$  elements for some n. An element of a boolean algebra is called an atom if it covers 0.

### Lemma 4.3.

In a distributive lattice, if  $b \wedge \bar{c} = 0$ , then  $b \leq c$ .

### Proof.

We know that 
$$0 \lor c = c$$
  $(b \land \bar{c}) \lor c = c$  (given)  $c \lor (b \land \bar{c}) = c$  (commutative law)  $(c \lor b) \land (c \lor \bar{c}) = c$  (distributive law)  $(c \lor b) \land 1 = c$   $(c \lor b) = c$   $(b \lor c) = c$  Thus  $b < b \lor c \implies b < c$ .



#### Lemma 4.4.

Let  $(A, \leq, \vee, \wedge, ^-)$  be a finite boolean algebra. Let b be any nonzero element in A and  $a_1, a_2, \ldots, a_k$  be all the atoms of A such that  $a_i \leq b$ . Then  $b = a_1 \vee a_2 \vee \ldots a_k$ .

### Proof.

#### Lemma 4.5.

Let  $(A, \leq, \vee, \wedge, ^-)$  be a finite boolean algebra. Let b be any nonzero element in A and  $a_1, a_2, \ldots, a_k$  be all the atoms of A such that  $a_i \leq b$ . Then  $b = a_1 \lor a_2 \lor \ldots a_k$  is the unique way to represent b as a join of atoms.

#### Proof.

Suppose that we have alternatinve representation  $b = a_{i1} \lor a_{i2} \lor \dots a_{it}$ . Since b is the lub of  $a_{i1}, a_{i2}, \dots a_{it}$ , it is true that  $a_{i1} \leq b, a_{i2} \leq b, \ldots, a_{it} \leq b$ . Consider an atom  $a_{iu}$   $(1 \leq u \leq t)$ . Since  $a_{iu} \leq b$ .

we have 
$$a_j \wedge b = a_{ju}$$

$$a_{ju} \wedge (a_1 \vee a_2 \vee \ldots a_k = a_{ju})$$

$$(a_{ju} \wedge a_1) \vee (a_{ju} \wedge a_2) \vee \dots (a_{ju} \wedge a_k) = a_{ju}$$

Then for some 
$$a_i$$
  $(1 \le i \le k)$ ,  $a_{iu} \land a_i \ne 0$ .

Since  $a_{iu}$  and  $a_i$  are atoms, we must have  $a_{iu} = a_1$ . Thus each atom in the alternative representation is an atom in the original one, and the lemma follows.

From the above lemmas, it is clear that there is one to one correspondence between the elements of a boolean lattice and subset of atoms. As a matter of fact, there is one to one correspondence from  $(A, \leq)$  to  $(P(S), \subseteq)$ , where S is the set of all atoms.

#### Theorem 4.6.

Let  $(A, \vee, \wedge, ^-)$  be a finite boolean algebra. Let S be the set of all atoms. Then  $(A, \vee, \wedge, ^-)$  is isomorphic to the algebraic system defined by the lattice  $(P(S), \subseteq)$ .

It follows from the above lemmas that there exists a finite boolean algebra of  $2^n$  elements for any n > 0.

**Boolean expression:** Let Let  $(A, \vee, \wedge, ^-)$  be a finite boolean algebra. A boolean expression over  $(A, \vee, \wedge, ^-)$  is defined as follows:

- An element of A is a boolean expression.
- Any variable name is a boolean expression.
- If  $e_1$  and  $e_2$  are boolean expressions, then  $\overline{e_1}, e_1 \lor e_2$  and  $e_1 \land e_2$  are boolean expressions.

# Example 5.1.

$$0 \lor x$$
,  $(x_1 \lor x_2) \land \overline{(2 \lor 3)}$ 

Let  $E(x_1, x_2, ..., x_n)$  be a boolean expression of n variables over a boolean algebra  $(A, \vee, \wedge, ^-)$ . By assignment of values to the variables  $x_1, x_2, ..., x_n$ , we mean an assignment of elements of A to be the values of the variables. For an assignment of values to the variables, we can evaluate  $E(x_1, x_2, ..., x_n)$  by substituting the variables in the expression by their values.

Two boolean expressions of n variables are said to be equivalent if thet assume the same vales for every assignment of values to the n variables. If  $E_1(x_1, x_2, \ldots, x_n)$  and  $E_2(x_1, x_2, \ldots, x_n)$  are equivalent, then we write  $E_1(x_1, x_2, \ldots, x_n) = E_2(x_1, x_2, \ldots, x_n)$ .

### Example 5.2.

$$(x_1 \wedge x_2) \vee (x_1 \wedge \bar{x_3})$$
 is equivalent to  $x_1 \wedge (x_2 \vee \bar{x_3})$ .

**Boolean function:** A function  $f: A^n \to A$  is said to be a boolean functionnif it can be specified by a boolean expression of n variables.

**Minterm:** A booleam expression of n variables  $x_1, x_2, \ldots, x_n$  is said to be a minterm if it is of the form  $\tilde{x_1} \wedge \tilde{x_2} \wedge \cdots \wedge \tilde{x_n}$  where  $\tilde{x_i}$  is either  $x_i$  or  $\bar{x_i}$ . **Disjunctive normal form (DNF):** A boolean expression over  $(\{0,1\},\wedge,\vee,^-)$  is said to be in disjunctive normal form if it is join of minterms.

Example 5.3.

$$(x_1 \wedge \bar{x_2} \wedge x_3) \vee (\bar{x_1} \wedge \bar{x_2} \wedge x_3) \vee (x_1 \wedge x_2 \wedge x_3)$$

**Maxterm:** A booleam expression of n variables  $x_1, x_2, \ldots, x_n$  is said to be a maxterm if it is of the form  $\tilde{x_1} \vee \tilde{x_2} \vee \cdots \vee \tilde{x_n}$  where  $\tilde{x_i}$  is either  $x_i$  or  $\bar{x_i}$ . **Conjunctive normal form (CNF):** A boolean expression over  $(\{0,1\},\wedge,\vee,^-)$  is said to be in conjunctive normal form if it is meet of maxterms.

# Example 5.4.

$$(x_1 \vee \bar{x_2} \vee x_3) \wedge (\bar{x_1} \vee \bar{x_2} \vee x_3)$$

**DNF:** Given a function  $\{0,1\}^n \to \{0,1\}$ , we can obtain a boolean expression in DNF corresponding to this function by having a minterm corresponding to each ordered n tuple of 0's and 1's for which the value of the function is 1. For each n tuple with the functional value is 1, we have the minterm  $\tilde{x_1} \vee \tilde{x_2} \vee \cdots \vee \tilde{x_n}$  where  $\tilde{x_i} = \begin{cases} x_i & \text{if } i^{th} \text{ componet is 1} \\ \bar{x_i} & \text{if } i^{th} \text{ componet is 0} \end{cases}$ .

**CNF:** We can obtain a boolean expression in CNF corresponding to this function by having a maxterm corresponding to each ordered n tuple of 0's and 1's for which the value of the function is 1. For each n tuple with the functional value is 0, we have the minterm  $\tilde{x_1} \vee \tilde{x_2} \vee \cdots \vee \tilde{x_n}$  where

$$\tilde{x}_i = \begin{cases} x_i & \text{if } i^{th} \text{ componet is } 0 \\ \bar{x}_i & \text{if } i^{th} \text{ componet is } 1 \end{cases}$$

**Q8.** Let  $E(x_1, x_2, x_3) = (x_1 \wedge x_2) \vee (x_1 \wedge x_3) \vee (\bar{x_2} \wedge x_3)$  be a boolean expression over  $(\{0, 1\}, \wedge, \vee, \bar{\ })$ . Write the boolean expression in both DNF and CNF.

# Sol:

	$(x_1 \wedge x_2)$	$(x_1 \wedge x_3)$	$(\bar{x_2} \wedge x_3)$	f	
000	0	0	0	0	
001	0	0	1	1	
010	0	0	0	0	
011	0	0	0	0	
100	0	0	0	0	
101	0	1	1	1	
110	1	0	0	1	
111	1	1	0	1	

DNF: 
$$(\bar{x_1} \land \bar{x_2} \land x_3) \lor (x_1 \land \bar{x_2} \land x_3) \lor (x_1 \land x_2 \land \bar{x_3}) \lor (x_1 \land x_2 \land x_3)$$
  
CNF:  $(x_1 \lor x_2 \lor x_3) \land (x_1 \lor \bar{x_2} \lor x_3) \land (x_1 \lor \bar{x_2} \lor \bar{x_3}) \land (\bar{x_1} \lor x_2 \lor x_3)$ 



# References

[1] Liu C L, Elements of discrete mathematics, 2<sup>nd</sup> edition, McGraw Hill Book Company, New Dehli, (2007).

# **THANK YOU**