LATTICES AND BOOLEAN ALGEBRA

Definition,
Types of lattices,
Hasse diagram,
Partially ordered sets.
Boolean Algebra - Basic definition
duality , Basic theorem ,
Boolean algebra as Lattices,
Representation, Theorem,
Sum - of - products form for Boolean Algebra,
Minimal Boolean Expression,
Prime implicants,
Logic gates and circuits

DEFINITION : Antisymmetric Relations
A binary relation R on a set A is antisymmetric iff for all elements x and y of A, whenever xRy and y Rx, then x = y.
DEFINITION : Partial Order on a Set; Poset
a) A binary relation R on a set A is a partial order on A iff R is reflexive, antisymmetric, and transitive.
b) A set A together with a partial order R on A is called a partially ordered set / poset.

DEFINITION : Connected Relations
A binary relation R on a set A is connected iff for all elements x and y of A, either xRy or yRx.
DEFINITION : Total Order / Linear Order on a Set
A binary relation R on a set A is a total order / linear order on A iff R is a connected partial order on A.

EXAMPLE
Show that the following divides-relations are partial orders on A. Is either a total order?
a) m| n iff m divides n, A = N.
b) m| n iff m divides n, A = the set of all positive-integer divisors of 36.

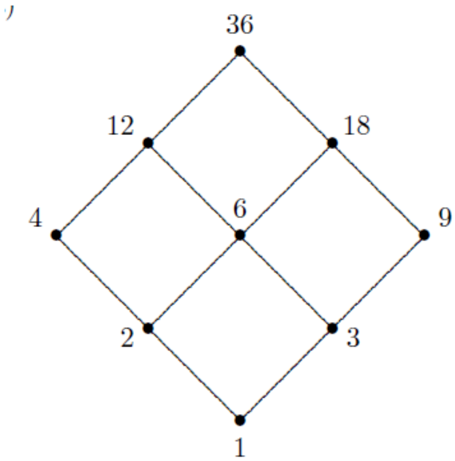
Solution

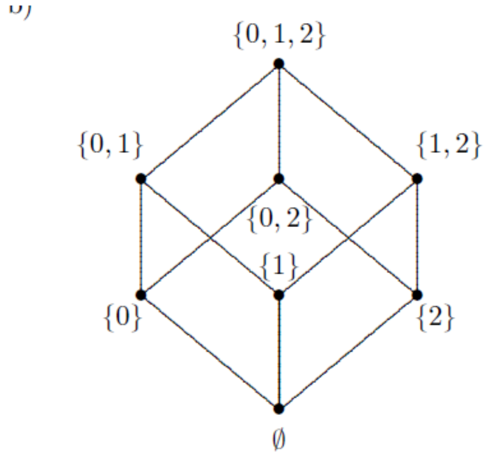
a) Since n | n for all n 2 N, the relation is reflexive. It is also antisymmetric: if m| n and n |m, then m = n. And it is transitive: if k |m and m| n, then k | n.
It is not connected, however. For example, neither 2 nor 3 divides the other. Thus, the relation is not a total order.
b) Here the divisibility relation is restricted to A = {1, 2, 3, 4, 6, 9, 12, 18, 36}.
The relation here remains reflexive, antisymmetric, transitive, and not connected.
Thus, it too is not a total order on A.

EXAMPLE
Diagram the following posets:
a) The poset of Example 3b: the divisors of 36 ordered by m| n.
b) The poset P(S) for S = {0, 1, 2}, ordered by R _ T.

Solution

These are graphed by the following Hasse diagrams.



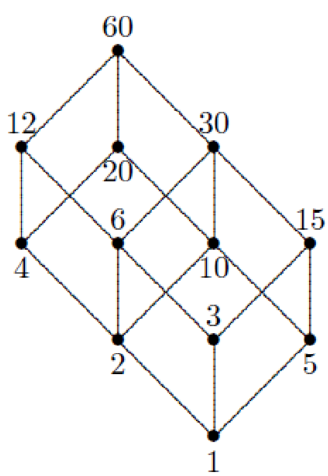


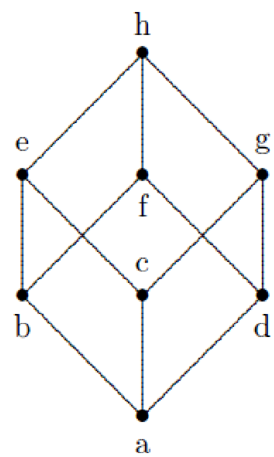
DEFINITION : Extremal Elements
Suppose hA,_i is a poset, M and m are elements of A, and S is a subset of A.
a) M is a maximal element of S iff M is in S and there is no x in S such that M < x;
M is a maximum of S iff M is in S and x _ M for all x in S.
b) m is a minimal element of S iff m is in S and there is no x in S such that x < m;
m is a minimum of S iff m is in S and m _ x for all x in S.

EXAMPLE
Identify extreme elements in the following posets:
a) The divisors of 60, ordered by divisibility.
b) The set {a, b, c, d, e, f, g, h}, ordered like the subsets of {0, 1, 2} (see Example 4).

Solution

The Hasse diagrams of these posets are given below. Note how the “dimensionality” of the first diagram corresponds to the number of prime factors in the factorization of 60 (see also Exercises 1 – 7).

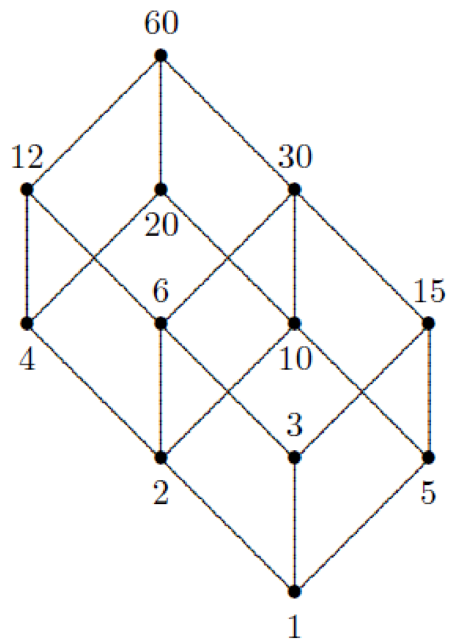


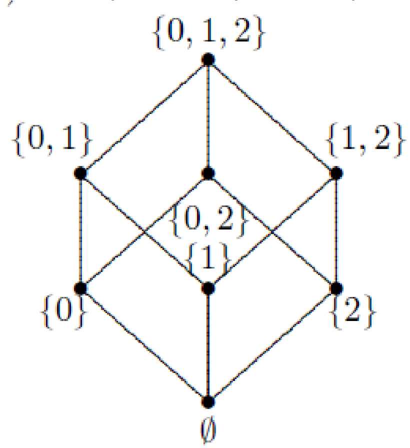


DEFINITION : Meet, Join
Let hA,_i be a poset and let x and y be any pair of elements of A.
a) The meet of x and y, denoted by x^y, is the maximum of all lower bounds for x and y;
i.e., x ^ y = max{w 2 A : w _ x, w _ y}, the greatest lower bound for x and y.
b) The join of x and y, denoted by x _ y, is the minimum of all upper bounds for x and y;
i.e., x _ y = min{z 2 A: x _ z, y _ z}, the least upper bound for x and y.

DEFINITION 7.2 - 2: Lattice
A poset A,<= is a lattice iff every pair of elements in A have both a meet and a join.

EXAMPLE
Show that the following posets are lattices, and interpret their meets and joins:
a) The poset of the divisors of 60, ordered by divisibility (see Example 7.1-6a).
b) The poset of the subsets of {0, 1, 2},ordered by the subset relation (see Example 7.1-4b).





a) The poset consisting of all the divisors of 60 is a lattice; every pair of elements has both a meet and a join.
The meet (greatest lower bound) of two divisors is their greatest common divisor:
for example, 6 ^ 20 = gcd(6, 20) = 2.
The join (least upper bound) of two divisors is their least common multiple:
for example, 6 _ 20 = lcm(6, 20) = 60.
b) The poset consisting of all the subsets of {0, 1, 2} is also a lattice.
The meet (greatest lower bound) of two subsets is the intersection of the two subsets:
for example, {0, 1} ^ {1, 2} = {0, 1} \ {1, 2} = {1}.
The join (least upper bound) is the union of the two subsets:
for example, {0, 1} _ {1, 2} = {0, 1} [{1, 2} = {0, 1, 2}.
Both of these examples generalize. Given any positive integer n, the set of all its divisors forms a lattice in which the meet of two divisors is their greatest common divisor and their join is the least common multiple of the divisors (see Exercise 4a).

PROPOSITION : Basic Operational Properties of Meet and Join
Let A be a lattice with order relation <. Then the following properties hold:

Basic Laws of Boolean Algebra

Law	Description
Commutativity	$x \vee y = y \vee x$ $x \wedge y = y \wedge x$
Associativity	$x \vee (y \vee z) = (x \vee y) \vee z$ $x \wedge (y \wedge z) = (x \wedge y) \wedge z$
Distributivity	$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$
Identity	$x \vee 0 = x$ $x \wedge 1 = x$
Annihilation	$x \wedge 0 = 0$ $x \vee 1 = 1$
Idempotence	$x \vee x = x$ $x \wedge x = x$
Absorption	$x \wedge (x \vee y) = x$ $x \vee (x \wedge y) = x$

DEFINITION : Distributive Lattice
A lattice A is distributive iff the following distributive laws hold for any x, y, and z in A:
x ^ (y _ z) = (x ^ y) _ (x ^ z); x _ (y ^ z) = (x _ y) ^ (x _ z).
We already know that meet and join are commutative, so if a lattice satisfies the above distributive laws, it automatically satisfies the other distributive laws as well (see Exercise 25):
(x ^ y) _ z = (x _ z) ^ (y _ z) and (x _ y) ^ z = (x ^ z) _ (y ^ z).

DEFINITION : Bounded Lattices
A lattice hA,_i is bounded iff it has a minimum element and a maximum element. These are denoted by 0 and 1 respectively.
The extreme elements of bounded lattices interact with other elements of the lattice in the obvious ways, captured by the next proposition.
PROPOSITION : Extreme Elements in a Bounded Lattice
Suppose hA,_i is a bounded lattice having minimum 0 and maximum 1, and let x be any element in A. Then
a) 0 _ x = x = x _ 0; 1 ^ x = x = x ^ 1
b) 0 ^ x = 0 = x ^ 0; 1 _ x = 1 = x _ 1
Proof :
These all hold because 0 _ x _ 1; apply Proposition 1b (see Exercise 16).
DEFINITION : Complements in a Bounded Lattice
Suppose hA,_i is a bounded lattice with minimum 0 and maximum 1. A complement of an element x is an element z such that x ^ z = 0 and x _ z = 1.
DEFINITION : Complemented Lattices
A bounded lattice hA,_i is complemented iff every element has a complement.

Boolean Lattices: Definition and Properties

Complemented distributive lattices are an important type of lattice. Rather than call them by this mouthful, they are given a special name: they are called Boolean lattices.

DEFINITION : Boolean Lattices

A lattice hA, _, , 0, 1 i is a Boolean lattice iff it is a complemented distributive lattice.

EXAMPLE

Investigate all Boolean lattices with cardinalities 1 – 5.

Solution

–There is only one lattice structure of size 1: a single point. This forms a Boolean lattice, but not a very interesting one.

–There is also only one lattice structure of size 2: two points in a line. This lattice is also a Boolean lattice, but as a totally ordered set it, too, is not very interesting.

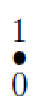
–There are no lattice structures of size 3 except the totally ordered one of three points in a line. However, this structure has no complement for the middle point (why not?), so it cannot be a Boolean lattice; in fact, no totally ordered set with more than two elements is a Boolean lattice (see Exercise 18).

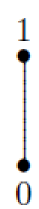
–There are two different lattice structures on four elements. There must be a top point and a bottom point; the other two must lie in the middle. These can either be side by side or in line. This gives two lattice structures : a four-point line and a diamond. The first is not a Boolean lattice, as we just noted, but the latter is.

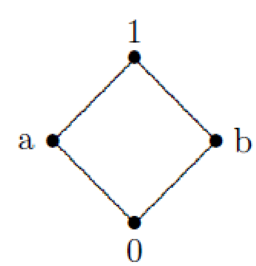
– Finally, given five points, one must be the top and another the bottom. The other three must lie between these two in some order. No such lattice structure turns out to be a Boolean lattice (see Exercise 26).

–Thus, the only order structures of cardinality 5 or less that are Boolean lattices are ones with 1, 2, or 4 elements. Hmm. That’s an interesting sequence! (See also Exercises 26 – 29).

–The Boolean lattice structures found so far are pictured below.







Boolean Algebra as an Axiomatic Theory

A Boolean algebra $\langle \mathcal{A}, +, \cdot, ^{-}, 0, 1 \rangle$ is a set $\mathcal{A}$ together with two binary operations $+$ and $\cdot$, a unary operation $^{-}$, and two distinguished elements 0 and 1 satisfying the following ten axioms:

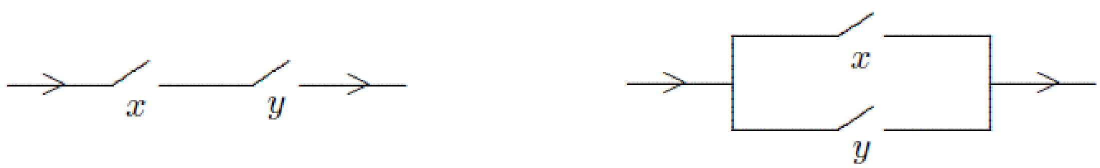
1. ***Commutative Laws***
   a) $x + y = y + x$ b) $x \cdot y = y \cdot x$
2. ***Associative Laws***
   a) $(x + y) + z = x + (y + z)$ b) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
3. ***Distributive Laws***
   a) $x \cdot (y + z) = x \cdot y + x \cdot z$ b) $x + (y \cdot z) = (x + y) \cdot (x + z)$
4. ***Identity Laws***
   a) $x + 0 = x = 0 + x$ b) $x \cdot 1 = x = 1 \cdot x$
5. ***Complementation Laws***
   a) $x + \overline{x} = 1 = \overline{x} + x$ b) $x \cdot \overline{x} = 0 = \overline{x} \cdot x$

EXAMPLE
Given a set U, P(U) forms a Boolean lattice under the partial order relation of _. Interpret P(U) as a Boolean algebra.

Solution
The operation of + in this case is [, that of · is \, and is set complementation.
The elements 0 and 1 are ; and U respectively.
All the laws hold for this interpretation, as we already know from our study of Set Theory.
Thus, there are infinitely many models of Boolean Algebra included in this example.

Boolean Algebra and Switching Circuits

The main link between Boolean Algebra and computer logic involves logic gates, which we will turn to shortly, but we will start by looking at the simpler case of switching circuits. This was Shannon's original idea for how Boolean Algebra could be applied to telecommunication.
7.4 -3
Simple switches have two states: open (no current passing through) and closed (current flowing through). We will represent an open-switch state with 0 and a closed-switch state with 1.* Switches can be connected either in series or in parallel, as shown in the following diagrams. Switches in series are represented by the product of the switch labels since current flows through the circuit (yields output 1) iff it flows through both switches. Switches in parallel are similarly denoted by a Boolean sum of the switch labels.



$\mathbf{x \cdot y}$ $\mathbf{x + y}$

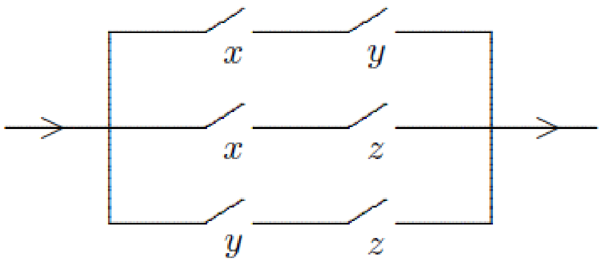
Series and Parallel Circuits

EXAMPLE

Design a series-parallel switching circuit and a Boolean expression for the ternary majority function .

Solution

Since we want output 1 (current flowing through) when two or more switches are closed (value 1), the following circuit models the ternary majority function. The Boolean expression for this function/circuit is given below the diagram



$$\mathbf{x \cdot y + x \cdot z + y \cdot z}$$

.

Every Boolean expression not equal to 0 in the variables $x_1, x_2, \ldots, x_n$ can be written as a sum of products of distinct literals in these variables.

EXAMPLE

Determine a sum-of-products decomposition for the Boolean expression $(x+yz)^2+y(yz)+z$.

Solution

Following the method of the theorem's proof, we have the following sequence of equivalent expressions. Both of the last two lines give a solution.

$$\begin{aligned}
(x+\overline{y}z)^2 + y(\overline{yz}) + z &= x + \overline{y}z + y(\overline{y} + \overline{z}) + z && \text{Idem, DeM} \\
&= x + \overline{y}z + y\overline{y} + y\overline{z} + z && \text{Distrib} \\
&= x + \overline{y}z + y\overline{z} + z && \text{Compl} \\
&= x + y\overline{z} + z && \text{Absorp}
\end{aligned}$$

DEFINITION : Maxterm, Maxterm Expansion

Let B be the standard Boolean algebra on {0, 1} and let $x_1, x_2, \ldots, x_n$ be defined on B.

a) A maxterm in the variables $x_1, x_2, \ldots, x_n$ is an n-fold sum $m_1 + m_2 + \cdots + m_n$, where for each i either $m_i = x_i$ or $m_i = x_i$.

b) A maxterm expansion in the variables $x_1, x_2, \ldots, x_n$ is a product of distinct maxterms.

EXAMPLE

Determine the maxterm expansion for the Boolean function given by the following table.

x_1	x_2	x_3	$f(x_1, x_2, x_3)$	Maxterm
0	0	0	1	
0	0	1	0	$x_1 + x_2 + \overline{x}_3$
0	1	0	1	
0	1	1	1	
1	0	0	1	
1	0	1	1	
1	1	0	1	
1	1	1	0	$\overline{x}_1 + \overline{x}_2 + \overline{x}_3$

Prime Implicants

W. V. Quine defined a **prime implicant** of F to be an**implicant** that is minimal - that is, the removal of any literal from P results in a non-**implicant** for F. Essential **prime implicants** (aka core **prime implicants**) are **prime implicants** that cover an output of the function that no combination of other **prime implicants** is ...

AB \ CD	00	01	11	10
00	0	0	0	1
01	0	0	1	1
11	0	1	1	0
10	0	1	0	0

C B A D

Example:

$\wedge$	$y=0$	$y=1$
$x=0$	0	0
$x=1$	0	1

$\vee$	$y=0$	$y=1$
$x=0$	0	1
$x=1$	1	1

$\rightarrow$	$y=0$	$y=1$
$x=0$	1	1
$x=1$	0	1

$\oplus$	$y=0$	$y=1$
$x=0$	0	1
$x=1$	1	0

Figure 1. Truth tables

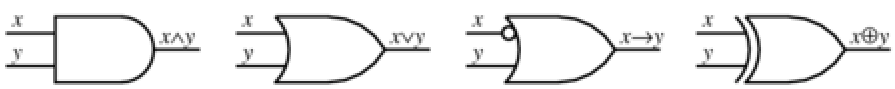


Figure 2. Logic gates

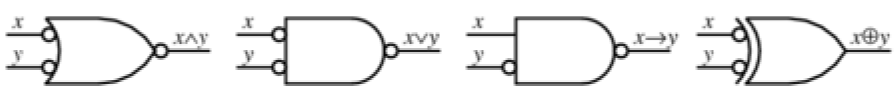


Figure 3. De Morgan equivalents

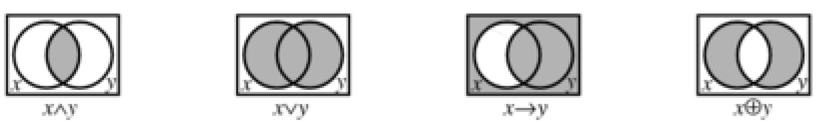
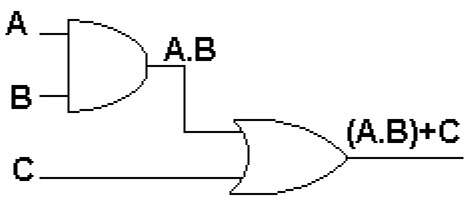
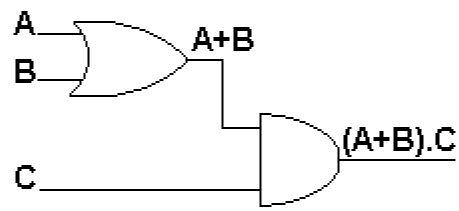


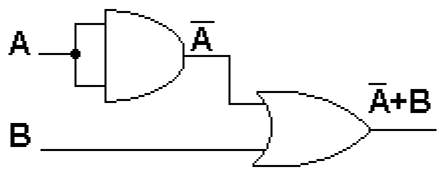
Figure 4. Venn diagrams



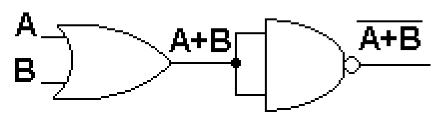
A and B high or C high
will make the output high.



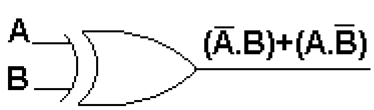
A or B high and C high
will make the output high.

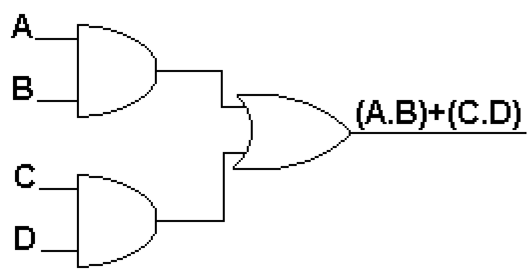


A low or B high
will make the ouput high.



The long bar above the output means that the output goes low when A or B go high.





Ex3:

- As with common arithmetic, Boolean operations have rules of precedence.
- The NOT operator has highest priority, followed by AND and then OR.
- This is how we chose the (shaded) function subparts in our table.

$F(x,y,z) = x\bar{z}+y$

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

Ex4:

Min- & Maxterms with n = 3

x	y	z	Minterms term	Minterms designation	Maxterms term	Maxterms designation
0	0	0	$x'y'z'$	m_0	$x + y + z$	M_0
0	0	1	$x'y'z$	m_1	$x + y + z'$	M_1
0	1	0	$x'yz'$	m_2	$x + y' + z$	M_2
0	1	1	$x'yz$	m_3	$x + y' + z'$	M_3
1	0	0	$xy'z'$	m_4	$x' + y + z$	M_4
1	0	1	$xy'z$	m_5	$x' + y + z'$	M_5
1	1	0	xyz'	m_6	$x' + y' + z$	M_6
1	1	1	xyz	m_7	$x' + y' + z'$	M_7

Ex5:

Basic Identities of Boolean Algebra

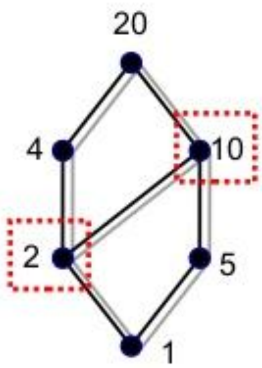
Basic Identities of Boolean Algebra

1.	$X+0=X$	2.	$X\cdot 1=X$	The relationship between a single variable X, its complement X′, and the binary constants 0 and 1
3.	$X+1=1$	4.	$X\cdot 0=0$	
5.	$X+X=X$	6.	$X\cdot X=X$	
7.	$X+\overline{X}=1$	8.	$X\cdot\overline{X}=0$	
9.	$\overline{\overline{X}}=X$			
10.	$X+Y=Y+X$	11.	$XY=YX$	Commutative
12.	$X+(Y+Z)=(X+Y)+Z$	13.	$X(YZ)=(XY)Z$	Associative
14.	$X(Y+Z)=XY+XZ$	15.	$X+YZ=(X+Y)(X+Z)$	Distributive
16.	$\overline{X+Y}=\overline{X}\cdot\overline{Y}$	17.	$\overline{X\cdot Y}=\overline{X}+\overline{Y}$	DeMorgan's

Ex6:

Complemented Lattice

- Example: D_{20} is not complemented lattice



D_{20}

Element	Its Complement
1	20
2	10
4	5
5	4
10	2
20	1

$$2 \wedge 10 \neq 0 \ \ (2 \wedge 10 = 2)$$

Ex7:

- **Theorem:** Let L be a bounded distributive lattice. If a complement exists, it is unique.

Proof: Let a' and a'' be complements of the element a in L, then

$$a \vee a' = 1, \quad a \vee a'' = 1; \qquad a \wedge a' = 0, \quad a \wedge a'' = 0$$

using the distributive laws, we obtain

$$a' = a' \vee 0 = a' \vee (a \wedge a'') = (a' \vee a) \wedge (a' \vee a'')$$
$$= 1 \wedge (a' \vee a'') = a' \vee a''$$

Also

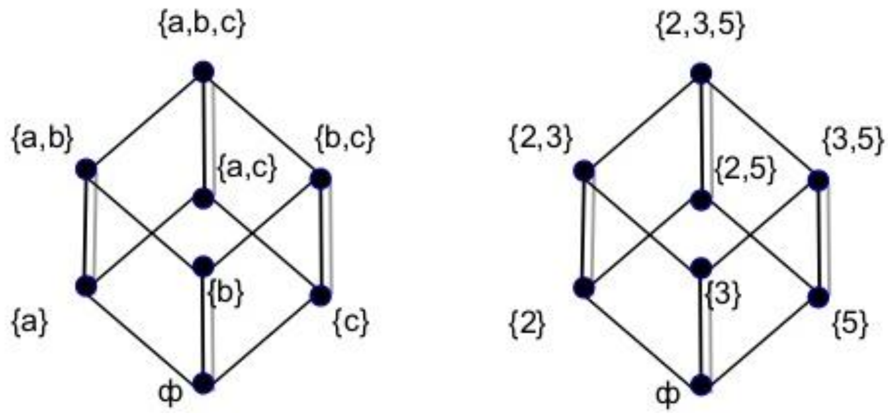
$$a'' = a'' \vee 0 = a'' \vee (a \wedge a') = (a'' \vee a) \wedge (a'' \vee a')$$
$$= 1 \wedge (a' \vee a'') = a' \vee a''$$

Hence a'=a''

Ex8:

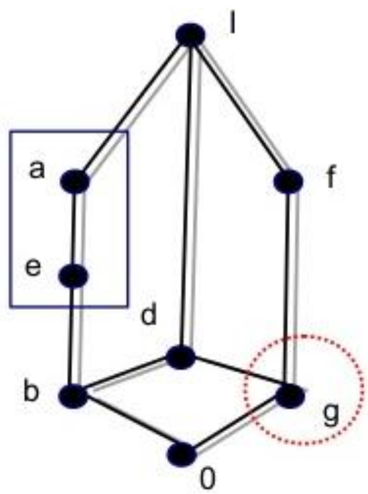
- Example:

  $S=\{a, b, c\}$ and $T=\{2,3,5\}$. consider the Hasse diagrams of the two lattices $(P(S), \subseteq)$ and $(P(T), \subseteq)$.



Ex9:

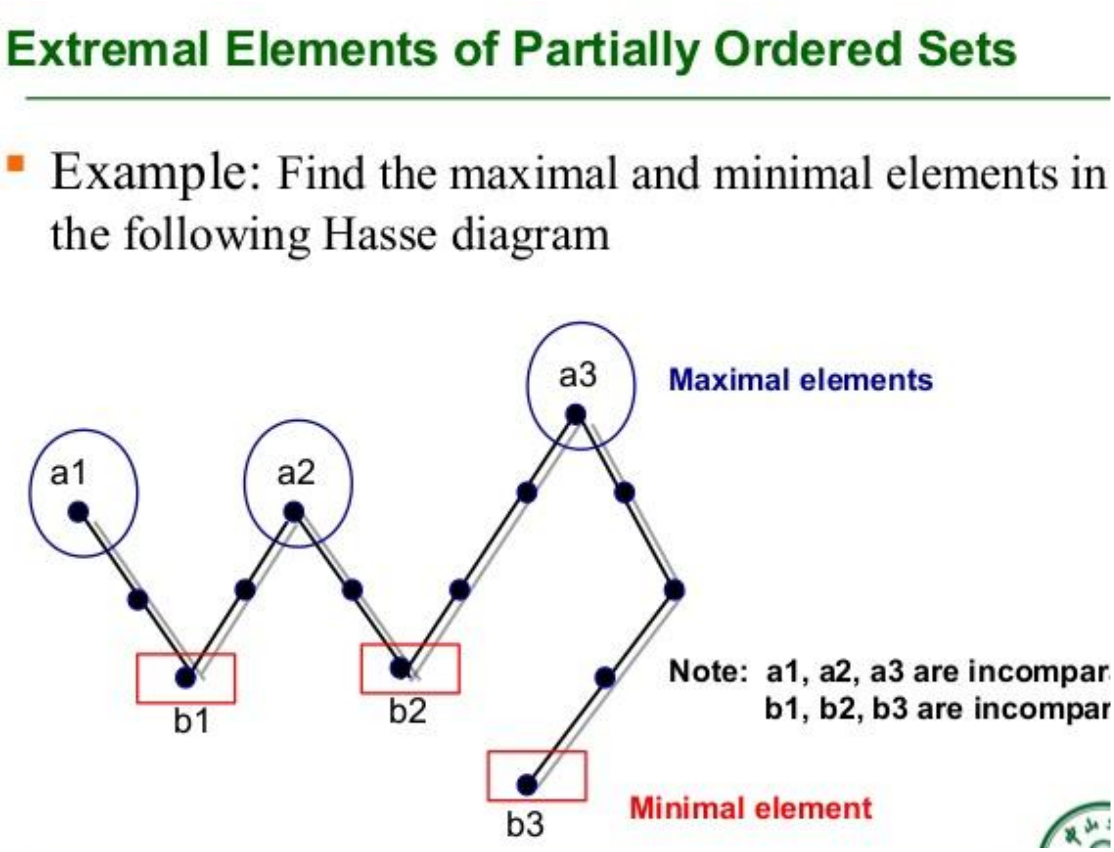
- Example: Show the lattice whose Hasse diagram shown below is not a Boolean algebra.



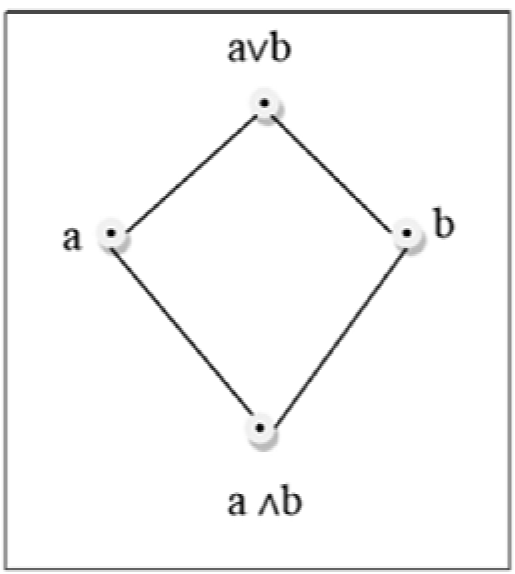
a and e are both gomplements of g

Theorem (e.g. properties 1~14) is usually used to show that a lattice L is not a Boolean algebra.

Ex10:


Extremal Elements of Partially Ordered Sets
Example: Find the maximal and minimal elements in the following Hasse diagram
a3
Maximal elements
a1
a2
b1
b2
Note: a1, a2, a3 are incompar
b1, b2, b3 are incompar
b3
Minimal element

Ex11:


a∨b
a
b
a ∧b

Ex12:

Boolean and Switching Algebras

- *Definition:* A **Boolean algebra** is a lattice that is distributive and complemented

- As an example, the lattice $(2^A, \subseteq)$ is a Boolean algebra with the join and meet of $x,y \in 2^A$ given by $x \cup y$ and $x \cap y$, respectively.
  - » It is distributive since $x \cup (y \cap z) = (x \cup y) \cap (x \cup z)$ and $x \cap (y \cup z) = (x \cap y) \cup (x \cap z)$
  - » It is complemented since x and $A - x$ are complements

- *Definition:* A **switching algebra** is a Boolean algebra whose carrier consists of two elements. This is the Boolean algebra with which you are probably already familiar:
  - » Carrier $B = \{0,1\}$
  - » Relation $\leq = \{(0,0),(0,1),(1,1)\}$
  - » Join: $0+0=0$, $0+1=1+0=1$, $1+1=1$
  - » Meet: $0 \cdot 0=0$, $0 \cdot 1=1 \cdot 0=0$, $1 \cdot 1=1$

Ex13:

Properties of Boolean Algebras

- *Theorem*: Complementation in a Boolean algebra is unique
  Proof: Suppose both x' and y are complements of x. Then, $x+x'=x+y=\mathbf{1}$ and $xx'=xy=0$. It follows that

$$y = y(x + x') = yx + yx' = yx' = x'y + x'x = x'(y + x) = x' \qquad (1)$$

- *Theorem*: In a Boolean algebra, $(x')'=x$
  Proof: By the definition of complement, $xx'=\mathbf{0}$ and $x+x'=\mathbf{1}$. Both meet and join are commutative, so $x'x=\mathbf{0}$ and $x'+x=\mathbf{1}$. So x is the complement of x'.

- *Theorem*: In a Boolean algebra,

$$x + x'y = x + y \qquad (2)$$
$$x(x' + y) = xy \qquad (3)$$

Proof: From the absorptive property of all lattices, $x+x'y = x+xy+x'y = x+(x+x')y = x+y$. The other equality follows from the principle of duality.

Ex14:

- The sum-of-products form for our function is: `F(x,y,z) = xz'+ y`

`F(x,y,z) = (x'yz')+(x'yz)+(xy'z')+(xyz')+(xyz)`

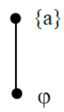
x	y	z	xz' + y
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	1

We note that this function is not in simplest terms. Our aim is only to rewrite our function in canonical sum-of-products form.

Ex15:

Definition: A **lattice** is a partially ordered set (L,) in which every subset {a, b} consisting of **two element** has a **least upper bound** and a **greatest lower bound.**

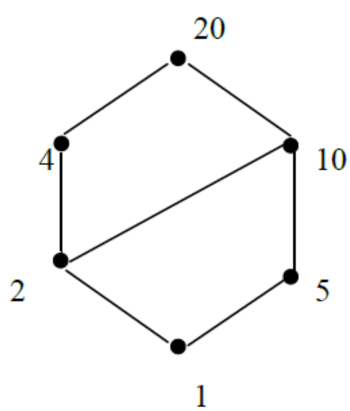
We denote lub({a, b}) by $a \wedge b$ and call it **join** or **sum of a and b.** Similarly, we denote GLB({a, b}) by $a \vee b$ and call it **meet** or **product of a and b.**
Thus **Lattice is** a mathematical structure with **two binary operations, join and meet.** Lattice structures often appear in computing and mathematical applications.
A totally ordered set is obviously a lattice but not all partially ordered sets are lattices.
Example 1. **Let A be any set and P(A) be its power set. The partially ordered set (P(A),) is a lattice in which the meet and join are the same as the operations and respectively. If A has single element, say a, then P(A) = { , {a}} and**
LUB({ , {a}) = {a}
GLB({ , {a}) =
The Hasse diagram of (P(A),) is a chain containing two elements and {a} as shown below:



If A has two elements, say a and b. Then P(A) = { , {a}, {b}, {a, b}}. The Hasse diagram of {P(A),) is then as shown below :

Example 3. Let n be a positive integer and let D_n be the set of all positive divisors of n. Then D_n is a lattice under the relation of divisibility. The Hasse diagram of the lattices D_8, D_{20} and D_{30} are respectively

$D_8 = \{1, 2, 4, 8\}$



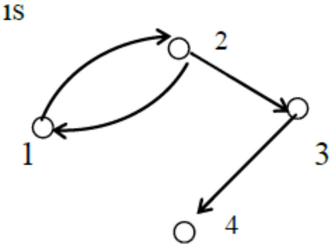
$D_{20} = \{1, 2, 4, 5, 10, 20\}$

1.18. The Transitive Closure of a Relation

Definition: The **Transitive closure** of a relation R is the smallest transitive relation containing R. It is denoted by R^{∞}.

Example: Let A = {1, 2, 3, 4} and R = [(1, 2), (2, 3), (3, 4), (2, 1)] Find the transitive closure of R.

Solution: The digraph of R is



We note that from vertex 1, we have paths to the vertices 2, 3, 4 and 1. Note that path from 1 to 1proceeds from 1 to 2 to 1. Thus we see that the ordered pairs (1, 1), (1, 2), (1, 3) and (1, 4) are in R^{∞}. Starting from vertex 2, we have paths to vertices 2, 1, 3 and 4 so the ordered pairs (2, 1), (2, 2), (2, 3) and (2, 4) are in R^{∞}. The only other path is from vertex 3 to 4, so we have

R^{∞} = {(1, 1), (1, 2), (1, 3), (1, 4), (2, 1), (2, 2), (2, 3), (2, 4), (3,4)}

Definition: Let (L, ≤) be a poset and let (L, ≥) be the dual poset. If (L, ≤) is a lattice, we can show that (L, ≥) is also a lattice. In fact, for any a and b in L, the L U B of a and b in (L, ≤) is equal to the GLB of a and b in (L, ≥). Similarly, the GLB of a and b in (L, ≤) is equal to L U B in (L, ≥).

1.19. Cartesian Product of Lattices

Theorem: If $(L_1, \leq)$ and $(L_2, \leq)$ are lattices, then $(L, \leq)$ is a lattice, where $L = L_1 \times L_2$ and the partial order $\leq$ of L is the product partial order.

Proof: **We denote the join and meet in L_1 by $\vee_1$, and $\wedge_1$ and the join and meet in L_2 by $\vee_2$ and $\wedge_2$ respectively. We know that Cartesian product of two posets is a poset. Therefore $L = L_1 \times L_2$ is a poset. Thus all we need to show is that if (a_1, b_1) and $(a_2, b_2) \in L$, then $(a_1, b_1) \vee (a_2, b_2)$and $(a_1, b_1) \wedge (a_2, b_2)$ exist in L.**

Further, we know that

$$(a_1, b_1) \vee (a_2, b_2) = (a_1 \vee_1 a_2,\ b_1 \vee_2 b_2)$$

and

$$(a_1, b_1) \wedge (a_2, b_2) = (a_1 \wedge_1 a_2,\ b_1 \wedge_2 b_2)$$

Since L_1 is lattice, $a_1 \vee_1 a_2$ and $a_1 \wedge_1 a_2$ exist. Similarly, since L_2 is a lattice, $b_1 \vee_2 b_2$ and $b_1 \wedge_2 b_2$ exist. Hence $(a_1, b_1) \vee (a_2, b_2)$ and $(a_1, b_1) \wedge (a_2, b_2)$ both exist and therefore $(L, \leq)$ is a lattice, called **the direct product of $(L_1, \leq)$ and $(L_2, \leq)$.**

Theorem : Let $(L, \leq)$ be a lattice and let $a, b, c \in L$. Then we have

L_1 : **Idempotent property**

(i) $a \vee a = a$
(ii) $a \wedge a = a$

L_2 : **Commutative property**

(i) $a \vee b = b \vee a$
(ii) $a \wedge b = b \wedge a$

L_3 : **Associative property**

(i) $a \vee (b \vee c) = (a \vee b) \vee c$
(ii) $a \wedge (b \wedge c) = (a \wedge b) \wedge c$

L_4 : **Absorption property**

(i) $a \vee (a \wedge b) = a$

(ii) $a \wedge (a \vee b) = a$

Proof: L_1 : The idempotent property follows from the definition of LUB and GLB.

L_2 : Commutativity follows from the symmetry of a and b in the definition of LUB and GLB.

L_3 : (i) From the definition of LUB, we have

$$a \le a \vee (b \vee c) \qquad (1)$$

$$b \vee c \le a \vee (b \vee c) \qquad (2)$$

Also $b \le b \vee c$ and $c \le b \vee c$ and so transitivity implies

$$b \le a \vee (b \vee c) \qquad (3)$$

and

$$c \le a \vee (b \vee c) \qquad (4)$$

Now, (1) and (3) imply that $a \vee (b \vee c)$ is an upper bound of a and b and hence by the definition of least upper bound, we have

$$a \vee b \le a \vee (b \vee c) \qquad (5)$$

Also by (4) and (5), $a \vee (b \vee c)$ is an upper bound of c and $a \vee b$. Therefore

$$(a \vee b) \vee c \le a \vee (b \vee c) \qquad (6)$$

Similarly

$$a \vee (b \vee c) \le (a \vee b) \vee c \qquad (7)$$

Hence, by antisymmetry of the relation $\le$, (6) and (7) yield

$$a \vee (b \vee c) = (a \vee b) \vee c$$

The proof of (ii) is analogous to the proof of part (i).

L_4 : (i) Since $a \wedge b \le a$ and $a \le a$, it follows that a is an upper bound of $a \wedge b$ and a. Therefore, by the definition of least upper bound

$$a \vee (a \wedge b) \le a \qquad (8)$$

On the other hand, by the definition of LUB, we have

$$a \le a \vee (a \wedge b) \qquad (9)$$

The expression (8) and (9) yields

$$a \vee (a \wedge b) = a.$$

(ii) Since $a \leq a \vee b$ and $a \leq a$, it follows that a is a lower bound of $a \vee b$ and a. Therefore, by the definition of GLB,

$$a \leq a \wedge (a \vee b) \qquad (10)$$

Also, by the definition of GLB, we have

$$a \wedge (a \vee b) \leq a \qquad (11)$$

Then (10) and (11) imply

$$a \wedge (a \vee b) = a$$

and the proof is completed.

In view of L_3, we can write $a \vee (b \vee c)$ and $(a \vee b) \vee c$ as $a \vee b \vee c$. Thus, we can express

LUB ($\{a_1, a_2, \ldots. a_n\}$) as $a_1 \vee a_2 \vee \ldots\ldots \vee a_n$

GLB ($\{a_1, a_2, \ldots. a_n\}$) as $a_1 \wedge a_2 \wedge \ldots\ldots \wedge a_n$

Remark: Using commutativity and absorption property, part (ii) of previous Theorem can be proved as follows :

Let $a \wedge b = a$. We note that

$$b \vee (a \wedge b) = b \vee a$$
$$= a \vee b \text{ (Commutativity)}$$

But

$$b \vee (a \wedge b) = b \quad \text{(Absorption property)}$$

Hence

$$a \vee b = b$$

and so by part (i), $a \leq b$. Hence $a \wedge b = a$ if and only if $a \leq b$.

Theorem: Let $(L, \leq)$ be a lattice. Then for any $a, b, c \in L$, the following properties hold :

1. (**Isotonicity**) **:** If $a \leq b$, then

   (i) $a \vee c \leq b \vee c$

   (ii) $a \wedge c \leq b \wedge c$

This property is called "Isotonicity".

2. $a \leq c$ and $b \leq c$ if and only if $a \vee b \leq c$

3. $c \leq a$ and $c \leq b$ if and only if $c \leq a \wedge b$

4. If $a \leq b$ and $c \leq d$, then

   (i) $a \vee c \leq b \vee d$

   (ii) $a \wedge c \leq b \wedge d$.

Proof : 1 (i). We know that

$$a \vee b = b \text{ if and only if } a \leq b.$$

Therefore, to show that $a \vee c \leq b \vee c$, we shall show that

$$(a \vee c) \vee (b \vee c) = b \vee c.$$

We note that

$$\begin{aligned}(a \vee c) \vee (b \vee c) &= [(a \vee c) \vee b] \vee c \\ &= a \vee (c \vee b) \vee c \\ &= a \vee (b \vee c) \vee c \\ &= (a \vee b) \vee (b \vee c) \\ &= b \vee c \quad (\because a \vee b = b \text{ and } c \vee c = c)\end{aligned}$$

The part 1 (ii) can be proved similarly.

2. If $a \leq c$, then 1(i) implies

$$a \vee b \leq c \vee b$$

But

$$b \leq c \Leftrightarrow b \vee c = c$$

$$\Leftrightarrow c \vee b = c \quad \text{(commutativity)}$$

Hence $a \leq c$ and $b \leq c$ if and only if $a \vee b \leq c$

3. If $c \leq a$, then 1(ii) implies

$$c \wedge b \leq a \wedge b$$

But

$$c \leq b \Leftrightarrow c \wedge b = c$$

Hence $c \leq a$ and $c \leq b$ if and only if $c \leq a \wedge b$.

4 (i) We note that 1(i) implies that

if $a \leq b$, then $a \vee c \leq b \vee c = c \vee b$

if $c \leq d$, then $c \vee b \leq d \vee b = b \vee d$

Hence, by transitivity

$$a \vee c \leq b \vee d$$

(ii) We note that 1(ii) implies that

if $a \leq b$, then $a \wedge c \leq b \wedge c = c \wedge b$

if $c \leq d$, then $c \wedge b \leq d \wedge b = b \wedge d$.

Therefore transitivity implies

$$a \wedge c \leq b \wedge d.$$

Theorem: Let $(L, \leq)$ be a lattice. If $a, b, c \in L$, then

(1) $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$

(2) $a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$

These inequalities are called "Distributive Inequalities".

Proof: We have

$$a \leq a \vee b \quad \text{and} \quad a \leq a \vee c \qquad \text{(i)}$$

Also, by the above theorem, if $x \leq y$ and $x \leq z$ in a lattice, then $x \leq y \wedge z$. Therefore (i) yields

$$a \leq (a \vee b) \wedge (a \vee c) \qquad \text{(ii)}$$

Also

$$b \wedge c \leq b \leq a \vee b$$

and

$$b \wedge c \leq c \leq a \vee c ,$$

that is, $b \wedge c \leq a \vee b$ and $b \wedge c \leq a \vee c$ and so, by the above argument, we have

$$b \wedge c \leq (a \vee b) \wedge (a \vee c) \qquad \text{(iii)}$$

Also, again by the above theorem if $x \leq z$ and $y \leq z$ in a lattice, then

$$x \vee y \leq z$$

Hence, (ii) and (iii) yield

$$a\, c\, (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$$

This proves (1).

The second distributive inequality follows by using the **principle of duality.**

Theorem: (Modular Inequality) : Let $(L, \leq)$ be a lattice. If $a, b, c \in L$, then

$$a \leq c \text{ if and only if } a \vee (b \wedge c) \leq (a \vee b) \wedge c$$

Proof: We know that

$$a \leq c \Leftrightarrow a \vee c = c \qquad (1)$$

Also, by distributive inequality,

$$a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$$

Therefore using (1) $a \leq c$ if and only if

$$a \vee (b \wedge c) \leq (a \vee c) \wedge c,$$

which proves the result.

The modular inequalities can be expressed in the following way also:

$$(a \wedge b) \vee (a \wedge c) \leq a \wedge [b \vee (a \wedge c)]$$

$$(a \vee b) \wedge (a \vee c) \geq a \vee [b \wedge (a \vee c)]$$

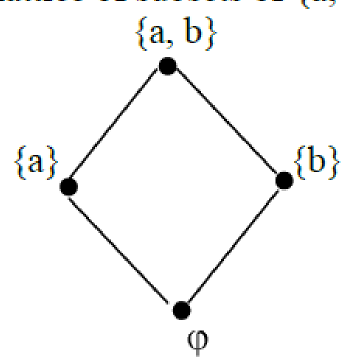
Example: Let Ĉ be collection of sets with binary operations Union and Intersection of sets. Then (Ĉ, $\cup$, $\cap$) is a lattice. In this lattice, the partial order relation is **set inclusion.** In fact, for A, B $\in$ Ĉ,

$$\mathbf{A \subseteq B \text{ iff } A \cup B = B}$$

Or

$$A \subseteq B \text{ iff } A \cap B = A.$$

For example, the diagram of lattice of subsets of {a, b} is



Sublattices:

Definition: Let $(L, \leq)$ be a lattice. A non-empty subset S of L is called a **sublattice** of L if $a \vee b \in S$ and $a \wedge b \in S$ whenever $a \in S$, $b \in S$.

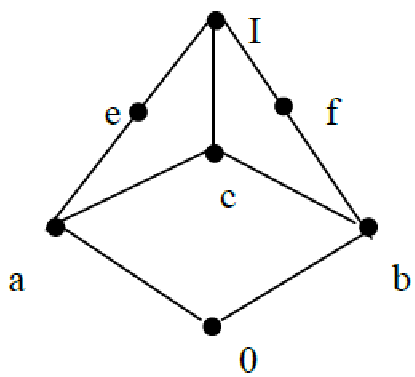
Or

Let $(L, \vee, \wedge)$ be a lattice and let $S \subseteq L$ be a subset of L. Then $(S, \vee, \wedge)$ is called a sublattice of $(L, \vee, \wedge)$ if and only if S is closed under both operations of join($\vee$) and meet($\wedge$).

From the definition it is clear that **sublattice itself is a lattice.**

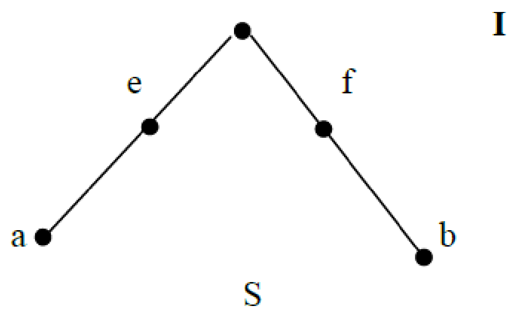
However, **any subset of L which is a lattice need not be a sublattice.**

For example, consider the lattice shown in the diagram:

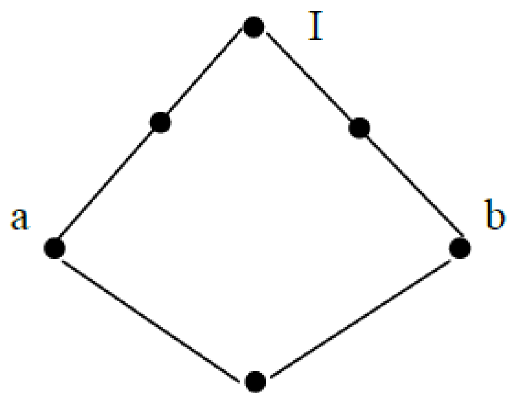


We note that

(i) the subset S shown by the diagram below is not a sublattice of L, since $a \wedge b \notin S$ and $a \vee b \notin S$.



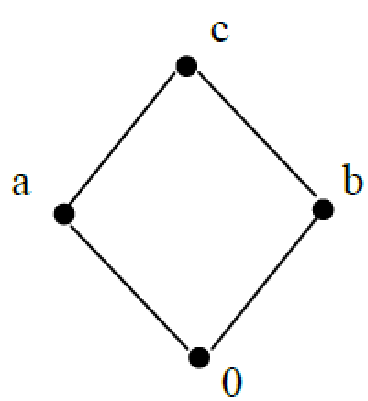
(ii) the set T shown below is not a sublattice of L since $a \vee b \notin T$.



T

However, T is a lattice when considered as a poset by itself.

(iii) the subset $\cup$ of L shown below is a sublattice of L:



U

Lattice Homomorphism:

Definition: Let $(L_1, \vee_1, \wedge_1)$ and $(L_2, \vee_2, \wedge_2)$ be two lattices. A mapping $f : L_1 \to L_2$ is called a **lattice homomorphism** from the lattice the lattice $(L_1, \vee_1, \wedge_1)$ to $(L_2, \vee_2, \wedge_2)$ if for any $a, b \in L_1$,

$$f(a \vee_1 b) = f(a) \vee_2 f(b) \text{ and } f(a \wedge_1 b) = f(a) \wedge_2 f(b)$$

Thus, here both the binary operations of join and meet are preserved. **There may be mapping which preserve only one of the two operations. Such mapping are not lattice homomorphism.**

Let $\leq_1$ and $\leq_2$ be partial order relations on $(L_1, \vee_1, \wedge_1)$ and $(L_2, \vee_2, \wedge_2)$ respectively. Let $f : L_1 \to L_2$ be lattice homomorphism. If $a, b \in L_1$, then

$$a \leq_1 b \Leftrightarrow a \vee_1 b = b$$

and so

$$\begin{aligned} f(b) &= f(a \vee_1 b) \\ &= f(a) \vee_2 f(b) \\ &\Leftrightarrow f(a) \leq_2 f(b) \end{aligned}$$

Thus

$$a \leq_1 b \Leftrightarrow f(a) \leq_2 f(b)$$

Thus order **relations are also preserved** under lattice homomorphism.

If a lattice homomorphism $f: L_1 \to L_2$ is one-to-one and onto, then it is called **lattice isomorphism.**

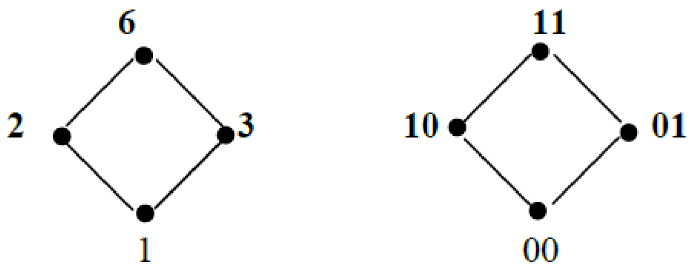
If there exists an isomorphism between two lattices, then the lattices are called **isomorphic**.

Since lattice isomorphism preserves order relation, therefore isomorphic lattices can be represented by the same diagram in which nodes are replaced by images.

Example : **Let $D_6 = \{1, 2, 3, 6\}$, set of divisors of 6. Then D_6 is isomorphic to B_2. In fact $f : D_6 \to B_2$ defined by**

$$f(1) = 00,\ f(2) = 10,\ f(3) = 01,\ f(6) = 11$$

is an isomorphism.



D_6 B_2

Example: Let A = {a, b} and P(A) = {φ, {a}, {a, b}} then the lattice (P(A), ⊆) is isomorphic to the lattice (D_6, 1) with divisibility as the partial order relation. In fact, we define a mapping $f : D_6 \to P(A)$ by

$$f(1) = \varphi,\ f(2) = \{a\},\ f(3) = \{b\},\ f(6) = \{a, b\}\ ,$$

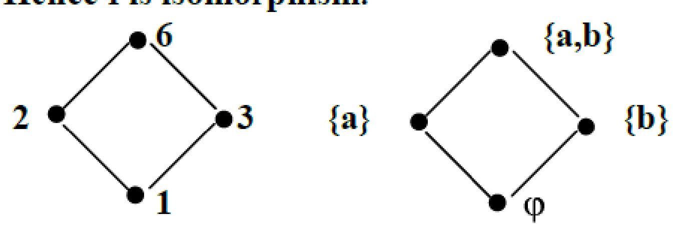
then f is bijective and we note that

$$1|2 \Leftrightarrow \{\varphi\} \subseteq \{a\} \Leftrightarrow f(1) \subseteq f(2)$$

$$2|6 \Leftrightarrow \{a\} \subseteq \{a, b\} \Leftrightarrow f(2) \subseteq f(6)$$

and so on.

Hence f is isomorphism.



D_6 **P ({a, b})**

Definition: **Let (L, ∧,∨) be a lattice. Then lattice homomorphism f : L L is called an** endomorphism.

Definition: **Let (L, ∧,∨) be lattice. Then the lattice isomorphism f: L L is called an** automorphism.

1.26 Bounded, Complemented and Distributive Lattices

Definition: **A lattice L is said to be** bounded **if it has a greatest element I and a least element 0.**

For the lattice (L, $\vee$, $\wedge$) with L = $\{a_1, a_2, \ldots, a_n\}$,

$$a_1 \vee a_2 \vee \ldots \vee a_n = I \text{ and } a_1 \wedge a_2 \wedge \ldots \wedge a_n = 0.$$

Example : **The lattice** Z^+ **of all positive integers under partial order of divisibility** is not a bounded lattice **since it has a least element (the integer 1) but no** greatest element.

Example: **The lattice** Z **of integers under partial order $\leq$ (less than or equal to) is** not bounded since it has neither a greatest element nor a least element.

Example: **Let A be a non-empty set. Then the lattice (P(A), $\subseteq$)** is bounded. **Its greatest element is A and the least element is empty set ϕ.**

If (L, $\leq$) is a bounded Lattice, then for all a $\in$ L

$$0 \leq a \leq I$$

$$a \vee 0 = a, \; a \wedge 0 = 0$$

$$a \vee I = I, \; a \wedge I = a$$

Thus 0 acts as identity of the operation $\vee$ and I acts as identity of the operation $\wedge$.

Definition: **Let (L $\vee$, $\wedge$, 0, I) be a bounded lattice with greatest element I and the least element 0. Let a $\in$ L. Then an element b $\in$ L is called a** complement **of a if**

$$a \vee b = I \text{ and } a \wedge b = 0$$

Definition: **A lattice (L, $\vee$, $\wedge$, 1, 0) is called** complemented **if it is bounded and if every element of L has at least one complement.**

Example: **The lattice (P(A), $\subseteq$) of the power set of any set A is a bounded lattice, where meet and join operations on e(A) are $\cap$ and $\cup$ respectively. Its bounds are φ and A. The lattice (P(A), $\subseteq$) is complemented in which the complement of any subset B of A is A – b.**

Definition: **A lattice (L, $\vee$, $\wedge$) is called a** distributive lattice **if for any elements a, b and c in L,**

$$(1)\ a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$
$$(2)\ a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

Properties (1) and (2) are called distributive properties.

Thus, in a distributive lattice, the operations $\wedge$ and $\vee$ are distributive over each other.

We further note that, by the principle of duality, the condition (1) holds if and only if (2) holds. Therefore it is sufficient to verify any one of these two equalities for all possible combinations of the elements of a lattice.

If a lattice L is not distributive, we say that L is non-distributive.

Example: **For a set S, the lattice (P(S), $\subseteq$) is distributive. The meet and join operation in P(S) are $\cap$ and $\cup$ respectively. Also we know, by set theory, that for A, B, C $\in$ P(S),**

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Theorem: **Every chain is a distributive lattice.**

Proof: **Let $(L, \leq)$ be a chain and $a, b, c \in L$. We shall show that distributive law holds for any $a, b, c \in L$. Two cases arise :**

Case 1. **Let $a \leq b$ or $a \leq c$. In this case**

$$a \wedge (b \vee c) = a$$

and

$$(a \wedge b) \vee (a \wedge c) = a$$

and hence

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

Also, by Principle of Duality

$$a \wedge (b \vee c) = (a \vee b) \wedge (a \vee c)$$

Case II. **Let $b \leq a$ or $c \leq a$. Then we have**

$$a \wedge (b \vee c) = (b \vee c)$$

and

$$(a \wedge b) \vee (a \wedge c) = (b \vee c)$$

Hence

$$a \wedge (b \vee c) = (b \vee c)$$

Hence distributive law holds for any $a, b, c \in L$.

Boolean Algebra:

Definition: A non-empty set B with two binary operations $\vee$ and $\wedge$, a unary operation $'$, and two distinct elements 0 and I is called a **Boolean Algebra** if the following axioms holds for any elements a, b, c $\in$ B:

[B_1]: **Commutative Laws:**

$$a \vee b = b \vee a \qquad \text{and} \qquad a \wedge b = b \wedge a$$

[B_2]: **Distributive Law:**

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \text{ and } a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

[B_3]: **Identity Laws:**

$$a \vee 0 = a \qquad \text{and} \qquad a \wedge I = a$$

[B_4]: **Complement Laws:**

$$a \vee a' = I \qquad \text{and} \qquad a \wedge a' = 0$$

We shall call 0 as zero element, 1 as unit element and a' the complement of a.

We denote a Boolean Algebra by (B, $\vee$, $\wedge$, ~, 0, I).

Example 1. Let A be a non-empty set and P(A) be its power set. Then the set algebra (P(A), $\cup$, $\cap$, $-$, ϕ, A) is a Boolean algebra.

Example 4. The poset D_{30} = {1, 2, 3, 5, 6, 10, 15, 30} has eight element. Define $\vee$, $\wedge$ and $'$ on D_{30} by

$$a \vee b = \mathrm{lcm}(a, b)\ , \quad a \wedge b = \gcd(a, b) \qquad \text{and} \qquad a' = \frac{30}{a}.$$

Then D_{30} is a Boolean Algebra with 1 as the zero element and 30 as the unit element.

Example 5: Let S be the set of statement formulas involving n statement variables. The algebraic system (S, $\wedge$, $\vee$, ~, F, T) is a Boolean algebra in which $\wedge, \vee$, ~ denotes the operations of conjunction, disjunction and negation respectively. The element F and T denotes the formulas which are contradictions and Tautologies respectively. The partial ordering corresponding to $\wedge$, $\vee$ is implication $\Rightarrow$.

Example 3 : Let B_n be the set of n tuples whose members are either 0 or 1. Let $a = (a_1, a_2, \ldots, a_n)$ and $b = (b_1, b_2, \ldots, b_n)$ be any two members of B_n. Then we define

$$a \vee_1 b = (a_1 \vee b_1, a_2 \vee b_2, \ldots, a_n \vee b_n)$$

$$a \wedge_1 b = (a_1 \wedge b_1, a_2 \wedge b_2, \ldots, a_n \wedge b_n) ,$$

where $\vee$ and $\wedge$ are logical operations on $\{0, 1\}$, and

$$a' = (\sim a_1, \sim a_2, \ldots, \sim a_n) ,$$

where $\sim 0 = 1$ and $\sim 1 = 0$.

If 0_n represents $(0, 0, \ldots, 0)$ and $1_n = (1, 1, \ldots, 1)$, then $(B_n, \vee_1, \wedge_1, ', 0_n, 1_n)$ is a Boolean algebra.

This algebra is known as Switching Algebra and represents a switching network with n inputs and one output.

Definition: A finite lattice is called a **Boolean Algebra** if it is isomorphic with B_n for some non-negative integer n.

For example, D_{30} is isomorphic to B_3. In fact, the mapping f: $D_{30} \rightarrow B_3$ defined by

$$f(1) = 000, \quad f(2) = 100, \quad f(3) = 010, \quad f(5) = 001,$$

$$f(6) = 110, \quad f(10) = 101, \quad f(15) = 011, \quad f(30) = 111$$

Is an isomorphism. Hence D30 is a Boolean algebra.

If a finite L does not contain 2^n elements for some non-negative integer n, then L cannot be a Boolean Algebra.

For example, consider $D_{20} = \{1, 2, 4, 5, 10, 20\}$ that has 6 elements and $6 \neq 2^n$ for any integer $n \geq 0$. Therefore, D_{20} is not a Boolean algebra.

If | L | = 2^n, then L may or not be a Boolean Algebra. If L is isomorphic to B_n, then it is Boolean algebra, otherwise it is not.

For large value of n, we use the following theorem for determining whether D_n is a Boolean Algebra or not.

Duality: The **dual of any statement** in a Boolean algebra B is obtained **by interchanging** $\vee$ and $\wedge$ and interchanging the zero element and unit element in the original statement.

For example, the dual of $a \wedge 0 = 0$ is $a \wedge I = I$

Principle of duality: The dual of any theorem in a Boolean Algebra is also a theorem.
(Thus, dual theorem is proved by using the **dual of each step of the proof of the original statement).**

Properties of Boolean algebra:

Theorem: Let a, b and c be any elements in a Boolean algebra $(B, \vee, \wedge, ', 0, I)$. Then

1. Idempotent Laws:

(i) $a \vee a = a$ (ii) $a \wedge a = a$

2. Boundedness Laws:

(i) $a \vee I = I$ (ii) $a \wedge 0 = 0$

3. Absorption Laws:

(i) $a \vee (a \wedge b) = a$ (ii) $a \wedge (a \vee b) = a$

4. Associative Laws:

(i) $(a \vee b) \vee c = a \vee (b \vee c)$ (ii) $(a \wedge b) \wedge c = a \wedge (b \wedge c)$