

# Partial Orderings, Lattices, and Boolean Algebra

# Partial Orderings

## ■ Definition:

A binary relation  $R$  on a set is called a **partial ordering** if it is **reflexive**, **antisymmetric**, and **transitive**.

## Example:

- “refines” is a partial ordering on the set of all the partitions.

## ■ Notation:

$\leq$  is used as a **generic symbol** for partial ordering.

E.g., let  $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$ .

Consider “divides” relation on  $A$ :  $x$  divides  $y$  if  $x$  is a factor of  $y$ .

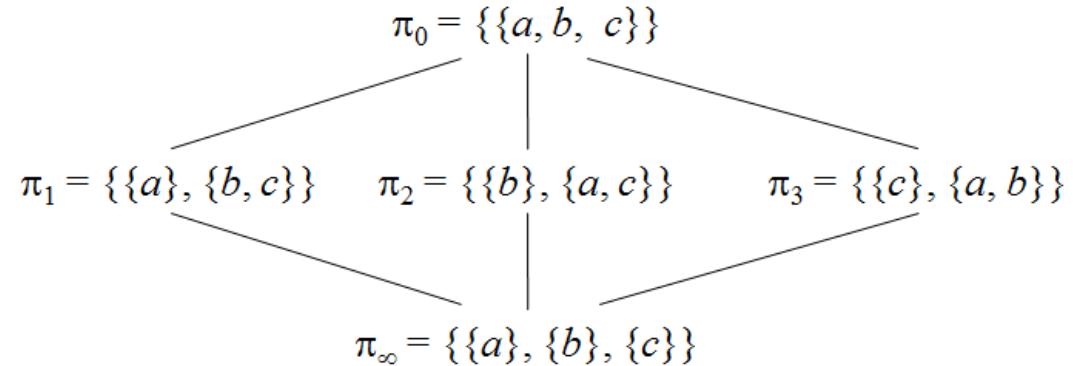
→  $2 \leq 6$  and  $3 \leq 6$  are true but  $5 \leq 6$  is not true.

## ■ Definition:

When  $R$  is a partial ordering on a set  $A$ , the pair  $(A, R)$  is called a **partially ordered set** or a **poset**.

## ■ Examples of posets:

- $(\mathbf{R}, \leq)$
- (the set of all the partitions, refines)
- $(\mathbf{Z}^+, \text{divides})$
- $(\wp(A), \subseteq)$



## ■ Theorem:

If  $R$  is a partial ordering on a set  $A$ , then  $R^c$  is also a partial ordering on  $A$ .

## ■ Definition:

Let  $R$  be a partial ordering on a set  $A$  and let  $X \subseteq A$ . The restriction of  $R$  on  $X$ , denoted  $R/X$ , is defined by

$$R/X = \{(x, y) \mid x \in X \wedge y \in X \wedge (x, y) \in R\}$$

### Example:

$$A = \mathbf{Z}^+ \quad X = \{1, 2, 3, 4, 5, 6, 7\}$$

□ divides/ $X = \{(1, 1), (1, 2), \dots, (1, 7), (2, 2), (2, 4), (2, 6), (3, 3), (3, 6), (4, 4), (5, 5), (6, 6), (7, 7)\}$

## ■ Theorem:

Let  $R$  be a partial ordering on a set  $A$  and let  $X \subseteq A$ . Then  $R/X$  is a partial ordering on  $X$ .

## ■ Definition:

Let  $R$  be a partial ordering on a set  $A$ . If  $a, b \in A$  are such that either  $(a, b) \in R$  or  $(b, a) \in R$  then  $a$  and  $b$  are said to be **comparable**.

### Example:

$$A = \{a, b, c\} \quad R = \{(a, a), (b, b), (c, c), (a, b)\}$$

- $a$  and  $b$  are comparable.
- $a$  and  $c$  are not comparable.  $b$  and  $c$  are not comparable.

## ■ Definition:

Let  $R$  be a partial ordering on a set  $A$  such that every pair  $a, b \in A$  is comparable. Then  $R$  is said to be a **linear ordering (total ordering)** and  $(A, R)$  is said to be a **linearly ordered set (totally ordered set)** or a **chain**.

## ■ Definition:

A relation  $R$  on a set  $A$  is called a **strict partial ordering** if it is irreflexive, asymmetric, and transitive.

### Example:

$$A = \{a, b, c\} \quad R = \{(a, a), (b, b), (c, c), (a, b)\}$$

□  $R' = \{(a, b)\}$  is a strict partial ordering

- Notation:

- < is used as a generic symbol for strict partial ordering.

$$< = \{(x, y) \mid (x, y) \in \leq \wedge x \neq y\} = \leq - E_A$$

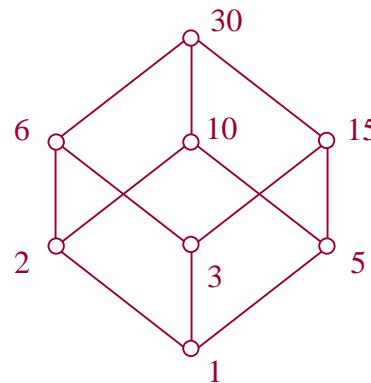
- Definition:

- Let < be a strict partial ordering on a set A. Then the covers relation with respect to < on A, denoted by  $\text{covers}_<$ , is defined as follows:

$$\text{covers}_< = \{(x, y) \mid y < x \text{ and there is no } z \text{ such that } y < z \text{ and } z < x\}$$

## Example:

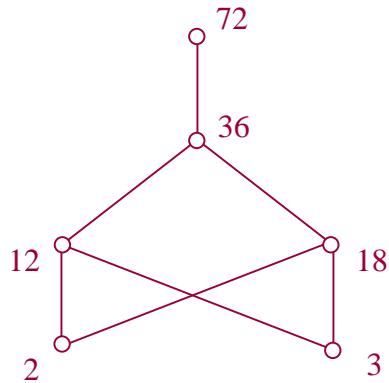
- “divides” relation on  $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$
- $\leq = \leq - E_A$   
 $= \{(1, 2), \dots, (1, 30), (2, 6), (2, 10), (2, 30), (3, 6), (3, 15), (3, 30), (5, 10), (5, 15), (5, 30), (6, 30), (10, 30), (15, 30)\}$
- $covers_{\leq} = \{(30, 15), (30, 10), (30, 6), (15, 5), (15, 3), (10, 5), (10, 2), (6, 3), (6, 2), (5, 1), (3, 1), (2, 1)\}$



Hasse Diagram

## Example:

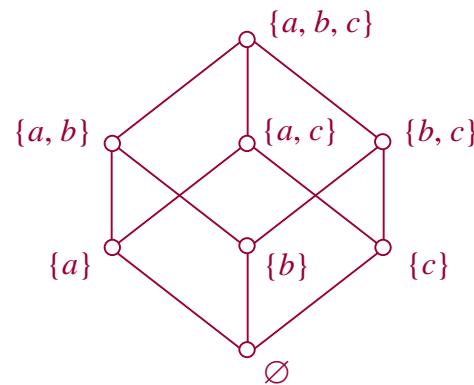
- “divides” relation on  $A = \{2, 3, 12, 18, 36, 72\}$
- $\leq = \{(2, 12), (2, 18), (2, 36), (2, 72), (3, 12), (3, 18), (3, 36), (3, 72), (12, 36), (12, 72), (18, 36), (18, 72), (36, 72)\}$
- $\text{covers}_{\leq} = \{(72, 36), (36, 18), (36, 12), (18, 3), (18, 2), (12, 3), (12, 2)\}$



We can restore  $\leq$  from the Hasse diagram.

## Example:

- $(\wp(A), \subseteq)$  where  $A = \{a, b, c\}$
- $\text{covers}_< = \{(\{a, b, c\}, \{a, b\}), (\{a, b, c\}, \{a, c\}), (\{a, b, c\}, \{b, c\}),$   
 $(\{a, b\}, \{a\}), (\{a, b\}, \{b\}), (\{a, c\}, \{a\}), (\{a, c\}, \{c\}),$   
 $(\{b, c\}, \{b\}), (\{b, c\}, \{c\}), (\{a\}, \emptyset), (\{b\}, \emptyset), (\{c\}, \emptyset)\}$



## Example:

- “less than or equal to” relation on  $A = \{1, 2, 3, 4, 5\}$
- This relation is a linear ordering.
- The poset is called a linearly ordered set, totally ordered set, or chain.

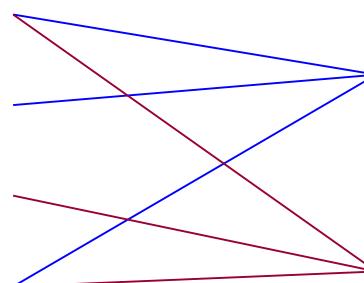


## Example:

□ Consider the Identity relation  $E_A$  on  $A = \{a, b, c\}$

□ This relation is

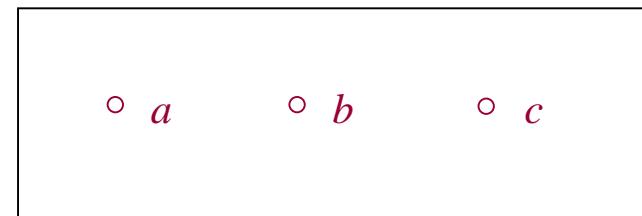
- reflexive
- symmetric
- antisymmetric
- transitive



equivalence relation

partial ordering

Hasse diagram of  $E_A$ :



# Bounds

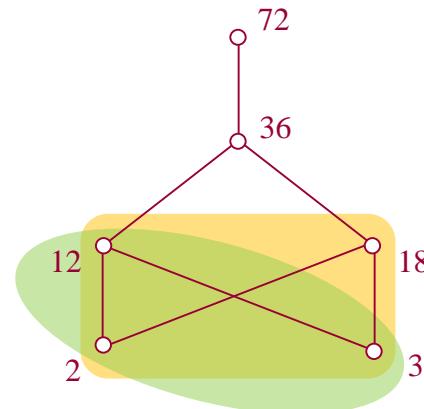
## ■ Definition:

Let  $(A, \leq)$  be a poset and let  $X \subseteq A$ . Then,

- $a \in X$  is the **greatest element** of  $X$  if  $x \leq a$  for every  $x \in X$ .
- $a \in X$  is the **least element** of  $X$  if  $a \leq x$  for every  $x \in X$ .
- $a \in X$  is the **maximal element** of  $X$  if there is no  $x \in X$  such that  $a < x$ .
- $a \in X$  is the **minimal element** of  $X$  if there is no  $x \in X$  such that  $x < a$ .

## Example:

- “divides” relation on  $A = \{2, 3, 12, 18, 36, 72\}$
- $X_1 = \{2, 3, 12\}$ 
  - greatest element of  $X_1$ : 12
  - least element of  $X_1$ : none
- $X_2 = \{2, 3, 12, 18\}$ 
  - greatest element of  $X_2$ : none
  - least element of  $X_2$ : none



## ■ Theorem:

Let  $(A, \leq)$  be a poset and let  $X \subseteq A$ . Then the greatest (least) element of  $X$  if it exists is unique.

### *Proof:*

Let there be two elements  $a$  and  $b$  that are the greatest elements of  $X$ .

Then,  $a \leq b$  because  $b$  is the greatest element of  $X$  and  $a \in X$ .

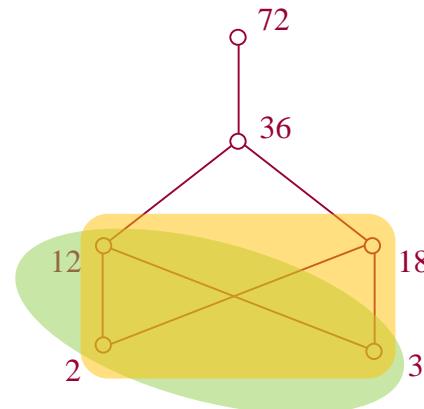
Similarly,  $b \leq a$  because  $a$  is the greatest element of  $X$  and  $b \in X$ .

From  $a \leq b$  and  $b \leq a$ , we conclude  $a = b$  because  $\leq$  is antisymmetric.

□

## Example:

- “divides” relation on  $A = \{2, 3, 12, 18, 36, 72\}$
- $X_1 = \{2, 3, 12\}$ 
  - maximal element of  $X_1$ : 12
  - minimal element of  $X_1$ : 2, 3
- $X_2 = \{2, 3, 12, 18\}$ 
  - maximal element of  $X_2$ : 12, 18
  - minimal element of  $X_2$ : 2, 3



## ■ Theorem:

Let  $(A, \leq)$  be a poset and let  $X \subseteq A$ . If  $a \in X$  is the unique maximal (minimal) element of  $X$  then  $a$  is the greatest (least) element of  $X$ .

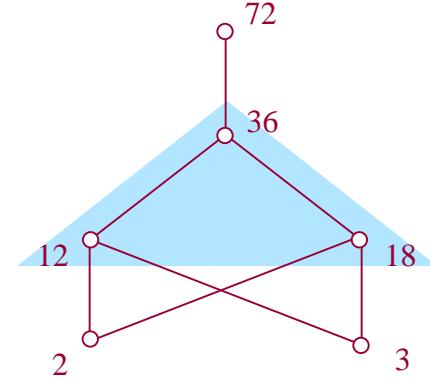
## ■ Definition:

Let  $(A, \leq)$  be a poset and let  $X \subseteq A$ . Then,

- $a \in A$  is the **upper bound** of  $X$  if  $x \leq a$  for every  $x \in X$ .
- $a \in A$  is the **lower bound** of  $X$  if  $a \leq x$  for every  $x \in X$ .

## Example:

- “divides” relation on  $A = \{2, 3, 12, 18, 36, 72\}$
- $X = \{12, 18, 36\}$ 
  - greatest element: 36
  - least element: none
  - maximal element: 36
  - minimal element: 12, 18
  - upper bound: 36, 72
  - lower bound: 2, 3



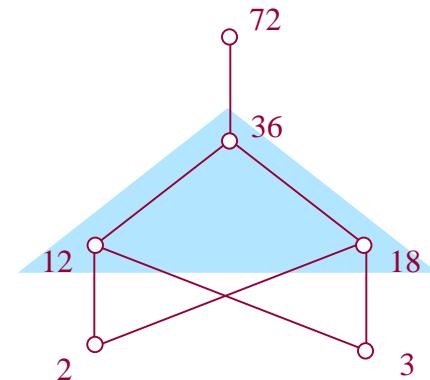
## ■ Definition:

Let  $(A, \leq)$  be a poset and let  $X \subseteq A$ . Then,

- The least element of the set of upper bounds of  $X$  is called the **least upper bound (LUB, supremum)** of  $X$ .
- The greatest element of the set of lower bounds of  $X$  is called the **greatest lower bound (GLB, infimum)** of  $X$ .

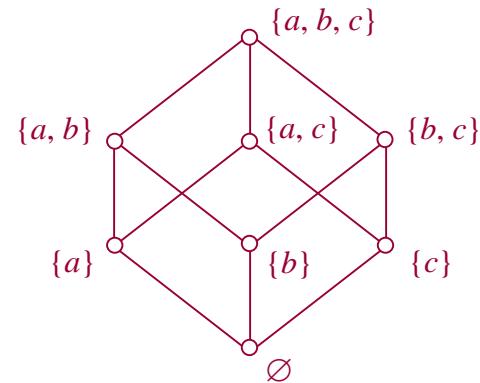
## Example:

- “divides” relation on  $A = \{2, 3, 12, 18, 36, 72\}$
- $X = \{12, 18, 36\}$ 
  - LUB of  $X$ : 36
  - GLB of  $X$ : none



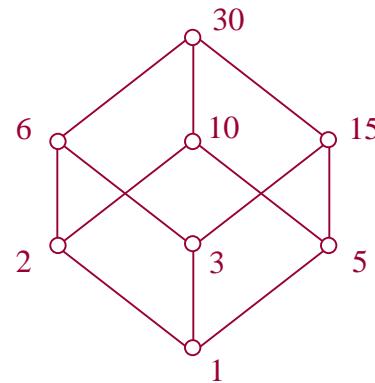
## Example:

- Consider the poset  $(\wp(A), \subseteq)$  where  $A = \{a, b, c\}$ .
- Let  $X_i, X_j \in \wp(A)$ . Then,
  - LUB of  $\{X_i, X_j\} = X_i \cup X_j$
  - GLB of  $\{X_i, X_j\} = X_i \cap X_j$



## Example:

- Consider the poset  $(A, \text{divides})$  where  $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$ .
- Let  $a, b \in A$ . Then,
  - LUB of  $\{a, b\}$  = LCM (Least Common Multiple) of  $a$  and  $b$
  - GLB of  $\{a, b\}$  = GCD (Greatest Common Divisor) of  $a$  and  $b$



# Isomorphism

## ■ Definition:

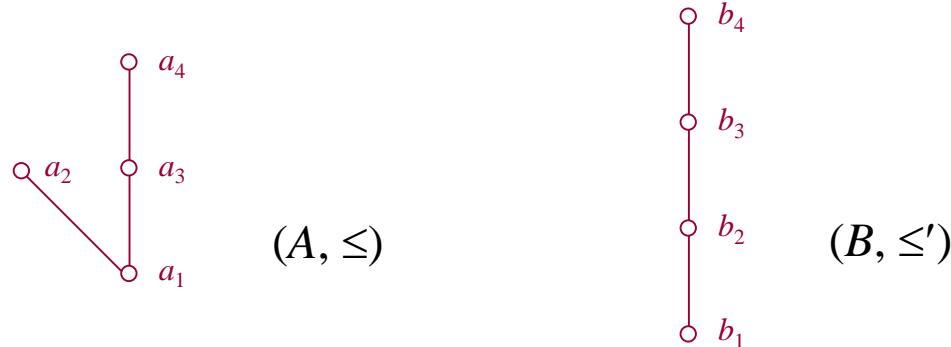
Let  $(A, \leq)$  and  $(B, \leq')$  be two posets and let  $f: A \rightarrow B$ . The function  $f$  is said to be **order preserving** with respect to  $\leq$  and  $\leq'$  if and only if for every  $x, y \in A$  if  $x \leq y$  then  $f(x) \leq' f(y)$ .

## Example:

□  $f: A \rightarrow B$

$$A = \{a_1, a_2, a_3, a_4\}$$

$$B = \{b_1, b_2, b_3, b_4\}$$



□  $f(a_i) = b_i (1 \leq i \leq 4)$  is order preserving.

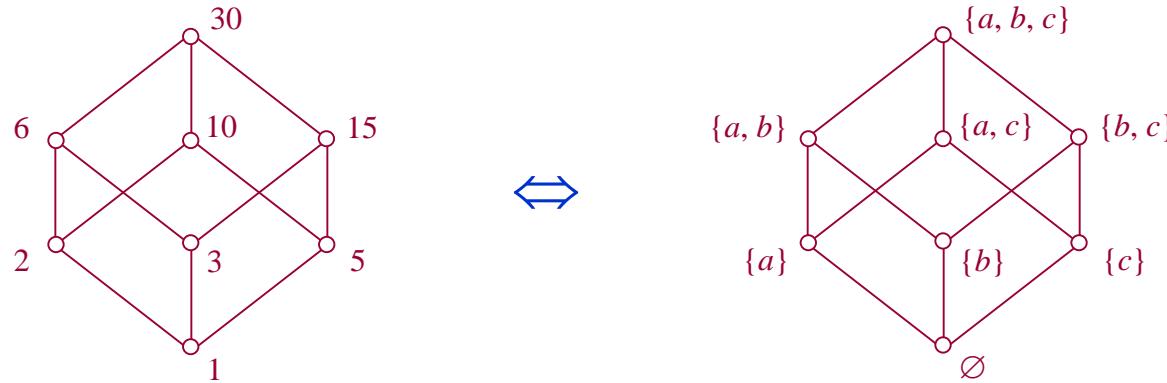
$$a_i \leq a_j \rightarrow f(a_i) = b_i \leq' b_j = f(a_j) \text{ for all } i, j.$$

□  $f^{-1}: B \rightarrow A$  is not order preserving.

## ■ Definition:

Let  $(A, \leq)$  and  $(B, \leq')$  be two posets and let  $f: A \rightarrow B$ . If both  $f$  and  $f^{-1}$  is order preserving, then  $f$  is said to be an **order isomorphism** (or just **isomorphism**) between  $(A, \leq)$  and  $(B, \leq')$  and the posets are said to be **order-isomorphic** (or just **isomorphic**).

## Example:

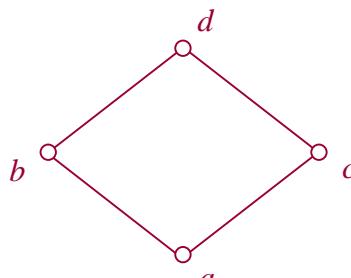


# Lattices

## ■ Definition:

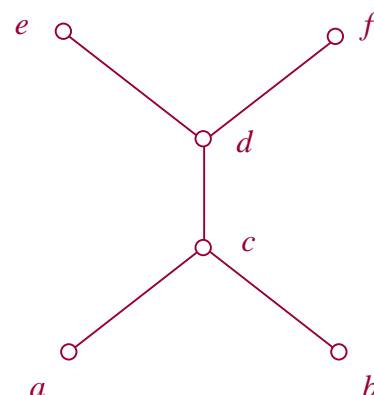
A poset  $(A, \leq)$  is said to be a **lattice** if for every  $a, b \in A$  there is an LUB and a GLB.

## Examples:



Lattice

$$\begin{aligned} \text{GLB}(b, c) &= a & \text{LUB}(b, c) &= d \\ \text{GLB}(a, b) &= a & \text{LUB}(a, b) &= b \end{aligned}$$



Not a lattice



Lattice



Not a lattice  
(identity relation)

- Operation:

- An  $n$ -ary **operation** on a set  $A$  is a function.

$$f : A \times \underbrace{A \times \cdots \times A}_{n} \rightarrow A$$

- Binary operation:

$$f : A \times A \rightarrow A$$

- On a lattice, GLB and LUB are binary operations.

- $\text{GLB}(a, b) = a * b$
    - $\text{LUB}(a, b) = a + b$

## ■ Theorem:

If  $(A, \leq)$  is a lattice, then for any  $x, y \in A$

1.  $x * y = x$  iff  $x \leq y$
2.  $x + y = y$  iff  $x \leq y$

**Proof** of 1:

(if part)

Assume  $x \leq y$ .

Since  $x \leq x$  and  $x \leq y$ ,  $x$  is a lower bound of  $x$  and  $y$ .

We know  $x * y$  is also a lower bound and it is the greatest lower bound.

Thus  $x \leq x * y$ .

### *Proof of 1:*

But  $x * y$  is a lower bound of  $x$  and  $y$ . Thus  $x * y \leq x$ .

From  $x \leq x * y$  and  $x * y \leq x$ , we conclude that  $x * y = x$ .

(only if part)

Assume  $x * y = x$ .

We know  $x * y$  is the greatest lower bound of  $x$  and  $y$ .

Thus  $x * y \leq y$ .

Since  $x * y = x$ , we conclude that  $x \leq y$ .

□

## ■ Theorem:

If  $(A, \leq)$  is a lattice, then for every  $x, y, z \in A$  the following are true:

- |                                |                             |                  |
|--------------------------------|-----------------------------|------------------|
| 1. $x * x = x$                 | $x + x = x$                 | idempotent laws  |
| 2. $x * y = y * x$             | $x + y = y + x$             | commutative laws |
| 3. $x * (y * z) = (x * y) * z$ | $x + (y + z) = (x + y) + z$ | associative laws |
| 4. $x * (x + y) = x$           | $x + (x * y) = x$           | absorption laws  |

### ***Proof of 1:***

Using the previous theorem and the fact that  $x \leq x$ , we can easily show that  $x * x = x$  and  $x + x = x$ .  $\square$

**Proof of 4:**  $x * (x + y) = x$

$x \leq x + y$  because  $x + y$  is the least upper bound of  $x$  and  $y$ .

Again, using the previous theorem,  $x * (x + y) = x$ .  $\square$

■ **Lemma:**

Let  $(A, \leq)$  be a lattice. For every  $x, y, z \in A$ , if  $y \leq z$  then  $x * y \leq x * z$ .

**Proof :**

Note that  $x * z$  is the greatest lower bound of  $x$  and  $z$ .

All we need to show is that  $x * y$  is a lower bound of  $x$  and  $z$ .

Obviously,  $x * y \leq x$ .

Since  $x * y \leq y$  and  $y \leq z$ , we have  $x * y \leq z$ .

Therefore,  $x * y$  is a lower bound of  $x$  and  $z$ .  $\square$

**Proof** of 3:  $x * (y * z) = (x * y) * z$

First we want to prove that  $x * (y * z) \leq (x * y) * z$ .

Note that  $(x * y) * z$  is the greatest lower bound of  $x * y$  and  $z$ .

All we need to show is that  $x * (y * z)$  is a lower bound of  $x * y$  and  $z$ .

Since  $y * z \leq y$ , we get  $x * (y * z) \leq x * y$  by the previous lemma.

From  $x * (y * z) \leq y * z$  and  $y * z \leq z$ , we get  $x * (y * z) \leq z$ .

Therefore,  $x * (y * z)$  is a lower bound of  $x * y$  and  $z$ .

Now, we want to prove that  $(x * y) * z \leq x * (y * z)$ .

Notice that  $(x * y) * z \leq x * y \leq x$ .

Since  $x * y \leq y$ , we get  $(x * y) * z \leq y * z$  by the previous lemma and the commutative law.

**Proof of 3:**  $x * (y * z) = (x * y) * z$

Hence,  $(x * y) * z$  is a lower bound of  $x$  and  $y * z$ .

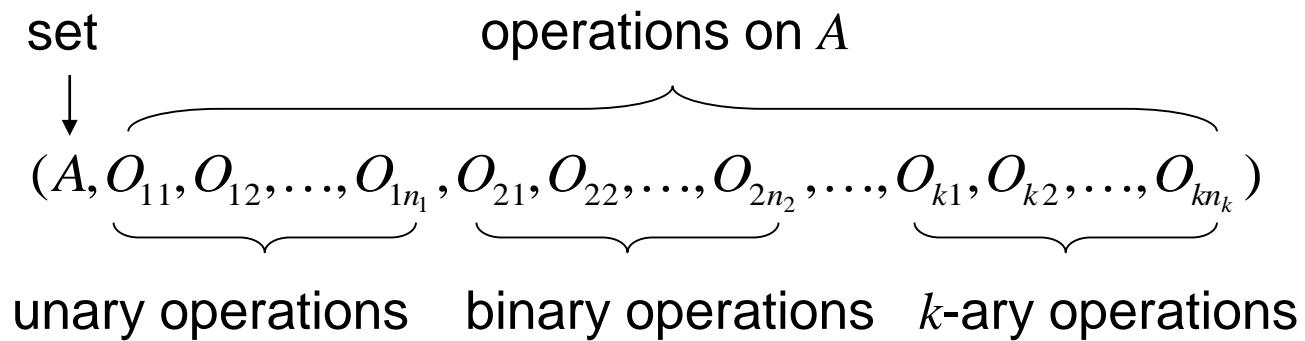
But,  $x * (y * z)$  is the greatest lower bound of  $x$  and  $y * z$ .

Therefore,  $(x * y) * z \leq x * (y * z)$ .

From  $x * (y * z) \leq (x * y) * z$  and  $(x * y) * z \leq x * (y * z)$ ,

we conclude that  $x * (y * z) = (x * y) * z$ .  $\square$

# Algebra



## ■ Theorem:

Let  $(A, *, +)$  be an algebra such that the following four pairs of laws are satisfied:

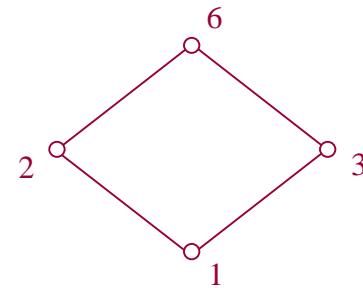
- |                                |                             |
|--------------------------------|-----------------------------|
| 1. $x * x = x$                 | $x + x = x$                 |
| 2. $x * y = y * x$             | $x + y = y + x$             |
| 3. $x * (y * z) = (x * y) * z$ | $x + (y + z) = (x + y) + z$ |
| 4. $x * (x + y) = x$           | $x + (x * y) = x$           |

Then  $(A, \leq)$  is a lattice if  $x \leq y$  when  $x * y = x$  and/or  $x + y = y$  for every  $x, y \in A$ .

## Example:

- $A = \{1, 2, 3, 6\}$ ,  $a * b = \text{GCD}(a, b)$ ,  $a + b = \text{LCM}(a, b)$ 
  - $\text{GCD}(a, a) = a$
  - $\text{GCD}(a, b) = \text{GCD}(b, a)$
  - $\text{GCD}(a, \text{GCD}(b, c)) = \text{GCD}(\text{GCD}(a, b), c)$
  - $\text{GCD}(a, \text{LCM}(a, b)) = a$
- $(a, b) \in R$  when  $\text{GCD}(a, b) = a$  and/or  $\text{LCM}(a, b) = b$ .
  - $R = \{(1, 1), (1, 2), (1, 3), (1, 6), (2, 2), (2, 6), (3, 3), (3, 6), (6, 6)\}$

$R$  is a partial ordering.  
 $(A, R)$  is a lattice.



## ***Proof:***

First, we want to show that  $\leq$  is a partial ordering.

Since  $x * x = x$  for every  $x \in A$  by 1, we have  $x \leq x$  for every  $x \in A$  and so  $\leq$  is reflexive.

Let  $x \leq y$  and  $y \leq x$ . Then  $x * y = x$  and  $y * x = y$ .

But  $x * y = y * x$  is given by 2, and so  $x = y$ .

Thus  $\leq$  is antisymmetric.

Let  $x \leq y$  and  $y \leq z$ . Then  $x * y = x$  and  $y * z = y$ .

Substituting  $y * z$  for  $y$  in  $x * y = x$ , we get  $x * (y * z) = x$ .

By applying 3, we get  $(x * y) * z = x$ .

Substituting  $x$  for  $x * y$ , we get  $x * z = x$ .

Thus  $x \leq z$  and so  $\leq$  is transitive.

## *Proof:*

Since  $\leq$  is reflexive, antisymmetric, and transitive,  $\leq$  is a partial ordering.

Now we have to show that there exists a GLB and an LUB of  $x$  and  $y$  for every  $x, y \in A$ .

Since  $x * (x + y) = x$  for every  $x, y \in A$  by 4, we have  $x \leq x + y$ .

Similarly since  $y * (y + x) = y$ , we have  $y \leq y + x = x + y$ .

From  $x \leq x + y$  and  $y \leq x + y$ , we conclude that  $x + y$  is an upper bound of  $x$  and  $y$ .

If  $x + y$  is the only upper bound, then it is the LUB of  $x$  and  $y$ .

If not, we need to show that  $x + y$  is the least one among all the upper bounds of  $x$  and  $y$ .

## *Proof:*

Suppose there is another upper bound, say  $z$ , of  $x$  and  $y$ .

In this case,  $x \leq z$  and  $y \leq z$ , and thus  $x + z = z$  and  $y + z = z$ .

Substituting  $y + z$  for  $z$  in the left hand side of  $x + z = z$ , we get  $x + (y + z) = z$ .

Using 3, we get  $(x + y) + z = z$ .

Hence,  $x + y \leq z$  and thus  $x + y$  is the LUB of  $x$  and  $y$ .

We can similarly show that  $x * y$  is the GLB of  $x$  and  $y$ .

Therefore,  $(A, \leq)$  is a lattice.

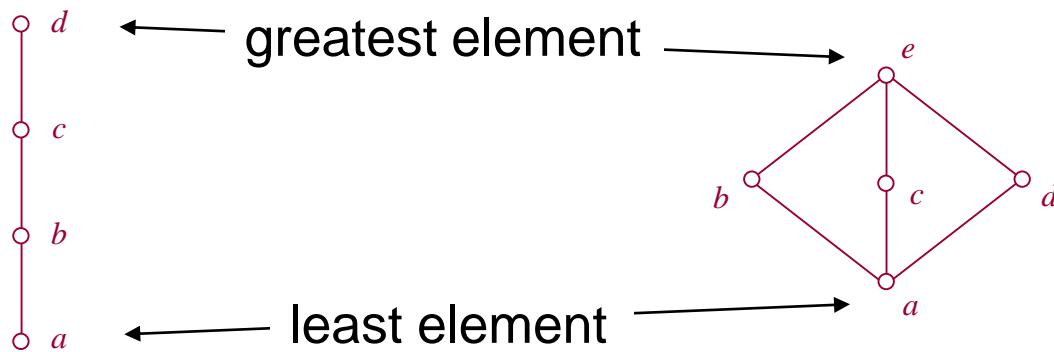
□

# Boolean Lattice and Boolean Algebra

## ■ Definition:

A lattice  $(A, \leq)$  is said to be a **bounded lattice** if the set  $A$  has a greatest element and a least element.

## Example:



- Note:

- In a bounded lattice  $(A, \leq)$ ,
    - the greatest element is usually denoted by '1', and
    - the least element is usually denoted by '0'.

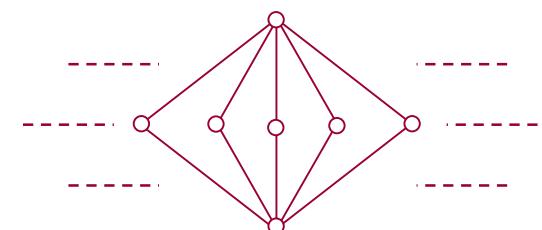
For all  $x \in A$ ,

- $0 \leq x$  and thus  $0 * x = 0$  and  $0 + x = x$
  - $x \leq 1$  and thus  $x + 1 = 1$  and  $x * 1 = x$

- Theorem:

If  $(A, \leq)$  is a finite lattice then it is a bounded lattice.

(The converse is not necessarily true.)



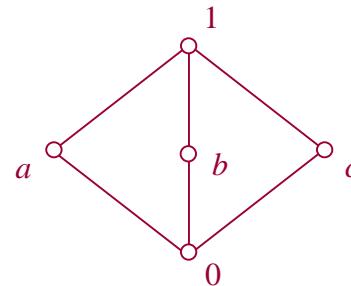
## ■ Definition:

A bounded lattice  $(A, \leq)$  is said to be a **complemented lattice** if for every  $x \in A$  there is an  $\bar{x} \in A$  such that  $x * \bar{x} = 0$  and  $x + \bar{x} = 1$ .

### Example:

□ Let  $x$  be a complement of  $a$ . Then,

- $a * x = 0 \rightarrow x = b, c, 0$
- $a + x = 1 \rightarrow x = b, c, 1$
- $\Rightarrow \bar{a} = b \text{ or } \bar{a} = c$



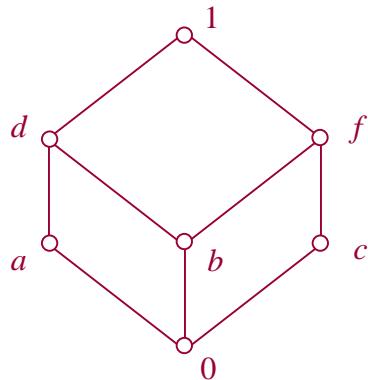
A complemented lattice

## Example:

□  $b * x = 0 \rightarrow x = a, c, 0$

□  $b + x = 1 \rightarrow x = 1$

→ There is no  $\bar{b}$ .



Not a complemented lattice

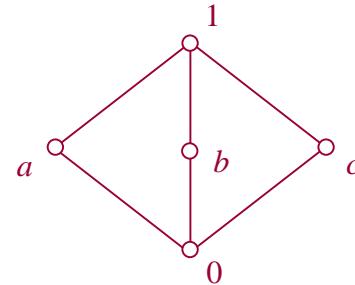
## ■ Definition:

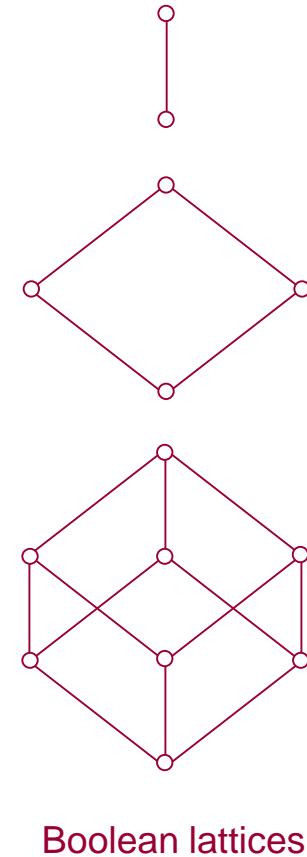
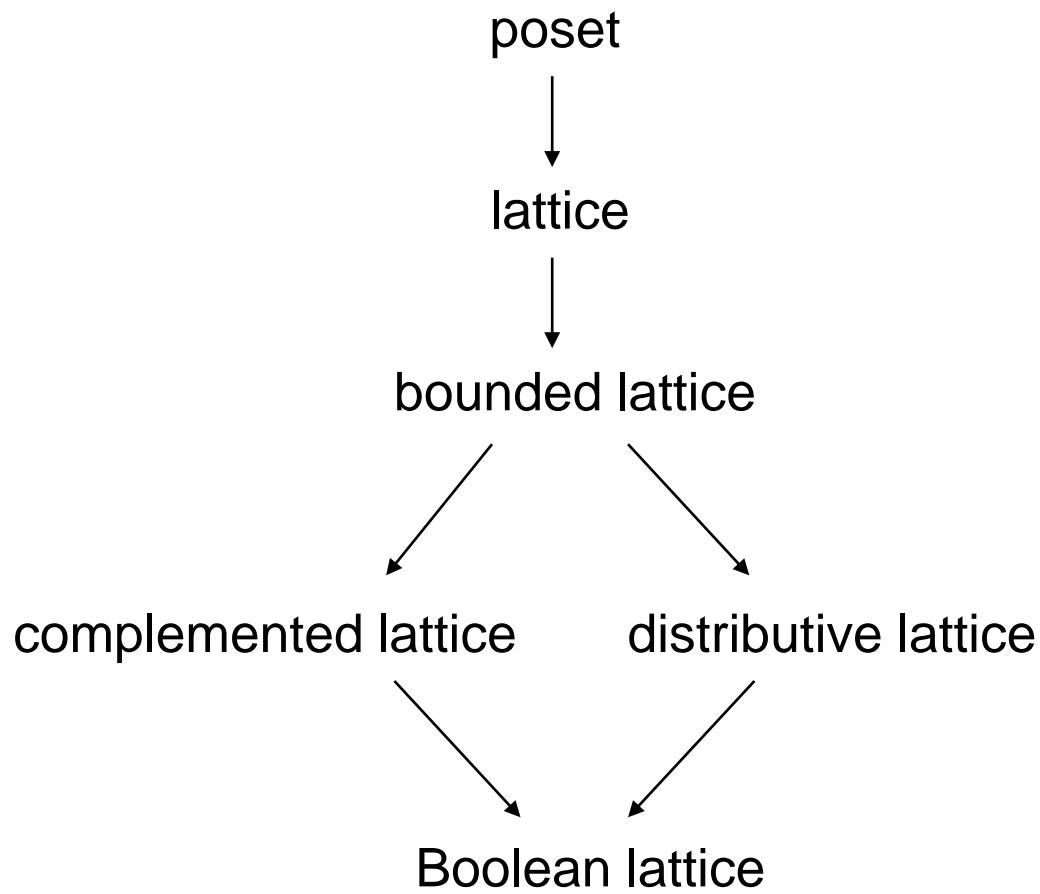
A bounded lattice  $(A, \leq)$  is said to be a **distributive lattice** if for every  $x, y, z \in A$  the following are satisfied:

1.  $x * (y + z) = (x * y) + (x * z)$ , and
2.  $x + (y * z) = (x + y) * (x + z)$

## Example:

- $a * (b + c) = a * 1 = a$
  - $(a * b) + (a * c) = 0 + 0 = 0$
- ➡ Not a distributive lattice





- Lattice and algebra:

- From a lattice  $(A, \leq)$  we can define an algebra  $(A, *, +)$ , and vice versa.

lattice  $(A, \leq) \cdots (A, *, +)$  algebra

Boolean lattice  $(A, \leq) \cdots (A, *, +, \neg, 0, 1)$  Boolean algebra

binary operations      unary operation      constants

- Boolean algebra:

- The following four laws are satisfied: (lattice)
    - idempotent law
    - commutative law
    - associative law
    - absorption law
  - $x + 0 = x$  and  $x * 1 = x$  for every  $x \in A$ . (bounded lattice)
  - For every  $x \in A$  there is  $\bar{x} \in A$  such that  $x * \bar{x} = 0$  and  $x + \bar{x} = 1$ . (complemented lattice)
  - For every  $x, y, z \in A$  we have  $x * (y + z) = (x * y) + (x * z)$  and  $x + (y * z) = (x + y) * (x + z)$  (distributive lattice)