9.5
Equivalence Relations

Section Summary

- ✓ Equivalence Relations
- ✓ Equivalence Classes
- ✓ Equivalence Classes and Partitions

Equivalence Relations

【Definition】A relation R on a set A is an equivalence relation if R is

- reflexive
- symmetric
- transitive

a and b are equivalent (a~b):

a and *b* are related by an equivalence relation *R*

For example,

(1) $\{(a,b) \mid a+b=2m, a,b,m \in N\}$

(2) The similarity relation between two triangles

(3) The equivalent relation between two formulas in proposition logic

Equivalence relation are important throughout mathematics and computer science.

Equivalence Class

the equivalence class of x:

The set of all elements that are related to an element x of A

Notation: $[x]_R$ $[x]$

$$[x]_R = \{s \mid (s, x) \in R\}$$

a representative of the equivalence class $[x]_R$: $b \in [x]_R$

Congruence Modulo m

〖Example 1〗 Congruence Modulo 3

$$R = \{(a,b) \mid a \equiv b (\mathrm{mod}\, 3), a, b \in Z\}$$

Show that *R* is an equivalence relation. And find its equivalence class.

Solution:

$$a \equiv b (\mathrm{mod}\, 3) \text{ if and only if } 3 \mid (a-b)$$

① **reflexive**

***R* is reflexive, since** $3 \mid (a-a)$

② **symmetric**

$$(a,b) \in R \Rightarrow a \equiv b (\mathrm{mod}\, 3) \Rightarrow 3 \mid (a-b) \Rightarrow a-b = 3k, k \in Z$$

$$\Rightarrow b-a = -3k \Rightarrow b \equiv a (\mathrm{mod}\, 3) \Rightarrow (b,a) \in R$$

③ **transitive**

$$3 \mid (a-b), 3 \mid (b-c)$$

$$a-c = (a-b)+(b-c) \Rightarrow 3 \mid (a-c)$$

[0]={…, -6, -3, 0, 3, 6, …}={ 3*k* | *k* ∈ *Z* }

[1]={…, -5, -2, 1, 4, 7, …}={ 3*k*+1 | *k* ∈ *Z* }

[2]={…, -4, -1, 2, 5, 8, …}={ 3*k*+2 | *k* ∈ *Z* }

Congruence Modulo *m* :

$$R = \{(a,b) \mid a \equiv b (\mathrm{mod}\, m), a, b \in Z\}$$

Congruence class Modulo *m* :

$$[0]_m, [1]_m \ldots, [m-1]_m$$

$$[a]_m = \{\ldots, a-2m, a-m, a, a+m, a+2m, \ldots\}$$

〖Example 2〗 Suppose that A is a nonempty set, and f is a function that has A as its domain. Let R be the relation on A consisting of all ordered pairs (x,y) where $f(x)=f(y)$.

(1) Show that R is an equivalence relation.

(2) What are the equivalence class of R.

Solution:

(1) $R = \{(x, y) \mid x, y \in A \wedge f(x) = f(y)\}$

① **reflexive**

② **symmetric**

③ **transitive**

(2) $[x] = \{y \mid y \in A \wedge f(x) = f(y)\}$

$\{f^{-1}(b) \mid b \in f(A)\}$

〖Example3〗 Let n be a positive integer and S a set of strings. Suppose that R_n is the relation on S such that sR_nt iff $s=t$, or both s and t have at least n characters and the first n characters of s and t are the same.

(1) Show that for every set S of strings and every positive integer n, R_n is an equivalence relation on S.

(2) What is the equivalence class of the string 0111 with respect to the equivalence relation R_3.

Solution:

(1) ① **reflexive**

② **symmetric**

③ **transitive**

(2) $[011]_{R3}$ = {011,0110,0111,01100,01101,01110,01111,…}

Partition of a Set

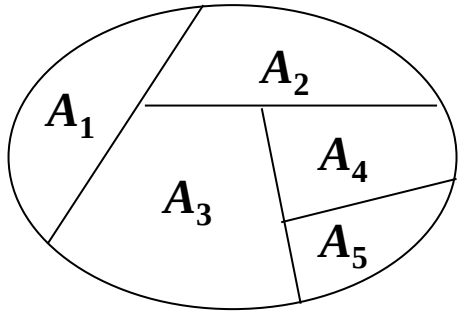
【Definition】 Let $\{A_1, A_2, \ldots\}$ be a collection of subsets of A. Then the collection forms a **partition** of A if and only if

- $A_i \neq \phi$ for $i \in Z$
- $A_i \cap A_j = \phi$, when $i \neq j$
- $\forall a \in A, \exists i$ such that $a \in A_i (i = 1,2,\ldots)$

$\bigcup_{i \in Z} A_i = A$

Notation:

$$pr(A) = \{A_1, A_2, \ldots\}$$



Equivalence Classes and Partitions

【 Theorem 1】 Let R be an equivalence relation on a set A. The following statements are equivalent:

(1) aRb

(2) $[a]=[b]$

(3) $[a]\cap[b]\neq\phi$

Proof:

■ **Show that (1) implies (2)**

$$[a]=[b]\Rightarrow([a]\subseteq[b])\wedge([b]\subseteq[a])$$

$$\left.\begin{array}{l} x\in[a]\Rightarrow(a,x)\in R \\ aRb\Rightarrow(a,b)\in R\Rightarrow(b,a)\in R \end{array}\right\}\Rightarrow(b,x)\in R\Rightarrow x\in[b]\Rightarrow[a]\subseteq[b]$$

(1) aRb
(2) $[a]=[b]$
(3) $[a]\cap[b]\neq\phi$

- **Show that (2) implies (3)**

$$\left.\begin{array}{l}[a]=[b]\\ \textbf{\textit{R} is reflexive} \Rightarrow \textbf{[}a\textbf{] is nonempty}\end{array}\right\} \Rightarrow [a]\cap[b]\neq\phi$$

- **Show that (3) implies (1)**

$$[a]\cap[b]\neq\phi \quad \Rightarrow \exists x\in[a]\cap[b]$$

$$\Rightarrow (a,x)\in R,(b,x)\in R$$

$$\Rightarrow (a,b)\in R$$

【Theorem 2】 Let *R* be an equivalence relation on a set *A*. Then the equivalence classes of *R* form a partition of *A*. Conversely, given a partition $\{A_i \mid i \in I\}$ of the set *A*, there is an equivalence relation *R* that has the sets $A_i, i \in I$, as its equivalence classes.

Proof:

- **the equivalence class of *R* :** $A_1, A_2, ..., A_n$

an equivalence relation on a set A $\leftrightarrow$ a partition of A

(1) $A_i \neq \phi$ for $i \in Z$

(2) $A_i \cap A_j = \phi$, when $i \neq j$

$$A_i \cap A_j \neq \phi \Rightarrow A_i = A_j$$

(3) $\bigcup_{i \in Z} A_i = A$

$$\forall a \in A, (a, a) \in R \Rightarrow \exists i, a \in A_i$$

■ $pr(A) = \{A_1, A_2, ..., A_n\}$

$R : \forall a, b \in A, aRb$ if and only if $a, b \in A_i$

(1) $pr(A) = \{A_1, A_2, ..., A_n\} \quad \Rightarrow A = \bigcup_{i=1}^{n} A_i$

$\Rightarrow \forall a \in A, \exists i$ such that $a \in A_i (i = 1,2,...) \qquad \therefore aRa$

(2) $aRb \quad \Rightarrow a, b \in A_i \Rightarrow b, a \in A_i \qquad \therefore bRa$

(3) aRb, bRc

$\Rightarrow \exists i, j$ such that $a, b \in A_i, b, c \in A_j$

If $i \neq j$, Then $A_i \cap A_j = \phi$

$b \in A_i; \quad b \in A_j \quad \therefore A_i \cap A_j \neq \phi$

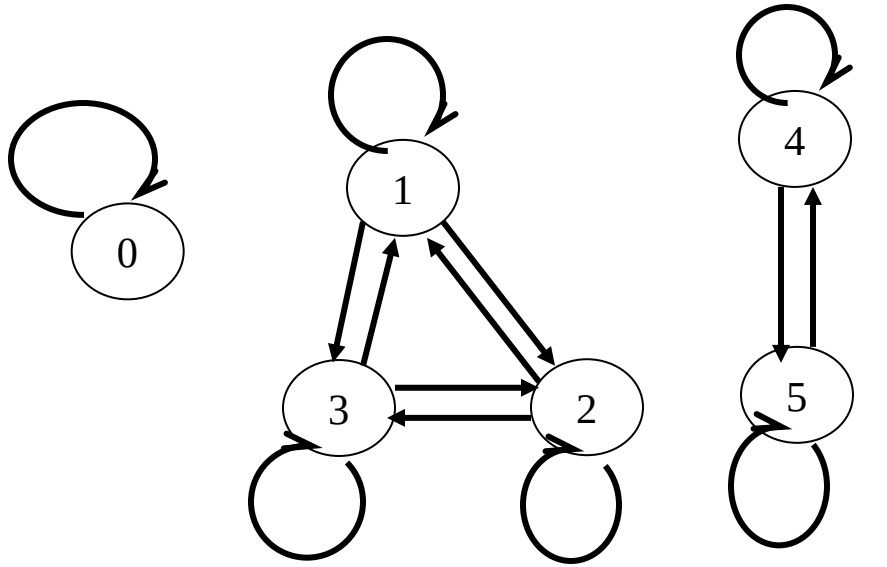
$i = j, \quad a, b, c \in A_i \Rightarrow aRc$

〖Example 4〗 Find the partition of the set *A* from *R*.

$A = \{0,1,2,3,4,5\}$,

$R = \{(0,0),(1,1),(2,2),(3,3),(1,2),(1,3),(2,1),(2,3),(3,1),(3,2),(4,4),(4,5),(5,4),(5,5)\}$

Solution:



[0]={0}

[1]={1,2,3}

[4]={4,5}

***pr*(*A*)={ [0], [1], [4]}**

〖Example5〗 Let R_3 be the relation from example 3. What are the sets in the partition of the set of all bit strings arising from the relation R_3 on the set of all bit strings?

Solution:

$[\lambda]_{R_3} = \{\lambda\}$ $[0]_{R_3} = \{0\}$ $[1]_{R_3} = \{1\}$

$[00]_{R_3} = \{00\}$ $[01]_{R_3} = \{01\}$ $[10]_{R_3} = \{10\}$ $[11]_{R_3} = \{11\}$

$[000]_{R_3} = \{000,0000,0001,00000,00001,00010,00011,\ldots\}$

$[001]_{R_3} = \{001,0010,0011,00100,00101,00110,00111,\ldots\}$

$[010]_{R_3} =$

$[011]_{R_3} =$

…

Question1 :

Congruence Modulo *m*

$$R = \{(a,b) \mid a \equiv b (\mathrm{mod}\, m), a, b \in Z\},\ pr(Z) = ?$$

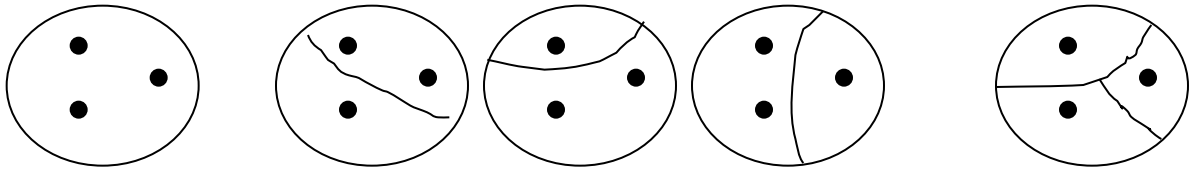
$$pr(Z) = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$$

Question2:

|A|=3. How many different equivalence relations on the set A are there?

Solution:

an equivalence relation on a set A $\leftrightarrow$ a partition of A



Question3:

IF $|A|=n$, the $p(n)$=? $p(n)$: the number of different equivalence relations on a set with n elements.

P.566, Ex.68

The operations of equivalence relations

【Theorem 3】 If R_1, R_2 are equivalence relations on A, then $R_1 \cap R_2$ is equivalence relations on A.

Proof:

$\forall a \in A \quad (a,a) \in R_1, (a,a) \in R_2$

$\therefore (a,a) \in R_1 \cap R_2$

It suffices to sh

- reflexive relations is reflexive,
- symmetric relations is symmetric,

and

- transitive relations is transitive.

The operations of equivalence relations

【Theorem 3】 If R_1, R_2 are equivalence relations on A, then $R_1 \cap R_2$ is equivalence relations on A.

If $(a,b) \in R_1 \cap R_2$

Then $(a,b) \in R_1$ and $(a,b) \in R_2$

Then $(b,a) \in R_1$ and $(b,a) \in R_2$

$(b,a) \in R_1 \cap R_2$

Proof:

It suffices to show that the inter

- **reflexive relations is reflexiv**
- **symmetric relations is symmetric,**

and

- **transitive relations is transitive.**

The operations of equivalence relations

【Theorem 3】 If R_1, R_2 are equivalence relations on A, then $R_1 \cap R_2$ is equivalence relations on A.

Proof:

It suffices to show th

- reflexive relation
- symmetric relatio

and

- transitive relations is transitive.

If $(a,b),(b,c) \in R_1 \cap R_2$
Then $(a,b),(b,c) \in R_1(R_2)$
Then $(a,c) \in R_1(R_2)$
$(a,c) \in R_1 \cap R_2$

【Theorem 4】 If R_1, R_2 are equivalence relations on A, then $R_1 \cup R_2$ is reflexive and symmetric relation on A.

Proof:

(1) reflexive

$$\forall a \in A \quad (a,a) \in R_1, (a,a) \in R_2 \quad \therefore (a,a) \in R_1 \cup R_2$$

(2) symmetric

$$(a,b) \in R_1 \cup R_2 \quad \Rightarrow (a,b) \in R_1 \text{ or } (a,b) \in R_2$$

$$\Rightarrow (b,a) \in R_1 \text{ or } (b,a) \in R_2 \quad \Rightarrow (b,a) \in R_1 \cup R_2$$

Question: **transitive?**

〖**Example 6**〗 $A=\{a,b,c\}$,

$R_1=\{(a,a),(b,b),(c,c),(a,b),(b,a)\}$

$R_2=\{(a,a),(b,b),(c,c),(b,c),(c,b)\}$

Is $R_1 \cup R_2$ a transitive relation ?

Solution:

$$R_1 \cup R_2=\{(a,a),(b,b),(c,c),(a,b),(b,a),(b,c),(c,b)\}$$

【 Theorem 】 If R_1, R_2 are equivalence relations on A, then $(R_1 \cup R_2)^*$ is an equivalence relation on A.

Proof:

(1) reflexive

(2) symmetric

(3) transitive

Homework:

SE：P. 615 3, 10, 16, 36, 39, 41

EE：P. 646 3, 10, 16, 36, 39, 41

9.6
Partial Orderings

Section Summary

- ✓ Partial Orderings and Partially-ordered Sets
- ✓ Lexicographic Orderings
- ✓ Hasse Diagrams
- ✓ Lattices
- ✓ Topological Sorting

Partial Orderings

Sometimes, relations do not specify the equality of elements in a set, but define an order on them.

【Definition】Let R be a relation on S. Then R is a partial ordering or partial order if R is

- reflexive
- antisymmetric
- transitive

Notation: (S, R) ---- partially ordered set or a poset

〖Example 1〗 (1) $R_1 = \{(a,b) \mid a \le b, a,b \in Z\}$ $(Z, \le)$

(2) $R_2 = \{(a,b) \mid a \mid b, a,b \in Z^+\}$ $(Z^+, |)$

(3) $R_3 = \{(s_1, s_2) \mid s_1 \subseteq s_2, s_1, s_2 \in P(S)\}$ $(P(S), \subseteq)$

Notation:

$a \le b$ (a is less than or equal to b): (S, R) is a poset, $(a, b) \in R$

$a < b$ (a is less then b): $a \le b$, but $a \ne b$

◆ comparable/ incomparable

【Definition】

The elements a and b of a poset $(S, \le)$ are called comparable if either $a \le b$ or $b \le a$. When a and b are elements of S such that neither $a \le b$ nor $b \le a$, a and b are called incomparable.

For example,

$(Z^+, |)$ $\quad 2 \nmid 7 \quad$ $2 \mid 4$

◆ total order/linear order

【Definition】If $(S,\leq)$ is a poset and every two elements of S are comparable, S is called a totally ordered or linearly ordered set, $\leq$ is called a total order or linear order. In this case $(S,\leq)$ is called a chain.

〖Example 2〗

(1) $(Z,\leq)$ is a poset. In this case either $a \leq b$ or $b \leq a$.
Hence, $\leq$ is a total order and $(Z,\leq)$ is a chain.

(2) $(Z^+,|)$ is a poset, not a totally ordered set.

(3) $(P(S),\subseteq)$ is a poset, not a totally ordered set.

◆ well-ordered

【Definition】 *(S, $\preccurlyeq$)* is a well-ordered set if it is a poset suth that $\preccurlyeq$ *is a total ordering and* every nonempty subset of *S* has a least element.

For example,

$(1) A = \{1,2,\ldots,n\}, (A, \leq)$

$(2) (N, \leq)$

$(3) A = \{x \mid 0 < x < 1\}, (A, \leq)$

◆ The principle of well-ordered induction

- ✓ To prove results about a well-ordered set
- ✓ Generalized induction

【Theorem】The principle of well-ordered induction

Suppose that S is a well-ordered set. Then P(x) is true for all $x \in S$,if

Inductive Step: for every $y \in S$, if P(x) is true for all $x \in S$ with $x < y$, then p(y) is true.

Proof:

Suppose it is not the case that $P(x)$ is true for all $x \in S$. Then there is an element $y \in S$ such that $P(y)$ is false. Consequently, the set $A = \{x \in S \mid P(x) \text{ is false}\}$ is nonempty. Because S is well-ordered, A has a least element a. By the choice of a as a least element of A, we know that $P(x)$ is true for all $x \in S$ with $x \prec a$. This implies by the inductive step $P(a)$ is true. This contradiction shows that $P(x)$ must be true for all $x \in S$.

Remark: *We do not need a basis step in a proof using the principle of well-ordered induction.*

Lexicographic Order

An example of lexicographic order:

Mr. Zhang plans to interview three applicants at 9:00, 10:00, 11:00 today. Meanwhile Mrs. Li plans to interview other three applicants. Unfortunately, both of them are sick and Mr. Liu will interview these six applicants.

Mr. Liu interview these applicants in following order:

(Mr. Zhang, 9:00), (Mr. Zhang, 10:00), (Mr. Zhang, 11:00),

(Mrs. Li, 9:00), (Mrs. Li, 10:00), (Mrs. Li , 11:00).

The interview order is obtained by defining a partial ordering on the Cartesian product of two posets.

A_1={Mr. Zhang, Mrs. Li}, A_2={9:00, 10:00, 11:00 }

◆ **The lexicographic order ≤ on $A_1 \times A_2$**

Given two posets $(A_1, \leq_1)$ and $(A_2, \leq_2)$, we construct an induced partial order R on $A_1 \times A_2$: $(x_1, y_1) \leq (x_2, y_2)$ if

$$x_1 \leq_1 x_2$$

or

$$x_1 = x_2 \quad and \quad y_1 \leq_2 y_2$$

〖Example 3〗 Let $A_1 = A_2 = Z^+$ and $R_1 = R_2 =|$. Then

(1) (2, 4) < (2, 8) since $x_1 = x_2$ and $y_1 R_2 y_2$

(2) (2, 4) is not related under *R* to (2, 6) since $x_1 = x_2$ but 4 does not divide 6.

(3) (2, 4) < (4, 5) since $x_1 R_1 x_2$

◆ **A lexicographic ordering is a partial ordering defined on a Cartesian product of two posets.**

Proof: $(A_1 \times A_2, \leq)$

① **reflexive**

$$\forall (a,b) \in A_1 \times A_2, \qquad (a,b) \leq (a,b)$$

② **antisymmetric**

$$\left.\begin{array}{l}(a_1,b_1) \leq (a_2,b_2)\\ (a_1,b_1) \neq (a_2,b_2)\end{array}\right\} \Rightarrow a_1 \leq_1 a_2 \qquad or \qquad a_1 = a_2, b_1 \leq_2 b_2$$

③ **transitive**

$$\left.\begin{array}{l}(a_1,b_1) \leq (a_2,b_2)\\ (a_2,b_2) \leq (a_3,b_3)\end{array}\right\} \Rightarrow (a_1,b_1) \leq (a_3,b_3)$$

- **The definition of lexicographic order extends naturally to multiple Cartesian products of partially ordered sets.**

〖Example 4〗 Using the same definitions of A_i *and* R_i as above,

(1) (2, 3, 4, 5) < (2, 3, 8, 2) since $x_1 = x_2$ *and* $y_1 = y_2$ and 4 divides 8.

(2) (2, 3, 4, 5) is not related to (3, 6, 8, 10) since 2 does not divide 3.

◆ lexicographic order of string

The string $a_1 a_2 \ldots a_m$ **is less then** $b_1 b_2 \ldots b_n$ **if and only if**

$$(a_1, a_2, \ldots, a_t) < (b_1, b_2, \ldots, b_t), or$$

$$(a_1, a_2, \ldots, a_t) = (b_1, b_2, \ldots, b_t) \quad and \quad m < n$$

Where $t = \min(m, n)$

For example,

Find the lexicographic ordering of the following strings.

discrete discredit discreet discreteness discretion

discredit < discreet < discrete < discreteness < discretion

Hasse Diagrams

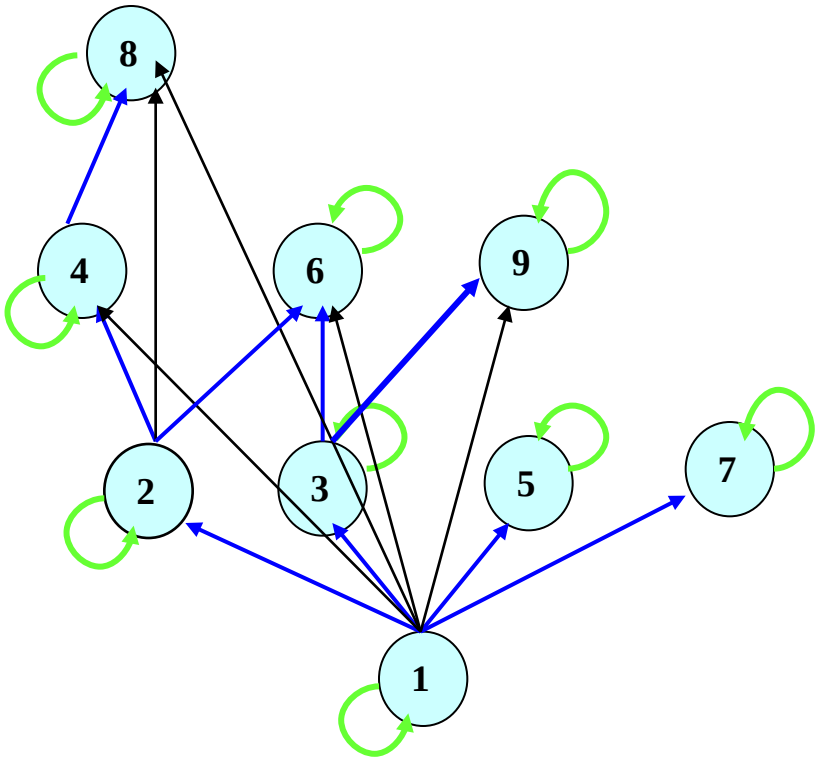
Hasse Diagrams

-- A method used to represent a partial ordering

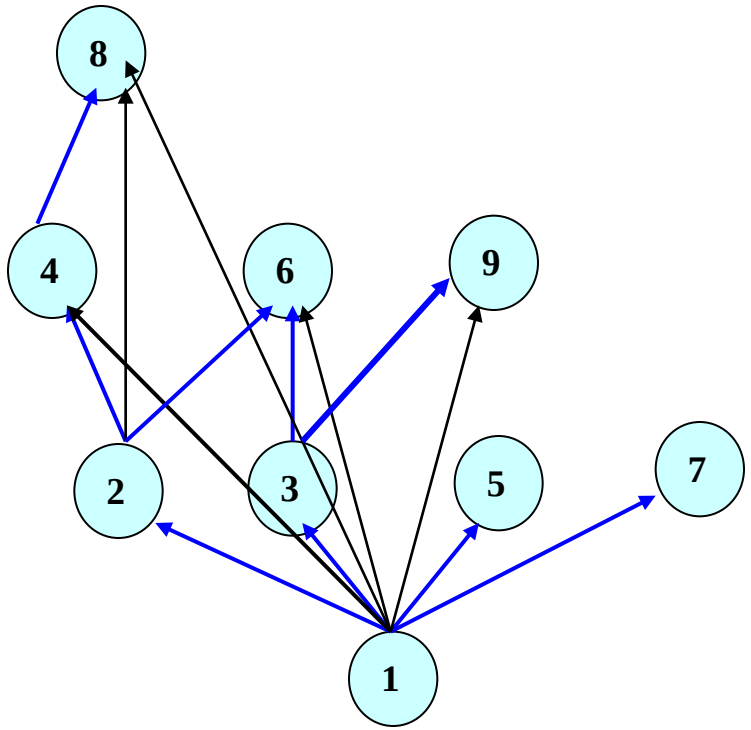
To construct a Hasse diagram:

1) Construct a digraph representation of the poset (A, R) so that all arcs point up (except the loops).
2) Eliminate all loops
3) Eliminate all arcs that are redundant because of transitivity
4) Eliminate the arrows at the ends of arcs since everything points up.

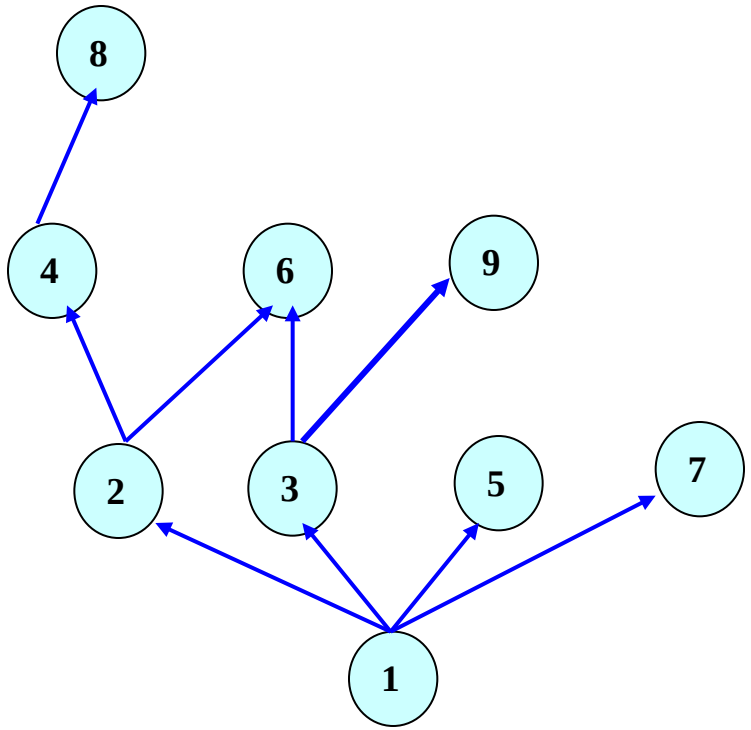
〖**Example 5**〗 $A = \{1,2,3,4,5,6,7,8,9\}$ $R = \{(a,b) \mid a \mid b, a, b \in A\}$



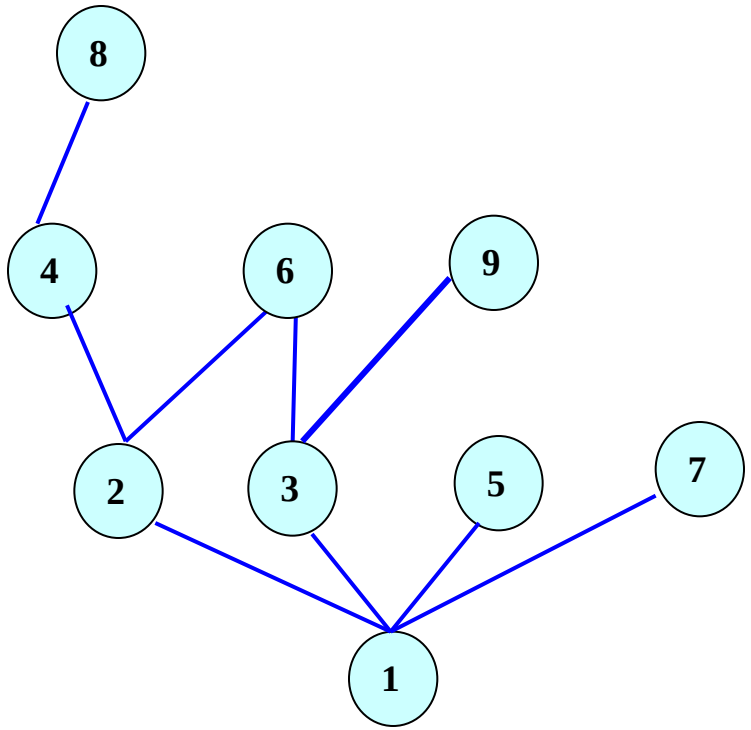
〖**Example 5**〗 $A = \{1,2,3,4,5,6,7,8,9\}$ $R = \{(a,b) \mid a \mid b, a, b \in A\}$



〖**Example 5**〗 $A = \{1,2,3,4,5,6,7,8,9\}$ $R = \{(a,b) \mid a \mid b, a, b \in A\}$



〖**Example 5**〗 $A = \{1,2,3,4,5,6,7,8,9\}$ $R = \{(a,b) \mid a \mid b, a, b \in A\}$



〖**Example 6**〗 (1) $A=\{1,2,3,4,5,6,7,8,9\}$ $R_1=\{(a,b)\mid a\le b, a,b\in A\}$

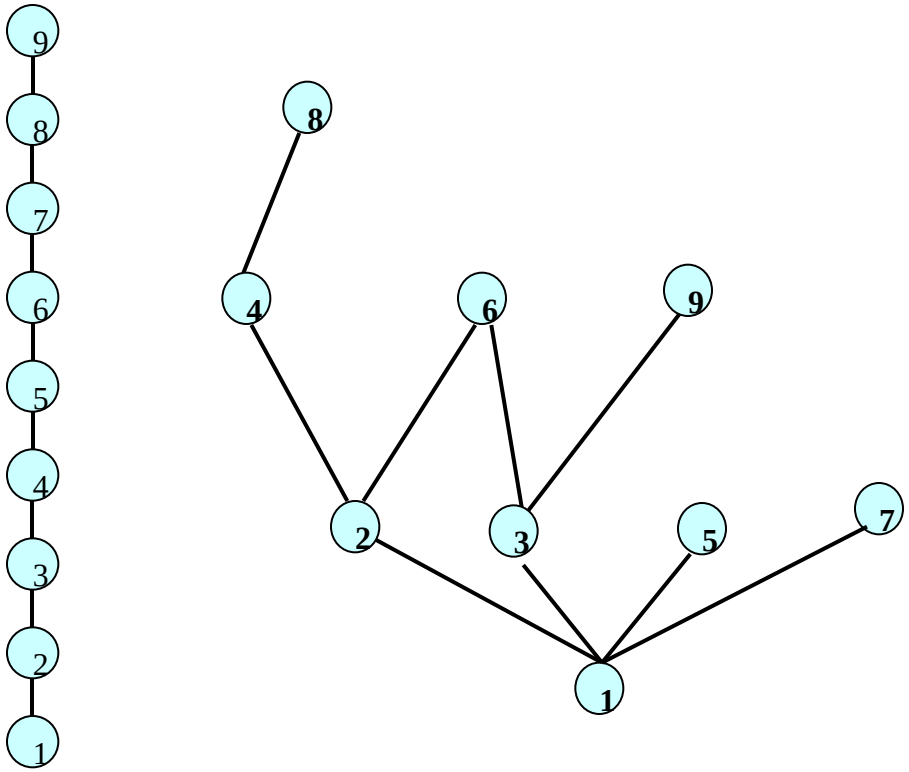
(2) $A=\{1,2,3,4,5,6,7,8,9\}$ $R_2=\{(a,b)\mid a\mid b, a,b\in A\}$

(3) $A=\{a,b,c\}$, $R_3=\{(s_1,s_2)\mid s_1\subseteq s_2, s_1,s_2\in P(A)\}$

〖**Example 6**〗 (1) $A=\{1,2,3,4,5,6,7,8,9\}$ $R_1=\{(a,b)\mid a\le b, a,b\in A\}$

(2) $A=\{1,2,3,4,5,6,7,8,9\}$ $R_2=\{(a,b)\mid a\mid b, a,b\in A\}$

(3) $A=\{a,b,c\}$, $R_3=\{(s_1,s_2)\mid s_1\subseteq s_2, s_1,s_2\in P(A)\}$

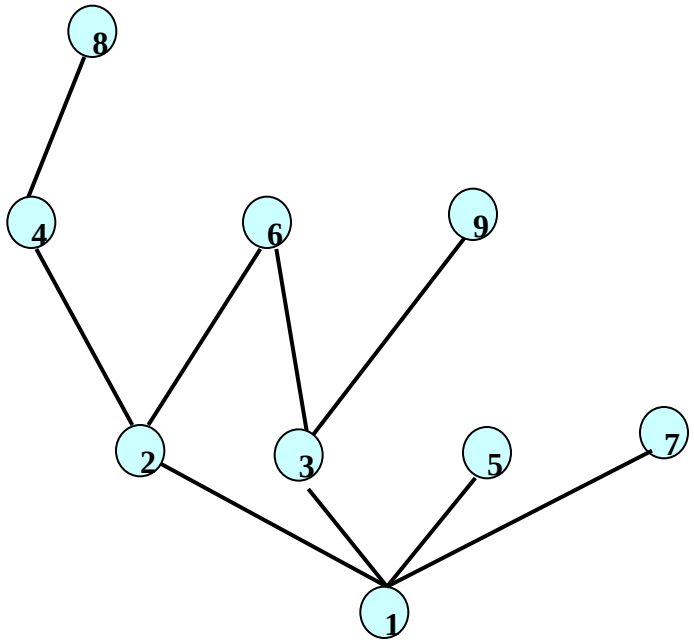


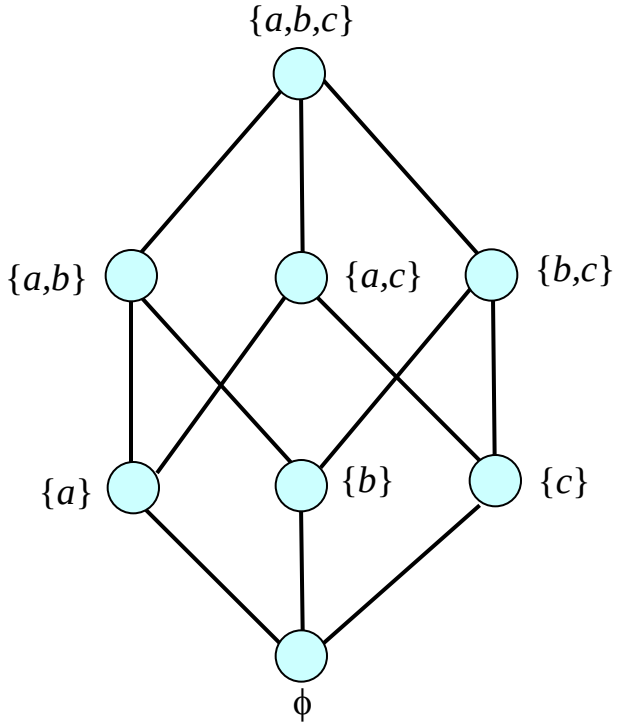
〖**Example 6**〗 (1) $A=\{1,2,3,4,5,6,7,8,9\}$ $R_1=\{(a,b)\mid a\le b, a,b\in A\}$

(2) $A=\{1,2,3,4,5,6,7,8,9\}$ $R_2=\{(a,b)\mid a\mid b, a,b\in A\}$

(3) $A=\{a,b,c\},$ $R_3=\{(s_1,s_2)\mid s_1\subseteq s_2, s_1,s_2\in P(A)\}$

$p(A)=\{\phi,\{a\},\{b\},\{c\},\{a,b\},\{b,c\},\{a,c\},\{a,b,c\}\}$





Chain and Antichain

【Definition】$(A,\leq)$ is a poset. $B \subseteq A$, if $(B,\leq)$ is a totally ordered set, the *B* is called a *chain* of $(A,\leq)$.

The length of chain: |B|, B is a definite set,

$B \subseteq A$, if $\forall a,b \in B(a \neq b),(a,b) \notin R,(b,a) \notin R$

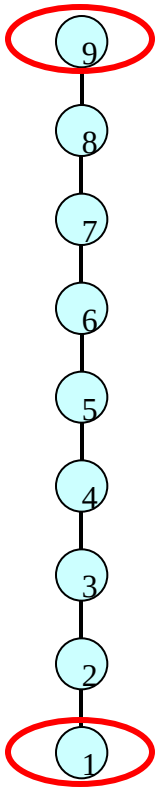
the *B* is called a *antichain* of $(A,\leq)$.

Maximal and Minimal Elements

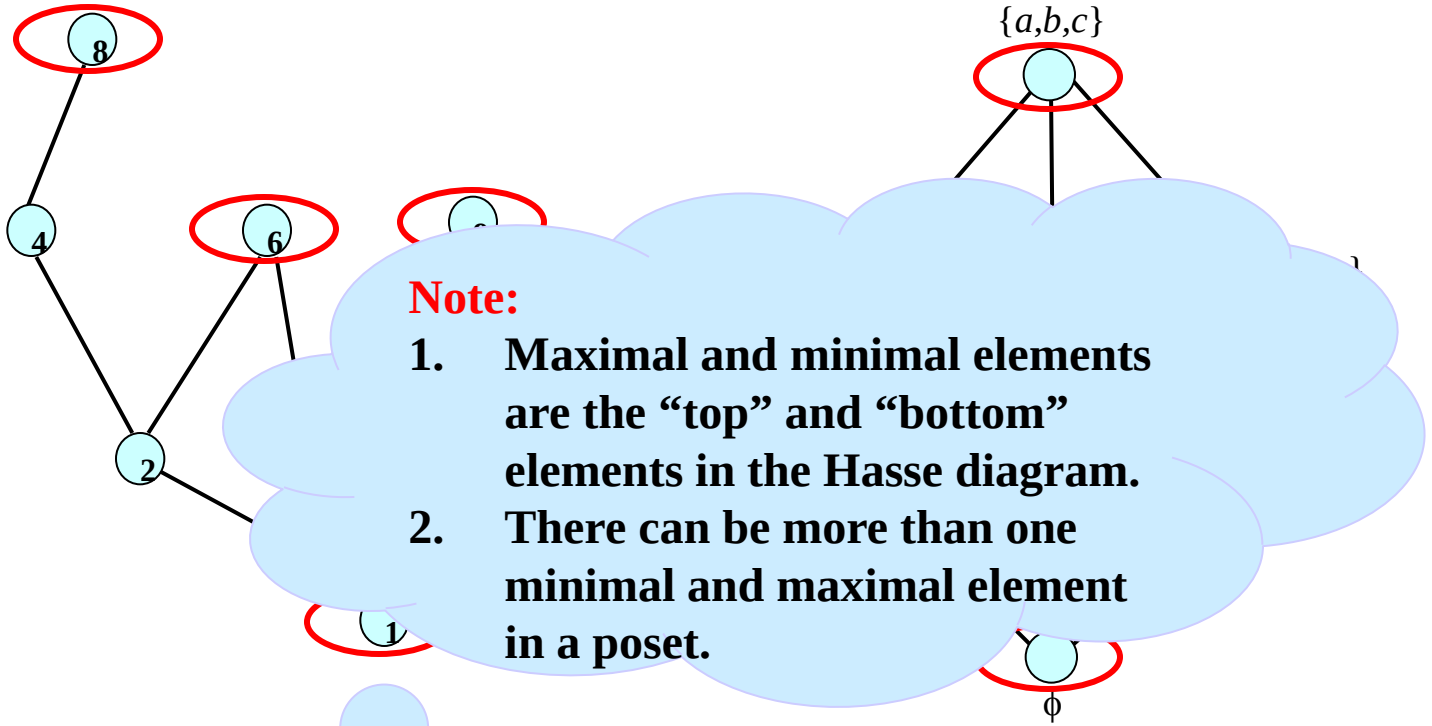
【Definition】Let $(A, \leq)$ be a poset. $a \in A$, then *a* is a **maximal element** if there does not exist an element *b* in *A* such that $a < b$.

Similarly for a **minimal element**.

For example,



(1)



(2)

(3)

Note:

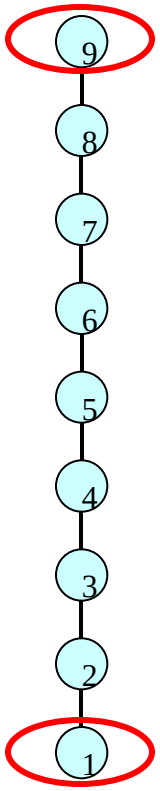
1. **Maximal and minimal elements are the "top" and "bottom" elements in the Hasse diagram.**
2. **There can be more than one minimal and maximal element in a poset.**

	maximal element	minimal element
(1)	9	1
(2)	8,6,9,5,7	1
(3)	$\{a, b, c\}$	ϕ

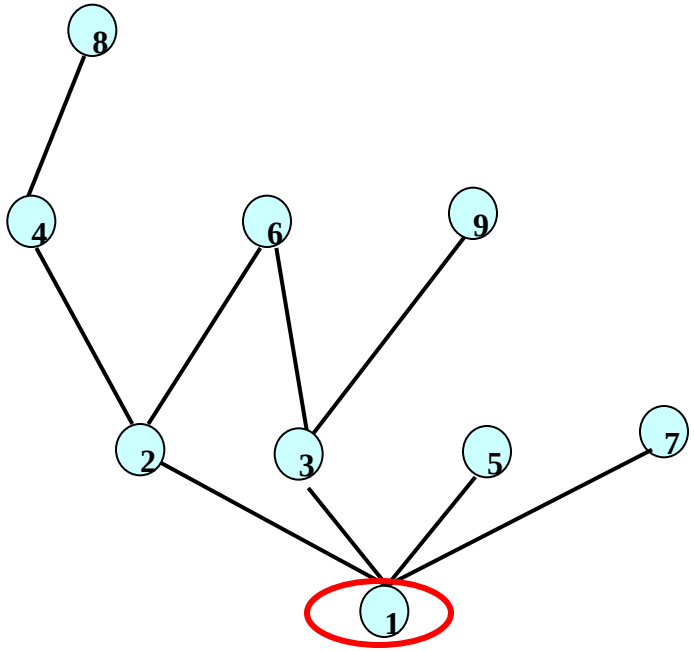
Greatest and Least Element

【Definition】Let $(A, \leq)$ be a poset. Then an element a in A is a greatest element of A if $b \leq a$ for every b in A, and a is a least element of A if $a \leq b$ for every b in A.

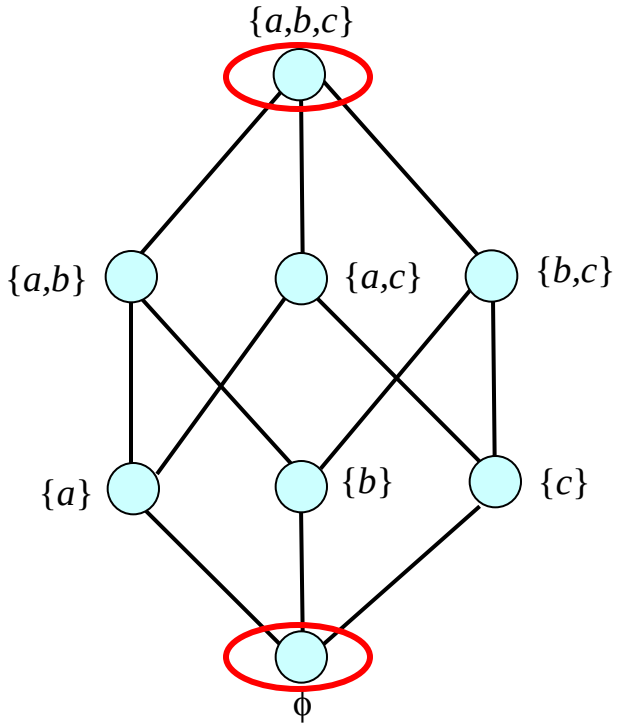
For example,



(1)



(2)



(3)

	The greatest element	The least element
(1)	**9**	**1**
(2)	**/**	**1**
(3)	**{*a*, *b*, *c*}**	**ϕ**

【 Theorem 】 The greatest and least element are unique when they exist.

Proof:

Suppose that a_1 is a greatest element in A. It follows that

$x \le a_1$ **for every x in A.**

Suppose that a_2 is a greatest element in A. It follows that

$x \le a_2$ **for every x in A.**

It implies that $a_2 \le a_1 \; and \; a_1 \le a_2$

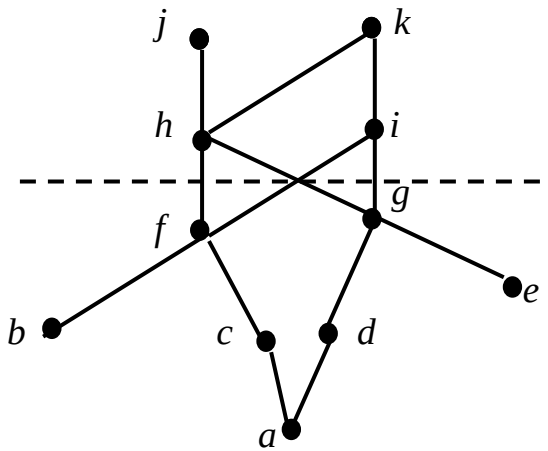
That is $a_1 = a_2$

Upper and Lower Bounds

【Definition】Let *A* be a subset of *S* in the poset $(S, \leq)$. If there exists an element *a* in *S* such that $b \leq a$ for all *b* in *A*, then *a* is called an upper bound of *A*. Similarly for lower bounds.

〖Example 7〗 $S = \{a, b, c, d, e, f, g, h, i, j, k\}$

$A = \{a, b, c, d, e, f, g\}, A' = \{h, i, j, k\}$



the upper bounds of set *A*: *h, i, k, j*

the lower bounds of set A: /

the upper bounds of set A': /

the lower bounds of set A': *f, g, a, b, c, d, e*

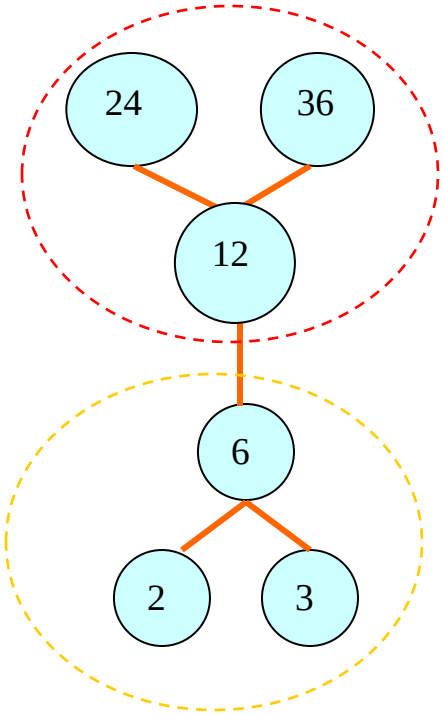
Least Upper and Greatest Lower Bounds

【Definition】 If *a* is an upper bound for *P* which is less than every other upper bounds then it is the least upper bound, denoted by lub(*S*).

Similarly for the greatest lower bound, glb(*S*).

〖**Example 7**〗$A=\{2,3,6,12,24,36\}$, $B_1=\{2,3,6\}$, $B_2=\{12,24,36\}$, R :|

Determine the maximal elements, minimal elements, greatest element, least element of set *A*, the upper bounds, lower bounds , least upper bound , greatest lower bound of set B_1, B_2 。



***A*:**

maximal elements: 24,36 minimal elements:2,3

the greatest element: / the least element: /

***B*$_1$:**

upper bounds: 6,12,24,36 lower bounds: /

The least upper bound: 6 The greatest lower bound:/

***B*$_2$:**

uper bounds: / lower bounds: 12,6,2,3

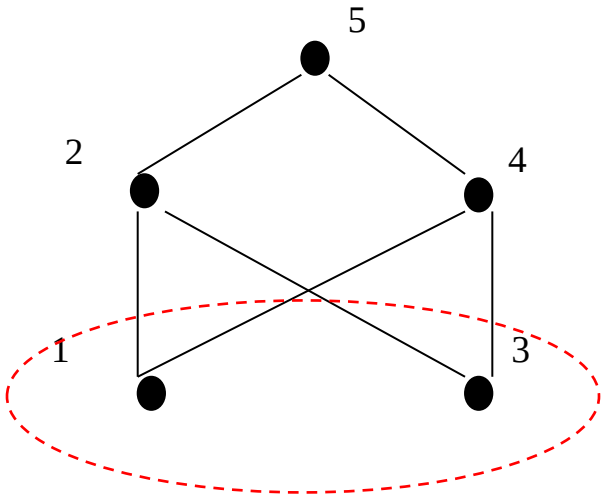
The least upper bound: / The greatest lower bound:12

Lattices

【Definition】A poset is called a lattice if every pair of elements has a lub and a glb.

〖Example 9〗 Determine whether the following poset is lattice.

(1)



(2) $(Z,\leq)$ **?**

lub：the larger of the two elements，

glb：the smaller of the two elements.

Hence, the poset $(Z,\leq)$ **is a lattice.**

Note: Every totally ordered set is a lattice.

(3) $(Z^+,|)$ **?**

$\forall a,b \in Z^+$

lub：the least common multiple，

glb：the greatest common divisor

Hence, the poset $(Z^+,|)$ **is a lattice.**

(4) $(P(s),\subseteq)$ **?**

$\forall s_1, s_2 \in P(s)$ **, lub：** $s_1 \cup s_2$ **glb：** $s_1 \cap s_2$

Hence, the poset $(P(s),\subseteq)$ **is a lattice.**

◆ The Lattices Model of Information Flow

- The Lattices Model can be used to represent different information flow policies.
- Multilevel security policy
  - Each pieces of information is assigned to a security class
  - Each security class is represented by a pair (*A*,*C*), where *A* is an authority level and *C* is a category.

  For example,
  - A={unclassified(0), confidential(1), secret(2), top secret(3)}
  - If the set of compartments is {spies, moles, double agents},then there are eight different categories, one for each of the eight subsets of the set of compartments, such as {spies, moles}.
- Order security classes by specifying that

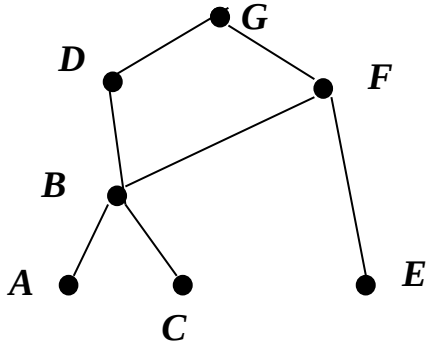
  $(A_1, C_1) \leq (A_2, C_2)$ iff $A_1 \leq A_2, C_1 \subseteq C_2$
- Information is permitted to flow from security classes

  $$(A_1, C_1) \text{ into } (A_2, C_2) \text{ iff } (A_1, C_1) \leq (A_2, C_2)$$
- The set of all security classes forms a lattices.

Topological Sorting

The problem of project schedul:

A project is broken down into seven tasks. A partial ordering on tasks is set up by considering task x < task y if task y can't be started until task x has been completed.



How can an order be found for these tasks?

We can impose a total ordering $\leq$ on a poset *compatible* with the partial order if $a \leq b$ whenever aRb .

(A,R) is a poset. $(A,\leq)$ is a total ordering.

If $a \leq b$ whenever aRb .

Constructing a compatible total ordering from a partial ordering is called topological sorting.

【 Lemma 1】 Every finite nonempty poset $(S, \leq)$ has a minimal element.

Proof:

Choose an element a_0 of S.

If a_0 is not minimal, then there is an element a_1 with $a_1 < a_0$.

If a_1 is not minimal, there is an element a_2 with $a_2 < a_1$.

Continue this process, so that

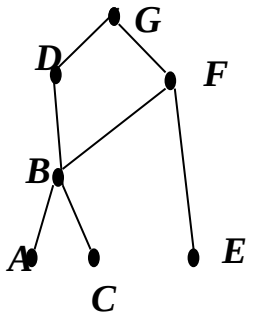
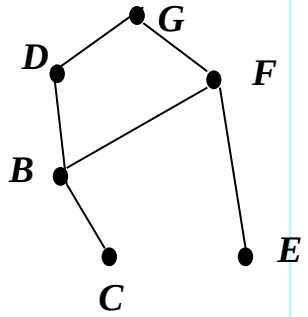
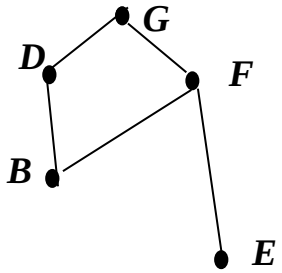
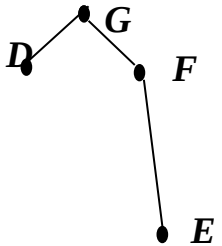
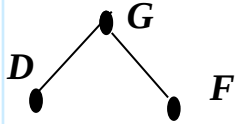
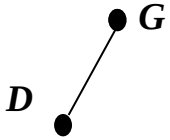
If a_n is not minimal, there is an element a_{n+1} with $a_{n+1} < a_n$.

Since there are only finite number of elements in the poset, this process must end with a minimal element.

Algorithm: To sort a poset (S, R).

- Select a (any) minimal element and put it in the list. Delete it from S.
- Continue until all elements appear in the list (and S is void).

The problem of project schedul:

						
A	**C**	**B**	**E**	**F**	**D**	**G**

The order for the task: A<C<B<E<F<D<G

Homework:

SE： P. 630 5, 10, 23(a),(c), 32, 44, 66

EE： P. 662 5, 10, 23(a),(c), 32, 44, 66