Discrete Mathematics and Its Applications

Lecture 6: Discrete Probability: Closures and Equivalence of Relations

MING GAO

DaSE@ECNU
(for course related communications)
mgao@dase.ecnu.edu.cn

Dec. 18, 2018

Outline

Closures of relations

Definition

If there is a relation S with property P (such as reflexivity, symmetry, or transitivity) containing R such that S is a subset of every relation with property P containing R, then S is called the closure of R with respect to P.

Reflexive closure

Question:
What is the reflexive closure of the relation $R = \{(a, b) | a < b\}$ on the set of integers?

Closures of relations

Definition

If there is a relation S with property P (such as reflexivity, symmetry, or transitivity) containing R such that S is a subset of every relation with property P containing R, then S is called the closure of R with respect to P.

Reflexive closure

Question:
What is the reflexive closure of the relation $R = \{(a, b)|a < b\}$ on the set of integers?
Solution:
The reflexive closure of R is

$$R \cup \Delta = \{(a, b)|a < b\} \cup \{(a, a)|a \in Z\} = \{(a, b)|a \leq b\}.$$

Closures of relations Cont'd

Symmetric closure

Question:
What is the symmetric closure of the relation $R = \{(a, b) | a < b\}$ on the set of integers?

Closures of relations Cont'd

Symmetric closure

Question:
What is the symmetric closure of the relation $R = \{(a, b)|a < b\}$ on the set of integers?
Solution:
The symmetric closure of R is

$$R \cup \Delta = \{(a, b)|a < b\} \cup \{(a, b)|a > b\} = \{(a, b)|a \neq b\}.$$

Paths in digraphs

Definition

A **path** from a to b in the directed graph G is a sequence of edges $(x_0, x_1), (x_1, x_2), (x_2, x_3), \cdots, (x_{n-1}, x_n)$ in G, where n is a nonnegative integer, and $x_0 = a$ and $x_n = b$. This path is denoted by $a, x_1, x_2, \cdots, x_{n-1}, b$ and has length n.

A path of length $n \geq 1$ that begins and ends at the same vertex is called a **circuit or cycle**.

- We view the empty set of edges as a path of length zero from a to a.

Paths in digraphs

Definition

A **path** from a to b in the directed graph G is a sequence of edges $(x_0, x_1), (x_1, x_2), (x_2, x_3), \cdots, (x_{n-1}, x_n)$ in G, where n is a nonnegative integer, and $x_0 = a$ and $x_n = b$. This path is denoted by $a, x_1, x_2, \cdots, x_{n-1}, b$ and has length n.
A path of length $n \geq 1$ that begins and ends at the same vertex is called a **circuit or cycle**.

- We view the empty set of edges as a path of length zero from a to a.
- A path in a directed graph can pass through a vertex more than once. Moreover, an edge in a directed graph can occur more than once in a path.

Paths in digraphs

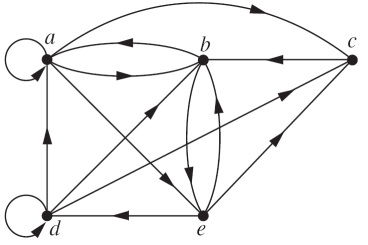
Definition

A **path** from a to b in the directed graph G is a sequence of edges $(x_0, x_1), (x_1, x_2), (x_2, x_3), \cdots, (x_{n-1}, x_n)$ in G, where n is a nonnegative integer, and $x_0 = a$ and $x_n = b$. This path is denoted by $a, x_1, x_2, \cdots, x_{n-1}, b$ and has length n.

A path of length $n \geq 1$ that begins and ends at the same vertex is called a **circuit or cycle**.

- We view the empty set of edges as a path of length zero from a to a.
- A path in a directed graph can pass through a vertex more than once. Moreover, an edge in a directed graph can occur more than once in a path.
- A path in a directed graph is obtained by traversing along edges (in the same direction as indicated by the arrow on the edge).

Example of path



Question:

Which of the following are paths in the directed graph shown in the figure:

- a, b, e, d;
- a, e, d, c, b;
- b, a, c, b, a, a, b;
- d, c;
- c, b, a;
- e, b, a, b, a, b, e?

What are the lengths of those that are paths?

Which of the paths in this list are circuits?

Theorem

Let R be a relation on a set A. There is a path of length n, where n is a positive integer, from a to b if and only if $(a, b) \in R^n$.

Theorem

Let R be a relation on a set A. There is a path of length n, where n is a positive integer, from a to b if and only if $(a, b) \in R^n$.

Proof: (**Mathematical induction:**)

By definition, there is a path from a to b of length one if and only if $(a, b) \in R$, so the theorem is true when $n = 1$.

Theorem

Let R be a relation on a set A. There is a path of length n, where n is a positive integer, from a to b if and only if $(a, b) \in R^n$.

Proof: (**Mathematical induction:**)

By definition, there is a path from a to b of length one if and only if $(a, b) \in R$, so the theorem is true when $n = 1$.

Assume that the theorem is true for the positive integer n.

Theorem

Let R be a relation on a set A. There is a path of length n, where n is a positive integer, from a to b if and only if $(a, b) \in R^n$.

Proof: (**Mathematical induction:**)

By definition, there is a path from a to b of length one if and only if $(a, b) \in R$, so the theorem is true when $n = 1$.

Assume that the theorem is true for the positive integer n. There is a path of length $n+1$ from a to b if and only if there is an element $c \in A$ such that there is a path of length one from a to c, so $(a, c) \in R$, and a path of length n from c to b, that is, $(c, b) \in R^n$.

Theorem

Let R be a relation on a set A. There is a path of length n, where n is a positive integer, from a to b if and only if $(a, b) \in R^n$.

Proof: (**Mathematical induction:**)

By definition, there is a path from a to b of length one if and only if $(a, b) \in R$, so the theorem is true when $n = 1$.

Assume that the theorem is true for the positive integer n. There is a path of length $n+1$ from a to b if and only if there is an element $c \in A$ such that there is a path of length one from a to c, so $(a, c) \in R$, and a path of length n from c to b, that is, $(c, b) \in R^n$. Consequently, by the inductive hypothesis, there is a path of length $n + 1$ from a to b if and only if there is an element c with $(a, c) \in R$ and $(c, b) \in R^n$. But there is such an element if and only if $(a, b) \in R^{n+1}$.

Theorem

Let R be a relation on a set A. There is a path of length n, where n is a positive integer, from a to b if and only if $(a, b) \in R^n$.

Proof: (**Mathematical induction:**)

By definition, there is a path from a to b of length one if and only if $(a, b) \in R$, so the theorem is true when $n = 1$.

Assume that the theorem is true for the positive integer n. There is a path of length $n+1$ from a to b if and only if there is an element $c \in A$ such that there is a path of length one from a to c, so $(a, c) \in R$, and a path of length n from c to b, that is, $(c, b) \in R^n$. Consequently, by the inductive hypothesis, there is a path of length $n+1$ from a to b if and only if there is an element c with $(a, c) \in R$ and $(c, b) \in R^n$. But there is such an element if and only if $(a, b) \in R^{n+1}$.

Therefore, there is a path of length $n+1$ from a to b if and only if $(a, b) \in R^{n+1}$. This completes the proof.

Connectivity relation

Definition

Let R be a relation on a set A. The *connectivity relation* R^* consists of the pairs (a, b) such that there is a path of length at least one from a to b in R.

- $R^* = \bigcup_{n=1}^{\infty} R^n$;

Connectivity relation

Definition

Let R be a relation on a set A. The *connectivity relation* R^* consists of the pairs (a, b) such that there is a path of length at least one from a to b in R.

- $R^* = \bigcup_{n=1}^{\infty} R^n$;
- Let R be the relation on the set of all people in the world that contains (a, b) if a has met b.
  - What is R^n, where n is a positive integer greater than one?
  - What is R^*?

Theorem

The transitive closure of a relation R equals the connectivity relation R^*.

Theorem

The transitive closure of a relation R equals the connectivity relation R^*.

Proof.

Note that $R \subset R^*$. To show that R^* is the transitive closure of R we must also show that R^* is transitive and that $R^* \subset S$ whenever S is a transitive relation that contains R.

Theorem

The transitive closure of a relation R equals the connectivity relation R^*.

Proof.

Note that $R \subset R^*$. To show that R^* is the transitive closure of R we must also show that R^* is transitive and that $R^* \subset S$ whenever S is a transitive relation that contains R.
First, if $(a, b) \in R^*$ and $(b, c) \in R^*$, then $\exists m, n$ s.t. $(a, b) \in R^n$ and $(b, c) \in R^m$. Thus $(a, c) \in R^{m+n} \subset R^*$.

Theorem

The transitive closure of a relation R equals the connectivity relation R^*.

Proof.

Note that $R \subset R^*$. To show that R^* is the transitive closure of R we must also show that R^* is transitive and that $R^* \subset S$ whenever S is a transitive relation that contains R.
First, if $(a, b) \in R^*$ and $(b, c) \in R^*$, then $\exists m, n$ s.t. $(a, b) \in R^n$ and $(b, c) \in R^m$. Thus $(a, c) \in R^{m+n} \subset R^*$.
Now suppose that S is a transitive relation containing R. Because S is transitive, $S^n \subset S$ (by Theorem 1 of previous slides) and S^n also is transitive (why?). Furthermore, because $S^* = \bigcup_{n=1}^{\infty} S^n$ and and $S^k \subset S$, it follows that $S^* \subset S$. Now note that if $R \subset S$, then $R^* \subset S^*$, because any path in R is also a path in S. Consequently, $R^* \subset S^* \subset S$. Thus, any transitive relation that contains R must also contain R^*. Therefore, R^* is the transitive closure of R. □

Lemma

Let R be a relation on set A of n elements. If there is a path of length at least one in R from a to b, then there is such a path with length not exceeding n. Moreover, when $a \neq b$, if there is a path of length at least one in R from a to b, then there is such a path with length not exceeding $n - 1$.

Lemma

Let R be a relation on set A of n elements. If there is a path of length at least one in R from a to b, then there is such a path with length not exceeding n. Moreover, when $a \neq b$, if there is a path of length at least one in R from a to b, then there is such a path with length not exceeding $n-1$.

Proof: Let m be the length of the shortest path from a to b in R, namely, $x_0 = a, x_1, x_2, \cdots, x_m = b$.

Lemma

Let R be a relation on set A of n elements. If there is a path of length at least one in R from a to b, then there is such a path with length not exceeding n. Moreover, when $a \neq b$, if there is a path of length at least one in R from a to b, then there is such a path with length not exceeding $n-1$.

Proof: Let m be the length of the shortest path from a to b in R, namely, $x_0 = a, x_1, x_2, \cdots, x_m = b$.

If $a = b$ and $m > n$, i.e., $m \geq n+1$. By the pigeonhole principle, because there are n vertices in A, among the m vertices at least two are equal. Suppose that $x_i = x_j$ with $0 \leq i < j \leq m-1$. Then the path contains a circuit from x_i to itself. This circuit can be deleted from the path from a to b, leaving a path, namely, $x_0, x_1, \cdots, x_i, x_{j+1}, \cdots, x_m$, from a to b of shorter length. Hence, the length of shortest path must have length less than or equal to n.

Lemma

Let R be a relation on set A of n elements. If there is a path of length at least one in R from a to b, then there is such a path with length not exceeding n. Moreover, when $a \neq b$, if there is a path of length at least one in R from a to b, then there is such a path with length not exceeding $n-1$.

Proof: Let m be the length of the shortest path from a to b in R, namely, $x_0 = a, x_1, x_2, \cdots, x_m = b$.

If $a = b$ and $m > n$, i.e., $m \geq n+1$. By the pigeonhole principle, because there are n vertices in A, among the m vertices at least two are equal. Suppose that $x_i = x_j$ with $0 \leq i < j \leq m-1$. Then the path contains a circuit from x_i to itself. This circuit can be deleted from the path from a to b, leaving a path, namely, $x_0, x_1, \cdots, x_i, x_{j+1}, \cdots, x_m$, from a to b of shorter length. Hence, the length of shortest path must have length less than or equal to n.

The case where $a \neq b$ is left as an exercise.

Theorem

From the above lemma, we have

$$R^* = \bigcup_{k=1}^{n} R^k$$

Theorem

Let M_R be the zero-one matrix of the relation R on a set with n elements. Then the zero-one matrix of the transitive closure R^* is

$$M_{R^*} = M_R \vee M_R^{[2]} \vee M_R^{[3]} \vee \cdots \vee M_R^{[n]}.$$

Example

Question:

Find the zero-one matrix of the transitive closure of the relation R where

$$M_R = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}.$$

Example

Question:

Find the zero-one matrix of the transitive closure of the relation R where

$$M_R = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}.$$

Solution:

The zero-one matrix of the transitive closure of R is

$$M_{R^*} = M_R \vee M_R^{[2]} \vee M_R^{[3]}.$$

Example

Question:
Find the zero-one matrix of the transitive closure of the relation R where

$$M_R = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}.$$

Solution:
The zero-one matrix of the transitive closure of R is

$$M_{R^*} = M_R \vee M_R^{[2]} \vee M_R^{[3]}.$$

We have,

$$M_R^{[2]} = M_R^{[3]} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}, M_R^* = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}.$$

Algorithm

ALGORITHM 1 A Procedure for Computing the Transitive Closure.

procedure *transitive closure* ($\mathbf{M}_R$: zero–one $n \times n$ matrix)
$\mathbf{A} := \mathbf{M}_R$
$\mathbf{B} := \mathbf{A}$
for $i := 2$ **to** n
    $\mathbf{A} := \mathbf{A} \odot \mathbf{M}_R$
    $\mathbf{B} := \mathbf{B} \vee \mathbf{A}$
return $\mathbf{B}$ {$\mathbf{B}$ is the zero–one matrix for R^*}

Algorithm

ALGORITHM 1 A Procedure for Computing the Transitive Closure.

procedure *transitive closure* ($\mathbf{M}_R$: zero–one $n \times n$ matrix)
$\mathbf{A} := \mathbf{M}_R$
$\mathbf{B} := \mathbf{A}$
for $i := 2$ **to** n
    $\mathbf{A} := \mathbf{A} \odot \mathbf{M}_R$
    $\mathbf{B} := \mathbf{B} \vee \mathbf{A}$
return $\mathbf{B}$\{$\mathbf{B}$ is the zero–one matrix for R^*\}

- A Boolean products can be found in $n^2(2n-1)$ bit operations;
- $M_R^{[n]}$ requires that $n-1$ Boolean products of $n \times n$ zeroCone matrices be found;
- Computing M_{R^*} needs $(n-1)n^2$ bit operations.
- Overall, the algorithms is $O(n^4)$ bit operations.

Interior vertices

Interior vertices

If $a, x_1, x_2, \cdots, x_{m-1}, b$ is a path, vertices $x_1, x_2, \cdots, x_{m-1}$ are **interior vertices** of (a, b).

Interior vertices

Interior vertices

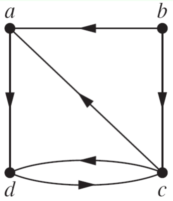
If $a, x_1, x_2, \cdots, x_{m-1}, b$ is a path, vertices $x_1, x_2, \cdots, x_{m-1}$ are **interior vertices** of (a, b).

We define a sequence of zero-one matrices, namely $W_0 = M_R$ and $W_k = [w_{ij}^k]$, where

$$w_{ij}^k = \begin{cases} 1, & \text{all interior vertices of } (v_i, v_j) \text{ are in } \{v_1, v_2, \cdots, v_k\}; \\ 0, & \text{otherwise.} \end{cases}$$

Note that $W_n = M_{R^*}$, because the $(i, j)-$th entry of M_{R^*} is 1 if and only if there is a path from v_i to v_j , with all interior vertices in $\{v_1, v_2, \cdots, v_n\}$.

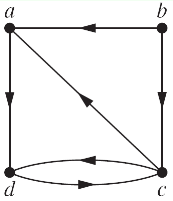
Example of W_k



Question: Find the matrices W_0, W_1, W_2, W_3, and W_4 for the relation R with the digraph in the figure.

$$W_0 = M_R = \begin{array}{cc} v_1 & a \\ v_2 & b \\ v_3 & c \\ v_4 & d \end{array} \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Example of W_k



Question: Find the matrices W_0, W_1, W_2, W_3, and W_4 for the relation R with the digraph in the figure.

$$W_0 = M_R = \begin{array}{cc} v_1 & a \\ v_2 & b \\ v_3 & c \\ v_4 & d \end{array} \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$W_1 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, W_2 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Example of W_k Cont'd

$$W_3 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}, W_4 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}.$$

Thus, we have

$$M_{R^*} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}.$$

Lemma

Let $W_k = [w_{ij}^{[k]}]$ be the zero-one matrix that has a 1 in its (i, j)th position if and only if there is a path from v_i to v_j with interior vertices from the set $\{v_1, v_2, \cdots, v_k\}$. Then

$$w_{ij}^{[k]} = w_{ij}^{[k-1]} \vee (w_{ik}^{[k-1]} \wedge w_{kj}^{[k-1]}),$$

whenever i, j, and k are positive integers not exceeding n.

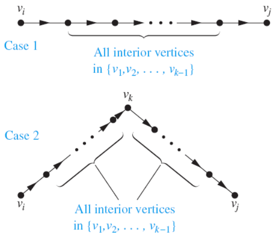
Lemma

Let $W_k = [w_{ij}^{[k]}]$ be the zero-one matrix that has a 1 in its (i, j)th position if and only if there is a path from v_i to v_j with interior vertices from the set $\{v_1, v_2, \cdots, v_k\}$. Then

$$w_{ij}^{[k]} = w_{ij}^{[k-1]} \vee (w_{ik}^{[k-1]} \wedge w_{kj}^{[k-1]}),$$

whenever i, j, and k are positive integers not exceeding n.

Proof.



Either a path from v_i to v_j already existed before v_k was permitted as an interior vertex, or allowing vk as an interior vertex produces a path that goes from v_i to v_k and then from v_k to v_j. These two cases are shown in the figure.

Warshall's Algorithm

ALGORITHM 2 Warshall Algorithm.

```
procedure Warshall (M_R : n × n zero–one matrix)
W := M_R
for k := 1 to n
    for i := 1 to n
        for j := 1 to n
        w_ij := w_ij ∨ (w_ik ∧ w_kj)
return W{W = [w_ij] is M_R*}
```

Warshall's Algorithm

ALGORITHM 2 Warshall Algorithm.

procedure *Warshall* ($\mathbf{M}_R$: $n \times n$ zero–one matrix)
$\mathbf{W} := \mathbf{M}_R$
for $k := 1$ **to** n
    for $i := 1$ **to** n
        for $j := 1$ **to** n
        $w_{ij} := w_{ij} \vee (w_{ik} \wedge w_{kj})$
return $\mathbf{W}\{\mathbf{W} = [w_{ij}]$ is $\mathbf{M}_{R^*}\}$

- To find all n^2 entries of W_k from those of W_{k-1} requires $2n^2$ bit operations.;
- The algorithm computes the sequence of n zero-one matrices $W_1, W_2, \cdots, W_n = M_{R^*}$, the total number of bit operations used is $n \cdot 2n^2 = 2n^3$.

Equivalence relations

Definition

A relation on a set A is called an **equivalence relation** if it is reflexive, symmetric, and transitive.

Two elements a and b that are related by an equivalence relation are called **equivalent**. The notation $a \sim b$ is often used to denote that a and b are equivalent elements with respect to a particular equivalence relation.

- Every element should be equivalent to itself;
- a is related to b, and b is related to a by the symmetric property;
- If a and b are equivalent and b and c are equivalent, it follows that a and c are equivalent.

Examples

Let R be the relation on the set of integers such that aRb if and only if $a = b$ or $a = -b$. Is R an equivalence relation?

Examples

Let R be the relation on the set of integers such that aRb if and only if $a = b$ or $a = -b$. Is R an equivalence relation?

Let R be the relation on the set of real numbers such that aRb if and only if $a - b$ is an integer. Is R an equivalence relation?

Examples

Let R be the relation on the set of integers such that aRb if and only if $a = b$ or $a = -b$. Is R an equivalence relation?

Let R be the relation on the set of real numbers such that aRb if and only if $a - b$ is an integer. Is R an equivalence relation?

Let m be an integer with $m > 1$. Show that the relation

$$R = \{(a, b) | a \equiv b (\text{mod } m)\}$$

is an equivalence relation on the set of integers.

Examples

Let R be the relation on the set of integers such that aRb if and only if $a = b$ or $a = -b$. Is R an equivalence relation?

Let R be the relation on the set of real numbers such that aRb if and only if $a - b$ is an integer. Is R an equivalence relation?

Let m be an integer with $m > 1$. Show that the relation

$$R = \{(a, b) | a \equiv b (\text{mod } m)\}$$

is an equivalence relation on the set of integers.

Let R be the relation on the set of real numbers such that xRy if and only if x and y are real numbers that differ by less than 1, that is $|x - y| < 1$. Show that R is not an equivalence relation.

Equivalence Classes

Definition

Let R be an equivalence relation on a set A. The set of all elements that are related to an element a of A is called the **equivalence class** of a. The equivalence class of a with respect to R is denoted by $[a]_R$. When only one relation is under consideration, we can delete the subscript R and write $[a]$ for this equivalence class.

- $$[a]_R = \{s|(a, s) \in R\};$$
- If $b \in [a]_R$, then b is called a **representative** of this equivalence class;
- Any element of a class can be used as a representative of this class.

Examples

Question: What is the equivalence class of an integer for R such that aRb if and only if $a = b$ or $a = -b$?
Solution: $[a] = \{a, -a\}$.

Examples

Question: What is the equivalence class of an integer for R such that aRb if and only if $a = b$ or $a = -b$?
Solution: $[a] = \{a, -a\}$.

Question: What are the equivalence classes of 0 and 1 for congruence modulo 4?
Solution: $[0] = \{\cdots, -8, -4, 0, 4, 8, \cdots\}$,
$[1] = \{\cdots, -7, -3, 1, 5, 9, \cdots\}$.

Examples

Question: What is the equivalence class of an integer for R such that aRb if and only if $a = b$ or $a = -b$?
Solution: $[a] = \{a, -a\}$.

Question: What are the equivalence classes of 0 and 1 for congruence modulo 4?
Solution: $[0] = \{\cdots, -8, -4, 0, 4, 8, \cdots\}$,
$[1] = \{\cdots, -7, -3, 1, 5, 9, \cdots\}$.

Let m be an integer with $m > 1$. Show that the relation

$$R = \{(a, b) | a \equiv b (\text{mod } m)\}$$

is an equivalence relation on the set of integers.

Theorem

Let R be an equivalence relation on a set A. These statements for elements a and b of A are equivalent:

(i) aRb;

(ii) $[a] = [b]$;

(iii) $[a] \cap [b] \neq \emptyset$.

Theorem

Let R be an equivalence relation on a set A. These statements for elements a and b of A are equivalent:

(i) aRb;

(ii) $[a] = [b]$;

(iii) $[a] \cap [b] \neq \emptyset$.

Proof.

(i)$\Rightarrow$ (ii):

Assume that aRb and $c \in [a]$.

Theorem

Let R be an equivalence relation on a set A. These statements for elements a and b of A are equivalent:

(i) aRb;

(ii) $[a] = [b]$;

(iii) $[a] \cap [b] \neq \emptyset$.

Proof.

(i)$\Rightarrow$ (ii):

Assume that aRb and $c \in [a]$.

Because R is symmetric and transitive, we know bRa and aRc, it further follows that bRc. Hence, $c \in [b]$, i.e., $[a] \subset [b]$.

Similarly, we can know that $[b] \subset [a]$.

Thus, we have $[a] = [b]$, completing the proof of this statement. □

Proof Cont'd

Proof.

(ii)$\Rightarrow$ (iii):

Assume that $[a] = [b]$.

Proof Cont'd

Proof.

(ii)$\Rightarrow$ (iii):

Assume that $[a] = [b]$. First $[a]$ is nonempty because $a \in [a]$ (because R is reflexive).

Proof Cont'd

Proof.

(ii)$\Rightarrow$ (iii):

Assume that $[a] = [b]$. First $[a]$ is nonempty because $a \in [a]$ (because R is reflexive).

Thus $[a] \cap [b] \neq \emptyset$.

(iii)$\Rightarrow$ (i):

Suppose that $[a] \cap [b] \neq \emptyset$. Then there is an element c with $c \in [a]$ and $c \in [b]$.

Proof Cont'd

Proof.

(ii)$\Rightarrow$ (iii):

Assume that $[a] = [b]$. First $[a]$ is nonempty because $a \in [a]$ (because R is reflexive).

Thus $[a] \cap [b] \neq \emptyset$.

(iii)$\Rightarrow$ (i):

Suppose that $[a] \cap [b] \neq \emptyset$. Then there is an element c with $c \in [a]$ and $c \in [b]$.

In other words, aRc and bRc. By the symmetric property, cRb.

Proof Cont'd

Proof.

(ii)$\Rightarrow$ (iii):
Assume that $[a] = [b]$. First $[a]$ is nonempty because $a \in [a]$ (because R is reflexive).
Thus $[a] \cap [b] \neq \emptyset$.
(iii)$\Rightarrow$ (i):
Suppose that $[a] \cap [b] \neq \emptyset$. Then there is an element c with $c \in [a]$ and $c \in [b]$.
In other words, aRc and bRc. By the symmetric property, cRb.
Then by transitivity, because aRc and cRb, we have aRb. □

Note that

- $\bigcup_{a \in A} [a]_R = A$;
- $[a] = [b]$ or $[a] \cap [b] = \emptyset$.

Partition

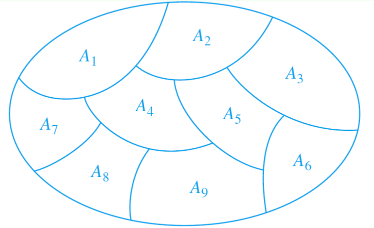
Definition

A *partition* of a set S is a collection of disjoint nonempty subsets of S that have S as their union.

Partition

Definition

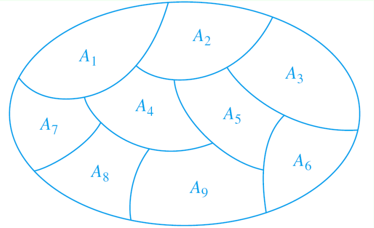
A *partition* of a set S is a collection of disjoint nonempty subsets of S that have S as their union.



Partition

Definition

A *partition* of a set S is a collection of disjoint nonempty subsets of S that have S as their union.



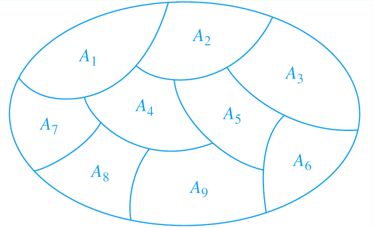
That is, the collection of subsets A_i, $i \in I$ (where I is an index set) forms a partition of S if and only if

- $A_i \neq \emptyset$ for $i \in I$;
- $A_i \cap A_j = \emptyset$ when $i \neq j$;
- $\bigcup_{i \in I} A_i = S$.

Partition

Definition

A *partition* of a set S is a collection of disjoint nonempty subsets of S that have S as their union.



That is, the collection of subsets A_i, $i \in I$ (where I is an index set) forms a partition of S if and only if

- $A_i \neq \emptyset$ for $i \in I$;
- $A_i \cap A_j = \emptyset$ when $i \neq j$;
- $\bigcup_{i \in I} A_i = S$.

- The equivalence classes of an equivalence relation on a set form a partition of the set.
- Conversely, every partition of a set can be used to form an equivalence relation?

Theorem

Let R be an equivalence relation on S. Then the equivalence classes of R form a partition of S. Conversely, given a partition $\{A_i | i \in I\}$ of S, there is an equivalence relation R that has $A_i, i \in I$, as its equivalence classes.

Theorem

Let R be an equivalence relation on S. Then the equivalence classes of R form a partition of S. Conversely, given a partition $\{A_i | i \in I\}$ of S, there is an equivalence relation R that has $A_i, i \in I$, as its equivalence classes.

Proof: $\Rightarrow$: (Obvious)

Theorem

Let R be an equivalence relation on S. Then the equivalence classes of R form a partition of S. Conversely, given a partition $\{A_i | i \in I\}$ of S, there is an equivalence relation R that has $A_i, i \in I$, as its equivalence classes.

Proof: $\Rightarrow$: (Obvious)

$\Leftarrow$: Assume that $\{A_i | i \in I\}$ is a partition on S and R is the relation on S consisting of the pairs $(x, y) \in A_i$.

Theorem

Let R be an equivalence relation on S. Then the equivalence classes of R form a partition of S. Conversely, given a partition $\{A_i|i \in I\}$ of S, there is an equivalence relation R that has $A_i, i \in I$, as its equivalence classes.

Proof: $\Rightarrow$: (Obvious)

$\Leftarrow$: Assume that $\{A_i|i \in I\}$ is a partition on S and R is the relation on S consisting of the pairs $(x, y) \in A_i$.

- Since $(a, a) \in R$ for every $a \in S$, because a is in the same subset as itself. Hence, R is reflexive;
- If $(a, b) \in R$, then b and a are in the same subset of the partition, so that $(b, a) \in R$ as well. Hence, R is symmetric.
- If $(a, b) \in R$ and $(b, c) \in R$, then a and b are in the same subset X in the partition, and b and c are in the same subset X of the partition. Consequently, a and c belong to the same subset of the partition, so $(a, c) \in R$. Thus, R is transitive.

Example I

What are the sets in the partition of the integers arising from congruence modulo 4?

Example I

What are the sets in the partition of the integers arising from congruence modulo 4?

$$
\begin{aligned}
[0]_4 &= \{\cdots, -8, -4, 0, 4, 8, \cdots\}, \\
[1]_4 &= \{\cdots, -7, -3, 1, 5, 9, \cdots\}, \\
[2]_4 &= \{\cdots, -6, -2, 2, 6, 10, \cdots\}, \\
[3]_4 &= \{\cdots, -5, -1, 3, 7, 11, \cdots\},
\end{aligned}
$$

Example I

What are the sets in the partition of the integers arising from congruence modulo 4?

$$
\begin{aligned}
[0]_4 &= \{\cdots, -8, -4, 0, 4, 8, \cdots\}, \\
[1]_4 &= \{\cdots, -7, -3, 1, 5, 9, \cdots\}, \\
[2]_4 &= \{\cdots, -6, -2, 2, 6, 10, \cdots\}, \\
[3]_4 &= \{\cdots, -5, -1, 3, 7, 11, \cdots\},
\end{aligned}
$$

The congruence classes modulo m provide a useful illustration of Theorem 2. There are m different congruence classes modulo m, corresponding to the m different remainders possible when an integer is divided by m. These m congruence classes are denoted by $[0]_m, [1]_m, \cdots, [m-1]_m$. They form a partition of the set of integers.

Example II

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 if and only if $s = t$, or both s and t have at least n characters and the first n characters of s and t are the same. What are the sets in the partition given by R_3?

Example II

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 if and only if $s = t$, or both s and t have at least n characters and the first n characters of s and t are the same. What are the sets in the partition given by R_3?

Solution: Note that every bit string of length less than three is equivalent to itself. Hence $[\lambda]_{R_3} = \{\lambda\}$, $[0]_{R_3} = \{0\}$, $[1]_{R_3} = \{1\}$, $[00]_{R_3} = \{00\}$, $[01]_{R_3} = \{01\}$, $[10]_{R_3} = \{10\}$, and $[11]_{R_3} = \{11\}$.

Example II

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 if and only if $s = t$, or both s and t have at least n characters and the first n characters of s and t are the same. What are the sets in the partition given by R_3?

Solution: Note that every bit string of length less than three is equivalent to itself. Hence $[\lambda]_{R_3} = \{\lambda\}$, $[0]_{R_3} = \{0\}$, $[1]_{R_3} = \{1\}$, $[00]_{R_3} = \{00\}$, $[01]_{R_3} = \{01\}$, $[10]_{R_3} = \{10\}$, and $[11]_{R_3} = \{11\}$.

$$[000]_{R_3} = \{000, 0000, 0001, 00000, 00001, 00010, 00011, \cdots\},$$
$$[001]_{R_3} = \{001, 0010, 0011, 00100, 00101, 00110, 00111, \cdots\},$$
$$[010]_{R_3} = \{010, 0100, 0101, 01000, 01001, 01010, 01011, \cdots\},$$
$$[011]_{R_3} = \{011, 0110, 0111, 01100, 01101, 01110, 01111, \cdots\},$$
$$[100]_{R_3} = \{100, 1000, 1001, 10000, 10001, 10010, 10011, \cdots\},$$
$$[101]_{R_3} = \{101, 1010, 1011, 10100, 10101, 10110, 10111, \cdots\},$$
$$[110]_{R_3} = \{110, 1100, 1101, 11000, 11001, 11010, 11011, \cdots\},$$
$$[111]_{R_3} = \{111, 1110, 1111, 11100, 11101, 11110, 11111, \cdots\}.$$

Partial orderings

Definition

A relation R on a set S is called a **partial ordering** or **partial order** if it is reflexive, antisymmetric, and transitive. A set S together with a partial ordering R is called a **partially ordered set**, or poset, and is denoted by (S, R). Members of S are called elements of the poset.

Partial orderings

Definition

A relation R on a set S is called a **partial ordering** or **partial order** if it is reflexive, antisymmetric, and transitive. A set S together with a partial ordering R is called a **partially ordered set**, or poset, and is denoted by (S, R). Members of S are called elements of the poset.

- We often use relations to order some or all of the elements of sets;
- $(a, b) \in R \rightarrow (b, a) \notin R$, otherwise $a = b$;
- $\forall a \in S, (a, a) \in R$;
- $\forall a \forall b \forall c((a, b) \in R, (b, c) \in R \rightarrow (a, c) \in R)$.

Examples

Show that the "greater than or equal" relation ($\geq$) is a partial ordering on the set of integers.

Examples

Show that the "greater than or equal" relation ($\geq$) is a partial ordering on the set of integers.

Show that the divisibility relation $|$ is a partial ordering on the set of positive integers.

Examples

Show that the "greater than or equal" relation ($\geq$) is a partial ordering on the set of integers.

Show that the divisibility relation $|$ is a partial ordering on the set of positive integers.

Show that the inclusion relation $\subseteq$ is a partial ordering on the power set of a set S.

Examples

Show that the "greater than or equal" relation ($\geq$) is a partial ordering on the set of integers.

Show that the divisibility relation $\mid$ is a partial ordering on the set of positive integers.

Show that the inclusion relation $\subseteq$ is a partial ordering on the power set of a set S.

Let R be the relation on the set of people such that xRy if x and y are people and x is older than y. Show that R is not a partial ordering.

Customarily, the notation $a \preceq b$ is used to denote that $(a, b) \in R$ in an arbitrary poset (S, R). ($a \prec b$ denotes $a \preceq b$, but $a \neq b$)

Comparable

Definition

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

Comparable

Definition

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

- In the poset $(Z^+, |)$, are the integers 3 and 9 comparable? Are 5 and 7 comparable?

Comparable

Definition

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

- In the poset $(Z^+, |)$, are the integers 3 and 9 comparable? Are 5 and 7 comparable?
- The poset $(Z^+, |)$ is not totally ordered because it contains elements that are incomparable, such as 5 and 7.

Comparable

Definition

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

- In the poset $(Z^+, |)$, are the integers 3 and 9 comparable? Are 5 and 7 comparable?
- The poset $(Z^+, |)$ is not totally ordered because it contains elements that are incomparable, such as 5 and 7.
- The set of ordered pairs $Z^+ \times Z^+$ with $(a_1, a_2) \preceq (b_1, b_2)$ if $a_1 < b_1$, or if $a_1 = b_1$ and $a_2 \leq b_2$ (the lexicographic ordering), is a well-ordered set. How about $Z \times Z$?

Totally ordered

Definition

If $(S, \preceq)$ is a poset and every two elements of S are comparable, S is called a **totally ordered** or **linearly ordered set**, and $\preceq$ is called a total order or a linear order. A totally ordered set is also called a **chain**.

Totally ordered

Definition

If $(S, \preceq)$ is a poset and every two elements of S are comparable, S is called a **totally ordered** or **linearly ordered set**, and $\preceq$ is called a total order or a linear order. A totally ordered set is also called a **chain**.

- The poset $(Z, \leq)$ is totally ordered, because $a \leq b$ or $b \leq a$ whenever a and b are integers.

Totally ordered

Definition

If $(S, \preceq)$ is a poset and every two elements of S are comparable, S is called a **totally ordered** or **linearly ordered set**, and $\preceq$ is called a total order or a linear order. A totally ordered set is also called a **chain**.

- The poset $(Z, \leq)$ is totally ordered, because $a \leq b$ or $b \leq a$ whenever a and b are integers.
- The adjective "partial" is used to describe partial orderings because pairs of elements may be incomparable.

Totally ordered

Definition

If $(S, \preceq)$ is a poset and every two elements of S are comparable, S is called a **totally ordered** or **linearly ordered set**, and $\preceq$ is called a total order or a linear order. A totally ordered set is also called a **chain**.

- The poset $(Z, \leq)$ is totally ordered, because $a \leq b$ or $b \leq a$ whenever a and b are integers.
- The adjective "partial" is used to describe partial orderings because pairs of elements may be incomparable.
- When every two elements in the set are comparable, the relation is called a total ordering.

Totally ordered

Definition

If $(S, \preceq)$ is a poset and every two elements of S are comparable, S is called a **totally ordered** or **linearly ordered set**, and $\preceq$ is called a total order or a linear order. A totally ordered set is also called a **chain**.

- The poset $(Z, \leq)$ is totally ordered, because $a \leq b$ or $b \leq a$ whenever a and b are integers.
- The adjective "partial" is used to describe partial orderings because pairs of elements may be incomparable.
- When every two elements in the set are comparable, the relation is called a total ordering.
- $(S, \preceq)$ is a **well-ordered set** if it is a poset such that $\preceq$ is a total ordering and every nonempty subset of S has a least element.

The principle of well-ordered induction

Theorem

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 $x \prec y$, then $P(y)$ is true.

The principle of well-ordered induction

Theorem

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 $x \prec y$, then $P(y)$ is true.

Proof.

Suppose it is not the case that $P(x)$ is true for all $x \in S$, i.e., there is an element $y \in S$ such that $P(y)$ is false.

The principle of well-ordered induction

Theorem

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 $x \prec y$, then $P(y)$ is true.

Proof.

Suppose it is not the case that $P(x)$ is true for all $x \in S$, i.e., there is an element $y \in S$ such that $P(y)$ is false.
Consequently, the set $A = \{x \in S | P(x) \text{ is false}\}$ is nonempty.

The principle of well-ordered induction

Theorem

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 $x \prec y$, then $P(y)$ is true.

Proof.

Suppose it is not the case that $P(x)$ is true for all $x \in S$, i.e., there is an element $y \in S$ such that $P(y)$ is false.
Consequently, the set $A = \{x \in S | P(x) \text{ is false}\}$ 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.

The principle of well-ordered induction

Theorem

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 $x \prec y$, then $P(y)$ is true.

Proof.

Suppose it is not the case that $P(x)$ is true for all $x \in S$, i.e., there is an element $y \in S$ such that $P(y)$ is false.
Consequently, the set $A = \{x \in S | P(x) \text{ is false}\}$ 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 $x \in S$. □

Lexicographic ordering

Definition

A **lexicographic ordering** can be defined on the cartesian product of n posets $(A_i, \preceq_i)$ for $i = 1, 2, \cdots, n$. Define the partial ordering $\preceq$ on $A_1 \times A_2 \times \cdots A_n$ by $(a_1, a_2, \cdots, a_n) \prec (b_1, b_2, \cdots, b_n)$ if $a_1 \prec_1 b_1$, or if there is an integer $i > 0$ such that $a_1 = b_1, \cdots, a_i = b_i$, and $a_{i+1} \prec_{i+1} b_{i+1}$.

Lexicographic ordering

Definition

A **lexicographic ordering** can be defined on the cartesian product of n posets $(A_i, \preceq_i)$ for $i = 1, 2, \cdots, n$. Define the partial ordering $\preceq$ on $A_1 \times A_2 \times \cdots A_n$ by $(a_1, a_2, \cdots, a_n) \prec (b_1, b_2, \cdots, b_n)$ if $a_1 \prec_1 b_1$, or if there is an integer $i > 0$ such that $a_1 = b_1, \cdots, a_i = b_i$, and $a_{i+1} \prec_{i+1} b_{i+1}$.

- Let $(A_1, \preceq_1)$ and $(A_2, \preceq_2)$ be two posets. The **lexicographic ordering** $\preceq$ on $A_1 \times A_2$ is defined by $(a1, a2) \prec (b1, b2)$, either if $a_1 \prec_1 b_1$ or if both $a_1 = b_1$ and $a_2 \prec_2 b_2$.

Lexicographic ordering

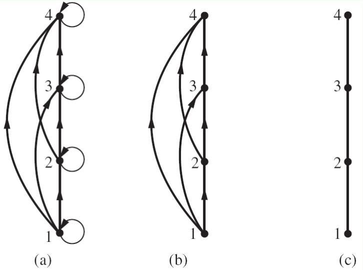
Definition

A **lexicographic ordering** can be defined on the cartesian product of n posets $(A_i, \preceq_i)$ for $i = 1, 2, \cdots, n$. Define the partial ordering $\preceq$ on $A_1 \times A_2 \times \cdots A_n$ by $(a_1, a_2, \cdots, a_n) \prec (b_1, b_2, \cdots, b_n)$ if $a_1 \prec_1 b_1$, or if there is an integer $i > 0$ such that $a_1 = b_1, \cdots, a_i = b_i$, and $a_{i+1} \prec_{i+1} b_{i+1}$.

- Let $(A_1, \preceq_1)$ and $(A_2, \preceq_2)$ be two posets. The **lexicographic ordering** $\preceq$ on $A_1 \times A_2$ is defined by $(a1, a2) \prec (b1, b2)$, either if $a_1 \prec_1 b_1$ or if both $a_1 = b_1$ and $a_2 \prec_2 b_2$.
- Determine whether $(3, 5) \prec (4, 8)$, whether $(3, 8) \prec (4, 5)$, and whether $(4, 9) \prec (4, 11)$ in the poset $(Z \times Z, \preceq)$, where $\preceq$ is the lexicographic ordering constructed from the usual $\leq$ relation on Z.

Hasse diagrams

Many edges in the directed graph for a finite poset do not have to be shown because they must be present.



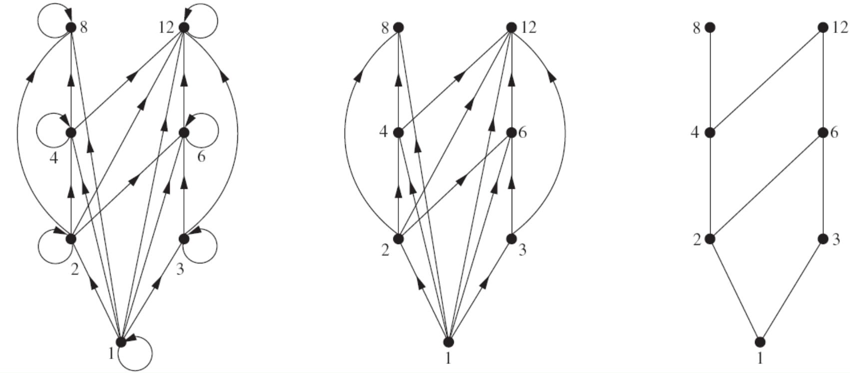
In general, we can represent a finite poset $(S, \preceq)$ using this procedure:

- Remove these loops;
- Remove all edges (x, y) if $\exists z \in S$ such that $x \prec z$ and $z \prec y$;
- Arrange each edge so that its initial vertex is below its terminal vertex;
- Remove all the arrows on the directed edges.

The resulting diagram is called the **Hasse diagram** of $(S, \preceq)$.

Example

Draw the Hasse diagram representing the partial ordering $\{(a, b) | a \text{ divides } b\}$ on $\{1, 2, 3, 4, 6, 8, 12\}$.



Maximal and minimal elements

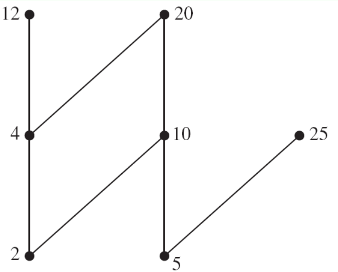
Definition

Element a is **maximal** in the poset $(S, \preceq)$ if there is no $b \in S$ such that $a \prec b$. Element a is **minimal** if there is no element $b \in S$ such that $b \prec a$.

Maximal and minimal elements

Definition

Element a is **maximal** in the poset $(S, \preceq)$ if there is no $b \in S$ such that $a \prec b$. Element a is **minimal** if there is no element $b \in S$ such that $b \prec a$.

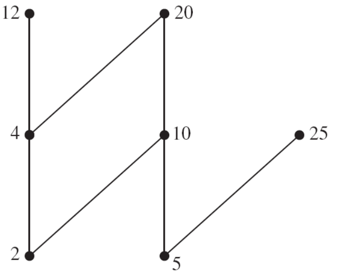


Which elements of the poset $(\{2, 4, 5, 10, 12, 20, 25\}, |)$ are maximal, and which are minimal?

Maximal and minimal elements

Definition

Element a is **maximal** in the poset $(S, \preceq)$ if there is no $b \in S$ such that $a \prec b$. Element a is **minimal** if there is no element $b \in S$ such that $b \prec a$.



Which elements of the poset $(\{2, 4, 5, 10, 12, 20, 25\}, |)$ are maximal, and which are minimal? The Hasse diagram in the figure for this poset shows that the maximal elements are 12, 20, and 25, and the minimal elements are 2 and 5.

Greatest and least elements

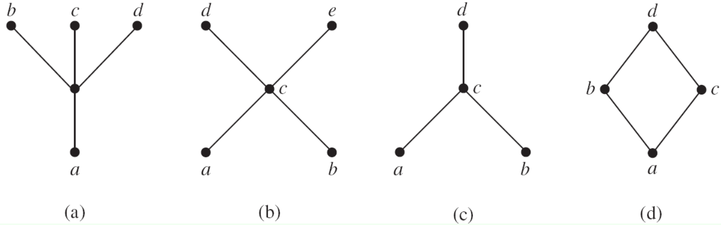
Definition

Element a is **greatest element** of $(S, \preceq)$ if $b \preceq a$ for all $b \in S$.
Element a is **least element** of $(S, \preceq)$ if $a \preceq b$ for all $b \in S$.

Greatest and least elements

Definition

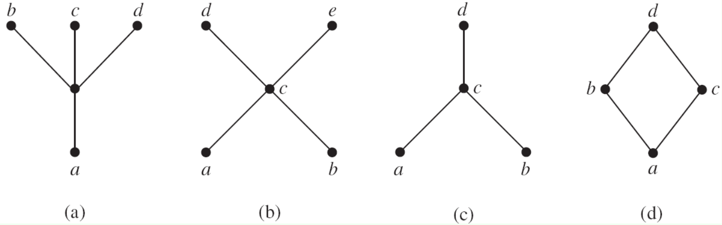
Element a is **greatest element** of $(S, \preceq)$ if $b \preceq a$ for all $b \in S$.
Element a is **least element** of $(S, \preceq)$ if $a \preceq b$ for all $b \in S$.



Greatest and least elements

Definition

Element a is **greatest element** of $(S, \preceq)$ if $b \preceq a$ for all $b \in S$. Element a is **least element** of $(S, \preceq)$ if $a \preceq b$ for all $b \in S$.



Determine whether the posets represented by each of the Hasse diagrams in the figure have a greatest element and a least element.

Upper and lower bounds

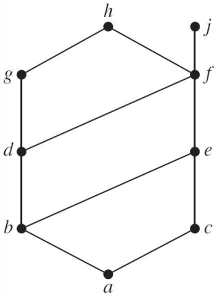
Definition

If u is an element of S such that $a \preceq u$ for all elements $a \in A$, then u is called an **upper bound** of A. Likewise, if l is an element of S such that $l \preceq a$ for all elements $a \in A$, then l is called a **lower bound** of A.

Upper and lower bounds

Definition

If u is an element of S such that $a \preceq u$ for all elements $a \in A$, then u is called an **upper bound** of A. Likewise, if l is an element of S such that $l \preceq a$ for all elements $a \in A$, then l is called a **lower bound** of A.

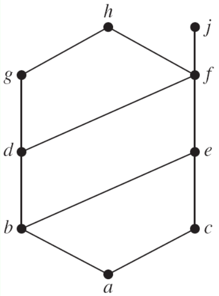


Question: Find the lower and upper bounds of the subsets $\{a, b, c\}$, $\{j, h\}$, and $\{a, c, d, f\}$ in the poset with the Hasse diagram shown in the figure.

Upper and lower bounds

Definition

If u is an element of S such that $a \preceq u$ for all elements $a \in A$, then u is called an **upper bound** of A. Likewise, if l is an element of S such that $l \preceq a$ for all elements $a \in A$, then l is called a **lower bound** of A.



Question: Find the lower and upper bounds of the subsets $\{a, b, c\}$, $\{j, h\}$, and $\{a, c, d, f\}$ in the poset with the Hasse diagram shown in the figure.

Solution: The upper bounds of $\{a, b, c\}$ are e, f, j, and h, and its only lower bound is a. There are no upper bounds of $\{j, h\}$, and its lower bounds are a, b, c, d, e, and f . The upper bounds of $\{a, c, d, f\}$ are f, h, and j , and its lower bound is a.

Least upper and greatest lower bounds

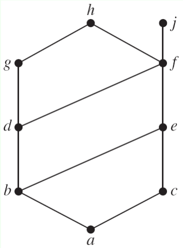
Definition

Element x is called the **least upper bound** of the subset A if x is an upper bound that is less than every other upper bound of A. Similarly, element y is called the **greatest lower bound** of A if y is a lower bound of A and $z \preceq y$ whenever z is a lower bound of A.

Least upper and greatest lower bounds

Definition

Element x is called the **least upper bound** of the subset A if x is an upper bound that is less than every other upper bound of A. Similarly, element y is called the **greatest lower bound** of A if y is a lower bound of A and $z \preceq y$ whenever z is a lower bound of A.

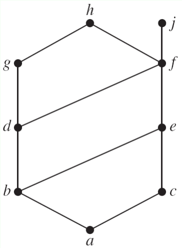


Question: Find the greatest lower and the least upper bounds of $\{b, d, g\}$ in the figure.

Least upper and greatest lower bounds

Definition

Element x is called the **least upper bound** of the subset A if x is an upper bound that is less than every other upper bound of A. Similarly, element y is called the **greatest lower bound** of A if y is a lower bound of A and $z \preceq y$ whenever z is a lower bound of A.



Question: Find the greatest lower and the least upper bounds of $\{b, d, g\}$ in the figure.

Solution: The upper bounds of $\{b, d, g\}$ are g and h. Because $g \prec h$, g is the least upper bound. The lower bounds of $\{b, d, g\}$ are a and b. Because $a \prec b$, b is the greatest lower bound.

The least upper and greatest lower bounds of A are unique if they exist. The greatest lower bound and least upper bound of a subset A are denoted by $glb(A)$ and $lub(A)$, respectively.

Lattices

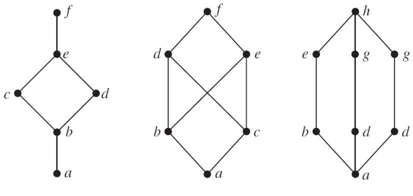
Definition

A partially ordered set in which every pair of elements has both a least upper bound and a greatest lower bound is called a **lattice**.

Lattices

Definition

A partially ordered set in which every pair of elements has both a least upper bound and a greatest lower bound is called a **lattice**.



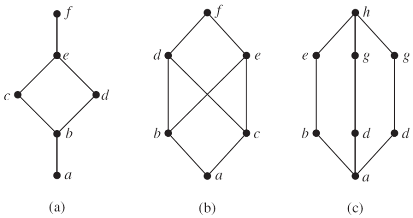
(a) (b) (c)

Question: Determine whether the posets represented by each of the Hasse diagrams in the figure are lattices.

Lattices

Definition

A partially ordered set in which every pair of elements has both a least upper bound and a greatest lower bound is called a **lattice**.



Question: Determine whether the posets represented by each of the Hasse diagrams in the figure are lattices.

Solution: The posets represented by the Hasse diagrams in (a) and (c) are both lattices. On the other hand, the poset with the Hasse diagram shown in (b) is not a lattice, because the elements b and c have no least upper bound.

Examples

Question: Is the poset $(Z^+, |)$ a lattice?
Solution:
Yes.

Examples

Question: Is the poset $(Z^+, |)$ a lattice?
Solution:
Yes.

Question: Determine whether the posets $(\{1, 2, 3, 4, 5\}, |)$ and $(\{1, 2, 4, 8, 16\}, |)$ are lattices.
Solution:
$(\{1, 2, 3, 4, 5\}, |)$ is a lattice, but $(\{1, 2, 4, 8, 16\}, |)$ is not.

Examples

Question: Is the poset $(Z^+, |)$ a lattice?
Solution:
Yes.

Question: Determine whether the posets $(\{1, 2, 3, 4, 5\}, |)$ and $(\{1, 2, 4, 8, 16\}, |)$ are lattices.
Solution:
$(\{1, 2, 3, 4, 5\}, |)$ is a lattice, but $(\{1, 2, 4, 8, 16\}, |)$ is not.

Question: Determine whether $(P(S), \subseteq)$ is a lattice where S is a set.
Solution:
Yes.

Topological sorting

Definition

A total ordering $\preceq$ is said to be **compatible** with the partial ordering R if $a \preceq b$ whenever aRb. Constructing a compatible total ordering from a partial ordering is called **topological sorting**.

Lemma

Every finite nonempty poset $(S, \preceq)$ has at least one minimal element.

Proof.

Choose an element a_0 of S. If a_0 is not minimal, then there is an element a_1 with $a_1 \prec a_0$.

Topological sorting

Definition

A total ordering $\preceq$ is said to be **compatible** with the partial ordering R if $a \preceq b$ whenever aRb. Constructing a compatible total ordering from a partial ordering is called **topological sorting**.

Lemma

Every finite nonempty poset $(S, \preceq)$ has at least one minimal element.

Proof.

Choose an element a_0 of S. If a_0 is not minimal, then there is an element a_1 with $a_1 \prec a_0$. If a_1 is not minimal, there is an element a_2 with $a_2 \prec a_1$.

Topological sorting

Definition

A total ordering $\preceq$ is said to be **compatible** with the partial ordering R if $a \preceq b$ whenever aRb. Constructing a compatible total ordering from a partial ordering is called **topological sorting**.

Lemma

Every finite nonempty poset $(S, \preceq)$ has at least one minimal element.

Proof.

Choose an element a_0 of S. If a_0 is not minimal, then there is an element a_1 with $a_1 \prec a_0$. If a_1 is not minimal, there is an element a_2 with $a_2 \prec a_1$. Continue this process, so that if a_n is not minimal, there is an element a_{n+1} with $a_{n+1} \prec a_n$.

Topological sorting

Definition

A total ordering $\preceq$ is said to be **compatible** with the partial ordering R if $a \preceq b$ whenever aRb. Constructing a compatible total ordering from a partial ordering is called **topological sorting**.

Lemma

Every finite nonempty poset $(S, \preceq)$ has at least one minimal element.

Proof.

Choose an element a_0 of S. If a_0 is not minimal, then there is an element a_1 with $a_1 \prec a_0$. If a_1 is not minimal, there is an element a_2 with $a_2 \prec a_1$. Continue this process, so that if a_n is not minimal, there is an element a_{n+1} with $a_{n+1} \prec a_n$.

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

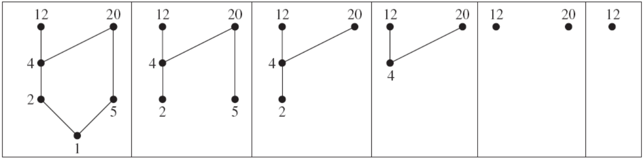
Least upper and greatest lower bounds

Definition

ALGORITHM 1 Topological Sorting.

procedure *topological sort* $((S, \preccurlyeq)$: finite poset)
$k := 1$
while $S \neq \emptyset$
  $a_k :=$ a minimal element of S {such an element exists by Lemma 1}
  $S := S - \{a_k\}$
  $k := k + 1$
return $a_1, a_2, \ldots, a_n$ $\{a_1, a_2, \ldots, a_n$ is a compatible total ordering of $S\}$

Find a compatible total ordering for the poset $(\{1, 2, 4, 5, 12, 20\}, |)$.



Take-aways

Conclusions

- Closure of Relations
- Transitive Closures
- Equivalence Relations
  - Equivalence Classes
  - Equivalence Classes and Partitions
- Partial Orderings
  - Lexicographic Order
  - Hasse Diagrams
  - Maximal and Minimal Elements
  - Lattices
  - Topological Sorting