

Discrete Mathematics for Computer Science

Lecture 16: Relation

Dr. Ming Tang

Department of Computer Science and Engineering
Southern University of Science and Technology (SUSTech)
Email: tangm3@sustech.edu.cn

Symmetric Relation

The number of **symmetric relations** on set A , where A has n elements, is $2^{n(n+1)/2}$.

Proof: When relation R is symmetric, it contains two types of elements (or pair of elements) from $A \times A$:

- (a, a) with $a \in A$: n such tuples in $A \times A$
- both (a, b) and (b, a) , with $a, b \in A$ and $a \neq b$: $C(n, 2)$ such tuples in $A \times A$

Each of these elements (or pair of elements) can be either in R or not. Thus, there are $2^{n(n-1)/2+n} = 2^{n(n+1)/2}$ symmetric relations.

Antisymmetric Relation

The number of **antisymmetric relations** on set A , where A has n elements, is $2^n 3^{n(n-1)/2}$.

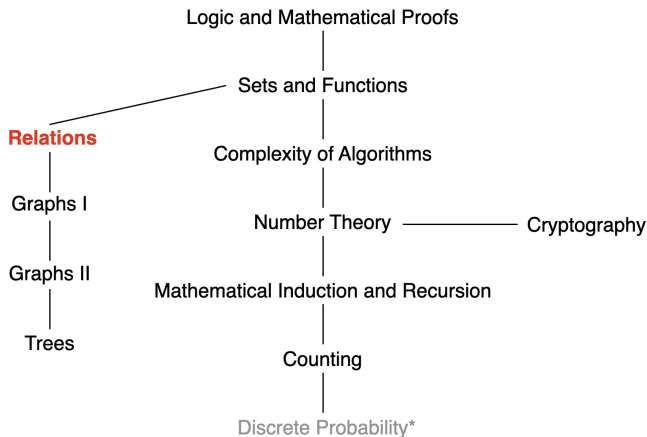
Proof: Consider the following two types of elements in $A \times A$:

- (a, a) with $a \in A$: There are n such tuples in $A \times A$. Each tuple can be either in R or not in R . Thus, there are 2^n possibilities.
- (a, b) or (b, a) , with $a, b \in A$ and $a \neq b$: There are $C(n, 2)$ pairs of a and b . For each of such pairs, there are three cases:
 - ▶ $(a, b) \in R$ and $(b, a) \notin R$;
 - ▶ $(a, b) \notin R$ and $(b, a) \in R$;
 - ▶ $(a, b) \notin R$ and $(b, a) \notin R$.

Thus, there are $3^{n(n-1)/2}$ possibilities.

Using product rule, there are $2^n 3^{n(n-1)/2}$ such relations.

This Lecture



Relation, n -ary Relations, Representing Relations,
Closures of Relations, ...

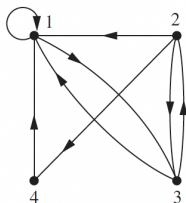
Directed Graph

A **directed graph**, or digraph, consists of a set V of **vertices** together with a set E of ordered pairs of elements of V called **edges**.

The vertex a is called the **initial vertex** of the edge (a, b) , and the vertex b is called the **terminal vertex** of this edge.

Example: Relation R is defined on $\{1, 2, 3, 4\}$:

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



Closures of Relations

Let $R = \{(1, 1), (1, 2), (2, 1), (3, 2)\}$ on $A = \{1, 2, 3\}$.

Is this relation R reflexive?

No. $(2, 2)$ and $(3, 3)$ are not in R .

The question is what is the minimal relation $S \supseteq R$ that is reflexive?

How to make R reflexive by minimum number of additions?

Add $(2, 2)$ and $(3, 3)$

Then $S = \{(1, 1), (1, 2), (2, 1), (3, 2), (2, 2), (3, 3)\} \supseteq R$.

The minimal set $S \supseteq R$ is called the reflexive closure of R .

Closures of Relations

The set S is called the **reflexive closure** of R if it:

- contains R
- is reflexive
- is minimal (is contained in **every** reflexive relation Q that contains R ($R \subseteq Q$), i.e., $S \subseteq Q$)

Closures on Relations

Relations can have different **properties**:

- reflexive
- symmetric
- transitive

We define:

- reflexive closures
- symmetric closures
- transitive closures

Closures

Definition: Let R be a relation on a set A . A relation S on A with property P is called the **closure of R with respect to P** if S is subset of every relation Q ($S \subseteq Q$) with property P that contains R ($R \subseteq Q$).

S is the minimal set containing R satisfying the property P .

Example: $R = \{(1, 2), (2, 3), (2, 2)\}$ on $A = \{1, 2, 3\}$. What is the symmetric closure S of R ?

$S = \{(1, 2), (2, 3), (2, 2), (2, 1), (3, 2)\}$.

What is the transitive closure S of R ?

$S = \{(1, 2), (2, 2), (2, 3), (1, 3)\}$.

Overview

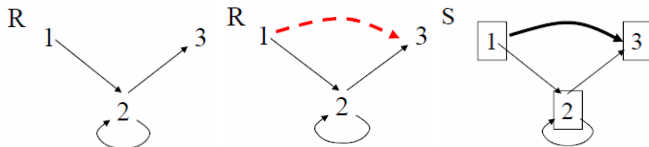
- Transitive Closure
- Path Length and Connectivity Relation
- Transitive Closure and Connectivity Relation

Transitive Closure

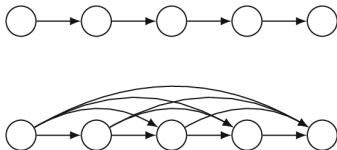
We can represent the relation on the **graph**.

Finding a **transitive closure** corresponds to **finding** all pairs of **elements** that are **connected** with a **directed** path.

Example: $R = \{(1, 2), (2, 2), (2, 3)\}$ on $A = \{1, 2, 3\}$. Transitive closure:
 $S = \{(1, 2), (2, 2), (2, 3), (1, 3)\}$



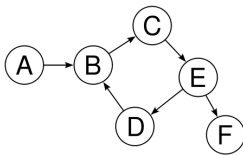
Example:



Overview

- Transitive Closure
- Path Length and Connectivity Relation
- Transitive Closure and Connectivity Relation

Paths in Directed Graphs



Definition: A **path** from a to b in the directed graph G is a sequence of edges $(x_0, x_1), (x_1, x_2), \dots, (x_{n-1}, x_n)$ in G , where n is nonnegative and $x_0 = a$ and $x_n = b$.

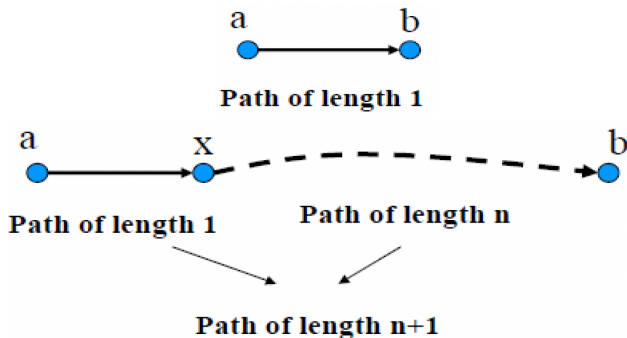
A path of length $n \geq 1$ that begins and ends at the same vertex is called a **circuit or cycle**.

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

Path Length

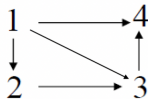
Theorem: Let R be relation on a set A . There is a path of length n from a to b if and only if $(a, b) \in R^n$.

Proof (by induction):



Recall that $R^{n+1} = R^n \circ R$

Path Length: Example



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

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

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

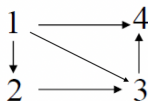
$$R^3 = \{(1, 4)\}$$

$$R^4 = \emptyset$$

Connectivity Relation

Definition: Let R be a relation on a set A . The **connectivity relation** R^* consists of **all pairs** (a, b) such that there is a path (of any length) between a and b in R :

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



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

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

$$R^3 = \{(1, 4)\}, R^4 = \emptyset$$

$$R^* = \{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}$$

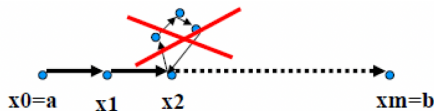
Connectivity

Lemma: Let A be a set with n elements, and R a relation on A . If there is a path from a to b with $a \neq b$, then there exists a path of length $\leq n - 1$.

Proof (by [intuition](#)): There are at most n different elements we can visit on a path if the path [does not have loops](#):



[Loops](#) may increase the length but the same node is visited more than once

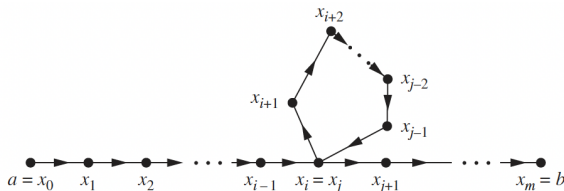


Connectivity

Lemma: Let A be a set with n elements, and R be a relation on A . If there is a path from a to b with $a \neq b$, then there exists a path of length $\leq n - 1$.

Proof: Suppose there is a path from a to b in R . Let m be the length of the shortest such path. Suppose that $x_0, x_1, x_2, \dots, x_m$, where $x_0 = a$ and $x_m = b$, is such a path.

Suppose that $a \neq b$ and that $m \geq n$. The $m + 1$ vertices are from n elements. According to the **pigeonhole principle** and $a \neq b$, at least two of the vertices x_0, x_1, \dots, x_{m-1} are equal.



There is a circuit that **can be deleted** until the length is $< n$.

Connectivity

Lemma: Let A be a set with n elements, and R a relation on A . If there is a path from a to b with $a \neq b$, then there exists a path of length $\leq n - 1$.

Lemma: 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 .

Overview

- Transitive Closure
- Path Length and Connectivity Relation
- Transitive Closure and Connectivity Relation

Connectivity

Theorem: The transitive closure of a relation R equals the connectivity relation R^* , where $R^* = \bigcup_{k=1}^{\infty} R^k$.

Recall: Finding a **transitive closure** corresponds to finding all pairs of elements that are connected with a directed path.

Recall: The **connectivity relation** R^* consists of **all pairs** (a, b) such that there is a path (of any length) between a and b in R :

Connectivity

Theorem: The transitive closure of a relation R equals the connectivity relation R^* , where $R^* = \bigcup_{k=1}^{\infty} R^k$.

R^* is a transitive closure of R :

- $R \subseteq R^*$
- R^* is transitive

If $(a, b) \in R^*$ and $(b, c) \in R^*$, then there are paths from a to b and from b to c in R . Thus, there is a path from a to c in R . This means that $(a, c) \in R^*$.

- $R^* \subseteq S$ whenever S is a transitive relation containing R
 - ▶ Suppose that S is a transitive relation containing R .
 - ▶ Transitive: $S^n \subseteq S$ for integer $n \geq 1$. (Recall S is transitive iff $S^n \subseteq S$). We have $R^* \subseteq S$.
 - ▶ $R \subseteq S$: then $R^* \subseteq S^*$, because any path in R is also a path in S .
 - ▶ Thus, $R^* \subseteq S^* \subseteq S$.

Find Transitive Closure

Recall that 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 . Thus,

$$R^* = R \cup R^2 \cup R^3 \cup \dots \cup R^n.$$

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

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

where $M_R^{[n]} = \underbrace{M_R \odot M_R \odot \dots \odot M_R}_{n \text{ } M'_R \text{'s}}$

Find Transitive Closure: Example

Find the transitive closure of the relation R where

$$\mathbf{M}_R = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}$$

Solution:

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

$$\mathbf{M}_{R^*} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix} \vee \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \vee \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}.$$

Find Transitive Closure: 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  $R^*$ }
```

- $n - 1$ Boolean products
- Each of these Boolean products use $n^2(2n - 1)$ bit operations.
- $O(n^4)$ bit operations.

Roy-Warshall Algorithm

The transitive closure can be found by Warshall's algorithm using only $O(n^3)$ bit operations.

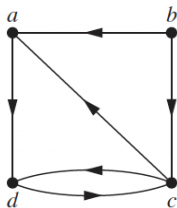
If $a, x_1, x_2, \dots, x_{m-1}, b$ is a path, its **interior vertices** are x_1, x_2, \dots, x_{m-1} .

Consider a list of vertices $v_1, v_2, \dots, v_k, \dots, v_n$. Define a zero-one matrix

$$\mathbf{W}_k = [w_{ij}^{(k)}],$$

where $w_{ij}^{(k)} = 1$ if there is a path from v_i to v_j such that **all the interior vertices** of this path are in the set $\{v_1, v_2, \dots, v_k\}$ and is 0 otherwise.

Example of W_k



Let $v_1 = a$, $v_2 = b$, $v_3 = c$, and $v_4 = d$.

W_0 is the matrix of the relation.

$$W_0 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

W_1 has 1 as its (i, j) th entry if

- W_0 has 1 as its (i, j) th entry (i.e., no interior) or
- there is a path from v_i to v_j that has $v_1 = a$ as an interior vertex



SUSTech

Southern University
of Science and
Technology

Roy-Warshall Algorithm

Consider a list of vertices $v_1, v_2, \dots, v_k, \dots, v_n$. Define a zero-one matrix

$$\mathbf{W}_k = [w_{ij}^{(k)}],$$

where $w_{ij}^{(k)} = 1$ if there is a path from v_i to v_j such that **all the interior vertices** of this path are in the set $\{v_1, v_2, \dots, v_k\}$ and is 0 otherwise.

Note that $\mathbf{W}_n = M_{R^*}$, 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 the set $\{v_1, v_2, \dots, v_n\}$.

Roy-Warshall Algorithm

Warshall's algorithm computes M_{R^*} by efficiently computing

$\mathbf{W}_0 = M_R, W_1, W_2, \dots, \mathbf{W}_n = M_{R^*}$.

Let $\mathbf{W}_k = [w_{ij}^{[k]}]$ 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 $\{v_1, v_2, \dots, v_k\}$. 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 .

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^*} }

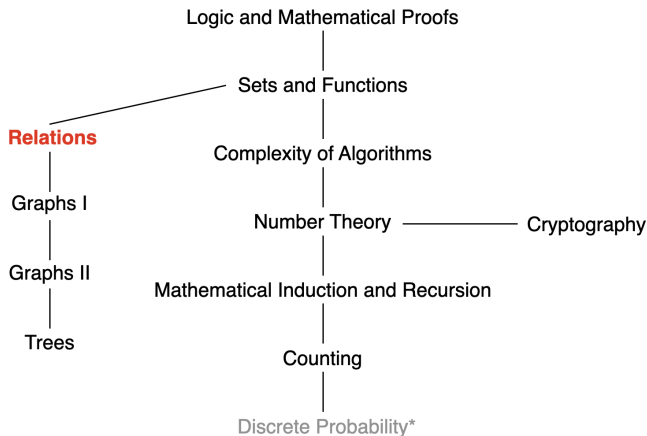
The transitive closure can be found by Warshall's algorithm using only $O(n^3)$ bit operations.



SUSTech

Southern University
of Science and
Technology

This Lecture



Relation, n -ary Relations, Representing Relations, Closures of Relations, **Relation Equivalence**, ...

Equivalence Relation

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

Example:

$$A = \{0, 1, 2, 3, 4, 5, 6\} \quad R = \{(a, b) : a \equiv b \pmod{3}\}$$

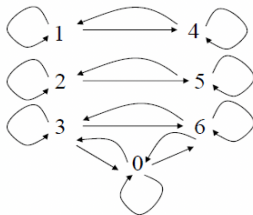
R has the following pairs:

- $(0, 0), (0, 3), (3, 0), (0, 6), (6, 0), (3, 3), (3, 6), (6, 3), (6, 6)$
- $(1, 1), (1, 4), (4, 1), (4, 4)$
- $(2, 2), (2, 5), (5, 2), (5, 5)$

Equivalence Relation

Relation R on $A = \{0, 1, 2, 3, 4, 5, 6\}$ has the pairs:

- $(0, 0), (0, 3), (3, 0), (0, 6), (6, 0), (3, 3), (3, 6), (6, 3), (6, 6)$
- $(1, 1), (1, 4), (4, 1), (4, 4)$
- $(2, 2), (2, 5), (5, 2), (5, 5)$



Is R reflexive? **Yes**

Is R symmetric? **Yes**

Is R transitive? **Yes**

R is an **equivalence relation**.

Examples of Equivalence Relations

- “Strings a and b have the same length.”
- “Integers a and b have the same absolute value.”
- “Real numbers a and b have the same fractional part (i.e., $a - b \in \mathbf{Z}$).”

Equivalence Class

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** , denoted by $[a]_R$. When only one relation is considered, we use the notation $[a]$.

$$[a]_R = \{b : (a, b) \in R\}$$

Example: $A = \{0, 1, 2, 3, 4, 5, 6\}$

$$R = \{(a, b) : a \equiv b \pmod{3}\}$$

$$[0] = [3] = [6] = \{0, 3, 6\}$$

$$[1] = [4] = \{1, 4\}$$

$$[2] = [5] = \{2, 5\}$$

Examples of Equivalence Classes

“Strings a and b have the same length.”

$[a]$ = the set of all strings of the same length as a .

“Integers a and b have the same absolute value.”

$[a]$ = the set $\{a, -a\}$

“Real numbers a and b have the same fractional part (i.e., $a - b \in \mathbf{Z}$).”

$[a]$ = the set $\{..., a - 2, a - 1, a, a + 1, a + 2, ...\}$

Equivalence Class

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

$$(i) aRb \quad (ii) [a] = [b] \quad (iii) [a] \cap [b] \neq \emptyset$$

Proof:

- (i) \rightarrow (ii): prove $[a] \subseteq [b]$ and $[b] \subseteq [a]$

Suppose $c \in [a]$. Then, aRc .

Because aRb and R is symmetric, we know that bRa .

Since R is transitive and bRa and aRc , it follows that bRc .

Hence, $c \in [b]$. This shows that $[a] \subseteq [b]$.

Equivalence Class

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

$$(i) aRb \quad (ii) [a] = [b] \quad (iii) [a] \cap [b] \neq \emptyset$$

Proof:

- (i) \rightarrow (ii): prove $[a] \subseteq [b]$ and $[b] \subseteq [a]$
- (ii) \rightarrow (iii): Assume that $[a] = [b]$. It follows that $[a] \cap [b] \neq \emptyset$ because $[a]$ is nonempty (because $a \in [a]$ as R is reflexive).
- (iii) \rightarrow (i): Suppose that $[a] \cap [b] \neq \emptyset$. There exists a c such that $c \in [a]$ and $c \in [b]$, i.e., aRc and bRc .

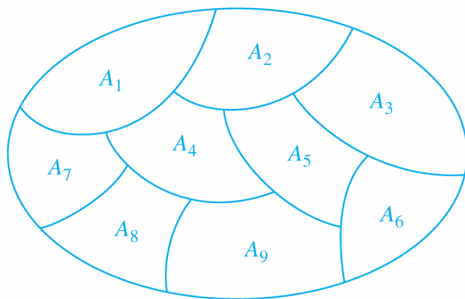
By the symmetric property, cRb .

Then by transitivity, because aRc and cRb , we have aRb .

Partition of a Set S

Definition: Let S be a set. A collection of nonempty subsets of S , i.e A_1, A_2, \dots, A_k , is called a partition of S if:

$$A_i \cap A_j = \emptyset, i \neq j \text{ and } S = \bigcup_{i=1}^k A_i$$



Example: $A = \{0, 1, 2, 3, 4, 5, 6\}$

$A_1 = \{0, 3, 6\}$, $A_2 = \{1, 4\}$, $A_3 = \{2, 5\}$

Is A_1, A_2, A_3 a partition of S ?

Equivalence Classes and Partitions

Theorem: Let R be an **equivalence relation** on a set A . Then, union of all the equivalence classes of R is A :

$$A = \bigcup_{a \in A} [a]_R$$

Theorem: The equivalence classes form a partition of A .

Theorem: Let $\{A_1, A_2, \dots, A_i, \dots\}$ be a partition of S . Then, there is an equivalence relation R on S , that has the sets A_i as its equivalence classes.

Equivalence Classes and Partitions: Example

List the ordered pairs in the equivalence relation R produced by the partition $A_1 = \{1, 2, 3\}$, $A_2 = \{4, 5\}$, and $A_3 = \{6\}$ of $S = \{1, 2, 3, 4, 5, 6\}$.

Solution: The subsets in the partition are the equivalence classes of R . The pair $(a, b) \in R$ if and only if a and b are in the same subset of the partition:

- $(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2),$ and $(3, 3)$ belong to R because $A_1 = \{1, 2, 3\}$ is an equivalence class;
- $(4, 4), (4, 5), (5, 4),$ and $(5, 5)$ belong to R because $A_2 = \{4, 5\}$ is an equivalence class;
- $(6, 6)$ belongs to R because 6 is an equivalence class.

Equivalence Classes and Partitions: Example

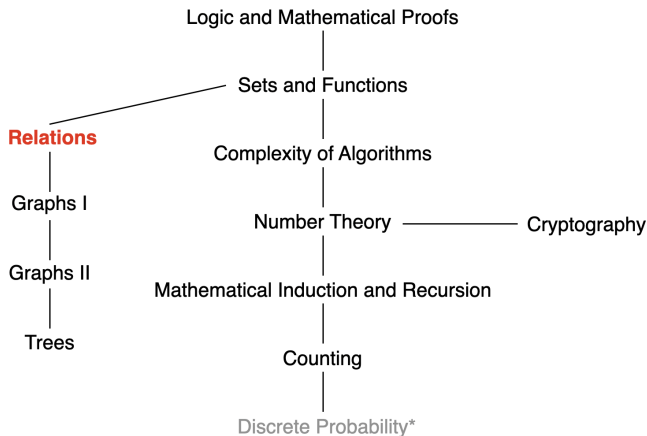
What are the sets in the partition of the integers arising from congruence modulo 4?

Solution: There are four congruence classes, corresponding to $[0]_4$, $[1]_4$, $[2]_4$, and $[3]_4$. They are the sets

- $[0]_4 = \{\dots, -8, -4, 0, 4, 8, \dots\}$
- $[1]_4 = \{\dots, -7, -3, 1, 5, 9, \dots\}$
- $[2]_4 = \{\dots, -6, -2, 2, 6, 10, \dots\}$
- $[3]_4 = \{\dots, -5, -1, 3, 7, 11, \dots\}$

These congruence classes are disjoint, and every integer is in exactly one of them.

This Lecture



Relation, n -ary Relations, Representing Relations, Closures of Relations, Relation Equivalence, Partial Ordering, **SUSTech**

Southern University
of Science and
Technology

Partial Ordering

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**, denoted by (S, R) .

Example: $S = \{1, 2, 3, 4, 5\}$, R denotes the “ \geq ” relation:

- Is R reflexive? **Yes**
- Is R antisymmetric? **Yes**
- Is R transitive? **Yes**

R is a partial ordering

Partial Ordering: Example

$S = \{1, 2, 3, 4, 5, 6\}$, R denotes the “|” relation

- Is R reflexive? Yes
- Is R antisymmetric? Yes
- Is R transitive? Yes

R is a partial ordering

Comparability

The notation $a \preceq b$ is used to denote that $(a, b) \in R$ in an arbitrary poset (S, R) .

The notation $a \prec b$ denotes that $a \preceq b$, but $a \neq b$.

Definition: The elements a and b of a poset (S, \preceq) are comparable if either $a \preceq b$ or $b \preceq a$. Otherwise, a and b are called incomparable.

Example: $S = \{1, 2, 3, 4, 5, 6\}$, R denotes the “|” relation.
2, 4 are comparable, 3, 5 are incomparable.

Total Ordering

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.

Example: $S = \{1, 2, 3, 4, 5, 6\}$, R denotes the “ \geq ” relation S is a chain.

Well-Ordered Set

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

Example: The set of ordered pairs of positive integers, $\mathbf{Z}^+ \times \mathbf{Z}^+$, with $(a_1, a_2), (b_1, b_2)$ 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**.

The set \mathbf{Z} , with the usual \leq ordering, is **not** well-ordered because the set of negative integers, which is a subset of \mathbf{Z} , has no least element.

The Principle of Well-Ordered Induction

The Principle of Well-Ordered Induction: Suppose that (S, \preccurlyeq) is a **well-ordered set**. Suppose x_0 is the least element of a well ordered set. Then $P(x)$ is true for all $x \in S$, **if**

Basic Step: $P(x_0)$ is true.

Inductive Step: For every $y \in S \setminus \{x_0\}$, if $P(x)$ is true for all $x \in S$ with $x \prec y$, then $P(y)$ is true.

Or equivalently,

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

The Principle of Well-Ordered Induction: Suppose that (S, \preccurlyeq) 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 $x \in S$. 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 $x \prec a$. By the inductive step, $P(a)$ is true.

This contradiction shows that $P(x)$ must be true for all $x \in S$.

Questions from Section 5 (Induction)

The Well-Ordering Property: Every nonempty set of nonnegative integers has a least element.

The principle of mathematical induction **follows from** the well-ordering property.

Question from students: Consider the set of **negative integers**. Although it does not have a least element, it has a greatest element. Can we solve it using mathematical induction?

Yes. We can solve it using the principle of well-ordered induction if we can find a relation \preceq such that (S, \preceq) is a well-ordered set.

Questions from Section 5 (Induction)

(i) The principle of mathematical induction, (ii) strong induction, and (iii) well-ordering property are all **equivalent** principles.

That is, **the validity of each** can be proved from **either** of the other two.
(See Section 5.2 Exercise 41, 42, 43)

- **(i) \rightarrow (ii)**: The inductive hypothesis of a proof by mathematical induction is **part of** the inductive hypothesis in a proof by strong induction.
- **(ii) \rightarrow (iii)** Use strong induction to show that the set of nonnegative integers has a least element.
- **(iii) \rightarrow (i)** The principle of mathematical induction follows from the well-ordering property.