Lecture 17

Relations

Suha Kwak

suha.kwak@postech.ac.kr

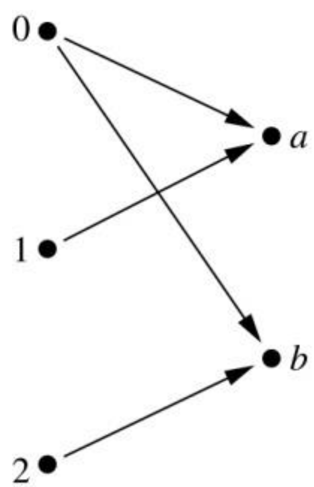
Dept. of Computer Science and Engineering

POSTECH

Relations and Their Properties

Binary Relation

- Definition
  - A binary relation R from a set A to a set B is a subset of $A \times B$.
- Example
  - Let $A = \{0,1,2\}$ and $B = \{a, b\}$.
  - $\{(0, a), (0, b), (1, a), (2, b)\}$ is a relation from A to B.
  - We can represent relations from a set A to a set B graphically or using a table:



R	a	b
0	×	×
1	×	
2		×

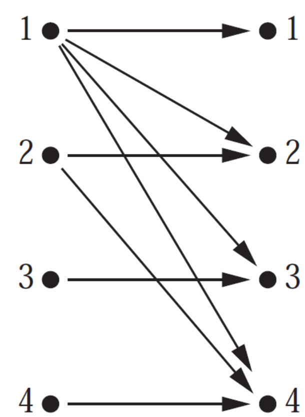
> Relations are more general than functions. A function is a relation where exactly one element of B is related to each element of A.

Binary Relation on a Set

- Definition
  - A binary relation R on a set A is a subset of $A \times A$ or a relation from A to A.

- Example 1
  - Suppose that $A = \{a, b, c\}$.
  - Then $R = \{(a, a), (a, b), (a, c)\}$ is a relation on A.

- Example 2
  - Let $A = \{1,2,3,4\}$.
  - The ordered pairs in the relation $R = \{(a, b) | a \text{ divides } b\}$ are $(1,1), (1,2), (1,3), (1,4), (2,2), (2,4), (3,3)$, and $(4,4)$.



R	1	2	3	4
1	×	×	×	×
2		×		×
3			×	
4				×

Binary Relation on a Set

- The number of binary relations on a set
  - Because a relation on A is a subset of $A \times A$, we count the subsets of $A \times A$.
  - Since $A \times A$ has n^2 elements when A has n elements, and a set with m elements has 2^m subsets, there are 2^{n^2} subsets of $A \times A$
  - Therefor, the number of binary relations on the set A is 2^{n^2}.

Binary Relation on a Set

- Example 3
  - Consider these relations on the set of integers:

$R_1 = \{(a,b) | a \leq b\}$,
$R_2 = \{(a,b) | a > b\}$,
$R_3 = \{(a,b) | a = b \text{ or } a = -b\}$,
$R_4 = \{(a,b) | a = b\}$,
$R_5 = \{(a,b) | a = b + 1\}$,
$R_6 = \{(a,b) | a + b \leq 3\}$.

These relations are on an infinite set and each of these relations is an infinite set.

  - Which of these relations contain each of the pairs $(1,1)$, $(1,2)$, $(2,1)$, $(1,-1)$, and $(2,2)$?

  - Solution:
    - $(1,1)$ is in R_1, R_3, R_4, and R_6.
    - $(1,2)$ is in R_1 and R_6.
    - $(2,1)$ is in R_2, R_5, and R_6.
    - $(1,-1)$ is in R_2, R_3, and R_6.
    - $(2,2)$ is in R_1, R_3, and R_4.

Reflexive Relations

- Definition
  - R is reflexive if and only if $(a, a) \in R$ for every element $a \in A$.
  - Written symbolically, R is reflexive if and only if
    $$\forall x[x \in A \rightarrow (x, x) \in R].$$
  - The empty relation on an empty set (*i.e.*, $A = \emptyset$) is reflexive.

- Example
  - The following relations on the integers are reflexive:
    - $R = \{(a, b) | a \leq b\}$
    - $R = \{(a, b) | a = b \text{ or } a = -b\}$
    - $R = \{(a, b) | a = b\}$
  - The following relations are not reflexive:
    - $R = \{(a, b) | a > b\}$
    - $R = \{(a, b) | a = b + 1\}$
    - $R = \{(a, b) | a + b \leq 3\}$

Symmetric Relations

- Definition
  - R is symmetric if and only if $(b, a) \in R$ whenever $(a, b) \in R$ for all $a, b \in A$.
  - Written symbolically, R is symmetric if and only if
    $$\forall x \forall y\ [(x, y) \in R \to (y, x) \in R].$$
- Example
  - The following relations on the integers are symmetric:
    - $R = \{(a, b) | a = b \text{ or } a = -b\}$
    - $R = \{(a, b) | a = b\}$
    - $R = \{(a, b) | a + b \leq 3\}$
  - The following are not symmetric:
    - $R = \{(a, b) | a \leq b\}$
    - $R = \{(a, b) | a > b\}$
    - $R = \{(a, b) | a = b + 1\}$

Antisymmetric Relations

- Definition
  - A relation R on a set A such that $\forall a, b \in A$ if $(a, b) \in R$ and $(b, a) \in R$, then $a = b$ is called antisymmetric.
  - Written symbolically, R is antisymmetric if and only if
    $$\forall x \forall y\ [(x, y) \in R \land (y, x) \in R \rightarrow x = y].$$
- Example
  - The following relations on the integers are antisymmetric:
    - $R = \{(a, b) | a \leq b\}$
    - $R = \{(a, b) | a > b\}$
    - $R = \{(a, b) | a = b\}$
    - $R = \{(a, b) | a = b + 1\}$
  - The following relations are not antisymmetric:
    - $R = \{(a, b) | a = b \text{ or } a = -b\}$
    - $R = \{(a, b) | a + b \leq 3\}$

For any integer,
if a $a \leq b$ and $b \leq a$,
then $a = b$.

POSTECH

Transitive Relations

- Definition
  - A relation R on a set A is transitive if whenever $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$, for all $a, b, c \in A$.
  - Written symbolically, R is transitive if and only if
    $\forall x \forall y \forall z[(x, y) \in R \wedge (y, z) \in R \rightarrow (x, z) \in R]$.

- Example
  - The following relations on the integers are transitive:
    - $R = \{(a, b) | a \leq b\}$
    - $R = \{(a, b) | a > b\}$
    - $R = \{(a, b) | a = b \text{ or } a = -b\}$
    - $R = \{(a, b) | a = b\}$
  - The following are not transitive:
    - $R = \{(a, b) | a = b + 1\}$
    - $R = \{(a, b) | a + b \leq 3\}$

For every integer,
If $a \leq b$ and $b \leq c$,
then $a \leq c$.

POSTECH

Combining Relations

- Given two relations R_1 and R_2, we can combine them using basic set operations to form new relations such as $R_1 \cup R_2$, $R_1 \cap R_2$, $R_1 - R_2$, and $R_2 - R_1$.

- Example
  - Let $A = \{1,2,3\}$ and $B = \{1,2,3,4\}$.
  - The relations $R_1 = \{(1,1),(2,2),(3,3)\}$ and $R_2 = \{(1,1),(1,2),(1,3),(1,4)\}$ can be combined using basic set operations to form new relations:

$$R_1 \cup R_2 = \{(1,1),(1,2),(1,3),(1,4),(2,2),(3,3)\}$$

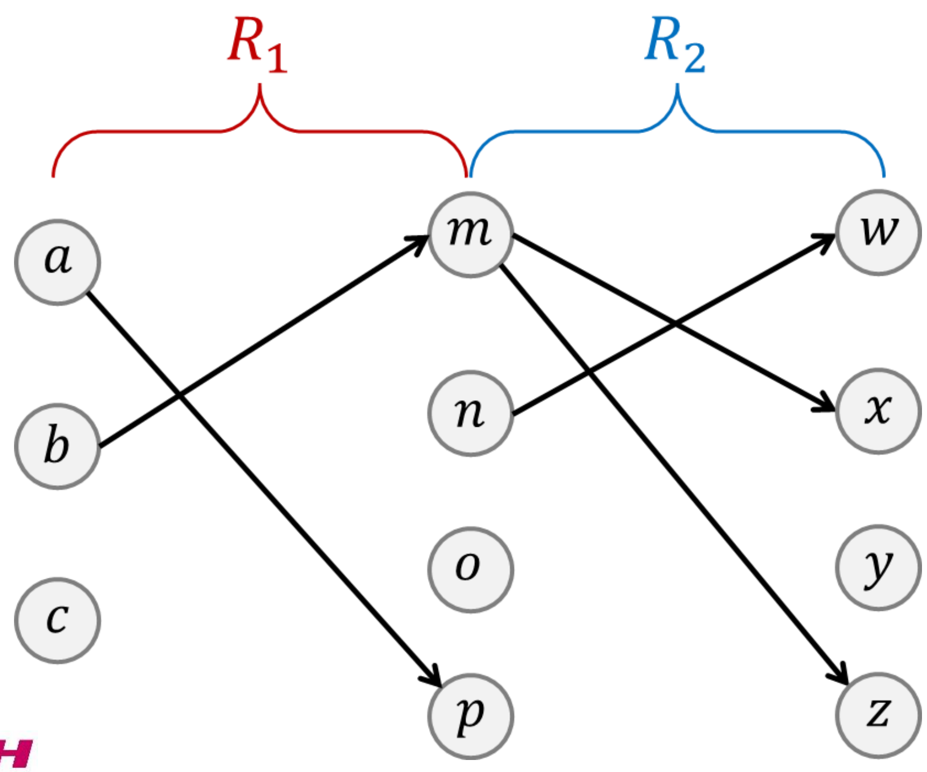
$$R_1 \cap R_2 = \{(1,1)\}$$

$$R_1 - R_2 = \{(2,2),(3,3)\}$$

$$R_2 - R_1 = \{(1,2),(1,3),(1,4)\}$$

Composition

- Definition
  - Suppose that R_1 is a relation from a set A to a set B and R_2 is a relation from B to a set C.
  - Then the composition (or composite) of R_2 with R_1 is a relation from A to C where if (x, y) is a member of R_1 and (y, z) is a member of R_2, then (x, z) is a member of $R_2 \circ R_1$.



$R_2 \circ R_1$
$= \{(b, x), (b, z)\}$

Powers of a Relation

- Definition
  - Let R be a binary relation on A. Then the powers R^n of the relation R can be defined inductively by:
    - Basis Step: $R^1 = R$
    - Inductive Step: $R^{n+1} = R^n \circ R$
- Theorem 1
  - The relation R on a set A is transitive if and only if $R^n \subseteq R$ for $n = 1,2,3, \ldots$.
  - In other words, the powers of a transitive relation are subsets of the relation.

Powers of a Relation

- Proof of Theorem 1: "If" part

The relation R on a set A is transitive if $R^n \subseteq R$ for $n = 1,2,3, \ldots$.

- Suppose that $R^n \subseteq R$ for $n = 1,2,3, \ldots$; in particular, $R^2 \subseteq R$.
- Note that if $(a, b) \in R$ and $(b, c) \in R$, then by the definition of composition, $(a, c) \in R^2$.
- Because $R^2 \subseteq R$, this means that $(a, c) \in R$.
- Hence, R is transitive.

Remind the definition of transitive relation
$\forall x \forall y \forall z [(x, y) \in R \land (y, z) \in R \rightarrow (x, z) \in R\ ]$

Powers of a Relation

- Proof of Theorem 1: “Only if” part (using math induction)

$R^n \subseteq R$ for $n = 1,2,3, \ldots$ if the relation R on a set A is transitive.

  - Basis step: this part of the theorem is trivially true for $n = 1$.
  - Inductive step:
    - Assume that $R^n \subseteq R$, where n is a positive integer. We will show that this inductive hypothesis implies that $R^{n+1} \subseteq R$.
    - Assume that $(a, b) \in R^{n+1}$. Then, since $R^{n+1} = R^n \circ R$, there is an element $x \in A$ such that $(a, x) \in R$ and $(x, b) \in R^n$.
    - The inductive hypothesis $R^n \subseteq R$ implies that $(x, b) \in R$.
    - Furthermore, because R is transitive, and $(a, x) \in R$ and $(x, b) \in R$, it follows that $(a, b) \in R$.
    - We have shown that an arbitrary element (a, b) of R^{n+1} is included in R given the inductive hypothesis. Thus, $R^{n+1} \subseteq R$ when $R^n \subseteq R$.

Representing Relations

Representing Relations Using Matrices

- A relation between finite sets can be represented using a zero-one matrix.
  - Suppose R is a relation from $A = \{a_1, a_2, \ldots, a_m\}$ to $B = \{b_1, b_2, \ldots, b_n\}$.
  - The elements of the two sets can be listed in any particular arbitrary order. When $A = B$, we use the same ordering.
  - The relation R is represented by the matrix $M_R = [m_{ij}]$, where

$$m_{ij} = \begin{cases} 1, & \text{if } (a_i, b_j) \in R, \\ 0, & \text{if } (a_i, b_j) \notin R. \end{cases}$$

  - The matrix representing R has a 1 as its (i, j) entry when a_i is related to b_j and a 0 if a_i is not related to b_j.

Representing Relations Using Matrices

- Example 1
  - Suppose that $A = \{1,2,3\}$ and $B = \{1,2\}$. Let R be the relation from A to B containing (a, b) if $a \in A$, $b \in B$, and $a > b$.
  - Then what is the matrix representing R?
    Assume the ordering of elements is the same as the increasing numerical order.
  - Solution
    - Because $R = \{(2,1), (3,1), (3,2)\}$, the matrix is

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

Representing Relations Using Matrices

- Example 2
  - Let $A = \{a_1, a_2, a_3\}$ and $B = \{b_1, b_2, b_3, b_4, b_5\}$. Which ordered pairs are in the relation R represented by the matrix below:

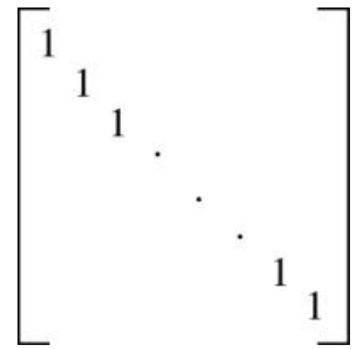
$$M_R = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

  - Solution
    - Because R consists of those ordered pairs (a_i, b_j) with $m_{ij} = 1$, it follows that:

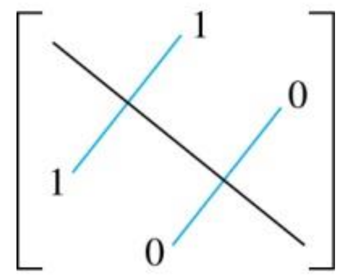
$$R = \{(a_1, b_2), (a_2, b_1), (a_2, b_3), (a_2, b_4), (a_3, b_1), (a_3, b_3), (a_3, b_5)\}.$$

Matrices of Relations on Sets

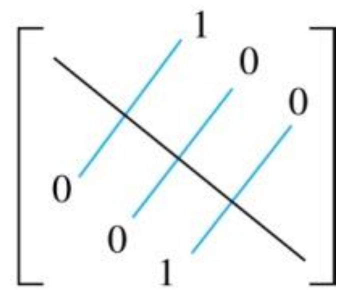
- If R is a reflexive relation, all the elements on the main diagonal of M_R are equal to 1.



- R is a symmetric relation if and only if $m_{ij} = 1$ whenever $m_{ji} = 1$.
- On the other hand, R is an antisymmetric relation, if and only if $m_{ij} = 0$ or $m_{ji} = 0$ when $i \neq j$.



(a) Symmetric



(b) Antisymmetric

Matrices of Relations on Sets

- Example 3
  - Suppose that the relation R on a set is represented by the matrix

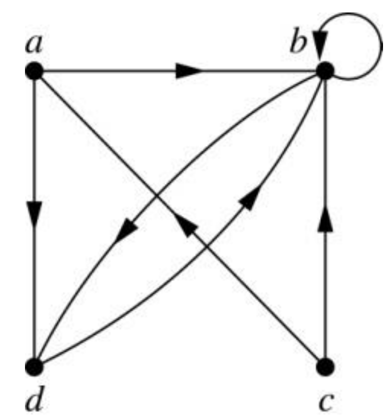
$$M_R = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}.$$

  - Is R reflexive, symmetric, and/or antisymmetric?

  - Solution
    - Because all the diagonal elements are equal to 1, R is reflexive.
    - Because M_R is symmetric, R is symmetric.
    - Because both m_{12} and m_{21} are 1, M_R is not antisymmetric.

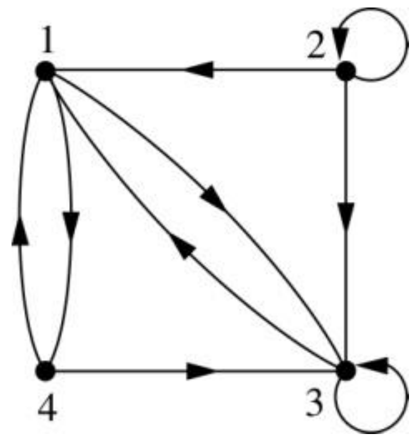
Representing Relations Using Digraphs

- Definition
  - 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.
  - An edge of the form (a, a) is called a loop.
- Example 1
  - The directed graph with vertices a, b, c, and d, and edges (a, b), (a, d), (b, b), (b, d), (c, a), (c, b), and (d, b) is



Representing Relations Using Digraphs

- Example 2
  - What are the ordered pairs in the relation represented by the directed graph below?

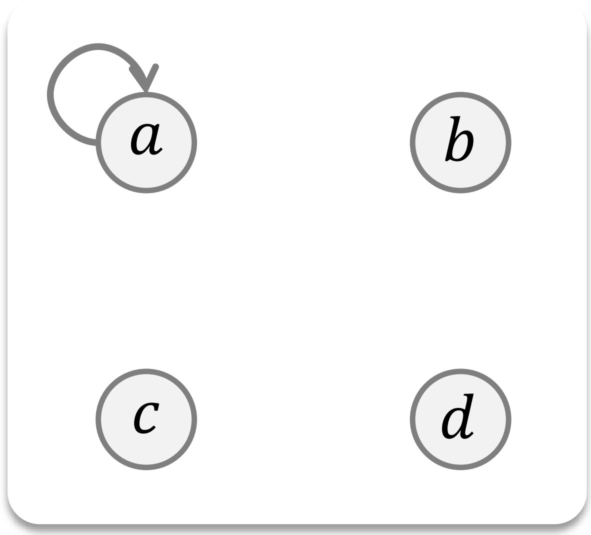


- Solution
  - The ordered pairs in the relation are $(1,3), (1,4), (2,1), (2,2), (2,3), (3,1), (3,3), (4,1)$, and $(4,3)$.

Representing Relations Using Digraphs

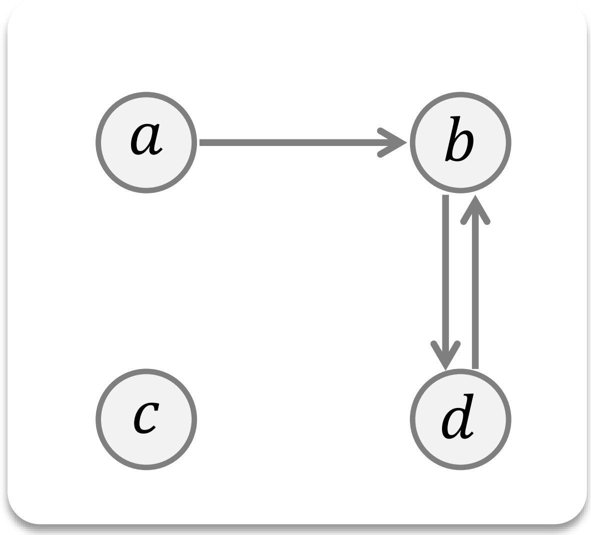
- Determining properties of a relation from its digraph
  - *Reflexivity*:
    A loop must be present at all vertices in the graph.
  - *Symmetry*:
    If (x, y) is an edge, then so is (y, x).
  - *Antisymmetry*:
    If (x, y) with $x \neq y$ is an edge, then (y, x) is not an edge.
  - *Transitivity*:
    If (x, y) and (y, z) are edges, then so is (x, z).

Representing Relations Using Digraphs



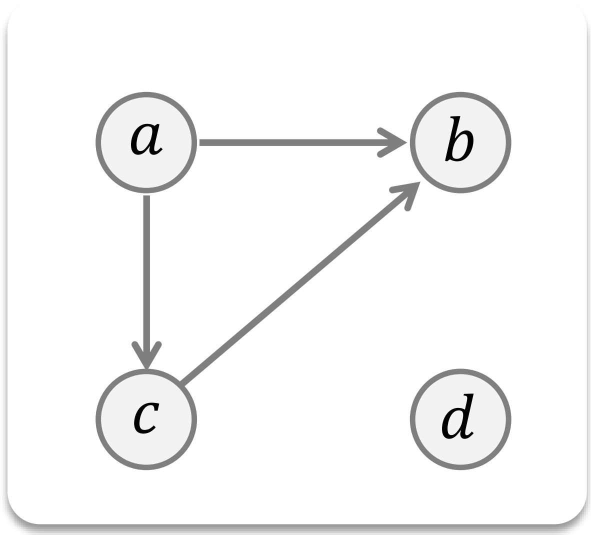
Reflexive?	No, not every vertex has a loop.
Symmetric?	Yes (trivially), there is no edge from one vertex to another.
Antisymmetric?	Yes (trivially), there is no edge from one vertex to another.
Transitive?	Yes (trivially), since there is no edge from one vertex to another.

Representing Relations Using Digraphs



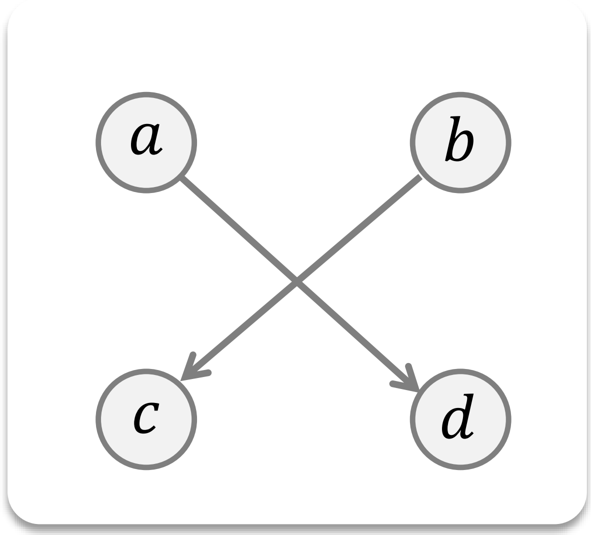
Reflexive?	No, there is no loop.
Symmetric?	No, there is an edge from a to b, but not from b to a.
Antisymmetric?	No, there is an edge from d to b and b to d.
Transitive?	No, there are edges from a to c and from c to b, but no edge from a to d.

Representing Relations Using Digraphs



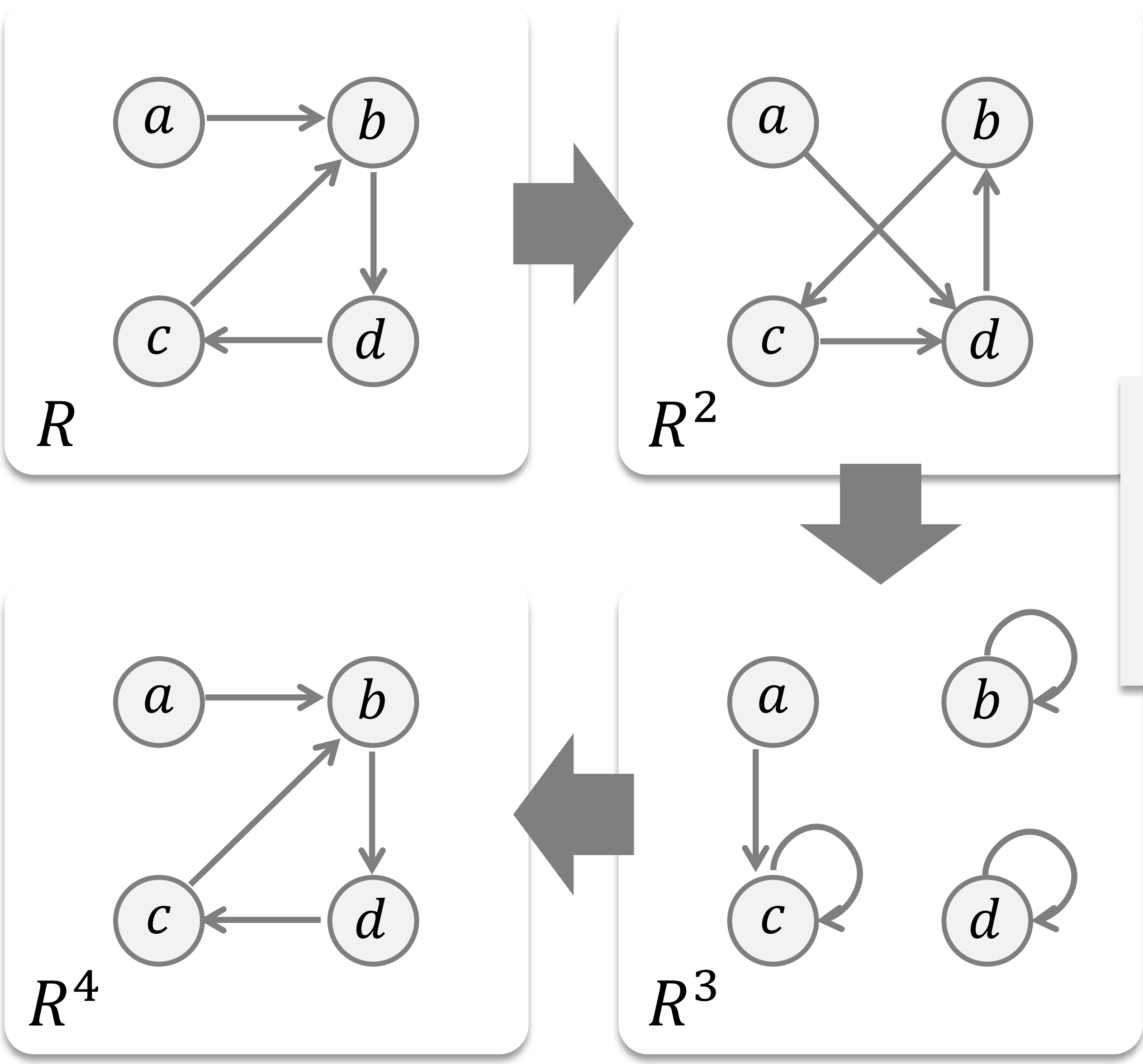
Reflexive?	No, there is no loop.
Symmetric?	No, for example, there is no edge from c to a.
Antisymmetric?	Yes, whenever there is an edge from one vertex to another, there is not one going back.
Transitive?	Yes.

Representing Relations Using Digraphs



Reflexive?	No, there is no loop.
Symmetric?	No, for example, there is no edge from d to a.
Antisymmetric?	Yes, whenever there is an edge from one vertex to another, there is not one going back.
Transitive?	Yes (trivially), there are no two edges where the first edge ends at the vertex where the second begins.

Example of the Powers of a Relation

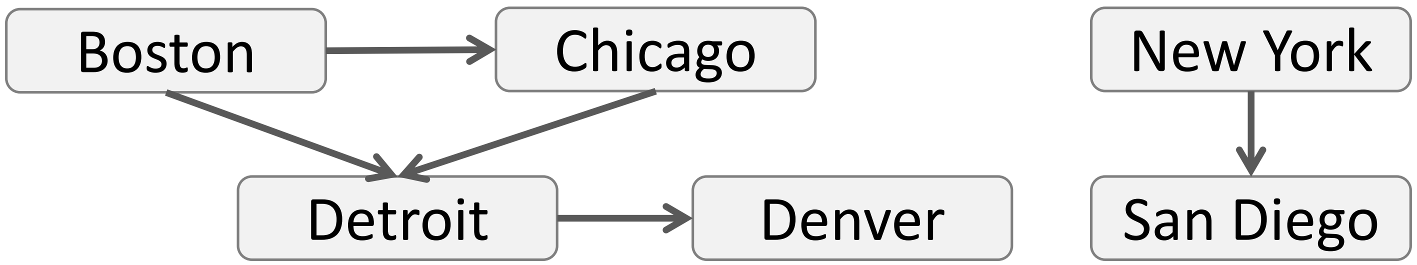


The pair (x, y) is in R^n if there is a path of length n from x to y in R (following the direction of the arrows).

Closures of Relations

Closures

- Example
  - Direct, one-way telephone lines between data centers:



  - Let R be the relation containing (a, b) if there is a telephone line from the data center in a to that in b.
  - How can we determine if there is some (possibly indirect) link composed of one or more telephone lines from one center to another?
  - R cannot be used directly to answer this; as it is not transitive, it does not contain all the pairs that can be linked.

Closures

- Example (cont'd)
  - Instead, we can find all pairs of data centers that have a link by constructing a transitive relation S containing R such that S is a subset of every transitive relation containing R.
    ($i.e.$, S is the smallest transitive relation that contains R.)
  - This relation is called the transitive closure of R.

- A general description
  - Let R be a relation on a set A.
  - R may or may not have some property $\mathbf{P}$, such as reflexivity, symmetry, or transitivity.
  - If there is a relation S with property $\mathbf{P}$ containing R such that S is a subset of every relation with property $\mathbf{P}$ containing R, then S is called the closure of R with respect to $\mathbf{P}$.

Reflexive Closures

- How to produce the reflexive closure of R?
  - Given a relation R on a set A, the reflexive closure of R can be formed by adding to R all pairs of the form (a, a) with $a \in A$, not already in R.
  - The addition of these pairs produces a new relation that is reflexive, contains R, and is contained within any reflexive relation containing R.
  - We see that the reflexive closure of R equals $R \cup \Delta$, where $\Delta = \{(a, a) | a \in A\}$ is the *diagonal relation* on A.
- Example
  - What is the reflexive closure of the relation $R = \{(a, b) | a < b\}$ on the set of integers?
  - The reflexive closure of R is $R \cup \Delta = \{(a, b) | a < b\} \cup \{(a, a) | a \in \boldsymbol{Z}\} = \{(a, b) | a \leq b\}$.

Symmetric Closures

- How to produce the symmetric closure of R?
  - The symmetric closure of a relation R can be constructed by adding all ordered pairs of the form (b, a), where (a, b) is in the relation, that are not already present in R.
  - The symmetric closure can be constructed by taking the union of a relation with its inverse; that is, $R \cup R^{-1}$ is the symmetric closure of R, where $R^{-1} = \{(b, a) | (a, b) \in R\}$.

- Example
  - What is the symmetric closure of the relation $R = \{(a, b) | a > b\}$ on the set of positive integers?
  - The symmetric closure of R is $R \cup R^{-1} = \{(a, b) | a > b\} \cup \{(b, a) | a > b\} = \{(a, b) | a \neq b\}$.

Paths in Directed Graphs

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

Paths in Directed Graphs

- The term *path* also applies to relations.
  - Carrying over the definition from directed graphs to relations, there is a path from a to b in R if there is a sequence of elements $a, x_1, x_2, x_3, \ldots, x_{n-1}, b$ with $(a, x_1) \in R$, $(x_1, x_2) \in R$, … , and $(x_{n-1}, b) \in R$.

- 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 $(a, b) \in R^n$.
    (Refer to the "Example of the Powers of a Relation".)

Transitive Closures

- Finding the transitive closure of a relation is equivalent to determining which pairs of vertices in the associated directed graph are connected by a path.

- Definition: Connectivity relation
  - 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.
  - Because R^n consists of the pairs (a, b) such that there is a path of length n from a to b, it follows that R^* is the union of all the sets R^n, $R^* = \bigcup_{n=1}^{\infty} R^n$.

Transitive Closures

- Example of the connectivity relation
  - 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?
    - The relation R^2 contains (a, b) if there is a person c such that $(a, c) \in R$ and $(c, b) \in R$, that is, if there is a person c such that a has met c and c has met b.
    - Similarly, R^n consists of those pairs (a, b) such that there are people $x_1, x_2, x_3, \dots, x_{n-1}$ such that a has met x_1, x_1 has met x_2, $\dots$, and x_{n-1} has met b.
  - What is R^*?
    - The relation R^* contains (a, b) if there is a sequence of people, starting with a and ending with b, such that each person in the sequence has met the next person in the sequence.

Transitive Closures

- Theorem
  - The transitive closure of a relation R equals the connectivity relation R^*.
  - Proof
    - R^* contains R by definition. To show that R^* is the transitive closure of R, we must also show that R^* is transitive and that $R^* \subseteq S$ whenever S is a transitive relation that contains R.
    - If $(a, b) \in R^*$ and $(b, c) \in R^*$, then there are (possibly indirect) paths from a to b and from b to c in R.
    - We obtain a path from a to c by starting with the path from a to b and following it with the path from b to c.
    - Hence, by $(a, c) \in R^*$. It follows that R^* is transitive.

Transitive Closures

- Theorem
  - The transitive closure of a relation R equals the connectivity relation R^*.
  - Proof (cont'd)
    - Suppose that S is a transitive relation containing R.
    - Because S is transitive, $S^n \subseteq S$.
      (See the proof of Theorem in p.13 of lecture note 17.)
    - Since $S^* = \bigcup_{k=1}^{\infty} S^k$ and $S^k \subseteq S$, it follows that $S^* \subseteq S$.
    - Now note that if $R \subseteq S$, then $R^* \subseteq S^*$, because any path in R is also a path in S.
    - Consequently, $R^* \subseteq S^* \subseteq S$.
    - Hence any transitive relation that contains R must also contain R^*. Therefore, R^* is the transitive closure of R.

Transitive Closures

- Lemma
  - Let A be a set with n elements, and let R be a relation on A.
  - 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 $n - 1$.

- From this lemma, we see that $R^* = \bigcup_{k=1}^{n} R^k$.
  - There is a path in R^* between two vertices if and only if there is a path between them in R^i for some positive integer $i \leq n$.
  - The zero-one matrix for the transitive closure (R^*) is the join of the zero-one matrices of the first n powers of the zero-one matrix of R. (See the theorem in the next page.)

Transitive Closures

- 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

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

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^*}

Equivalence Relations

Equivalence Relations

- Definition 1
  - A relation on a set A is called an equivalence relation if it is reflexive, symmetric, and transitive.

- Definition 2
  - 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.

Equivalence Relations

- Example
  - Suppose that R is the relation on the set of strings of English letters such that $\boxed{aRb}$ if and only if $l(a) = l(b)$, where $l(x)$ is the length of the string x.

    Two elements a and b are related by the relation R.
  - Is R an equivalence relation?
  - Solution
    - Show that all properties of an equivalence relation hold.
    - *Reflexivity*
      Because $l(a) = l(a)$, it follows that aRa for all strings a.
    - *Symmetry*
      Suppose that aRb. Since $l(a) = l(b)$, $l(b) = l(a)$ also holds and bRa.
    - *Transitivity*
      Suppose that aRb and bRc. Since $l(a) = l(b)$ and $l(b) = l(c)$, $l(a) = l(c)$ also holds and aRc.

Congruence Modulo m

- Example
  - Let m be an integer with $m > 1$.
  - Show that the relation $R = \{(a, b) | a \equiv b \pmod{m}\}$ is an equivalence relation on the set of integers.
  - Solution
    - Recall that $a \equiv b \pmod{m}$ if and only if m divides $a - b$.
    - *<u>Reflexivity</u>*
      $a \equiv a \pmod{m}$ since $a - a = 0$ is divisible by m since $0 = 0 \cdot m$.
    - *<u>Symmetry</u>*
      Suppose that $a \equiv b \pmod{m}$. Then $a - b$ is divisible by m, and so $a - b = km$, where k is an integer. It follows that $b - a = -km$, thus $b \equiv a \pmod{m}$.

Congruence Modulo m

- Example
  - Let m be an integer with $m > 1$.
  - Show that the relation $R = \{(a, b) | a \equiv b \pmod{m}\}$ is an equivalence relation on the set of integers.
  - Solution (cont'd)
    - *Transitivity*
      Suppose that $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$.
      Then m divides both $a - b$ and $b - c$, and there are integers k and l with $a - b = km$ and $b - c = lm$.
      Thus, $a - c = (a - b) + (b - c) = km + lm = (k + l)m$, which suggests that $a - c$ also divisible by m.
    - Since all the three properties hold, congruence module m is an equivalence relation.

Divides

- Example
  - Show that the "divides" relation on the set of positive integers is not an equivalence relation.
  - Solution
    - The reflexivity, and transitivity do hold, but symmetry does not. Hence, "divides" is not an equivalence relation.
    - *Reflexivity*
      $a \mid a$ for all a.
    - *Not Symmetric*
      A counter-example: $2 \mid 4$, but $4 \nmid 2$.
    - *Transitivity*
      Suppose that a divides b and b divides c. Then there are positive integers k and l such that $b = ak$ and $c = bl$. Hence, $c = akl$, so a divides c. Therefore, the relation is transitive.

Equivalence Classes

- Definition 3
  - 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 $[a]_R$.
    - $[a]_R = \{s | (a, s) \in R\}$.
    - When only one relation is under consideration, we can write $[a]$, without the subscript R, for this equivalence class.
  - 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 the class.

Equivalence Classes

- Congruence class modulo m
  - The equivalence classes of the relation "*congruence modulo* m" are called the "*congruence classes modulo* m".
  - The congruence class of an integer a modulo m is denoted by $[a]_m$; $[a]_m = \{\dots, a-2m, a-m, a, a+m, a+2m, \dots\}$.

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

Equivalence Classes and Partitions

- Theorem 1
  - Let R be an equivalence relation on a set A. Then these statements for elements a and b of A are equivalent:

    (*i*) aRb

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

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

  - Proof: (*i*) implies (*ii*).
    - Assume that aRb and that $c \in [a]$. Then aRc.
    - Because aRb and R is symmetric, bRa.
    - Because R is transitive and bRa and aRc, it follows that bRc.
    - Hence, $c \in [b]$. Therefore, $[a] \subseteq [b]$.
    - A similar argument shows that $[b] \subseteq [a]$.
    - Since $[a] \subseteq [b]$ and $[b] \subseteq [a]$, we have shown that [a] = [b].

Equivalence Classes and Partitions

- Theorem 1
  - Let R be an equivalence relation on a set A. Then these statements for elements a and b of A are equivalent:

    (i) aRb

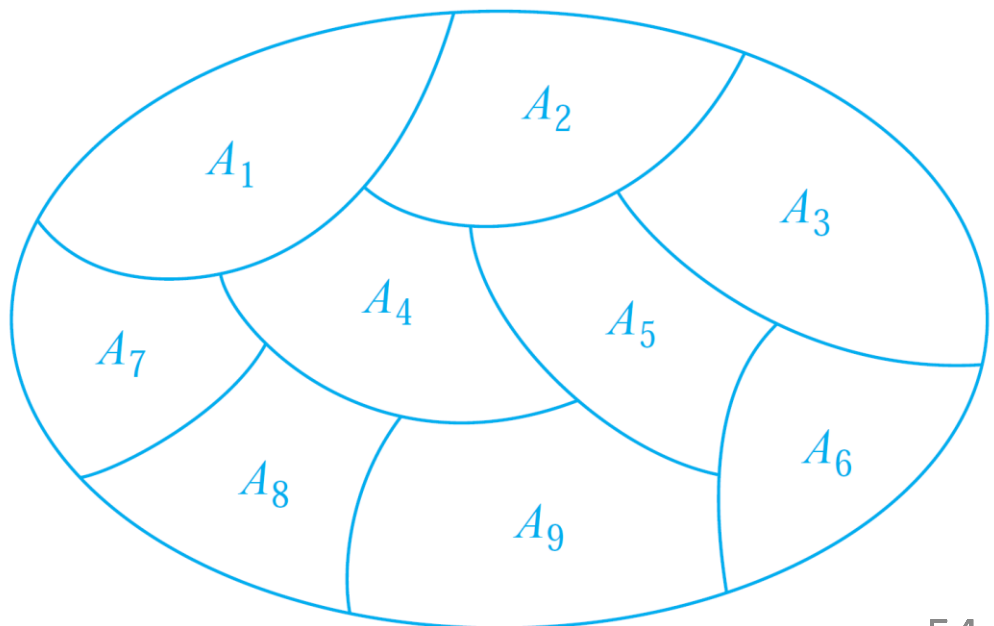
    (ii) $[a] = [b]$

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

  - Proof: (*ii*) implies (*iii*).
    - Assume that $[a] = [b]$. It follows that $[a] \cap [b] \neq \emptyset$ because $[a]$ is nonempty (since R is reflexive, $a \in [a]$).
  - Proof: (*iii*) implies (*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 of R, cRb. Then by transitivity, because aRc and cRb, we have aRb.

Partition of a Set

- Definition
  - A partition of a set S is a collection of disjoint nonempty subsets of S that have S as their union.
  - In other words, the collection of subsets A_i, where $i \in I$ (I: a set of indices), forms a partition of S if and only if
    - $A_i \neq \emptyset$ for $i \in I$,
    - $A_i \cap A_j = \emptyset$ when $i \neq j$, and
    - $\bigcup_{i \in I} A_i = S$.



An Equivalence Relation Partitions a Set

- Equivalence relation partitioning a set
  - Let R be an equivalence relation on a set A.
  - The union of all the equivalence classes of R is all of A, since an element a of A is in its own equivalence class $[a]_R$.
    - In other words, $\bigcup_{a \in A} [a]_R = A$.
  - From Theorem 1, it follows that these equivalence classes are either equal or disjoint, so $[a]_R \cap [b]_R = \emptyset$ when $[a]_R \neq [b]_R$.
  - Therefore, the equivalence classes form a partition of A, because they split A into disjoint subsets.

Theorem 1. The following statements are equivalent:
(*i*) aRb
(*ii*) $[a] = [b]$
(*iii*) $[a] \cap [b] \neq \emptyset$

An Equivalence Relation Partitions a Set

- Theorem 2
  - Let R be an equivalence relation on a set S. Then the equivalence classes of R form a partition of S.
  - Conversely, given a partition $\{A_i | i \in I\}$ of the set S, there is an equivalence relation R that has the sets A_i, $i \in I$, as its equivalence classes.
  - Proof
    - We have already shown the first part of the theorem.
    - For the second part, assume that $\{A_i | i \in I\}$ is a partition of S.
    - Let R be the relation on S consisting of the pairs (x, y) where x and y belong to the same subset A_i in the partition.
    - We must show that R satisfies the properties of an equivalence relation.

An Equivalence Relation Partitions a Set

- Theorem 2
  - Let R be an equivalence relation on a set S. Then the equivalence classes of R form a partition of S.
  - Conversely, given a partition $\{A_i | i \in I\}$ of the set S, there is an equivalence relation R that has the sets A_i, $i \in I$, as its equivalence classes.
  - Proof (cont'd)
    - *Reflexivity*: For every $a \in S$, $(a, a) \in R$ because a is in the same subset as itself.
    - *Symmetry*: If $(a, b) \in R$, then b and a are in the same subset of the partition, so $(b, a) \in R$.
    - *Transitivity*: If $(a, b) \in R$ and $(b, c) \in R$, then a and b are in the same subset of the partition, as are b and c. Since the subsets are disjoint and b belongs to both, the two subsets of the partition must be identical. Therefore, $(a, c) \in R$ since a and c belong to the same subset of the partition.