

CS 214

Introduction to Discrete Structures

Chapter 5

Relations, Functions, and Matrices

Mikel D. Petty, Ph.D.



Chapter sections and objectives

- 5.1 Relations
 - Identify ordered pairs related by a binary relation
 - Test a binary relation for the reflexive, symmetric, transitive, and antisymmetric properties
 - Find reflexive, symmetric, and transitive closures
 - Identify partial orders and construct Hasse diagrams
 - Recognize an equivalence relation
- 5.2 Topological sorting *Not covered in CS 214*
 - Draw and use PERT charts
 - Extend a partial ordering with a topological sort
- 5.3 Relations and databases *Not covered in CS 214*

- 5.4 Functions

- Determine whether a binary relation is a function
- Test a function for the one-to-one and onto properties
- Create composite functions
- Decide if a function has an inverse, and what it is
- Use cycle notation for permutation functions
- Compute the number of functions between finite sets

- 5.5 Order of Magnitude

- Use order of magnitude to measure function growth
- Use order of magnitude to classify algorithms

- 5.6 The Mighty Mod Function Not covered in CS 214

- 5.7 Matrices Not covered in CS 214

- Perform matrix arithmetic
- Perform Boolean operations on Boolean matrices

Sample problem

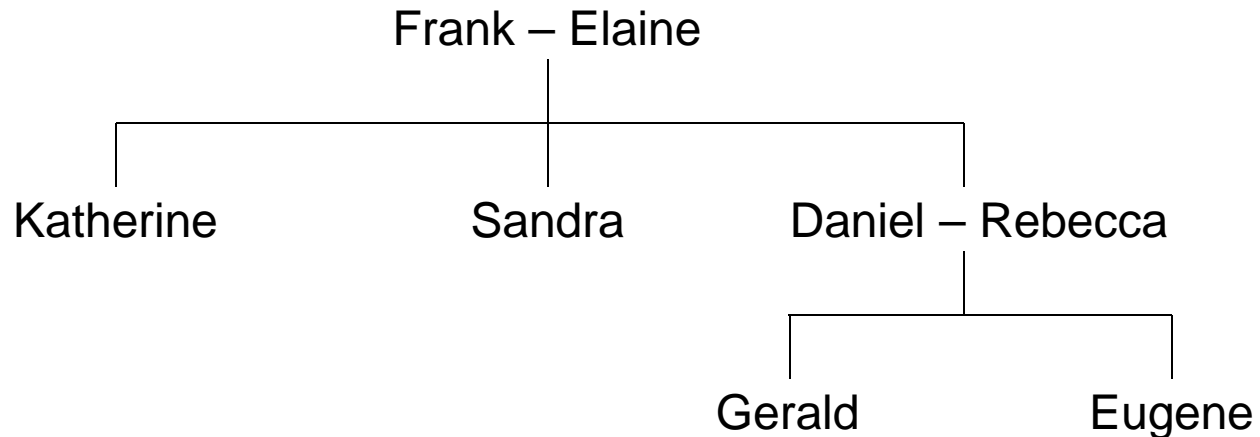
Your company has developed a program to use on a small parallel processing machine. The program executes processes P1, P2 and P3 in parallel; these processes all need results from P4, so they must wait for P4 to complete execution before they begin. Processes P7 and P10 execute in parallel but must wait until P1, P2, and P3 finish. P4 requires results from P5 and P6. P5 and P6 execute in parallel. P8 and P11 execute in parallel, but P8 must wait for P7 to complete and P11 must wait for P10 to complete. P9 must wait for results from P8 and P11.

In what order should the processes be executed on a single processor machine?

5.1 Relations

Binary relations

- Concept
 - Represent relationships between objects
 - e.g., real world: parent – child, older – younger
 - e.g., mathematics: \leq , \subseteq



- Binary relations
 - Generalize and abstract relationship notion
 - Represent relationship using set ideas
 - “Binary” means relating two objects at a time
 - Ordered pairs specify related objects

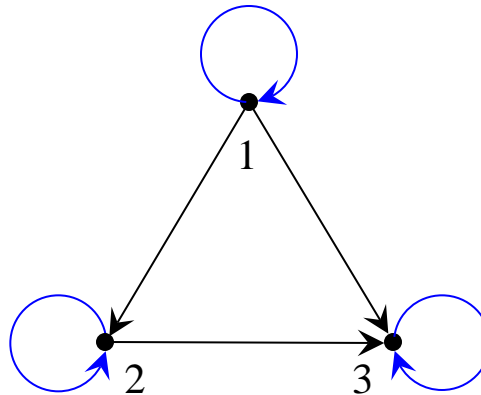
Representing relationships with ordered pairs

Set $S = \{1, 2, 3\}$

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

Equality (=) relationship: $\{(1, 1), (2, 2), (3, 3)\}$

Less than (<) relationship: $\{(1, 2), (1, 3), (2, 3)\}$



Example 1

Relation definition and notation

- Definition
 - **Binary relation**; given set S ,
a binary relation on S is a subset of $S \times S$
 - A relation is a set of ordered pairs of elements of S
- Notation
 - Relations are often denoted as ρ (rho) or σ (sigma)
 - Symbol ρ or σ may be used as an operator or a set,
e.g., $x \rho y \leftrightarrow (x, y) \in \rho$

Specifying relations

- Specifying (identifying pairs in a) relation
 - Exhaustively list all pairs in relation
 - Describe property that characterizes pairs, informally using words
 - Describe property that characterizes pairs, formally using equations and/or logic
- Characterizing property
 - Binary predicate satisfied by pairs in relation
 - e.g., $S = \text{people}$, $x \rho y \leftrightarrow x \text{ is the parent of } y$
 - e.g., $S = \mathbb{N}$, $x \rho y \leftrightarrow x < y$

Specifying relation examples

Set $S = \{1, 2\}$

$S \times S = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$

Define ρ as: $x \rho y \leftrightarrow x + y$ is odd

Then $(1, 2), (2, 1) \in \rho$

Example 3

Set $S = \{1, 2\}$

$S \times S = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$

Define σ as: $\sigma = \{(1, 1), (2, 1)\}$

Then $1 \sigma 1$ and $2 \sigma 1$ are true, but not $1 \sigma 2$.

Example 4

Specifying relation examples

For each of the following binary relations ρ on \mathbb{N} , which of the listed ordered pairs belong to ρ ?

- a. $x \rho y \leftrightarrow x = y + 1$ $(2, 2), (2, 3), (3, 3), (3, 2)$
- b. $x \rho y \leftrightarrow x \mid y$ $(2, 4), (2, 5), (2, 6)$
- c. $x \rho y \leftrightarrow x$ is odd $(2, 3), (3, 4), (4, 5), (5, 6)$
- d. $x \rho y \leftrightarrow x > y^2$ $(1, 2), (2, 1), (5, 2), (6, 4), (4, 3)$

Relation definition revisited

- Relations may be defined on more than one set
 - **Binary relation**; given sets S and T ,
a binary relation from S to T is a subset of $S \times T$.
 - **n -ary relation**; given n sets S_1, S_2, \dots, S_n ,
an n -ary relation on $S_1 \times S_2 \times \dots \times S_n$
is a subset of $S_1 \times S_2 \times \dots \times S_n$.
- Primary interest: binary relations on single set

Relation example

Set $S = \{1, 2, 3\}$, $T = \{2, 4, 7\}$

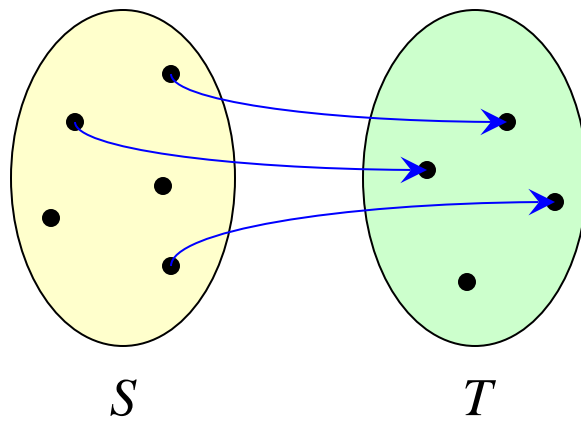
$S \times T = \{(1, 2), (1, 4), (1, 7), (2, 2), (2, 4), (2, 7),$
 $(3, 2), (3, 4), (3, 7)\}$

$\rho = \{(1, 2), (2, 4), (2, 7)\}$ is a relation on S and T .

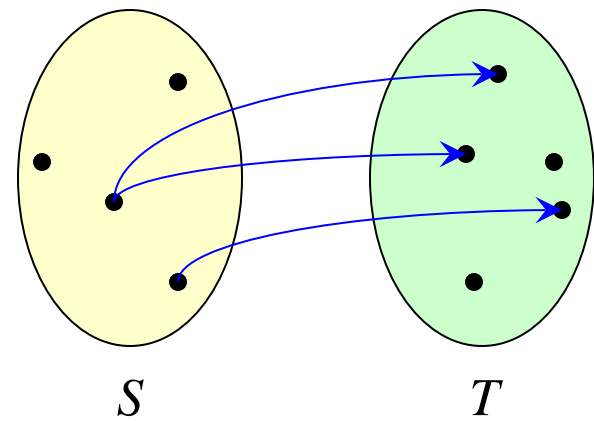
Example 5

Mappings in relations

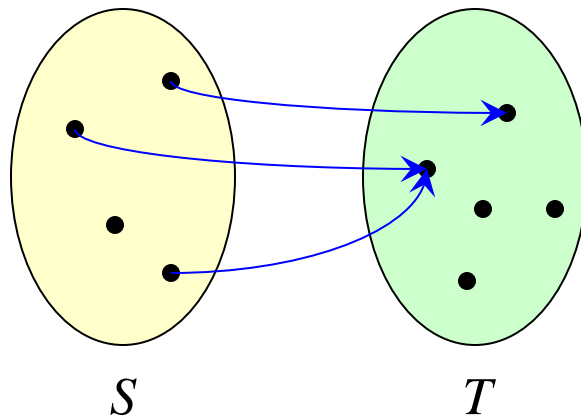
- Recap
 - If ρ is a binary relation on S ,
then ρ is a set of ordered pairs (s_1, s_2) ,
with $s_1, s_2 \in S$, $(s_1, s_2) \in \rho$, and $\rho \subseteq S \times S$
- Types of mappings
 - **one-to-one**; each s_1 and s_2 appears 1 time
 - Only once as first or second component
 - May appear as both
 - **one-to-many**; some s_1 appears > 1 time as first
 - **many-to-one**; some s_2 appears > 1 time as second
 - **many-to-many**; some s_1 appears more than once
and some s_2 appears more than once



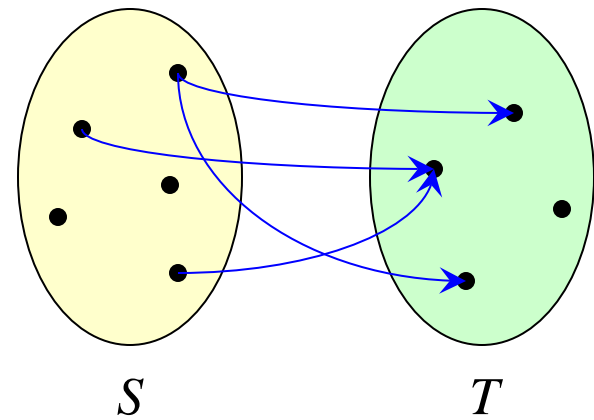
one-to-one



one-to-many



many-to-one



many-to-many

Figure 5.1

Relation mapping examples

Suppose $S = \{2, 5, 7, 9\}$ and $\rho \subseteq S \times S$.

What is the mapping in each of these relations?

- a. $\rho = \{(5, 2), (7, 5), (9, 2)\}$ many-to-one
- b. $\rho = \{(2, 5), (5, 7), (7, 2)\}$ one-to-one
- c. $\rho = \{(7, 9), (2, 5), (9, 9), (2, 7)\}$ many-to-many

Set operations on relations

- A binary relation on S is a subset of $S \times S$, i.e., a **set of ordered pairs**
- Binary relations are sets
 - Set operations \cap \cup ' may be applied to relations
 - Result is also a relation on S
- All binary relations on S
 - Let B be the set of all binary relations on S
 - i.e., B is the set of all subsets of $S \times S$
 - i.e., $B = \wp(S \times S)$

- Definitions

- union

Operator: $x (\rho \cup \sigma) y \leftrightarrow x \rho y \vee x \sigma y$

Set: $\rho \cup \sigma = \{(x, y) \mid (x, y) \in \rho \vee (x, y) \in \sigma\}$

- intersection

Operator: $x (\rho \cap \sigma) y \leftrightarrow x \rho y \wedge x \sigma y$

Set: $\rho \cap \sigma = \{(x, y) \mid (x, y) \in \rho \wedge (x, y) \in \sigma\}$

- complement

Operator: $x \rho' y \leftrightarrow \text{not } x \rho y$

Set: $\rho' = \{(x, y) \mid (x, y) \in (S \times S) \wedge (x, y) \notin \rho\}$

Relation set operations examples

Let ρ and σ be two binary relations on \mathbb{N} defined by $x \rho y \leftrightarrow x = y$ and $x \sigma y \leftrightarrow x < y$.

a. What is the relation $\rho \cup \sigma$?

$$x (\rho \cup \sigma) y \leftrightarrow x \leq y$$

b. What is the relation ρ' ?

$$x \rho' y \leftrightarrow x \neq y$$

c. What is the relation σ' ?

$$x \sigma' y \leftrightarrow x \geq y$$

d. What is the relation $\rho \cap \sigma$?

$$\emptyset$$

Relation identities

Commutative

1a. $\rho \cup \sigma = \sigma \cup \rho$

1b. $\rho \cap \sigma = \sigma \cap \rho$

Associative

2a. $(\rho \cup \sigma) \cup \gamma = \rho \cup (\sigma \cup \gamma)$

2b. $(\rho \cap \sigma) \cap \gamma = \rho \cap (\sigma \cap \gamma)$

Distributive

3a. $\rho \cup (\sigma \cap \gamma) = (\rho \cup \sigma) \cap (\rho \cup \gamma)$

3b. $\rho \cap (\sigma \cup \gamma) = (\rho \cap \sigma) \cup (\rho \cap \gamma)$

Identity

4a. $\rho \cup \emptyset = \rho$

4b. $\rho \cap S^2 = \rho$

Complement

5a. $\rho \cup \rho' = S^2$

5b. $\rho \cap \rho' = \emptyset$

where $S^2 = S \times S$ and \emptyset is the empty set.

Properties of relations

Relation ρ has the property if the implication is true.

For the examples,

$$S = \{1, 2, 3\}$$

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

reflexive

$$(\forall x)(x \in S \rightarrow (x, x) \in \rho)$$

$$\text{e.g., } (1, 1), (2, 2), (3, 3) \in \rho$$

symmetric

$$(\forall x)(\forall y)(x \in S \wedge y \in S \wedge (x, y) \in \rho \rightarrow (y, x) \in \rho)$$

$$\text{e.g., } (1, 2) \in \rho \rightarrow (2, 1) \in \rho$$

transitive

$$(\forall x)(\forall y)(\forall z)(x \in S \wedge y \in S \wedge z \in S \wedge (x, y) \in \rho \wedge (y, z) \in \rho \rightarrow (x, z) \in \rho)$$

$$\text{e.g., } (1, 2), (2, 3) \in \rho \rightarrow (1, 3) \in \rho$$

antisymmetric

$$(\forall x)(\forall y)(x \in S \wedge y \in S \wedge (x, y) \in \rho \wedge (y, x) \in \rho \rightarrow x = y)$$

$$\text{e.g., } (1, 2) \in \rho \rightarrow (2, 1) \notin \rho$$

Properties of relations example

Relation \leq on $S = \mathbb{N}$

$$\begin{aligned} \leq = \{ & (0, 0), (0, 1), (0, 2), (0, 3), \dots, \\ & (1, 1), (1, 2), (1, 3), (1, 4), \dots, \\ & (2, 2), (2, 3), (2, 4), (2, 5), \dots, \\ & (3, 3), (3, 4), (3, 5), (3, 6), \dots, \\ & \dots \\ & \dots (196, 196), (196, 197), (196, 198), (196, 199), \dots, \\ & \dots \\ & \} \end{aligned}$$

Example 6

Relation \leq on $S = \mathbb{N}$

Reflexive $(x, x) \in \leq$

Yes: for every $x \in \mathbb{N}$, $x \leq x$

Symmetric $(x, y) \in \leq \rightarrow (y, x) \in \leq$

No: $3 \leq 4$ but 4 not ≤ 3

Transitive $(x, y) \in \leq \wedge (y, z) \in \leq \rightarrow (x, z) \in \leq$

Yes: for every $x, y, z \in \mathbb{N}$, if $x \leq y$ and $y \leq z$ then $x \leq z$

Antisymmetric $(x, y) \in \leq \wedge (y, x) \in \leq \rightarrow x = y$

Yes: for every $x, y \in \mathbb{N}$, if $x \leq y$ and $y \leq x$ then $x = y$

Properties of relations example

Relation \subseteq on $S = \wp(\mathbb{N})$

$\wp(\mathbb{N}) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}, \{2\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}, \dots\}$

Reflexive

Yes: for every $A \in \wp(\mathbb{N})$, $A \subseteq A$

Symmetric

No: $\{0\} \subseteq \{0, 1\}$ but $\{0, 1\} \not\subseteq \{0\}$

Transitive

Yes: for every $A, B, C \in \wp(\mathbb{N})$, if $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$

Antisymmetric

Yes: for every $A, B \in \wp(\mathbb{N})$, if $A \subseteq B$ and $B \subseteq A$ then $A = B$

Example 7

Properties of relations example

$$S = \{1, 2, 3\}$$

- a. If relation ρ on S is reflexive, what pairs must be in ρ ?
 $(1, 1), (2, 2), (3, 3)$
- b. If relation ρ on S is symmetric, what pairs must be in ρ ?
Not enough information
- c. If relation ρ on S is symmetric and $(a, b) \in \rho$,
what pair must be in ρ ?
 (b, a)

d. If relation ρ on S is antisymmetric and $(a, b), (b, a) \in \rho$, what must be true?

$$a = b$$

e. Is the relation $\rho = \{(1, 2)\}$ on S transitive?

Trivially so; antecedent in transitive property is false

Symmetry and antisymmetry

- Explanation
 - Symmetry and antisymmetry not precisely opposites
 - Antisymmetric does not mean not symmetric
 - Not symmetric: $(x, y) \in \rho$ but $(y, x) \notin \rho$ (counterexample)
 - Antisymmetric: $(x, y), (y, x) \in \rho \rightarrow x = y$ (rule true)
- All four combinations are possible

$$S = \{1, 2, 3\}$$

	symmetric	not symmetric
antisymmetric	$\{(1, 1), (2, 2), (3, 3)\}$	$\{(1, 3)\}$
not antisymmetric	$\{(1, 2), (2, 1)\}$	$\{(1, 3), (1, 2), (2, 1)\}$

Properties of relations examples

a. $S = \mathbb{N}; x \rho y \leftrightarrow x + y \text{ even}$

reflexive yes

symmetric yes

transitive yes

antisymmetric no; $2 + 4$ even, $4 + 2$ even, $2 \neq 4$

b. $S = \mathbb{Z}^+; x \rho y \leftrightarrow x \mid y$

reflexive yes

symmetric no; $2 \mid 4$ true, $4 \nmid 2$ false

transitive yes

antisymmetric yes

c. $S =$ set of all lines in plane;

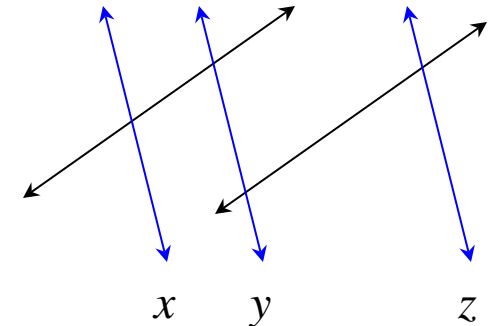
$x \rho y \leftrightarrow x$ is parallel to y or x coincides with y

reflexive yes

symmetric yes

transitive yes

antisymmetric no; $x \parallel y, y \parallel x \nRightarrow x = y$



d. $S = \mathbb{N}; x \rho y \leftrightarrow x = y^2$

reflexive no; $2 \neq 2^2$

symmetric no; $4 = 2^2, 2 \neq 4^2$

transitive no; $16 = 4^2, 4 = 2^2, 16 \neq 2^2$

antisymmetric yes

Proving properties of relations

- Scope of properties
 - Universal quantifiers in definition of each property
 - Implication must be true for every element $x, y, z \in S$
- Effect of properties
 - Typically, a property requires that specific pairs be in (or not in) the relation
 - To prove a property true for a relation, show that if antecedent true, then consequent true, or show that antecedent never true (trivially true) in definition of that property
 - To prove a property not true for a relation, exhibit a counterexample

Closures of relations

- Concept

- To “extend” relation ρ means to add ordered pairs
- Suppose relation ρ on S fails to have property P
 - Where P is reflexivity, symmetry, or transitivity
- ρ may be extended to ρ^* that does have property P

- Definition

- A binary relation ρ^* on S is the **closure** of ρ with respect to property P if
 - $\rho \subseteq \rho^*$
 - ρ^* has property P
 - ρ^* is a subset of any other relation that includes ρ and has property P
 - No subset of ρ^* has property P (i.e., “minimal”)

- Closures constructable by extending ρ
 - Reflexive
 - Symmetric
 - Transitive
- Closure not constructable by extending ρ
 - Antisymmetric

Closure example

$$S = \{1, 2, 3\}$$

$$\rho = \{(1, 1), (1, 2), (1, 3), (3, 1), (2, 3)\}$$

ρ not reflexive, not symmetric, not transitive

Reflexive closure of ρ

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

Symmetric closure of ρ

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

Transitive closure of ρ

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

Example 9

Types of relations

- Types of binary relations
 - Relation properties: reflexivity, symmetry, transitivity, antisymmetry
 - Relation properties define types
 - Types have particular properties
- Two types of special interest
 - **Partial ordering**; reflexive, antisymmetric, transitive
 - **Equivalence relation**; reflexive, symmetric, transitive

Partial orderings

- Definition
 - **Partial ordering**; binary relation on a set S that is reflexive, antisymmetric, and transitive
- Examples
 - $S = \wp(\mathbb{N})$; $x \rho y \leftrightarrow x \subseteq y$
 - $S = \mathbb{Z}^+$; $x \rho y \leftrightarrow x \mid y$
 - $S = \{0, 1\}$; $x = y^2$
- Notes
 - “ordering”; represents an order on elements of S
 - “partial”; not all elements of S necessarily related
 - May or may not be symmetric also
 - Some orderings disallowed by reflexive, e.g., $<$ on \mathbb{N}

Partial ordering example

Relation \leq on $S = \mathbb{R}$; $x \leq y \leftrightarrow x < y$ or $x = y$.

Theorem

Relation \leq is a partial ordering.

Proof

Reflexive. We must show $(x, x) \in \leq$ for every $x \in \mathbb{R}$.

But $x = x$ for every $x \in \mathbb{R}$, thus $(x, x) \in \leq$.

Antisymmetric. We must show $(x, y), (y, x) \in \leq \rightarrow x = y$ for every $x, y \in \mathbb{R}$.

If $(x, y), (y, x) \in \leq$, then $x \leq y$ and $y \leq x$, thus $x = y$.

continued next slide

Example 8.5.5, p. 501, S. S. Epp, *Discrete Mathematics with Applications*, Fourth Edition, Brooks/Cole, Boston MA, 2011.

Antisymmetric. We must show $(x, y), (y, x) \in \leq \rightarrow x = y$ for every $x, y \in \mathbb{R}$.

If $(x, y), (y, x) \in \leq$, then $x \leq y$ and $y \leq x$, thus $x = y$.

Transitive. We must show $(x, y), (y, z) \in \leq \rightarrow (x, z) \in \leq$ for every $x, y, z \in \mathbb{R}$.

If $(x, y), (y, z) \in \leq$, then $x \leq y$ and $y \leq z$, thus $x \leq z$.

If $x \leq z$ then $(x, z) \in \leq$. ■

Partially ordered set

- Definition
 - **Partially ordered set**; ordered pair (S, ρ)
where S is a set and ρ is a partial order on S
 - aka **poset**
- Notation
 - (S, \preceq) denotes arbitrary poset
 - \preceq denotes arbitrary partial ordering
 - $x < y$ denotes $x \preceq y$ and $x \neq y$

- Additional poset definitions

- Given (S, \preceq) and $x, y \in S$ with $x \prec y$,
 x is **predecessor** of y and y is **successor** of x
- Given (S, \preceq) and $x, y \in S$ with $x \prec y$,
if there is no z with $x \prec z \prec y$,
 x is **immediate predecessor** of y
- Given poset (S, \preceq) , subset $A \subseteq S$
and subset of \preceq of ordered pairs of elements in A
is a **restriction** of \preceq to A
 - Notation for restriction; \preceq partial ordering, (A, \preceq) poset
 - Reflexive, antisymmetric, transitive hold in restriction (A, \preceq)
 - Restriction (A, \preceq) is a partial ordering on A

Poset example

Poset (S, \preceq)

$S = \{1, 2, 3, 6, 12, 18\}$

Relation $x \preceq y \leftrightarrow x \mid y$

a. Ordered pairs of relation \preceq

$\{(1, 1), (1, 2), (1, 3), (1, 6), (1, 12), (1, 18),$
 $(2, 2), (2, 6), (2, 12), (2, 18),$
 $(3, 3), (3, 6), (3, 12), (3, 18),$
 $(6, 6), (6, 12), (6, 18),$
 $(12, 12), (18, 18)\}$

b. Predecessors of 6: 1, 2, 3

c. Immediate predecessors of 6: 2, 3

Poset example

Poset (S, \preceq)

$S = \{1, 2, 3, 6, 12, 18\}$

Relation $x \preceq y \leftrightarrow x \mid y$

$A = \{2, 3, 6\}$

Restriction (A, \preceq) of \preceq to A

Ordered pairs of relation \preceq

$\{(2, 2), (2, 6), (3, 3), (3, 6), (6, 6)\}$

Poset example

$(\wp(\mathbb{N}), \subseteq)$ already known to be a poset.

$(\wp(\{1, 2\}), \subseteq)$ a restriction, also a poset.

$$\wp(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$$

Ordered pairs of relation \subseteq

$$\begin{aligned} &\{(\emptyset, \emptyset), (\{1\}, \{1\}), (\{2\}, \{2\}), (\{1, 2\}, \{1, 2\}), \\ &\quad (\emptyset, \{1\}), (\emptyset, \{2\}), (\emptyset, \{1, 2\}), \\ &\quad (\{1\}, \{1, 2\}), (\{2\}, \{1, 2\})\} \end{aligned}$$

Example 10

Haase diagrams

- Purpose
 - Diagrammatic depiction of poset (S, \preceq)
 - S must be finite
- Specifics
 - Elements of S represented by dots (node, vertex)
 - Immediate predecessor relationship represented by connecting line (edge)
 - Successor placed above immediate predecessor

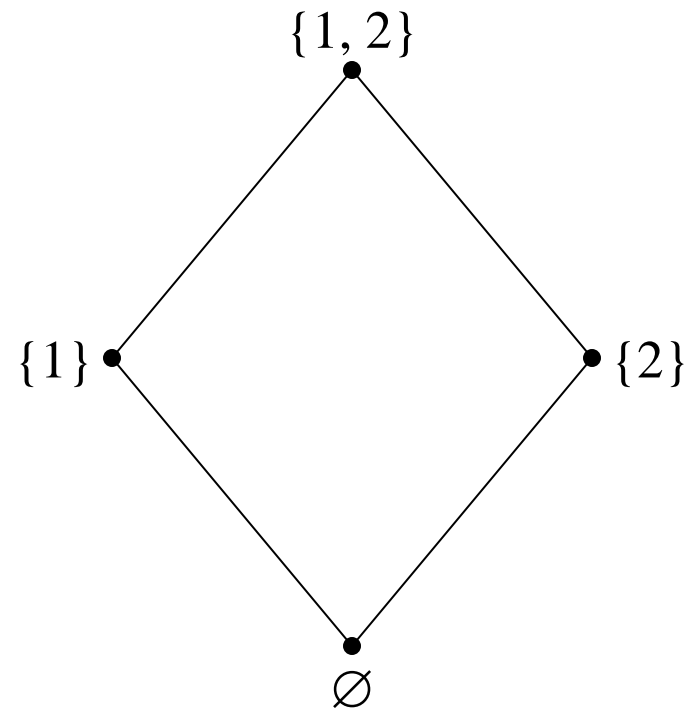
Hasse diagram example

Poset $(\wp(\{1, 2\}), \subseteq)$

$$\wp(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$$

Relation \subseteq

$\{(\emptyset, \emptyset), (\{1\}, \{1\}),$
 $(\{2\}, \{2\}), (\{1, 2\}, \{1, 2\}),$
 $(\emptyset, \{1\}), (\emptyset, \{2\}), (\emptyset, \{1, 2\}),$
 $(\{1\}, \{1, 2\}), (\{2\}, \{1, 2\})\}$



from \rightarrow to

Figure 5.2

Hasse diagram example

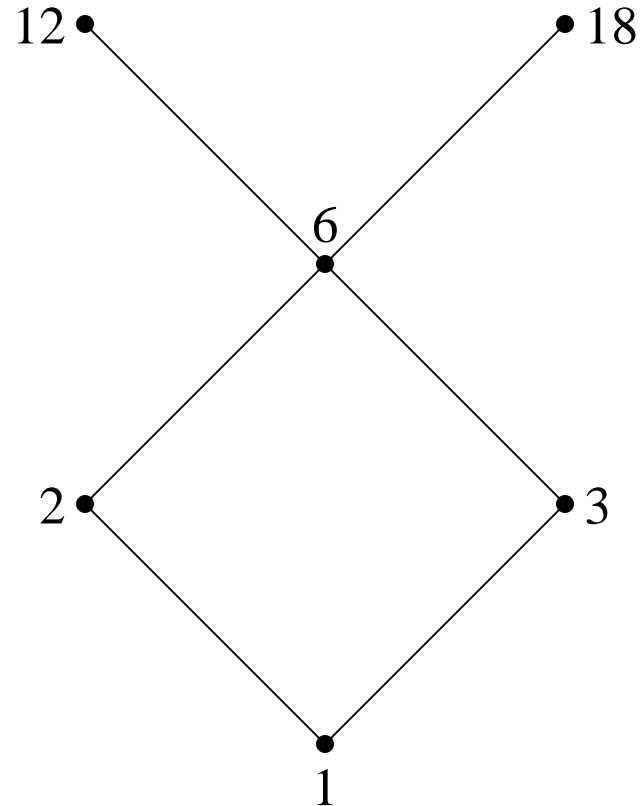
Poset (S, \leq)

$S = \{1, 2, 3, 6, 12, 18\}$

Relation $x \leq y \leftrightarrow x \mid y$

Relation \leq

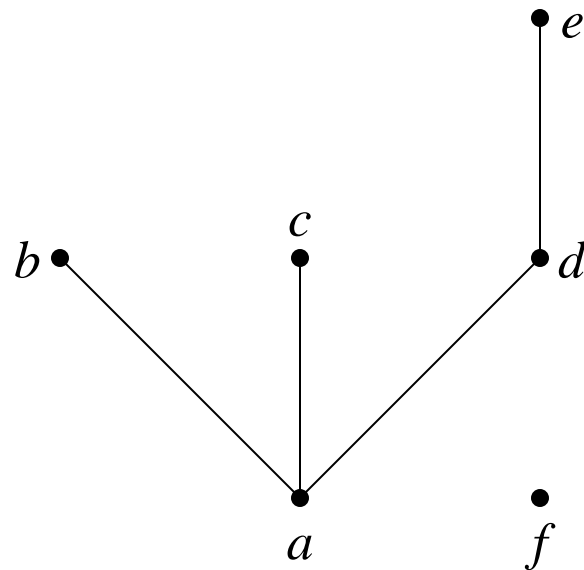
$\{(1, 1), (1, 2), (1, 3),$
 $(1, 6), (1, 12), (1, 18),$
 $(2, 2), (2, 6), (2, 12), (2, 18),$
 $(3, 3), (3, 6), (3, 12), (3, 18),$
 $(6, 6), (6, 12), (6, 18),$
 $(12, 12), (18, 18)\}$



from → to

Practice 9

Hasse diagram example



Poset (S, \leq)

$S = \{a, b, c, d, e, f\}$

Relation \leq

$\{(a, a), (b, b), (c, c),$
 $(d, d), (e, e), (f, f),$
 $(a, b), (a, c), (a, d),$
 $(a, e), (d, e)\}$

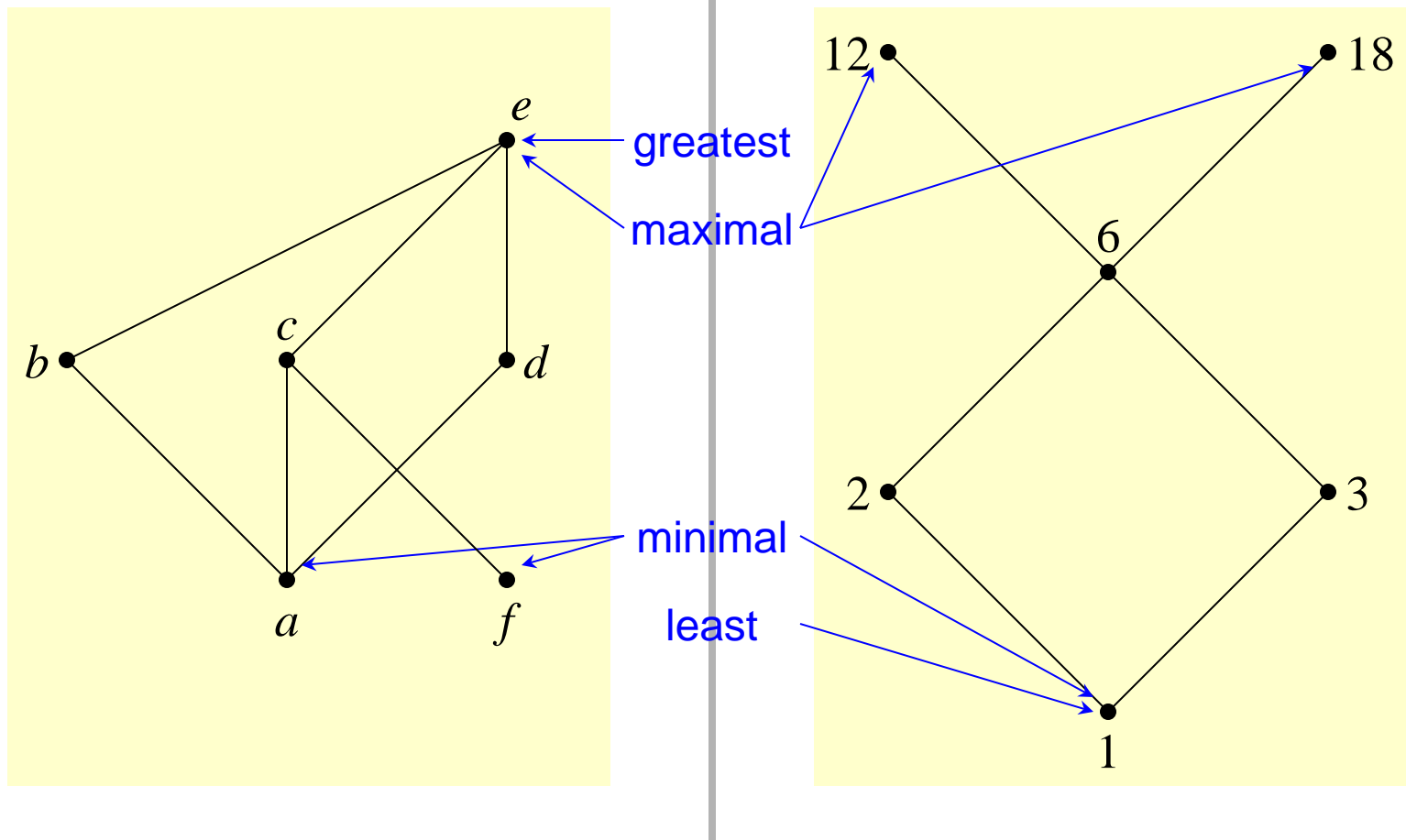
from \rightarrow to

Figure 5.3

Extreme elements

- Definitions for poset (S, \preceq)
 - **Least element**; $y \in S$ with $y \preceq x$ for all $x \in S$;
predecessor of all other elements
 - **Minimal element**; $y \in S$ with no $x \in S$ such that $x \prec y$;
has no predecessors
 - **Greatest element**; $y \in S$ with $x \preceq y$ for all $x \in S$;
successor of all other elements
 - **Maximal element**; $y \in S$ with no $x \in S$ such that $y \prec x$;
has no successors
- Notes
 - Least element always minimal but not vice versa
 - Greatest element always maximal but not vice versa

Extreme elements examples



Example 11

Total orderings

- Definitions
 - **Total ordering**; a partial ordering in which every element of S is related to every other
 - aka **chain, total order**
 - **Totally ordered set**; a set S and a total ordering \leq on S , denoted (S, \leq)
 - aka **linearly ordered set**
- Examples
 - Relation \leq on \mathbb{N}

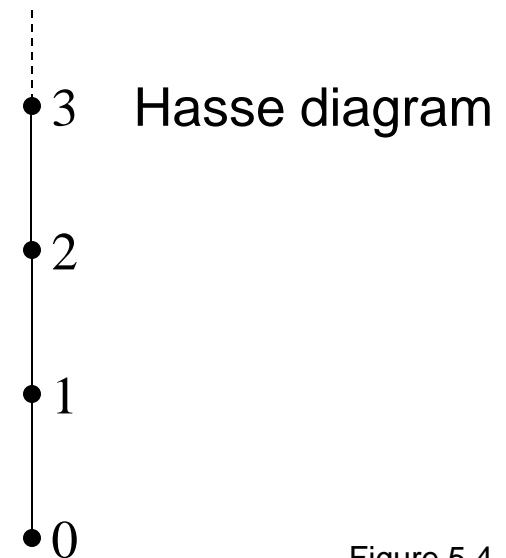


Figure 5.4

Equivalence relations

- Definition
 - **Equivalence relation**; binary relation on a set S that is reflexive, symmetric, and transitive
- Examples
 - $S = \{1, 2, 3\}$; $\rho = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)\}$
 - $S = \text{any set}$; $x \rho y \leftrightarrow x = y$
 - $S = \mathbb{N}$; $x \rho y \leftrightarrow x + y$ is even
- A relation may be both a partial ordering and an equivalence relation
 - i.e., reflexive, symmetric, transitive, and antisymmetric
 - e.g., $S = \{0, 1\}$; $x \rho y \leftrightarrow x = y^2$

Equivalence relation examples

Equivalence relation $S = \text{any set}$; $x \rho y \leftrightarrow x = y$

reflexive $x = x$

symmetric $x = y \rightarrow y = x$

transitive $x = y \wedge y = z \rightarrow x = z$

Equivalence relation $S = \mathbb{N}$; $x \rho y \leftrightarrow x + y \text{ even}$

reflexive $x + x = 2x \rightarrow \text{even}$

symmetric $x + y \text{ even} \rightarrow y + x \text{ even}$

transitive $x + y \text{ even} \wedge y + z \text{ even} \rightarrow x + z \text{ even}$

Partitions

- Definitions

- **Partition**; a partition of a set S is a collection of nonempty disjoint subsets of S whose union equals S
- e.g., set $\{1, 2, 3, 4, 5, 6\}$, partition $\{1, 2, 5\} \{4, 6\} \{3\}$
- Each element of S is in exactly one subset
- **Block**; one of the subsets making up a partition

- Example

- $S = \{x \mid x \text{ is a student in your class}\};$
 $x \rho y \leftrightarrow x \text{ sits in the same row } y$

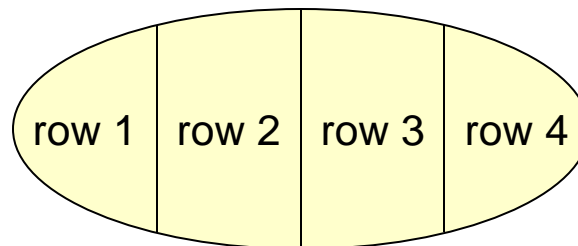


Figure 5.5

Partitions and equivalence relations

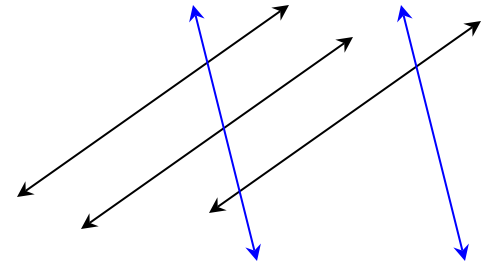
- Definition
 - **Equivalence class**; in an equivalence relation ρ on S , the set of elements to which a given element x is related by ρ , denoted $[x]$
 - Any element in an equivalence class may identify it; e.g., $x, y \in [x]$, then $[x] = [y]$
- Theorem
 - An equivalence relation ρ on a set S determines a partition of S , and a partition of S determines an equivalence relation ρ on S

Equivalence relation examples

- a. $S =$ set of all lines in the plane;
 $x \rho y \leftrightarrow x$ parallel to y or x coincides with y

Equivalence classes

Sets of lines with same slope



- b. $S = \mathbb{N}$; $x \rho y \leftrightarrow x = y$

Equivalence classes

$[n] = \{n\}$; singleton sets for each element of \mathbb{N}

- c. $S = \{1, 2, 3\}$; $\rho = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)\}$

Equivalence classes

$[1] = [2] = \{1, 2\}$

$[3] = \{3\}$

Equivalence relation example

$S = \{a/b \mid a, b \in \mathbb{Z}, b \neq 0\}$ set of all fractions

Informally, relation will relate equivalent fractions, e.g. $1/2 = 2/4$, so they will be related.

Formally, $a/b \sim c/d$ if and only if $ad = bc$

To prove that relation \sim is an equivalence relation, must show that \sim is reflexive, symmetric, and transitive.

The equivalence classes of S for \sim are

$$\left[\frac{1}{2} \right] = \left\{ \mathbf{K}, \frac{-3}{-6}, \frac{-2}{-4}, \frac{-1}{-2}, \frac{1}{2}, \frac{2}{4}, \frac{3}{6}, \mathbf{K} \right\}$$

$$\left[\frac{3}{10} \right] = \left\{ \mathbf{K}, \frac{-9}{-30}, \frac{-6}{-20}, \frac{-3}{-10}, \frac{3}{10}, \frac{6}{20}, \frac{9}{30}, \mathbf{K} \right\}$$

\mathbf{K}

The equivalence classes of S are the elements of \mathbb{Q} , in lowest terms.

Equivalence classes are sets of equivalent fractions.

Equivalence relation proof example

Theorem

Relation \sim is an equivalence relation

Proof

Reflexive. Must show $a/b \sim a/b$.

1. $ab = ba$ commutivity
2. $ab = ba \rightarrow a/b \sim a/b$ definition of \sim

Symmetric. Must show $a/b \sim c/d \rightarrow c/d \sim a/b$.

1. $a/b \sim c/d$ assumption
2. $a/b \sim c/d \rightarrow ad = bc$ definition of \sim
3. $ad = bc \rightarrow cb = da$ commutivity
4. $cb = da \rightarrow c/d \sim a/b$ definition of \sim

Transitive. Must show $a/b \sim c/d$ and $c/d \sim e/f \rightarrow a/b \sim e/f$.

1. $a/b \sim c/d$ and $c/d \sim e/f$ assumption
2. $a/b \sim c/d$ and $c/d \sim e/f$
 $\rightarrow ad = bc$ and $cf = de$ definition of \sim
3. $adf = bcf$ and $bcf = bde$
 $\rightarrow adf = bde$ multiply both sides first f , second b
4. $af = be \rightarrow a/b \sim e/f$ ■ divide both sides by d , $d \neq 0$

Equivalence relation proof example

Equivalence relation

$$S = \mathbb{N} \times \mathbb{N}$$

$$(x, y) \rho (z, w) \leftrightarrow y = w$$

Theorem

Relation ρ is an equivalence relation.

Proof

Reflexive. Must show $(x, y) \rho (x, y)$, i.e. $((x, y), (x, y)) \in \rho$.
 $y = y$, thus $(x, y) \rho (x, y)$.

Symmetric. Must show $(x, y) \rho (z, w) \rightarrow (z, w) \rho (x, y)$.

If $(x, y) \rho (z, w)$ then $y = w$ by definition of ρ .

Then $w = y$, which implies $(z, w) \rho (x, y)$.

Transitive. Must show $(x, y) \rho (z, w)$ and

$(z, w) \rho (s, t) \rightarrow (x, y) \rho (s, t)$.

$(x, y) \rho (z, w)$ implies $y = w$ and

$(z, w) \rho (s, t)$ implies $w = t$ by definition of ρ .

If $y = w$ and $w = t$, then $y = t$, and thus $(x, y) \rho (s, t)$. ■

Congruence modulo

- Definition
 - Congruence modulo n ;
for integers x, y and positive integer n ,
 $x \equiv y \pmod{n}$ iff $x - y$ is an integer multiple of n
- Congruence modulo and remainders
 - $x \equiv y \pmod{n}$ iff same remainder when divided by n

Assume same remainder r : $x = k_1n + r, y = k_2n + r$

$$\begin{aligned} & x - y \\ &= (k_1n + r) - (k_2n + r) \\ &= k_1n - k_2n \\ &= (k_1 - k_2)n \quad \text{integer multiple of } n \end{aligned}$$

Congruence modulo example

$$S = \mathbb{Z}; x \rho y \leftrightarrow x \equiv y \pmod{4}$$

Equivalence classes

$$[0] = \{ \dots, -8, -4, 0, 4, 8, \dots \}$$

$$[1] = \{ \dots, -7, -3, 1, 5, 9, \dots \}$$

$$[2] = \{ \dots, -6, -2, 2, 6, 10, \dots \}$$

$$[3] = \{ \dots, -5, -1, 3, 7, 11, \dots \}$$

mod 4 implies 4 equivalence classes

Congruence modulo on a computer

- Computer arithmetic
 - Largest integer variable n bits
 - Largest integer storable $2^n - 1$
 - If sum $x + y$ exceeds $2^n - 1$, what is result of addition?
- Possible results
 - Error message “integer overflow”
 - $x + y = (x + y) \pmod{2^n}$
- Example
 - Maximum integer that can be stored 255
 - $250 + 8 = (250 + 8) \pmod{256} = 2$

?

Relations summary

Type of binary relation	Properties	Features
Generic relation	Set of ordered pairs; $\rho \subseteq S \times S$	Represents relationships
Reflexive closure	Reflexive	ρ^* may extend ρ
Symmetric closure	Symmetric	ρ^* may extend ρ
Transitive closure	Transitive	ρ^* may extend ρ
Partial ordering	Reflexive, antisymmetric, transitive	Predecessors and successors
Equivalence relation	Reflexive, symmetric, transitive	Determines a partition

Table 4.1

Section 5.1 homework assignment

See homework list for specific exercises.



5.2 Topological sorting

Representing task sequences

- Concept
 - In a partial ordering on S some elements of S are predecessors of others
 - If S is a set of tasks, a predecessor can be understood as prerequisite task
 - Partial orderings can represent task scheduling
- Definition
 - **Partial ordering on tasks**; given set S of tasks and partial ordering \preceq on S , with $x, y \in S$, define
 - $x \preceq y \leftrightarrow x = y$ or x is prerequisite to y
 - $x \prec y \leftrightarrow x$ is prerequisite to y

Task sequence example

Task sequence for making rocking chair

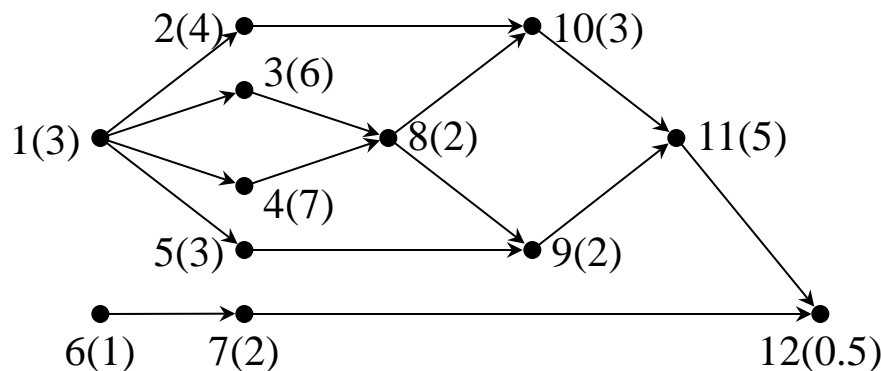
Task	Prerequisite tasks	Hours to perform
1. Select wood	None	3
2. Carve rockers	1	4
3. Carve seat	1	6
4. Carve back	1	7
5. Carve arms	1	3
6. Select fabric	None	1
7. Sew cushion	6	2
8. Assemble back and seat	3, 4	2
9. Attach arms	5, 8	2
10. Attach rockers	2, 8	3
11. Apply varnish	9, 10	6
12. Add cushions	7, 11	0.5



Example 16

PERT chart example

- PERT chart
 - Like Hasse diagram, but left to right
 - Arrows connect predecessor to successor
 - Task time shown, e.g. 1(3) is task 1, requires 3 hours
- Example
 - PERT chart for making rocking chair

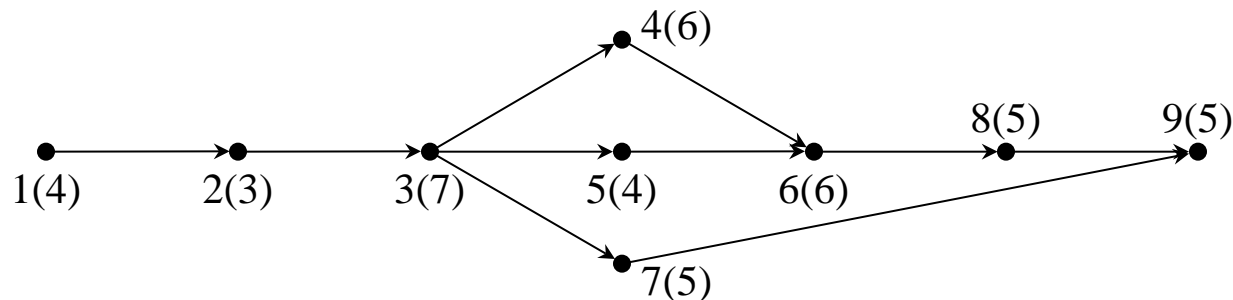


Example 16

PERT chart example

Building a house

Task	Prerequisite tasks	Days to perform
1. Clear lot	None	4
2. Pour pad	1	3
3. Do framing	2	7
4. Shingle roof	3	6
5. Add outside siding	3	4
6. Install plumbing and wiring	4, 5	6
7. Hang windows and doors	3	5
8. Install wallboard	6	5
9. Paint interior	7, 8	5



Practice 17

Task scheduling with PERT charts

- PERT chart syntax
 - Begin at left, end at right
 - Each task may start when all predecessors complete
- Task completion times
 - Task completion time is latest completion time of its predecessors, plus its perform time
 - Computing task completion times
 - Start with least task (no predecessors)
 - Move from left to right
 - Calculate completion time for each task after its predecessors
- Project completion time
 - Highest task completion time

PERT scheduling example

Task Completion time

1 3

2 $3 + 4 = 7$

3 $3 + 6 = 9$

4 $3 + 7 = 10$

5 $3 + 3 = 6$

6 1

7 $1 + 2 = 3$

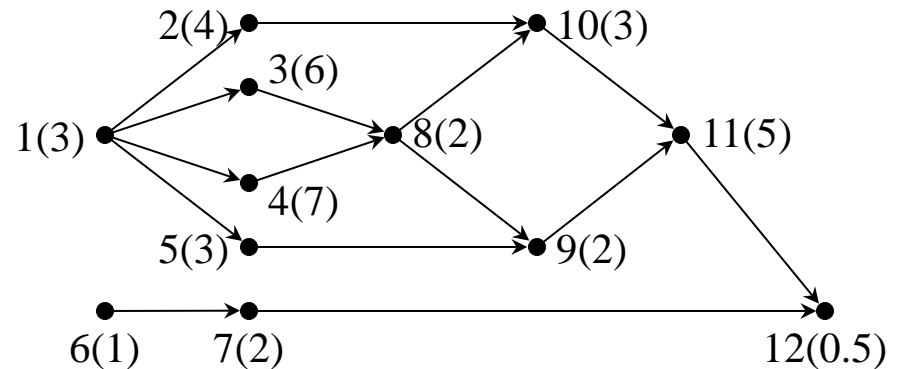
8 $\max(c(3), c(4)) + p(8) = \max(9, 10) + 2 = 12$

9 $\max(c(5), c(8)) + p(9) = \max(6, 12) + 2 = 14$

10 $\max(c(2), c(8)) + p(10) = \max(7, 12) + 3 = 15$

11 $\max(c(9), c(10)) + p(11) = \max(14, 15) + 5 = 20$

12 $\max(c(7), c(11)) + p(12) = \max(3, 20) + 0.5 = 20.5$



For task i : $c(i)$ = completion time, $p(i)$ = perform time

Example 17

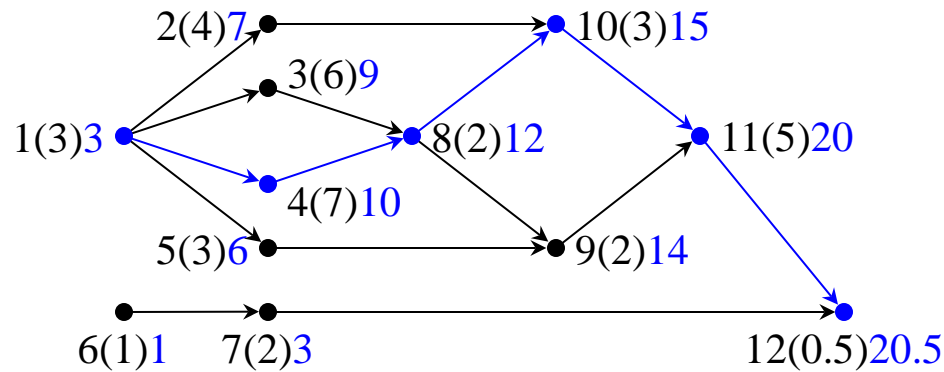
Critical path

- Definition
 - **Critical path**; sequence of tasks which determines overall project completion time
- Identifying critical path
 - Start with greatest task (latest completion time)
 - Select task's predecessor with latest completion time
 - Repeat until reaching a minimal task
- Project schedule changes
 - Increasing perform times of tasks on critical path will increase project completion time
 - Increasing perform times of tasks not on critical path may or may not change critical path

Critical path example

Critical path from greatest task 12, 11, 10, 8, 4, 1

From project start 1, 4, 8, 10, 11, 12

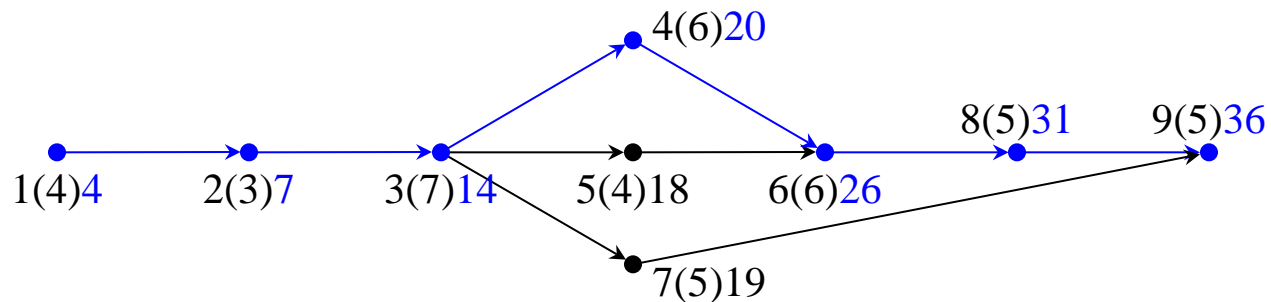


Example 17

Critical path example

Critical path from greatest task 9, 8, 6, 4, 3, 2, 1

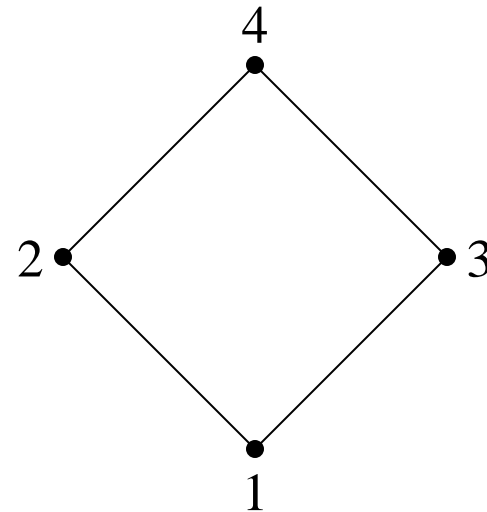
From project start 1, 2, 3, 4, 6, 8, 9



Partial and total orderings

Partial ordering

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



Total ordering

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

Total ordering

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

Topological sorting

- **Topological sorting**; process of constructing a total ordering from a partial ordering
 - Given partial ordering ρ on finite set S , extend it to total ordering σ
 - Total ordering σ must be consistent with partial ordering ρ , i.e., $x \rho y \rightarrow x \sigma y$
 - As a total ordering, σ relates every element of S to every other

Algorithm Topological Sort*TopSort*(finite set S ; partial ordering ρ on S)// Find a total ordering on S that is an extension on ρ .

// Local variable

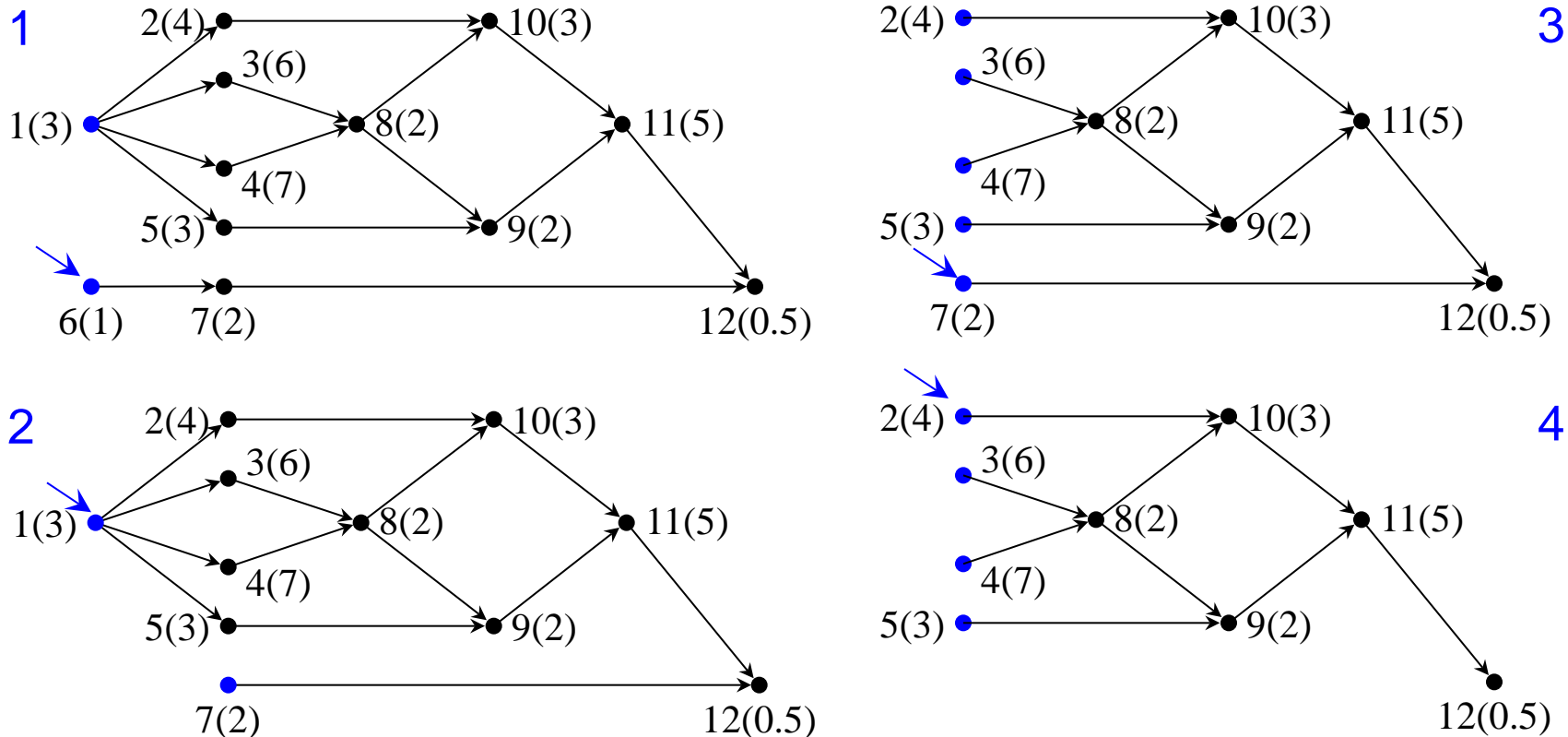
integer i // enumerates tasks in total ordering $i = 1$ **while** $S \neq \emptyset$ $x_i = \text{any minimal element in } S$ $S = S - \{x_i\}$ $i = i + 1$ **end while**// $x_1 < x_2 < x_3 < \dots < x_n$ is now a total ordering that extends ρ write($x_1, x_2, x_3, \dots, x_n$)**end** *TopSort*

?

Topological sorting example

Topological sort of rocking chair tasks

6, 1, 7, 2, 3, 5, 4, 8, 10, 9, 11, 12

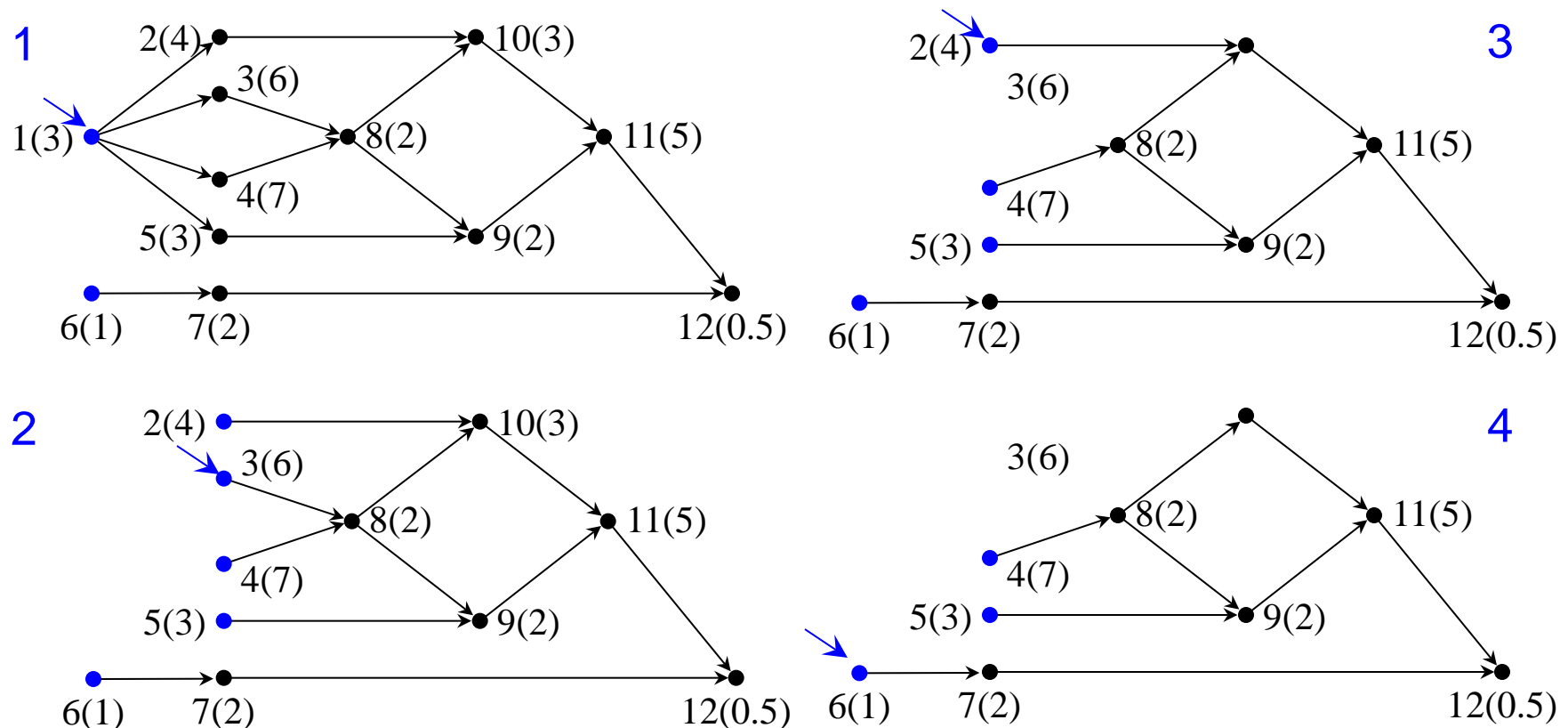


Example 18

Topological sorting example

Alternate topological sort of rocking chair tasks

1, 3, 2, 6, 7, 5, 4, 8, 9, 10, 11, 12



Practice 19

Topological sorting observations

- In any finite partially ordered set, there is at least one minimal element
- Resulting total ordering is not necessarily unique
 - Arbitrary choice among multiple minimal elements can cause different total orderings
- Resulting total ordering σ is a relation
 - Extension adds pairs to ρ to produce σ
 - Total ordering $x_1 < x_2 < x_3 < \dots < x_n$ implies pairs $(x_1, x_2), (x_2, x_3), \dots$

?

Solution to sample problem

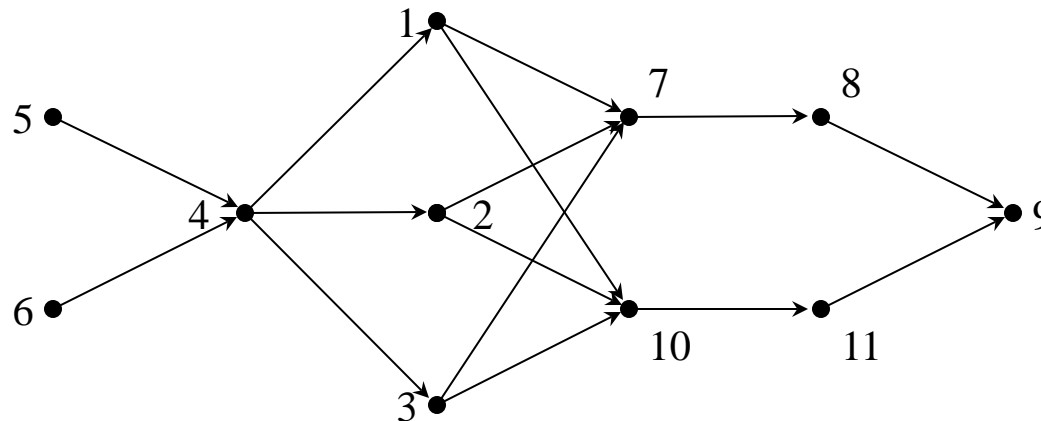
Your company has developed a program to use on a small parallel processing machine. The program executes processes P1, P2 and P3 in parallel; these processes all need results from P4, so they must wait for P4 to complete execution before they begin. Processes P7 and P10 execute in parallel but must wait until P1, P2, and P3 finish. P4 requires results from P5 and P6. P5 and P6 execute in parallel. P8 and P11 execute in parallel, but P8 must wait for P7 to complete and P11 must wait for P10 to complete. P9 must wait for results from P8 and P11.

In what order should the processes be executed on a single processor machine?

Exercise 15

Solve the problem by

1. Constructing partial ordering based on problem
2. Extending partial ordering to total ordering using topological sort
3. Scheduling processes based on total ordering



Partial ordering (represented as PERT chart)

Total ordering resulting from topological sort

5, 6, 4, 1, 2, 3, 7, 10, 8, 11, 9

Section 5.2 homework assignment

See homework list for specific exercises.



5.3 Relations and databases

5.4 Functions

Introduction to functions

- Functions
 - Simple idea, yet very important in mathematics
 - Familiar from pre-calculus and calculus
 - Relations gives new perspective on functions
- Ways of specifying functions
 - Functions as rules
 - Functions as equations for formulas
 - Functions as relations

Functions as rules

A function is a rule for associating an “output” value with a given “input” value.

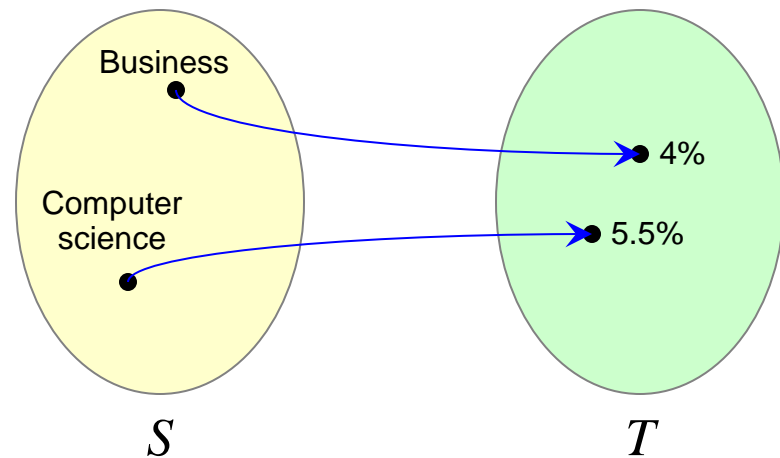
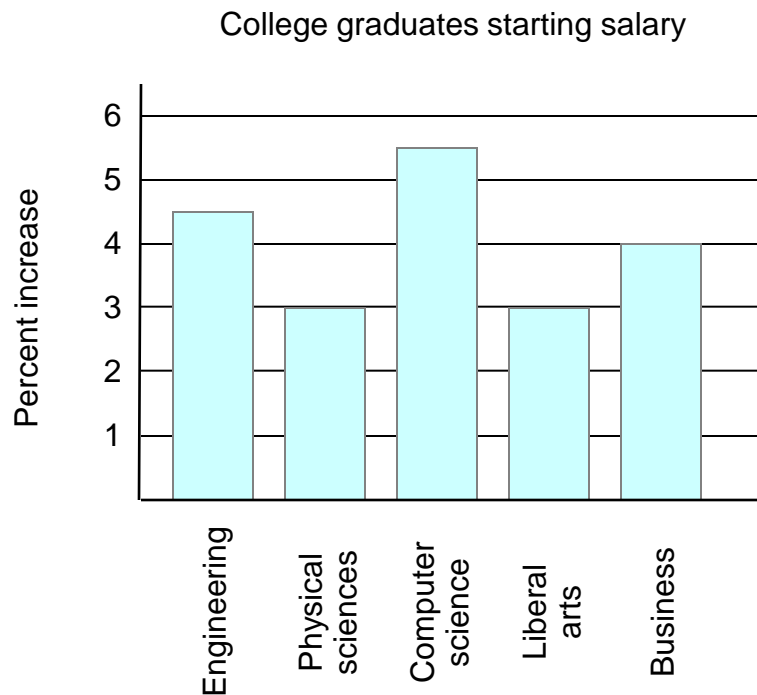
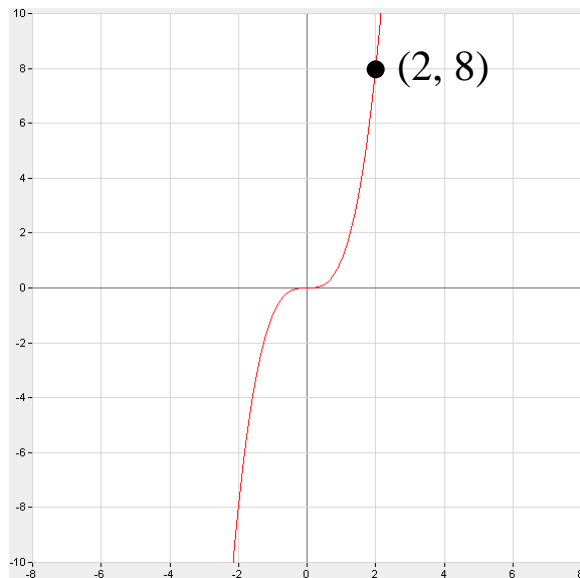


Figure 5.11, Figure 5.13

Functions as formulas

A function is an equation for producing an “output” value from a given “input” value.



$$g(x) = x^3$$

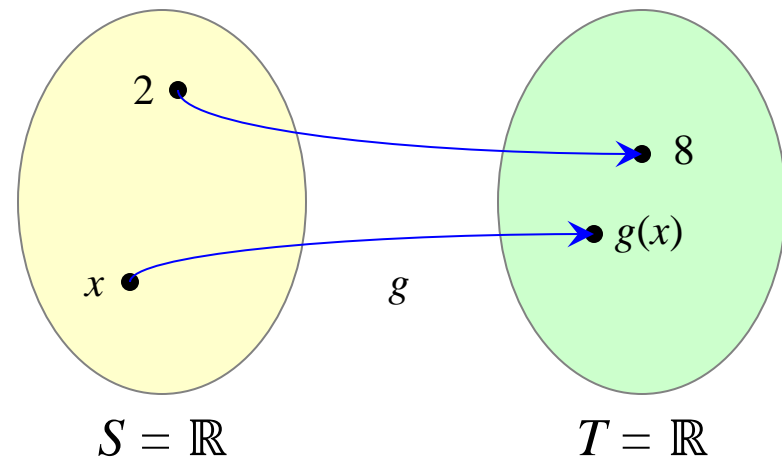


Figure 5.12, Figure 5.14

Parts of a function

- Set of “starting values” or inputs; **domain**
 - May be finite or infinite
- Set of “associated values” or outputs; **codomain**
 - May be finite or infinite
 - May be same set as “starting values”
- Mapping of inputs to outputs; **association**

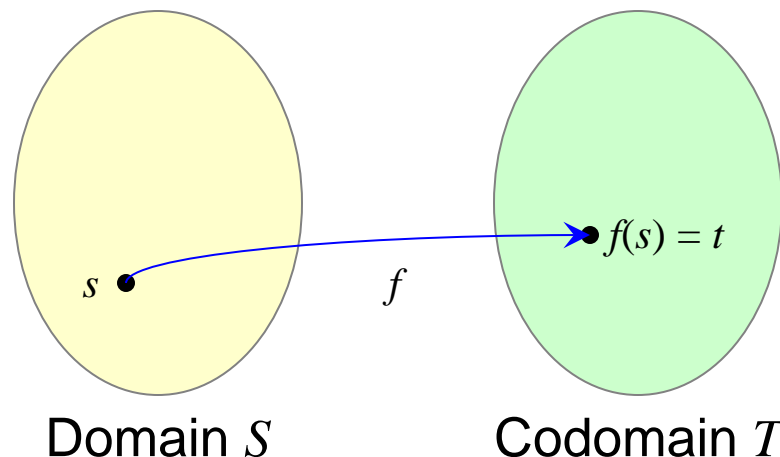
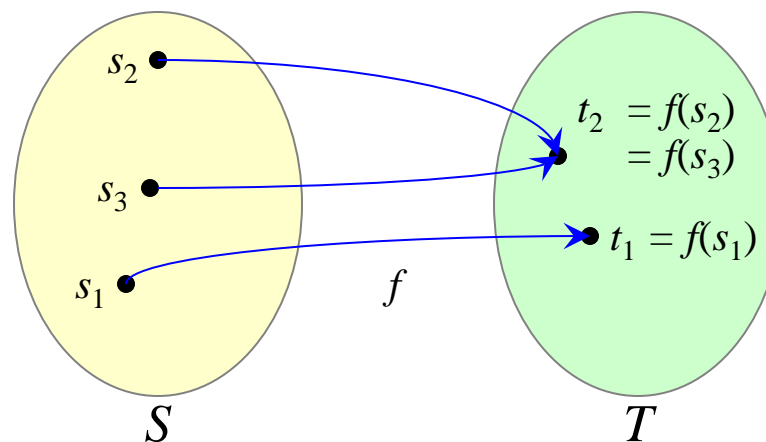


Figure 5.15

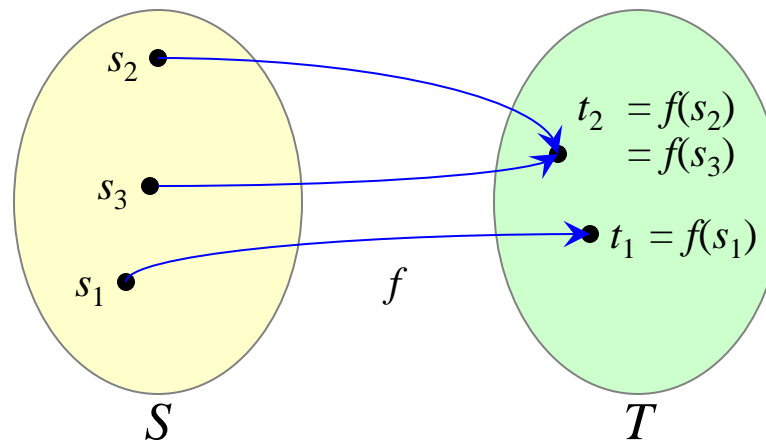
Functions as relations

- Suppose f is a function from set S to set T
- Function f is a binary relation
 - f determines a set of ordered pairs (s, t) , equivalently $(s, f(s))$, with $s \in S$, $t \in T$, and $t = f(s)$
 - f is a subset of $S \times T$



Relation $f = \{(s_1, t_1), (s_2, t_2), (s_3, t_2)\}$

- Function f is a special case of binary relations
 - Each element $s \in S$ must appear exactly once as the first element of pairs of f
 - Each element $t \in T$ may appear 0, 1, or > 1 times as the second element of pairs of f
 - One-to-many and many-to-many relations are not functions (but many-to-one relations may be)



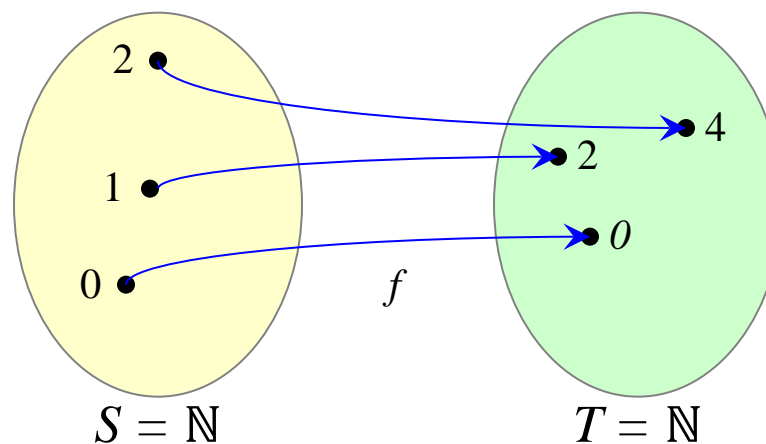
$$\text{Relation } f = \{(s_1, t_1), (s_2, t_2), (s_3, t_2)\}$$

Function terminology and notation

- Basic notation
 - Function f from set S to set T denoted $f: S \rightarrow T$
 - Set S is the **domain**
 - Set T is the **codomain**
- Images and preimages of elements
 - If (s, t) in f , then $t = f(s)$
 - t is the **image** of s under f (“output”)
 - s is the **preimage** of t under f (“input”)
- Images and preimages of sets
 - For $A \subseteq S$, $f(A) = \{f(a) \mid a \in A\}$; $f(A)$ is image of A
 - For $B \subseteq T$, $f^{-1}(B) = \{a \mid b \in B \wedge f(a) = b\}$ is preimage of B

Function example

Function	$f(x) = 2x$
Domain	\mathbb{N}
Codomain	\mathbb{N}
Relation	$\{(0, 0), (1, 2), (2, 4), (3, 6), \dots\}$
Image of $s = 1$	$2; f(s) = f(1) = 2$
Preimage of $t = 4$	$2; f(s) = f(2) = 4$



Function examples

Which of the following are functions?

a. $f: S \rightarrow T$, where $S = T = \{1, 2, 3\}$

and $f = \{(1, 1), (2, 3), (3, 1), (2, 1)\}$

No, $2 \in S$ has two values $3, 1 \in T$ associated with it

b. $g: \mathbb{Z} \rightarrow \mathbb{N}$, where $g(x) = |x|$

Yes

c. $h: \mathbb{N} \rightarrow \mathbb{N}$, where $h(x) = x - 4$

No, $h(x) \notin \mathbb{N}$ (codomain) for $x < 4$

d. $f: S \rightarrow T$, where $S =$ set of people in Huntsville,
 $T =$ set of SSNs, and f associates a person with an SSN

No, not everyone in Huntsville has an SSN

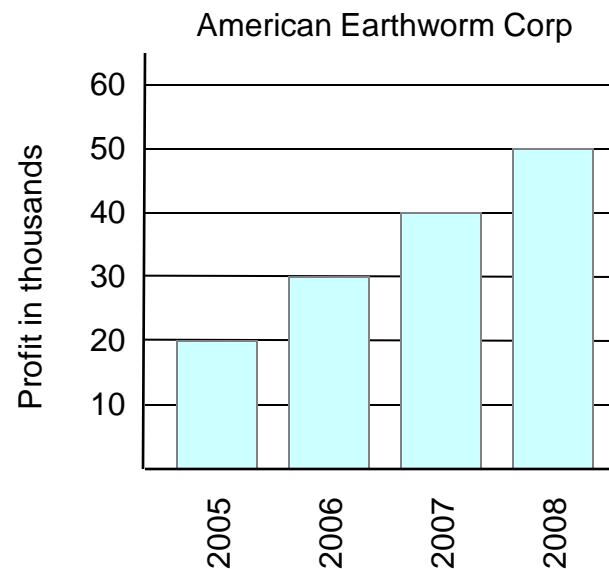
Practice 23

- e. $g: S \rightarrow T$, where $S = \{2005, 2006, 2007, 2008\}$,
 $T = \{\$20,000, \$30,000, \$40,000, \$50,000, \$60,000\}$,
and g is defined by graph below

Yes

- f. $h: S \rightarrow T$, where $S =$ set of all quadratic polynomials in x
with integer coefficients, $T = \mathbb{Z}$,
and $h(ax^2 + bx + c) = b + c$

Yes



g. $f: \mathbb{R} \rightarrow \mathbb{R}$, where $f(x) = 4x - 1$

Yes

h. $g: \mathbb{N} \rightarrow \mathbb{N}$, where $g(x) = \begin{cases} x+3 & \text{if } x \geq 5 \\ x & \text{if } x \leq 5 \end{cases}$

No, $5 \in \mathbb{N}$ (domain) has two values associated with it

Image and preimage examples

Given function $f: \mathbb{Z} \rightarrow \mathbb{Z}$, where $f(x) = x^2$

a. What is the image of -4? 16

b. What are the preimages of 9? -3, 3

What is the image of $\{-2, 0, 4\}$? $\{4, 0, 16\}$

What is the preimage of $\{25, 64\}$? $\{-5, 5, -8, 8\}$

Recursive sequences as functions

Recall recursively defined sequences, e.g., Fibonacci:

1. $F(1) = F(2) = 1$
2. $F(n) = F(n - 2) + F(n - 1)$ for $n > 2$

$F(1) = 1, F(2) = 1, F(3) = 2, F(4) = 3, F(5) = 5, F(6) = 8, \dots$

Recursive sequences may be thought of as:

1. relations, e.g., $F = \{(1, 1), (2, 1), (3, 2), (4, 3), (5, 5), \dots\}$
2. functions, e.g., $f: \mathbb{N}^+ \rightarrow \mathbb{N}^+$



Example 27

Functions of more than one variable

- Functions may have more than one variable
- Such functions are still relations,
e.g., $f: S_1 \times S_2 \times \dots \times S_n \rightarrow T$
- f associates with each n -tuple (s_1, s_2, \dots, s_n) , $s_i \in S_i$
a unique element of T

Example

$$f: \mathbb{Z} \times \mathbb{N} \times \{1, 2\} \rightarrow \mathbb{Z}, \text{ where } f(x, y, z) = x^y + z$$
$$f(-4, 3, 1) = (-4)^3 + 1 = -64 + 1 = -63$$

Example 28

Unary and binary operations as functions

- Unary operation on set S
 - Operation $\#$ associates $x^\#$ with each $x \in S$
 - Pairs in relation $\{(x_1, x_1^\#), (x_2, x_2^\#), \dots\}$
 - $\#$ defines a function with domain and codomain S
 - e.g., $x^\# = x^3$, $f(2) = 8$, pair $(2, 8)$ in relation
- Binary operation on set S
 - Operation \circ associates $x \circ y$ with each $(x, y) \in S \times S$
 - Pairs in relation $\{((x_1, y_1), x_1 \circ y_1), ((x_2, y_2), x_2 \circ y_2), \dots\}$
 - \circ defines a function with domain $S \times S$ and codomain S
 - e.g., $x \circ y = x + 2y$, $f(1, 2) = 5$, pair $((1, 2), 5)$ in relation

Example 29

Functions on non-numbers

S = finite strings of characters

For $s \in S$, $|s|$ = length (number of characters) of s

$|s|$ defines a function with domain S and codomain \mathbb{N}

$S = \{a, b, c, \dots, abc, \dots, wxyz, \dots, \textit{computer science}, \dots\}$

$s = a, |s| = 1$

$s = wxyz, |s| = 4$

$s = \textit{computer science}, |s| = 16$

Example 30

Functions on non-numbers example

S = set of propositional wffs with n distinct statement letters

Any $s \in S$ defines a function $w: \{T, F\}^n \rightarrow \{T, F\}$

- **domain** $\{T, F\}^n$, n -tuples of T-F values for the n distinct statement letters
- **codomain** $\{T, F\}$, truth value of wff given the input truth values for the statement letters
- **association** defined by the truth table for the wff

A	B	B'	$A \vee B'$
T	T	F	T
T	F	T	T
F	T	F	F
F	F	T	T

The image of 2-tuple (F, T) under w is F , i.e., $w(F, T) = F$.

Example 31

Floor and ceiling functions

Floor function $\lfloor x \rfloor = \text{largest integer } \leq x$

e.g., $\lfloor 2.8 \rfloor = 2$, $\lfloor -4.1 \rfloor = -5$

Ceiling function $\lceil x \rceil = \text{smallest integer } \geq x$

e.g., $\lceil 2.8 \rceil = 3$, $\lceil -4.1 \rceil = -4$

For both, domain is \mathbb{R} and codomain is \mathbb{Z}

Excel

`=FLOOR(x,1)`

`=CEILING(x,1)`

x is a cell reference

x	<code>=FLOOR(x,1)</code>	<code>=CEILING(x,1)</code>
2.8	2	3
-4.1	-5	-4
58	58	58
0	0	0
3.14159	3	4
-2.71828	-3	-2

Example 32

Modulo function

Modulo function $f(x) = x \bmod n$

associates with x the remainder when x divided by n

Note that $x = qn + r$, $0 \leq r < n$,
where q quotient and r remainder

$$25 = 12 \cdot 2 + 1; 25 \bmod 2 = 1$$

$$21 = 3 \cdot 7 + 0; 21 \bmod 7 = 0$$

$$15 = 3 \cdot 4 + 3; 15 \bmod 4 = 3$$

$$-17 = (-4) \cdot 5 + 3; -17 \bmod 5 = 3$$

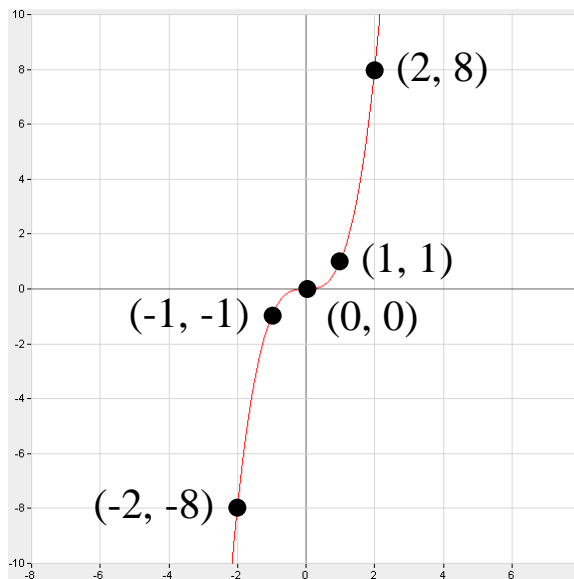
Two ways to think of mod function:

- Single function of two variables, i.e., $\bmod(x, n)$
- Many functions of one variable, i.e., $\bmod_n(x)$

Example 33

Functions parts revisited

- Parts of a function, e.g., $g(x) = x^3$
 - Domain
 - Codomain
 - Association (rule, mapping, formula)
- All three necessary to fully specify function



Curve

$$g: \mathbb{R} \rightarrow \mathbb{R}$$

Points

$$f: \mathbb{Z} \rightarrow \mathbb{R}$$

Not shown

$$k: \mathbb{R} \rightarrow \mathbb{C}$$

Function equality

- Two functions are **equal** if they have the same
 - Domain
 - Codomain
 - Association
- Proving function equality
 - State domain and codomain same
 - Show arbitrary element of domain is mapped to same element of codomain by both associations

Function equality example

$$S = \{1, 2, 3\}, T = \{1, 4, 9\}$$

$$f: S \rightarrow T, f = \{(1, 1), (2, 4), (3, 9)\}$$

$$g: S \rightarrow T, \quad g(n) = \frac{\sum_{k=1}^n (4k - 2)}{2}$$

$$h: S \rightarrow T, h(x) = x^2$$

Are f , g , and h equal?

$$f(1) = 1, f(2) = 4, f(3) = 9$$

$$g(1) = \frac{\sum_{k=1}^1 (4k - 2)}{2} = \frac{(4 \cdot 1 - 2)}{2} = 1$$

$$g(2) = \frac{\sum_{k=1}^2 (4k - 2)}{2} = \frac{(4 \cdot 2 - 2) + (4 \cdot 1 - 2)}{2} = 4$$

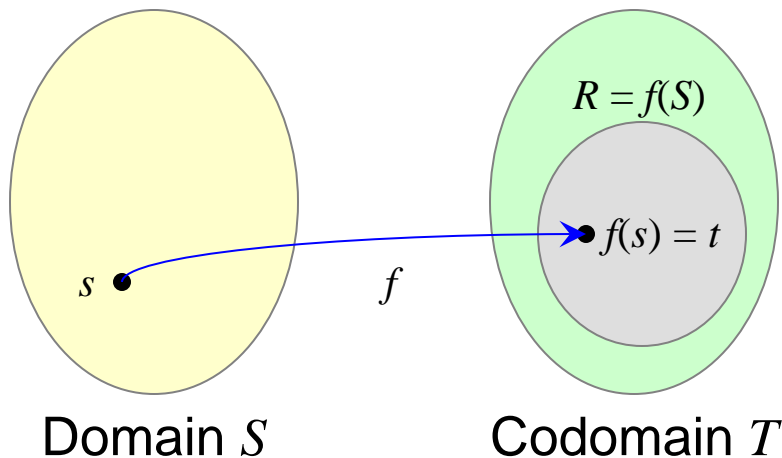
$$g(3) = \frac{\sum_{k=1}^3 (4k - 2)}{2} = \frac{(4 \cdot 3 - 2) + (4 \cdot 2 - 2) + (4 \cdot 1 - 2)}{2} = 9$$

$$h(1) = 1^2 = 1, h(2) = 2^2 = 4, h(3) = 3^2 = 9$$

Range of a function

- Definition

- Recall for $A \subseteq S$, $f(A) = \{f(a) \mid a \in A\}$; $f(A)$ is image of A
- For function $f: S \rightarrow T$, $f(S) = R = \{f(s) \mid s \in S\}$,
i.e., the image of the domain, is the **range** of f ; $R \subseteq T$



Example

Function

$$f: \mathbb{Z} \rightarrow \mathbb{Z}, f(x) = x^2$$

Range

$$f(\mathbb{Z}) = R = \{0, 1, 4, 9, \dots\}$$

$$R \subset \mathbb{Z}$$

Figure 5.19

Properties of functions

- Properties of all functions $f: S \rightarrow T$
 - Relation, i.e., $f = \{(s_1, t_1), (s_2, t_2), \dots\}$
 - For every element $s \in S$, $f(s) = t$,
 $t \in T$, t exists, and t is unique
- Properties a function may or may not have
 - onto (surjective)
 - one-to-one (injective)
 - one-to-one and onto (bijective)

Properties of functions: onto

- Definition
 - Function $f: S \rightarrow T$ with domain S , codomain T , range R
 - Function f is **onto** if $R = T$
 - aka **surjective**, i.e., “function f is a surjection”
- Equivalent definitions
 - ... every $t \in T$ is associated with an $s \in S$
 - ... every $t \in T$ appears at least once
as the second element in the ordered pairs of f
- Proving a function is onto
 - Already known that $R \subseteq T$
 - Prove $T \subseteq R$, i.e., for arbitrary $t \in T$, $t \in R$;
to do this, show there exists $s \in S$ such that $f(s) = t$
 - If $R \subseteq T$ and $T \subseteq R$, then $R = T$, thus f is onto

Onto function examples

Theorem

Function $g: \mathbb{R} \rightarrow \mathbb{R}$, $g(x) = x^3$, is onto.

Proof

Assume $r \in \mathbb{R}$ (codomain).

We seek $x \in \mathbb{R}$ (domain) such that $g(x) = r$.

Let $x = \sqrt[3]{r}$. Then $x \in \mathbb{R}$ (domain), and $g(x) = (\sqrt[3]{r})^3 = r$.

Thus any r in codomain is the image of $x = \sqrt[3]{r}$ in domain. ■

Theorem

Function $k: \mathbb{R} \rightarrow \mathbb{C}$, $k(x) = x^3$, is not onto.

Proof

Element $i = 0 + 1i \in \mathbb{C}$ is not the result of r^3 for any $r \in \mathbb{R}$. ■

Onto function example

Function $f: \{T, F\}^n \rightarrow \{T, F\}$ defined by propositional wff P .

When is f not onto?

When P is a tautology (always T)
or a contradiction (always F).

A	B	B'	$B \wedge B'$	$A \wedge (B \wedge B')$
T	T	F	F	F
T	F	T	F	F
F	T	F	F	F
F	F	T	F	F

Properties of functions: one-to-one

- Definition
 - Function $f: S \rightarrow T$ with domain S , codomain T , range R
 - Function f is **one-to-one**
if $s_1, s_2 \in S$ and $s_1 \neq s_2 \rightarrow f(s_1) \neq f(s_2)$
 - aka **injective**, i.e., “function f is an injection”
- Equivalent definitions
 - ... no $t \in T$ is associated with two distinct $s_1, s_2 \in S$
 - ... $f(s_1) = f(s_2) \rightarrow s_1 = s_2$
- Proving a function is one-to-one
 - Assume $s_1, s_2 \in S$ and $f(s_1) = f(s_2)$, prove $s_1 = s_2$

One-to-one function examples

Theorem

Function $g: \mathbb{R} \rightarrow \mathbb{R}$, $g(x) = x^3$, is one-to-one.

Proof

Let $x, y \in \mathbb{R}$ be arbitrary real numbers with $g(x) = g(y)$.
Then $x^3 = y^3$ and $x = y$. ■

Theorem

Function $g: \mathbb{R} \rightarrow \mathbb{R}$, $g(x) = x^2$, is not one-to-one.

Proof

$g(2) = g(-2) = 4$. ■

Properties of functions: one-to-one and onto

- Definition
 - Function $f: S \rightarrow T$ with domain S , codomain T , range R
 - Function f is **one-to-one and onto** if it is both one-to-one and onto
 - aka **bijective**, i.e., “function f is a bijection”
- Proving a function is one-to-one and onto
 - Prove one-to-one and prove onto

One-to-one and onto function examples

Theorem

Function $g: \mathbb{R} \rightarrow \mathbb{R}$, $g(x) = x^3$, is one-to-one and onto.

Proof

Function g is one-to-one (Example 36).

Function g is onto (Example 34). ■

Theorem

Function $g: \mathbb{R} \rightarrow \mathbb{R}$, $g(x) = x^2$, is not one-to-one and onto.

Proof

Function g is not one-to-one (Example 36). ■

Example 38

One-to-one and onto function example

Function $f: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R} \times \mathbb{R}$, $f(x, y) = (x + y, x - y)$,
e.g., $f(11, 25) = (36, -14)$

Theorem

Function f is one-to-one and onto.

Proof

One-to-one. Assume $(x_1, y_1), (x_2, y_2) \in \mathbb{R} \times \mathbb{R}$
and $f(x_1, y_1) = f(x_2, y_2)$; we must show $(x_1, y_1) = (x_2, y_2)$.

If $f(x_1, y_1) = f(x_2, y_2)$, then by definition of f ,
 $(x_1 + y_1, x_1 - y_1) = (x_2 + y_2, x_2 - y_2)$.

[continued next slide](#)

Example 7.2.10, p. 409, S. S. Epp, *Discrete Mathematics with Applications*,
Fourth Edition, Brooks/Cole, Boston MA, 2011.

Then x_1, y_1, x_2, y_2 satisfy these equations:

$$x_1 + y_1 = x_2 + y_2 \quad (1)$$

$$x_1 - y_1 = x_2 - y_2 \quad (2)$$

Adding equations (1) and (2) gives

$$2x_1 = 2x_2, \text{ so } x_1 = x_2.$$

Substituting $x_1 = x_2$ into equation (1) gives

$$x_1 + y_1 = x_1 + y_2, \text{ so } y_1 = y_2.$$

Thus $(x_1, y_1) = (x_2, y_2)$, and consequently, f is one-to-one.

continued next slide

Onto. Assume $(u, v) \in \mathbb{R} \times \mathbb{R}$ (codomain); we must show there exists $(r, s) \in \mathbb{R} \times \mathbb{R}$ (domain) such that $f(r, s) = (u, v)$.

Let $r = (u + v)/2$ and $s = (u - v)/2$.

Then $f(r, s)$

$$= f((u + v)/2, (u - v)/2)$$

$$= ((u + v)/2 + (u - v)/2, (u + v)/2 - (u - v)/2)$$

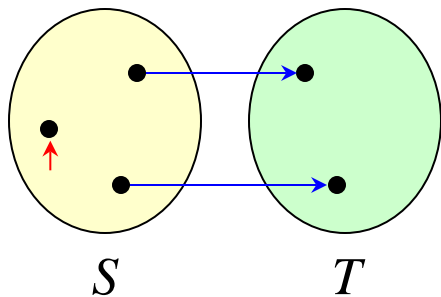
$$= ((u + v + u - v)/2, (u + v - u + v)/2)$$

$$= (2u/2, 2v/2)$$

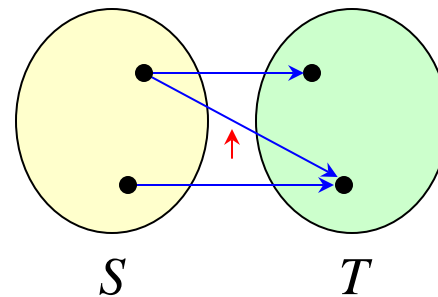
$$= (u, v)$$

Thus there exists $(r, s) \in \mathbb{R} \times \mathbb{R}$ such that $f(r, s) = (u, v)$, and consequently f is onto). ■

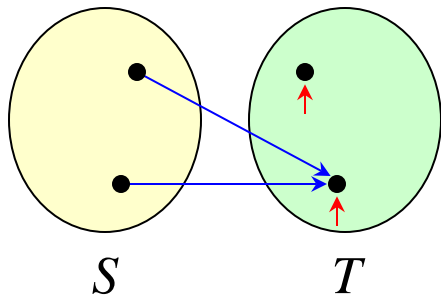
Properties of functions summary



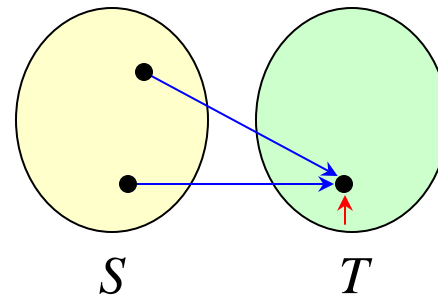
not a function



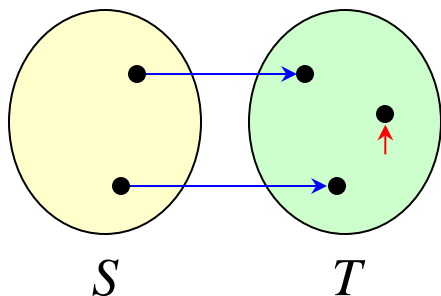
not a function



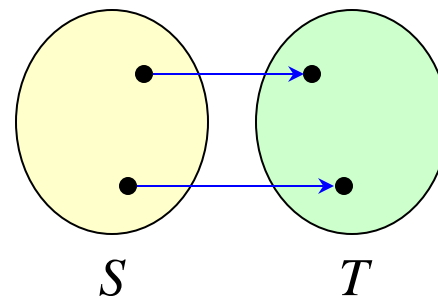
function
not one-to-one
not onto



function
not one-to-one
onto



function
one-to-one
not onto



function
one-to-one
onto

Figure 5.20

Composition of functions

- Definition

- Given functions $f: S \rightarrow T$ and $g: T \rightarrow U$, the **composition function** $g \circ f$ is a function from S to U , defined by $(g \circ f)(s) = g(f(s))$.
- aka **composition** and **composite function**
- Codomain of f is the domain of g ; more generally, range of f must be subset of domain of g

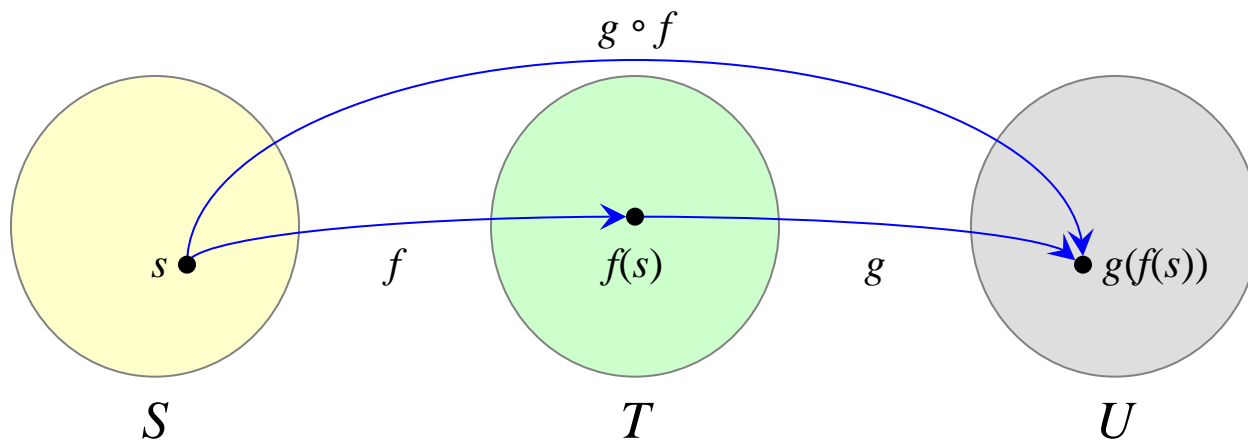


Figure 5.22

Composite function examples

Function $f: \mathbb{N} \rightarrow \mathbb{N}$, $f(x) = 3x + 1$

Function $g: \mathbb{N} \rightarrow \mathbb{N}$, $g(x) = x^2$

$$(g \circ f)(2) = g(f(2)) = 49$$

Function $f: \mathbb{N} \rightarrow \mathbb{N}$, $f(x) = 2x$

Function $g: \mathbb{R} \rightarrow \mathbb{R}$, $g(x) = \sqrt{x}$

$$(g \circ f)(2) = g(f(2)) = \sqrt{4} = 2$$

Composite function example

Two functions may be composed in either order; the order may affect the result.

Function $f: \mathbb{N} \rightarrow \mathbb{N}$, $f(x) = 2x$

Function $g: \mathbb{R} \rightarrow \mathbb{R}$, $g(x) = \sqrt{x}$

$$(g \circ f)(2) = g(f(2)) = \sqrt{4} = 2$$

$(f \circ g)(2) = f(g(2))$ undefined ($\sqrt{2} \notin \mathbb{N}$), thus not a function

Function $f: \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = x^2$

Function $g: \mathbb{R} \rightarrow \mathbb{R}$, $g(x) = \lfloor x \rfloor$

$$(g \circ f)(2.3) = g(f(2.3)) = g((2.3)^2) = g(5.29) = \lfloor 5.29 \rfloor = 5$$

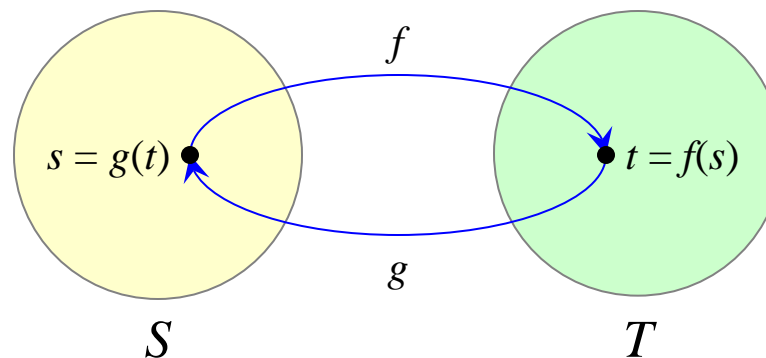
$$(f \circ g)(2.3) = f(g(2.3)) = f(\lfloor 2.3 \rfloor) = f(2) = 2^2 = 4$$

Function properties under composition

- Function composition preserves properties
 - Surjective (onto)
 - Injective (one-to-one)
 - Bijective (one-to-one and onto)
 - Computable (not in [Gersting 6e])
- If functions f , g both have a property, then $(f \circ g)$ and $(g \circ f)$ have the property

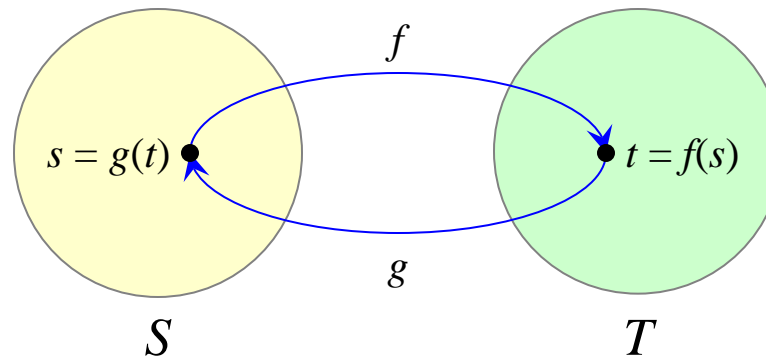
Identity functions and bijections

- Definition
 - **Identity function** $i_S: S \rightarrow S$ maps each $s \in S$ to itself
- Identity functions and bijections imply each other
 - $i_s = (g \circ f)$ where f and g are inverse bijections



Inverse functions and bijections

- Definition
 - Given function $f: S \rightarrow T$ and $g: T \rightarrow S$, if $i_S = (g \circ f)$ and $i_T = (f \circ g)$ are identity functions, then g is the **inverse function** of f
 - Inverse of function f denoted f^{-1}
- Inverse functions and bijections imply each other
 - Function $f: S \rightarrow T$ is a bijection iff f^{-1} exists



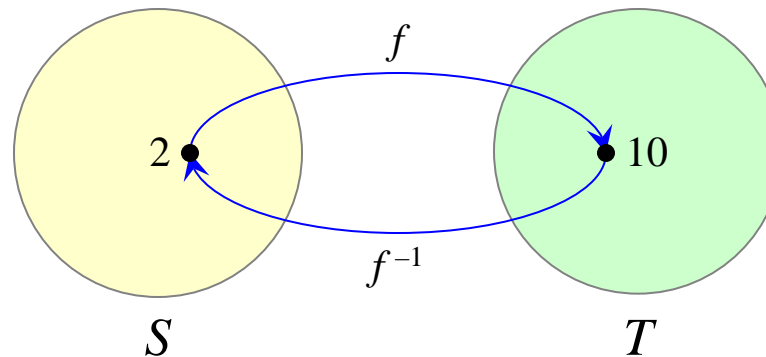
Inverse function example

Function $f: \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = 3x + 4$

Inverse function $f^{-1}: \mathbb{R} \rightarrow \mathbb{R}$, $f^{-1}(x) = (x - 4)/3$

$$f(2) = 3 \cdot 2 + 4 = 10$$

$$f^{-1}(10) = (10 - 4)/3 = 2$$



Practice 34

Function terminology summary

Term	Meaning
Function	Mapping from one set to another; associates each element of input set with exactly one element of output set
Domain	Input (starting, from) set for a function
Codomain	Output (ending, to) set for a function
Image	Output element (or set) to which input element (or set) is mapped
Preimage	Input element (or set) from which output element (or set) is mapped
Range	Image of the domain
Onto (surjective)	Range is entire codomain; every codomain element has preimage
One-to-one (injective)	No two elements of domain have same image
Bijjective	One-to-one and onto
Identity function	Function which maps each element of domain to itself
Inverse function	For a bijection, a new function that maps each codomain element to its preimage under the bijection

Permuting a set with functions

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

A permutation (ordered arrangement) of A : 2, 3, 1, 4

Function $f = \{(1, 2), (2, 3), (3, 1), (4, 4)\}$
generates this permutation.

?

Another way of writing f , called **array form**:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

Permutation functions

- Definition
 - For a given set A , define set of functions $S_A = \{f \mid f: A \rightarrow A \text{ and } f \text{ is a bijection}\}$
 - S_A is the set of all bijections of set A to itself
 - Such functions are called **permutations** of A
 - aka **permutation functions**
 - **Identity permutation** $i_A \in S_A$ maps every $a \in A$ to itself
- Composing permutation functions
 - S_A closed under composition, i.e., $f, g \in S_A$ implies function $g \circ f: A \rightarrow A$ in S_A
 - Composition a binary operation on S_A

Cycle notation for permutation functions

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

Permutation of A : 2, 3, 1, 4

In array form, function $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$

In cycle notation, function $f = (1, 2, 3)$

Each element maps to the element to its right in the cycle; elements not in the cycle map to themselves.

Cycle notation examples

a. Set $A = \{1, 2, 3, 4, 5\}$, permutation function $f \in S_A$

Array form $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 5 & 1 \end{pmatrix}$

Cycle notation $f = (1, 4, 5)$

b. Set $A = \{1, 2, 3, 4, 5\}$, permutation function $g \in S_A$

Cycle notation $g = (2, 4, 5, 3)$

Array form $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 5 & 3 \end{pmatrix}$

Composing permutation functions example

Set $A = \{1, 2, 3, 4\}$, permutation functions $f, g \in S_A$

$$f = (1, 2, 3) \quad f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

(Note: In the original image, the elements 2 and 3 in the first column of both permutation matrices are highlighted in yellow, and blue arrows point from these elements to the first row of the composition result below.)

Composition $g \circ f = (2, 3) \circ (1, 2, 3)$, but what is it?

$g(f(1)) = g(2) = 3$	$1 \rightarrow 2 \rightarrow 3$
$g(f(2)) = g(3) = 2$	$2 \rightarrow 3 \rightarrow 2$
$g(f(3)) = g(1) = 1$	$3 \rightarrow 1 \rightarrow 1$
$g(f(4)) = g(4) = 4$	$4 \rightarrow 4 \rightarrow 4$

$$g \circ f = (1, 3) \quad g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

Example 39

Disjoint cycles

Set $A = \{1, 2, 3, 4, 5\}$, permutation functions $f, g \in S_A$

$$f = (1, 2, 3, 4)$$

$$g = (3, 2, 4, 5)$$

$$\text{Composition } g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix}$$

cannot be written as a single cycle;

it consists of two disjoint cycles $(1, 4)$ and $(3, 5)$.

$$\text{Composition } g \circ f = (1, 4) \circ (3, 5)$$

Derangements

- Definition

- A permutation function $f: A \rightarrow A$
where no element of A is mapped to itself
is a **derangement**

- Notes

- Derangements, written as cycles, list all elements of A
- Non-derangement permutations omit at least element

Example

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

$$f = (1\ 2\ 5\ 3\ 4)$$

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix} \text{ is a derangement}$$

Example 40

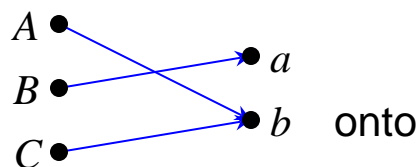
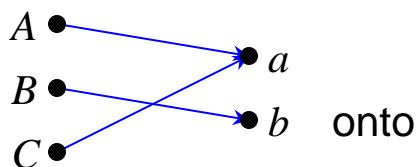
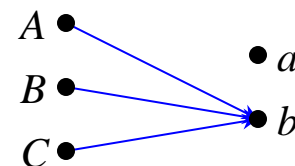
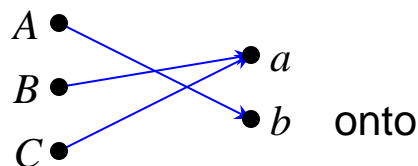
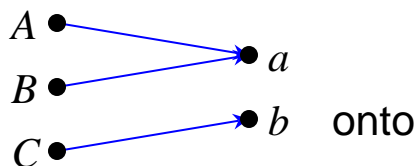
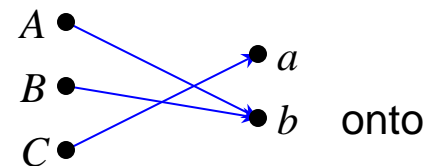
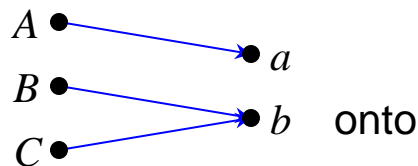
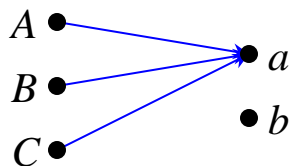
How many functions?

Set $S = \{A, B, C\}$, $T = \{a, b\}$

How many functions are there from S to T ? 8

How many are one-to-one? 0

How many are onto? 6



Example 41, Practice 38

Number of functions of all types

Sets S and T are finite, $|S| = m$ and $|T| = n$

How many functions from S to T are there?

Each of the m elements of S can be mapped to any of the n elements of T .

Number of functions $f: S \rightarrow T$

$$\underbrace{n \cdot n \cdot n \cdot \dots \cdot n}_{m \text{ terms}} = n^m = |T|^{|S|}$$

m terms

In Example 41, $|S| = m = 3$ and $|T| = n = 2$, $2^3 = 8$.

Number of one-to-one functions

Sets S and T are finite, $|S| = m$ and $|T| = n$

How many one-to-one functions from S to T are there?

$m \leq n$ required for the functions to be one-to-one.

Each of the m elements of S mapped to an element of T .
Each $t \in T$ may be the image of at most one $s \in S$.

Number of one-to-one functions $f: S \rightarrow T$, assuming $m \leq n$

$$\underbrace{n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot (n-(m-1))}_{m \text{ terms}} = \frac{n!}{(n-m)!} = P(n, m)$$

Number of onto functions

Sets S and T are finite, $|S| = m$ and $|T| = n$

How many onto functions from S to T are there?

$m \geq n$ required for the functions to be onto.

Calculated as all functions – non-onto functions;
specific formula follows from PI&E.

Number of onto functions $f: S \rightarrow T$, assuming $m \geq n$

$$n^m - C(n, 1)(n-1)^m + C(n, 2)(n-2)^m \\ - C(n, 3)(n-3)^m + \dots + (-1)^{n-1} C(n, n-1)(1)^m$$

Example 41: $2^3 - C(2, 1)(1)^3 = 8 - 2 \cdot 1 = 6$

Number of permutation functions

Set A , $|A| = n$

How many permutation functions on A are there?

Each of the n elements of A mapped to an element of A , with no repetitions.

Number of permutation functions $f: A \rightarrow A$

$$n \cdot (n - 1) \cdot (n - 2) \cdot \dots \cdot 1 = n!$$

$$P(n, n) = n!$$

Number of derangements

Set A , $|A| = n$

How many derangements on A are there?

Calculated as:

all permutation functions – non-derangements;
specific formula follows from PI&E.

Number of derangements $f: A \rightarrow A$

$$n! \cdot \left[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + (-1)^n \frac{1}{n!} \right]$$

Number of derangements example

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

How many derangements on A are there?

According to the formula

$$3! \cdot \left[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} \right] = \frac{3!}{2!} - \frac{3!}{3!} = 3 - 1 = 2$$

The derangements are

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

?

Example 42

Equivalent sets

- Definition
 - A set S is **equivalent** to a set T if there exists a bijection $f: S \rightarrow T$
 - Equivalent sets have the same **cardinality**
- Cardinality of finite and infinite sets
 - Finite sets: cardinality is the same thing as size, i.e., number of elements
 - Infinite sets: cardinality is based on equivalence, e.g., \mathbb{N} has same cardinality as \mathbb{Z} because there is a bijection \mathbb{N} to \mathbb{Z} , even though $\mathbb{N} \subset \mathbb{Z}$

Denumerability revisited

- Definitions

- Any finite set S is **denumerable** (aka countable)
- An infinite set S is **denumerable** if there exists a bijection $f: \mathbb{N} \rightarrow S$ (or vice versa)
- \mathbb{N} and an infinite denumerable set are equivalent

- Enumerations of denumerable sets

- Given a bijection $f: \mathbb{N} \rightarrow S$, elements of \mathbb{N} can be associated with elements of S
- A list of the elements of S in the order $f(0), f(1), f(2), \dots$ is an **enumeration** of S

Example enumerations

Give a bijection $f: \mathbb{N} \rightarrow \mathbb{Z}$

$$\mathbb{Z} = \{ \dots, -3, -2, -1, 0, 1, 2, 3, \dots \}$$

$$\begin{array}{ccccccc} & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\ \dots & 5 & 3 & 1 & 0 & 2 & 4 & 6 \dots \end{array}$$

$$f(x) = \begin{cases} x/2 & \text{if } x \text{ even} \\ -(x+1)/2 & \text{if } x \text{ odd} \end{cases}$$

Give a bijection $g: \mathbb{Z} \rightarrow \mathbb{N}$

$$\mathbb{N} = \{ 0, 1, 2, 3, 4, 5, 6, \dots \}$$

$$\begin{array}{ccccccc} \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\ 0 & 1 & -1 & 2 & -2 & 3 & -3 & \dots \end{array}$$

$$g(x) = \begin{cases} -2x & \text{if } x \leq 0 \\ 2x-1 & \text{if } x > 0 \end{cases}$$

Cantor's theorem

- Review
 - Power set $\wp(S)$ is the set of all subsets of S
 - For finite S , with $|S| = n$, $|\wp(S)| = 2^n$
- Cardinality of $\wp(S)$
 - Finite sets: $n < 2^n$ 1
thus S and $\wp(S)$ have different cardinality,
thus S and $\wp(S)$ not equivalent
 - Infinite sets: S and $\wp(S)$ also have different cardinality, 2
thus S and $\wp(S)$ not equivalent
 - **Cantor's theorem**: for any set S , 3
 S and $\wp(S)$ not equivalent
 - By Cantor's theorem, $\wp(\mathbb{N})$ is not equivalent to \mathbb{N} , 4
i.e., $\wp(\mathbb{N})$ is not denumerable.

Example 43

Proof of Cantor's theorem

Theorem

For any set S , S and $\wp(S)$ not equivalent.

Proof (by contradiction)

Assume by way of contradiction that S and $\wp(S)$ equivalent. 1

Let $f: S \rightarrow \wp(S)$ be a bijection from S to $\wp(S)$.

For any $s \in S$, $f(s) \in \wp(S)$, i.e., $f(s) \subseteq S$; possibly $s \in f(s)$. 2

Define set $X = \{x \in S \mid x \notin f(x)\}$.

$X \subseteq S$, i.e., $X \in \wp(S)$, thus there exists $y \in S$ with $f(y) = X$. 3

There are two cases, either $y \in X$ or $y \notin X$.

1. Suppose $y \in X$; then $y \notin f(y)$, but $f(y) = X$, so $y \notin X$. 4

2. Suppose $y \notin X$; then because $f(y) = X$, $y \notin f(y)$, so $y \in X$. 5

There is a contradiction in each case,
thus S and $\wp(S)$ also not equivalent. ■

Another proof of Cantor's theorem

Theorem

For any countably infinite set S , $\wp(S)$ is not countable.

Proof (by diagonalization)

Assume by way of contradiction that S and $\wp(S)$ equivalent.

Thus let $f: \mathbb{N} \rightarrow \wp(S)$ be a bijection from \mathbb{N} to $\wp(S)$.

Represent bijection f as a table; columns $s_1, s_2, \dots \in S$;

row i denotes subset $t_i \in \wp(S)$ such that $f(i) = t_i$;

for entry s_j in row i , 1 means $s_j \in t_i$, 0 means $s_j \notin t_i$.

	s_1	s_2	s_3	s_4	s_5	s_6	...
1	1	0	0	0	0	0	...
2	1	1	0	0	0	0	...
3	1	1	0	1	0	0	...
4	0	1	0	1	1	0	...
...							

Given the tabular representation of f

	s_1	s_2	s_3	s_4	s_5	s_6	...
1	1	0	0	0	0	0	...
2	1	1	0	0	0	0	...
3	1	1	0	1	0	0	...
4	0	1	0	1	1	0	...
...							
t_x	0	0	1	0	...		

Construct subset $t_x \in \wp(S)$ such that $s_i \in t_x$ iff $s_i \notin t_i$.

Then t_x is different from every subset t_i for the bijection f .

Because $t_x \in \wp(S)$ and different from every t_i ,

t_x is not included in f , a contradiction. ■

Theorem 11.1, p. 278, P. Linz, *An Introduction to Formal Languages and Automata Theory, Fourth Edition*, Jones and Bartlett, Sudbury MA, 2006.

Section 5.4 homework assignment

See homework list for specific exercises.



5.5 Order of Magnitude

Order of magnitude analogy

Different “order of magnitude” $\sim \times 10$

Same “within a multiplicative constant” $\sim \times 2$



Order of magnitude of functions

- Order of magnitude
 - Measure of rate of growth of functions
 - e.g., $f(x) = x$ grows more slowly than $g(x) = x^2$
- Method
 - Define binary relation on functions
 - In earlier topics, function defined relation,
e.g., $x \rho y \leftrightarrow x = y^2$
 - Here objects being related are functions,
e.g., $g(x) \rho h(x)$
 - Related functions have “same” rate of growth

Order of magnitude relation

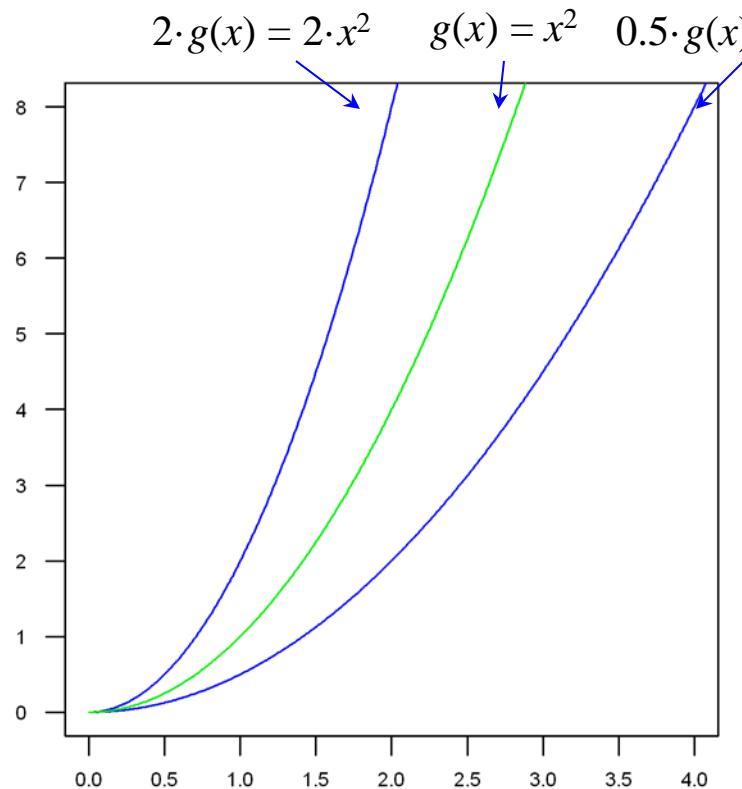
- Relation

- Let S be the set of all functions from \mathbb{R}^+ to \mathbb{R}^+
- Define $f \rho g \leftrightarrow$ there exist positive constants n_0, c_1, c_2 such that for all $x \geq n_0$, $c_1 g(x) \leq f(x) \leq c_2 g(x)$

- Meaning

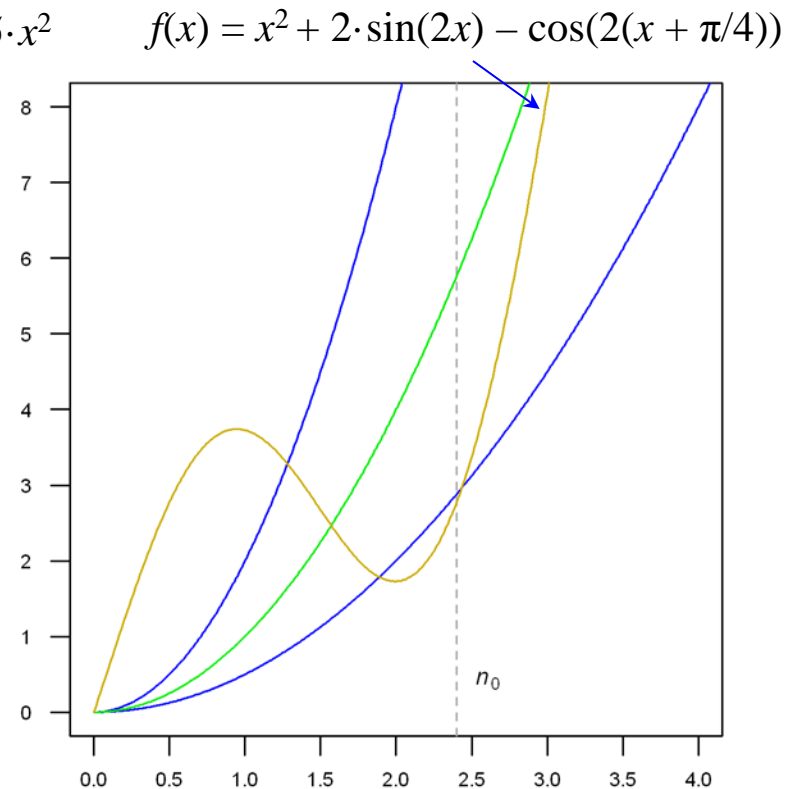
- Once x is larger than a threshold, the values of $f(x)$ and $g(x)$ are the same, to within multiplicative constants
- $f(x)$ and $g(x)$ are considered to have the same rate of growth, i.e., the same **order of magnitude**

Order of magnitude example



All functions within the boundaries
are same order of magnitude.

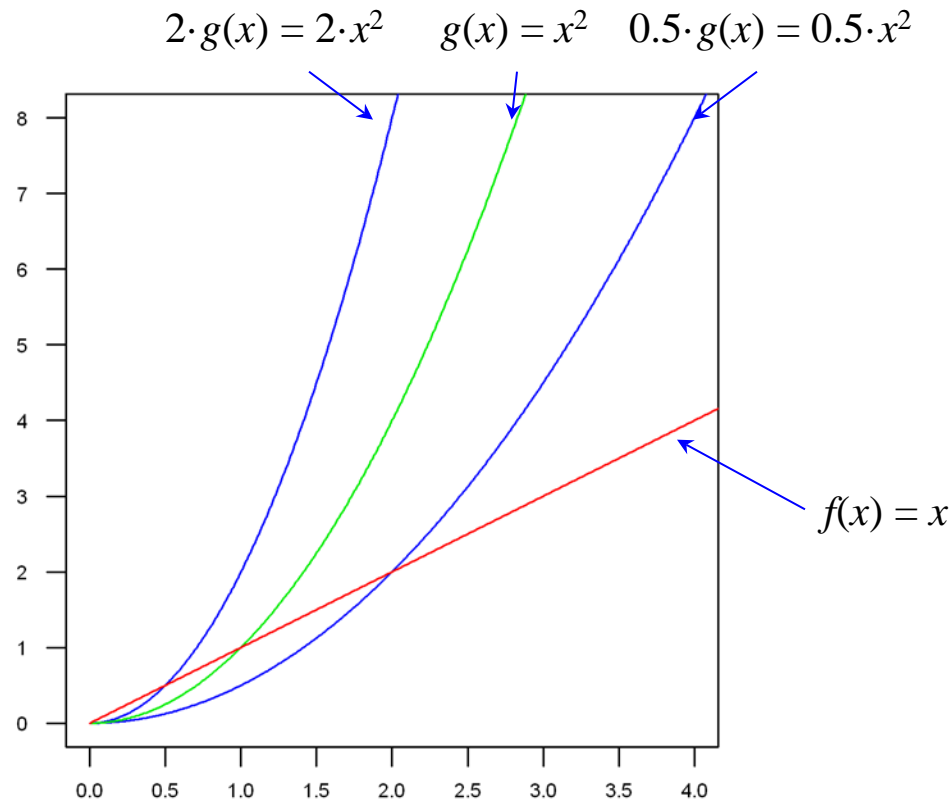
$$c_1 = 0.5, c_2 = 2$$



Beyond n_0 , $f(x)$ is within
boundaries, thus $f = \Theta(g)$.

Figure 5.26, Figure 5.27

Order of magnitude example



There is no n_0 above which $f(x)$ is within boundaries, regardless of c_1, c_2 .
Thus $f(x) = x$ is not same order of magnitude as $g(x) = x^2$.

Example 45, Figure 5.28

Order of magnitude example

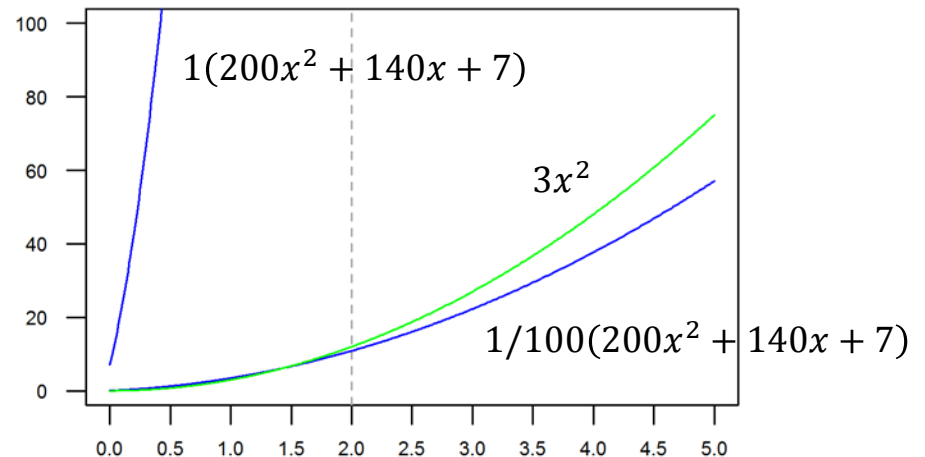
Let $f, g \in S$ be functions, $f(x) = 3x^2$ and $g(x) = 200x^2 + 140x + 7$

Let $n_0 = 2$, $c_1 = 1/100$, $c_2 = 1$; then for $x \geq 2$,

$$\frac{1}{100}(200x^2 + 140x + 7) \leq 3x^2 \leq 1(200x^2 + 140x + 7)$$

$$2x^2 + 1.4x + 0.07 \leq 3x^2 \leq 200x^2 + 140x + 7$$

Therefore $f \rho g$.



Example 44

Definition, properties, and notation

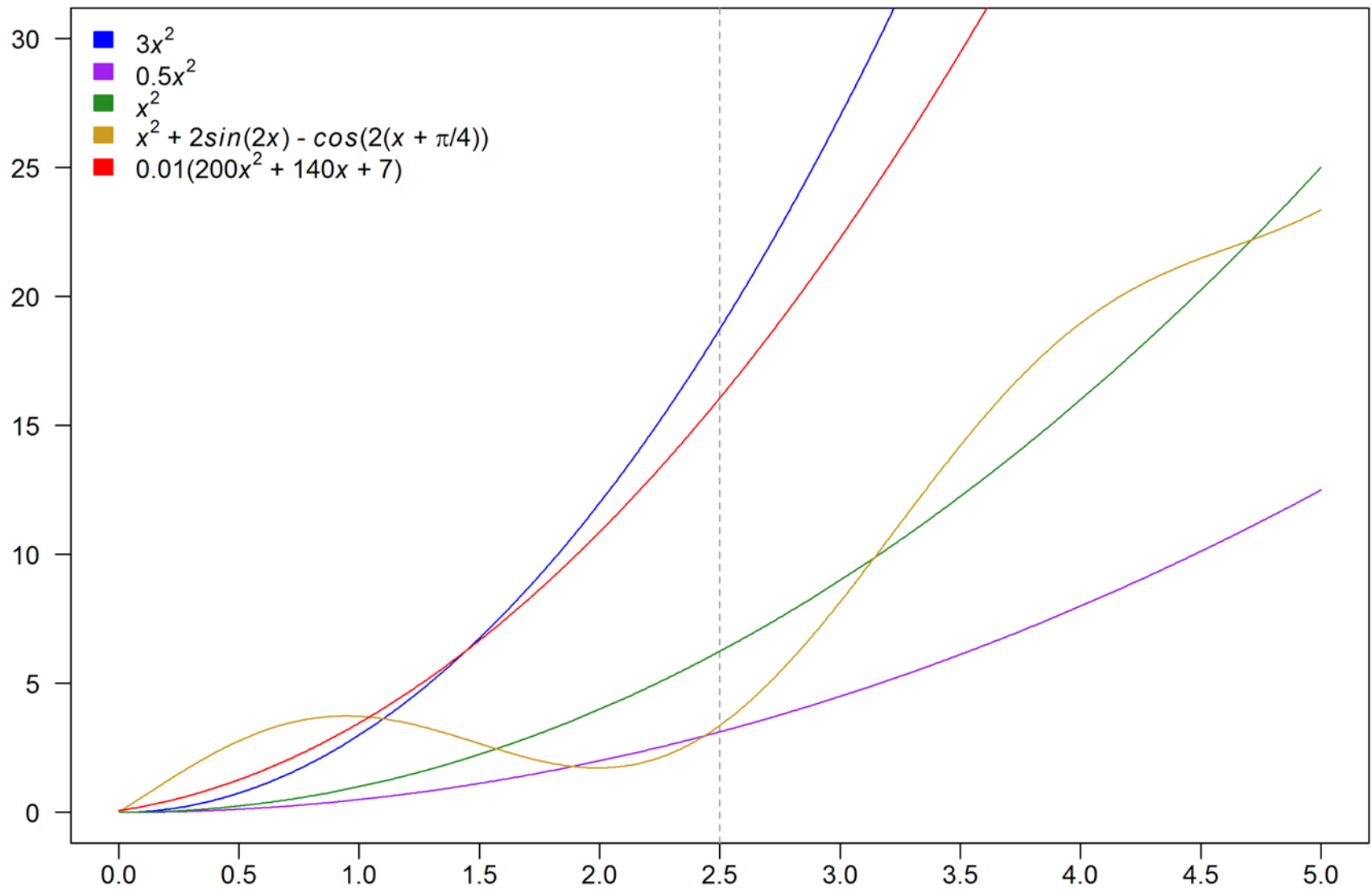
- Definition

- Let f and g be functions mapping \mathbb{R}^+ to \mathbb{R}^+ ; then f is the same **order of magnitude** as g , written $f = \Theta(g)$, if $f \rho g$, i.e., there exist positive constants n_0, c_1, c_2 such that for all $x \geq n_0$, $c_1 g(x) \leq f(x) \leq c_2 g(x)$

- Properties of ρ

- ρ is an equivalence relation, partitions S into equivalence classes
- Functions in the same equivalence class have the same order of magnitude

- Using order of magnitude notation
 - Written in simplest form,
e.g., $f = \Theta(x^2)$, not $f = \Theta(200x^2 + 140x + 7)$
 - Order of magnitude of a polynomial function is its highest degree term (with coefficient 1)
 - Standard $f = \Theta(x^2)$ notation imprecise;
 $\Theta(x^2)$ is a set of functions (the equivalence class),
 $f = \Theta(x^2)$ should be $f \in \Theta(x^2)$



Divide-and-conquer recurrence relations, revisited

Divide-and-conquer recurrence relation
and solution formula from Chapter 3

Recurrence relation
general form

$$S(n) = cS\left(\frac{n}{2}\right) + g(n) \quad \text{for } n \geq 2, n = 2^m$$

Solution formula

$$S(n) = c^{\log n} S(1) + \sum_{i=1}^{\log n} c^{(\log n)-i} g(2^i)$$

Generalized divide-and-conquer algorithms

- Chapter 3 RR applied to D&C algorithms that
 - Divide input into 2 parts
 - Operate recursively on 1 ($c = 1$) or 2 ($c = 2$) parts
 - Require $g(n)$ basic ops to divide and/or combine
- More general D&C algorithms
 - Divide input into b parts
 - Operate recursively on a parts
 - Require $g(n)$ basic ops to divide and/or combine

Recurrence relation
general form

$$S(n) = aS\left(\frac{n}{b}\right) + g(n)$$

for $n \geq 2$, $n = b^m$,
integer $m \geq 1$,
integer $a \geq 1$, integer $b > 1$

Divide-and-conquer “Master Theorem”

When $g(n)$ has the form $g(n) = n^c$,
“Master Theorem” applies.

If $S(n)$ is a D&C RR of the form

$$S(1) \geq 0$$

$$S(n) = aS\left(\frac{n}{b}\right) + n^c \quad \begin{array}{l} \text{for } n \geq 2, n = b^m, \text{ integer } m \geq 1, \\ \text{integer } a \geq 1, \text{ integer } b > 1, \text{ real } c \geq 0 \end{array}$$

Then

1. if $a < b^c$, then $S(n) = \Theta(n^c)$
2. if $a = b^c$, then $S(n) = \Theta(n^c \log n)$
3. if $a > b^c$, then $S(n) = \Theta(n^{\log_b a})$ (n to power $\log_b a$)

Master Theorem examples

Example 47 (Binary search)

$$\begin{aligned} C(1) &= 1 \\ C(n) &= C\left(\frac{n}{2}\right) + 1 \end{aligned} \quad \begin{aligned} &\text{for } n \geq 2, n = 2^m, \text{ integer } m \geq 1, \\ &\text{integer } a \geq 1, \text{ integer } b > 1, \text{ real } c \geq 0 \end{aligned}$$

$$a = 1, b = 2, c = 0$$

By the MT, because $a = b^c$ (case 2), $C(n) = \Theta(n^0 \log n) = \Theta(\log n)$, which matches Chapter 3 Examples 24 and 25.

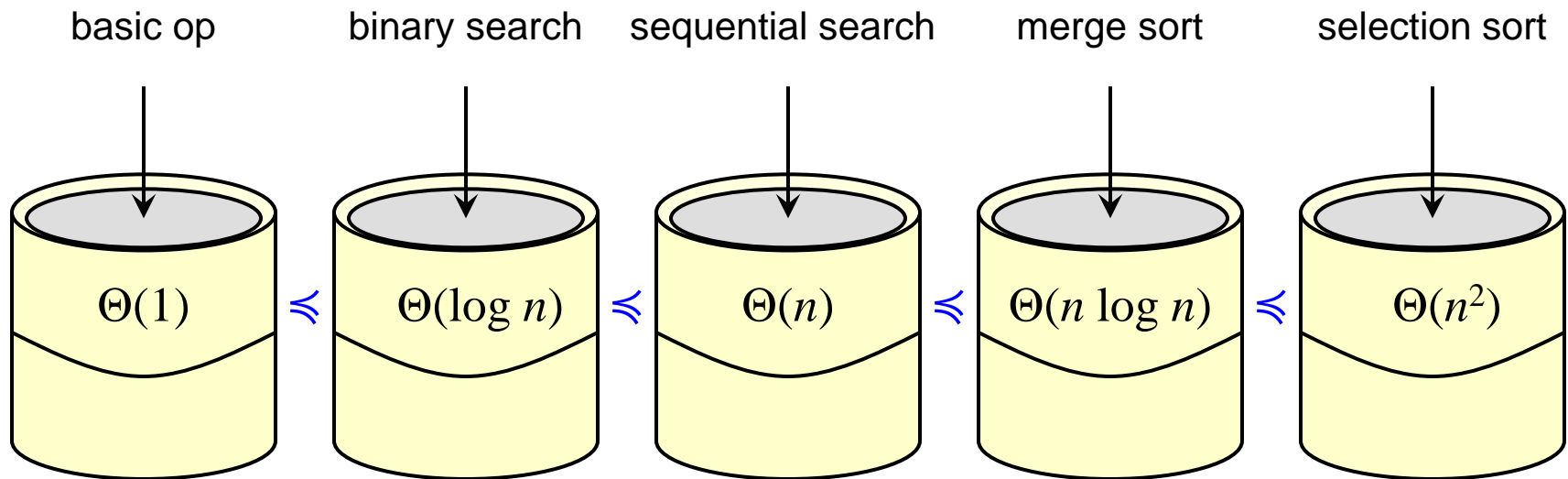
Example 46

$$\begin{aligned} S(1) &\geq 1 \\ S(n) &= 4S\left(\frac{n}{5}\right) + n^3 \end{aligned} \quad \begin{aligned} &\text{for } n \geq 2, n = 5^m, \text{ integer } m \geq 1, \\ &\text{integer } a \geq 1, \text{ integer } b > 1, \text{ real } c \geq 0 \end{aligned}$$

$$a = 4, b = 5, c = 3$$

By the MT, because $a < b^c$ (case 1), $S(n) = \Theta(n^3)$.

Computational complexity concept



Algorithm complexity is number of basic operations, as a function of input size n .

Algorithms compared on order of magnitude.

Many algorithms studied in CS are in one of these “bins”. Differences within bin not as important as between bins.

Computational complexity examples

Algorithm	# of basic ops	Order	[Gersting, 2014]
Binary search	$1 + \log n$	$\Theta(\log n)$	§ 3.1
Sequential search	n	$\Theta(n)$	§ 3.3
Grade calculation	$n + n(m - 1)$		§ 3.3
Pattern matching	$m(n - m + 1)$		§ 3.3
Polynomial evaluation	$3n$		§ 3.3
Merge sort	$n \log n - n + 1$	$\Theta(n \log n)$	§ 3.3
Upper triangular array sum	$n(n + 1)/2$	$\Theta(n^2)$	§ 3.3
Selection sort	$n(n - 1)/2$		§ 3.1
Bubble sort	$n(n - 1)/2$		§ 3.3
Fraction list	$n(n + 1)(2n + 1)/6$	$\Theta(n^3)$	§ 3.3

Comparing growth rates

Total computation time				
		Size of input n		
Algorithm	Order	10	50	100
A	n	0.001 second	0.005 second	0.01 second
A'	n^2	0.01 second	0.25 second	1 second
A''	2^n	0.1024 second	3570 years	4×10^{18} years

In table, 1 computation step requires 0.0001 second. Different orders of magnitude make a big difference in algorithm performance.

Problems for which no polynomial time algorithm is available are called **intractable**.

Table 5.4

Upper and lower bounds

- Order of magnitude
 - Notation $f = \Theta(g)$, pronounced “order g ”
 - Bounds f above and below
 - Finding bounds on both sides may not be possible
- Upper bound
 - Function f does not grow faster than function g , (i.e., \leq) within multiplicative constant
 - Notation $f = O(g)$, pronounced “big oh g ” or “order g ”
 - Definition $f = O(g)$ if there exist positive constants n_0, c such that for all $x \geq n_0$, $f(x) \leq c \cdot g(x)$
 - “Worst case”

- Strict upper bound
 - Function f does not grow as fast as function g , (i.e., $<$) within multiplicative constant
 - Notation $f = o(g)$, pronounced “little oh g ” or “order g ”
 - Definition $f = o(g)$ if there exist positive constants n_0, c such that for all $x \geq n_0$, $f(x) < c \cdot g(x)$
- Lower bound
 - Function f does not grow slower than function g , (i.e., \geq) within multiplicative constant
 - Notation $f = \Omega(g)$, pronounced “omega g ” or “order g ”
 - Definition $f = \Omega(g)$ if there exist positive constants n_0, c such that for all $x \geq n_0$, $c \cdot g(x) \leq f(x)$
 - “Best case”

Section 5.5 homework assignment

See homework list for specific exercises.



5.6 The Mighty Mod Function

5.7 Matrices

Introduction to matrices

- Definition and terminology
 - **Matrix**; rectangular arrangement of values
 - Values aka entries, elements
 - **Dimensions** of a matrix; number of rows and columns
 - Notation: matrix \mathbf{A} , element a_{ij} (row i , column j)
- Applications
 - Graphics programming (rotation matrix)
 - Linear programming (coefficients matrix)
 - Linear algebra (linear transformations)

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 4 \\ 3 & -6 & 8 \end{bmatrix} \quad \begin{array}{l} \mathbf{A} \text{ is a } 2 \times 3 \text{ matrix.} \\ a_{23} = 8 \end{array}$$

Example matrix

$$\mathbf{A} = \begin{bmatrix} 1 & 4 & -6 & 8 \\ 3 & 0 & 1 & -7 \end{bmatrix}$$

\mathbf{A} is a 2×4 matrix.

$$a_{23} = 1$$

$$a_{24} = -7$$

$$a_{13} = -6$$

Example matrix

Matrices may hold data.

Monthly average temperatures (F) in 3 cities;

3×12 matrix, rows are cities, columns are months.

$$\mathbf{A} = \begin{bmatrix} 23 & 26 & 38 & 47 & 58 & 71 & 78 & 77 & 69 & 55 & 39 & 33 \\ 14 & 21 & 33 & 38 & 44 & 57 & 61 & 59 & 49 & 38 & 25 & 21 \\ 35 & 46 & 54 & 67 & 78 & 86 & 91 & 94 & 89 & 75 & 62 & 51 \end{bmatrix}$$

Average April temperature in 3rd city in April, $a_{34} = 67$



Example 61

Example matrix

Matrices may represent relations.

Set $S = \{2, 5, 7, 9\}$, relation $\rho = \{(7, 9), (2, 5), (9, 9), (2, 7)\}$

Ordering function $f: S \rightarrow \{1, 2, 3, 4\}$,
 $f = \{(2, 1), (5, 2), (7, 3), (9, 4)\}$

Matrix \mathbf{R} represents ρ by $r_{f(i)f(j)} = 1$ if $(i, j) \in \rho$, else $r_{f(i)f(j)} = 0$.

$$\mathbf{R} = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad \begin{array}{l} (7, 9) \in \rho \rightarrow a_{f(7)f(9)} = a_{34} = 1 \\ (2, 5) \in \rho \rightarrow a_{f(2)f(5)} = a_{12} = 1 \\ (9, 9) \in \rho \rightarrow a_{f(9)f(9)} = a_{44} = 1 \\ (2, 7) \in \rho \rightarrow a_{f(2)f(7)} = a_{13} = 1 \end{array}$$

Example 62

Example matrix

Matrices may represent systems of linear equations.

Suppose you are ordering coffee for sidewalk café;
you want to order 70 pounds, mix of Kona and Columbian.
Kona is \$24 per pound, Columbian is \$14 per pound.
You are willing to spend \$1180.
How many pounds of each should you order?

System of linear equations

$$\begin{aligned}x + y &= 70 \\ 24x + 14y &= 1180\end{aligned}$$

$$\mathbf{A} = \begin{bmatrix} 1 & 1 \\ 24 & 14 \end{bmatrix} \quad \mathbf{A} \text{ is matrix of coefficients.}$$

Example 63

Matrix equality

- Definition
 - Two matrices are **equal** if they have the same dimensions and the same elements

$$\mathbf{X} = \begin{bmatrix} x_{11} & 4 \\ 1 & x_{22} \\ x_{31} & 0 \end{bmatrix}$$

$$\mathbf{Y} = \begin{bmatrix} 3 & 4 \\ 1 & 6 \\ 2 & y_{32} \end{bmatrix}$$

$$\mathbf{X} = \mathbf{Y} \text{ iff } x_{11} = 3, x_{22} = 6, x_{31} = 2, \text{ and } y_{32} = 0$$

Example 64

Square matrices

- Definitions

- A **square matrix** has the same number of rows and columns, i.e., $n \times n$
- In an $n \times n$ square matrix, elements $a_{11}, a_{22}, \dots, a_{nn}$ form the **main diagonal**
- In a **symmetric** $n \times n$ square matrix, elements $a_{ij} = a_{ji}$ for all $1 \leq i, j \leq n$
 - i.e., the upper triangular part is a reflection of the lower triangular part

lower triangular part \rightarrow

$\mathbf{A} = \begin{bmatrix} 1 & 5 & 7 \\ 5 & 0 & 2 \\ 7 & 2 & 6 \end{bmatrix}$

\leftarrow upper triangular part

\leftarrow main diagonal

Example 65

Mathematical arrays

- Definitions

- An **array** is an n -dimensional arrangement of data
- A **matrix** is a 2-dimensional array
- A **vector** is a 1-dimensional array

?

$$\mathbf{A} = [1 \quad 9 \quad 8 \quad 6]$$

Vector \mathbf{A} is 1×4
Element $a_3 = 8$

$$\mathbf{B} = \begin{bmatrix} 1 & 9 & 8 \\ 4 & 0 & 1 \\ 9 & 9 & 7 \end{bmatrix} \begin{bmatrix} 1 & 9 & 5 \\ 8 & 0 & 1 \\ 9 & 5 & 2 \end{bmatrix}$$

Array \mathbf{B} is $3 \times 3 \times 2$
Element $b_{132} = 5$

3D array, not two 2D arrays

Programming language arrays

Array data structures often available in programming languages, e.g., Java.

```
20     int array1[][] = { { 1, 2, 3 }, { 4, 5, 6 } };
21     int array2[][] = { { 1, 2 }, { 3 }, { 4, 5, 6 } };
22
23     ...
32
33     // loop through array's rows
34     for ( int row = 0; row < array.length; row++ ) {
35
36         // loop through columns of current row
37         for ( int column = 0;
38              column < array[ row ].length;
39              column++ )
40             outputArea.append( array[ row ][ column ] + " " );
41
42         outputArea.append( "\n" );
43     }
```

Matrix operations

- Introduction
 - Treat matrix, not elements, as object
 - Define operations on matrices
- Operations
 - Scalar multiplication
 - Matrix addition
 - Matrix subtraction
 - Matrix multiplication
- Special matrices
 - Zero matrix
 - Inverse matrix
 - Identity matrix

Scalar multiplication

To multiply a matrix by a constant (called a **scalar**), multiply each element of the matrix by the scalar.

$$\mathbf{A} = \begin{bmatrix} 1 & 4 & 5 \\ 6 & -3 & 2 \end{bmatrix}$$

scalar $r = 3$

$$r\mathbf{A} = \begin{bmatrix} 3 & 12 & 15 \\ 18 & -9 & 6 \end{bmatrix}$$

Example 66

Matrix addition

For addition both matrices must have same dimensions.

Given $n \times m$ matrices \mathbf{A} and \mathbf{B} ,

$\mathbf{C} = \mathbf{A} + \mathbf{B}$ is an $n \times m$ matrix with elements $c_{ij} = a_{ij} + b_{ij}$.

$$\mathbf{A} = \begin{bmatrix} 1 & 3 & 6 \\ 2 & 0 & 4 \\ -4 & 5 & 1 \end{bmatrix} \quad \mathbf{B} = \begin{bmatrix} 0 & -2 & 8 \\ 1 & 5 & 2 \\ 2 & 3 & 3 \end{bmatrix}$$

$$\mathbf{C} = \mathbf{A} + \mathbf{B} = \begin{bmatrix} 1 & 1 & 14 \\ 3 & 5 & 6 \\ -2 & 8 & 4 \end{bmatrix}$$

Example 67

Matrix operations examples

$$\mathbf{A} = \begin{bmatrix} 1 & 7 \\ -3 & 4 \\ 5 & 6 \end{bmatrix} \quad \mathbf{B} = \begin{bmatrix} 4 & 0 \\ 9 & 2 \\ -1 & 4 \end{bmatrix} \quad \text{scalar } r = 2$$

$$r\mathbf{A} + \mathbf{B} = \begin{bmatrix} 6 & 14 \\ 3 & 10 \\ 9 & 16 \end{bmatrix} \quad r\mathbf{A} + \mathbf{B} = (r\mathbf{A}) + \mathbf{B} \quad ?$$

$$r(\mathbf{A} + \mathbf{B}) = \begin{bmatrix} 10 & 14 \\ 12 & 12 \\ 8 & 20 \end{bmatrix}$$

Matrix subtraction

For subtraction both matrices must have same dimensions.

Given matrices $n \times m$ matrices **A** and **B**,

$$\mathbf{A} - \mathbf{B} = \mathbf{A} + (-1)\mathbf{B}.$$

$$\mathbf{A} = \begin{bmatrix} 1 & 3 & 6 \\ 2 & 0 & 4 \\ -4 & 5 & 1 \end{bmatrix} \quad \mathbf{B} = \begin{bmatrix} 0 & -2 & 8 \\ 1 & 5 & 2 \\ 2 & 3 & 3 \end{bmatrix}$$

$$\mathbf{A} - \mathbf{B} = \mathbf{A} + (-1)\mathbf{B} = \begin{bmatrix} 1 & 5 & -2 \\ 1 & -5 & 2 \\ -6 & 2 & -2 \end{bmatrix}$$

Zero matrix

- Definition
 - In a **zero matrix**, all elements are 0
 - Zero matrix denoted **0**

$$\mathbf{0} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Matrix addition identities

If \mathbf{A} and \mathbf{B} are $n \times m$ matrices and r and s are scalars, these matrix equations are true:

$\mathbf{0} + \mathbf{A} = \mathbf{A}$	identity
$\mathbf{A} + \mathbf{B} = \mathbf{B} + \mathbf{A}$	commutivity
$(\mathbf{A} + \mathbf{B}) + \mathbf{C} = \mathbf{A} + (\mathbf{B} + \mathbf{C})$	associativity
$r(s\mathbf{A}) = (rs)\mathbf{A}$	associativity
$r(\mathbf{A} + \mathbf{B}) = r\mathbf{A} + r\mathbf{B}$	distributivity
$(r + s)\mathbf{A} = r\mathbf{A} + s\mathbf{A}$	distributivity

To prove matrix identities, prove them for each element; e.g., to prove $\mathbf{A} + \mathbf{B} = \mathbf{B} + \mathbf{A}$, note that $a_{ij} + b_{ij} = b_{ij} + a_{ij}$ for each element in \mathbf{A} and \mathbf{B} .

Matrix multiplication

Matrix multiplication not as simple as other operations;
definition based on linear transformations.

To compute $\mathbf{A} \cdot \mathbf{B}$, number of columns of \mathbf{A}
must equal number of rows of \mathbf{B} ,
e.g., $\mathbf{A} \cdot \mathbf{B}$ can be found for $\mathbf{A} \ n \times m$ and $\mathbf{B} \ m \times p$.

Result $\mathbf{C} = \mathbf{A} \cdot \mathbf{B}$ is $n \times p$ matrix
with each element given by formula

$$c_{ij} = \sum_{k=1}^m a_{ik} \cdot b_{kj}$$

Matrix multiplication example

$$\mathbf{A} = \begin{bmatrix} 2 & 4 & 3 \\ 4 & -1 & 2 \end{bmatrix} \quad \mathbf{B} = \begin{bmatrix} 5 & 3 \\ 2 & 2 \\ 6 & 5 \end{bmatrix}$$

$$c_{11} = \sum_{k=1}^3 a_{1k} \cdot b_{k1} = a_{11} \cdot b_{11} + a_{12} \cdot b_{21} + a_{13} \cdot b_{31}$$

$$c_{11} = 2 \cdot 5 + 4 \cdot 2 + 3 \cdot 6 = 10 + 8 + 18 = 36$$

$$\mathbf{A} \cdot \mathbf{B} = \begin{bmatrix} 2 & 4 & 3 \\ 4 & -1 & 2 \end{bmatrix} \cdot \begin{bmatrix} 5 & 3 \\ 2 & 2 \\ 6 & 5 \end{bmatrix} = \begin{bmatrix} 36 & - \\ - & - \end{bmatrix}$$

Example 69

$$c_{12} = 2 \cdot 3 + 4 \cdot 2 + 3 \cdot 5 = 6 + 8 + 15 = 29$$

$$\mathbf{A} \cdot \mathbf{B} = \begin{bmatrix} 2 & 4 & 3 \\ 4 & -1 & 2 \end{bmatrix} \cdot \begin{bmatrix} 5 & 3 \\ 2 & 2 \\ 6 & 5 \end{bmatrix} = \begin{bmatrix} 36 & 29 \\ - & - \end{bmatrix}$$

$$c_{21} = 4 \cdot 5 + -1 \cdot 2 + 2 \cdot 6 = 20 + -2 + 12 = 30$$

$$\mathbf{A} \cdot \mathbf{B} = \begin{bmatrix} 2 & 4 & 3 \\ 4 & -1 & 2 \end{bmatrix} \cdot \begin{bmatrix} 5 & 3 \\ 2 & 2 \\ 6 & 5 \end{bmatrix} = \begin{bmatrix} 36 & 29 \\ 30 & - \end{bmatrix}$$

$$c_{22} = 4 \cdot 3 + -1 \cdot 2 + 2 \cdot 5 = 12 + -2 + 10 = 20$$

$$\mathbf{A} \cdot \mathbf{B} = \begin{bmatrix} 2 & 4 & 3 \\ 4 & -1 & 2 \end{bmatrix} \cdot \begin{bmatrix} 5 & 3 \\ 2 & 2 \\ 6 & 5 \end{bmatrix} = \begin{bmatrix} 36 & 29 \\ 30 & 20 \end{bmatrix}$$

Matrix multiplication algorithm

Algorithm based on definition of matrix multiplication

Algorithm MatrixMultiplication

// Computes $n \times p$ matrix $A \cdot B$ for $n \times m$ matrix A , $m \times p$ matrix B

// Stores result in C

for $i = 1$ to n **do**

for $j = 1$ to p **do**

$C[i, j] = 0$

for $k = 1$ to m **do**

$C[i, j] = C[i, j] + A[i, k] * B[k, j]$

endfor

endfor

endfor

write out product matrix C

Analysis of matrix multiplication algorithm

Basic operations: multiplications and additions,
one of each operation each time statement

$C[i, j] = C[i, j] + A[i, k] * B[k, j]$ is executed.

Statement within triply nested loop, executed npm times,
where n, p, m are matrix dimensions.

If **A** and **B** are $n \times n$ matrices, there are n^3 operations,
i.e., the algorithm is $\Theta(n^3)$.

Matrix multiplication examples

$$\mathbf{A} = \begin{bmatrix} 1 & 4 \\ 6 & -2 \end{bmatrix} \quad \mathbf{B} = \begin{bmatrix} 3 & 6 \\ 3 & 4 \end{bmatrix}$$

$$\mathbf{A} \cdot \mathbf{B} = \begin{bmatrix} 15 & 22 \\ 12 & 28 \end{bmatrix} \quad \mathbf{B} \cdot \mathbf{A} = \begin{bmatrix} 39 & 0 \\ 27 & 4 \end{bmatrix}$$

In general $\mathbf{A} \cdot \mathbf{B} \neq \mathbf{B} \cdot \mathbf{A}$,
unlike most more familiar multiplication operations.

Identity matrix

- Definition

- An $n \times n$ matrix with 1s on the main diagonal and 0s elsewhere is the **identity matrix**
- Identity matrix denoted **\mathbf{I}**

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

For any $n \times n$ matrix **\mathbf{A}** , **$\mathbf{I} \cdot \mathbf{A} = \mathbf{A} \cdot \mathbf{I} = \mathbf{A}$**

Inverse matrix

- Definition

- An $n \times n$ matrix \mathbf{A} is **invertible** if there exists $n \times n$ matrix \mathbf{B} such that $\mathbf{A} \cdot \mathbf{B} = \mathbf{B} \cdot \mathbf{A} = \mathbf{I}$
- Such a matrix \mathbf{B} is the **inverse** of matrix \mathbf{A} , denoted \mathbf{A}^{-1}

$$\mathbf{A} = \begin{bmatrix} -1 & 2 & -3 \\ 2 & 1 & 0 \\ 4 & -2 & 5 \end{bmatrix} \quad \mathbf{B} = \begin{bmatrix} -5 & 4 & -3 \\ 10 & -7 & 6 \\ 8 & -6 & 5 \end{bmatrix}$$

By the definition of matrix multiplication,
 $\mathbf{A} \cdot \mathbf{B} = \mathbf{B} \cdot \mathbf{A} = \mathbf{I}$, hence $\mathbf{B} = \mathbf{A}^{-1}$.

Example 71

Matrix multiplication identities

If **A**, **B**, and **C** are matrices of appropriate dimensions, and r and s are scalars, these matrix equations are true:

$$\mathbf{A} \cdot (\mathbf{B} \cdot \mathbf{C}) = (\mathbf{A} \cdot \mathbf{B}) \cdot \mathbf{C}$$

$$\mathbf{A} \cdot (\mathbf{B} + \mathbf{C}) = \mathbf{A} \cdot \mathbf{B} + \mathbf{A} \cdot \mathbf{C}$$

$$(\mathbf{A} + \mathbf{B}) \cdot \mathbf{C} = \mathbf{A} \cdot \mathbf{C} + \mathbf{B} \cdot \mathbf{C}$$

$$r\mathbf{A} \cdot s\mathbf{B} = rs(\mathbf{A} \cdot \mathbf{B})$$

$$\mathbf{A} \cdot \mathbf{0} = \mathbf{0} \cdot \mathbf{A} = \mathbf{0}$$

$$\mathbf{I} \cdot \mathbf{A} = \mathbf{A} \cdot \mathbf{I} = \mathbf{A}$$

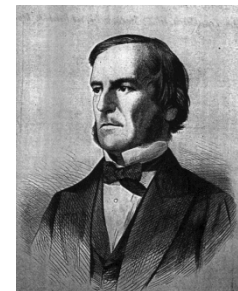
$$\mathbf{A} \cdot \mathbf{A}^{-1} = \mathbf{A}^{-1} \cdot \mathbf{A} = \mathbf{I}$$

Example 70

Boolean matrices

- Definition
 - **Boolean matrix**; matrix with only 0s and 1s as entries
- Applications
 - Graph reachability (Ch 6)
 - Boolean algebra and computer logic (Ch 7)
- Operations
 - Boolean multiplication and addition on elements
 - Boolean matrix multiplication

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



George Boole
1815 – 1864

Boolean multiplication and addition

Boolean addition and multiplication defined on elements of Boolean matrices, i.e., 0s and 1s, as follows:

Boolean multiplication: $x \wedge y = \min(x, y)$

Boolean addition: $x \vee y = \max(x, y)$

x	y	$x \wedge y$
1	1	1
1	0	0
0	1	0
0	0	0

aka Boolean and

x	y	$x \vee y$
1	1	1
1	0	1
0	1	1
0	0	0

aka Boolean or

Boolean matrix addition

For addition both matrices must have same dimensions.

Two types of boolean matrix addition;
the elements are combined using \wedge and \vee .

Given $n \times m$ boolean matrices \mathbf{A} and \mathbf{B} ,

$\mathbf{C} = \mathbf{A} \wedge \mathbf{B}$ is an $n \times m$ matrix with elements $c_{ij} = a_{ij} \wedge b_{ij}$.

$\mathbf{C} = \mathbf{A} \vee \mathbf{B}$ is an $n \times m$ matrix with elements $c_{ij} = a_{ij} \vee b_{ij}$.

$$\mathbf{A} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \mathbf{B} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\mathbf{C} = \mathbf{A} \wedge \mathbf{B} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \mathbf{C} = \mathbf{A} \vee \mathbf{B} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

Example 75

Boolean matrix multiplication

To compute $\mathbf{A} \times \mathbf{B}$, number of columns of \mathbf{A} must equal number of rows of \mathbf{B} ,
e.g., $\mathbf{A} \times \mathbf{B}$ can be found for $\mathbf{A} \ n \times m$ and $\mathbf{B} \ m \times p$.

Result $\mathbf{C} = \mathbf{A} \times \mathbf{B}$ is $n \times p$ boolean matrix with elements

$$c_{ij} = \bigvee_{k=1}^m (a_{ik} \wedge b_{kj})$$

Notational clarification

Boolean matrix multiplication	$\mathbf{A} \times \mathbf{B}$	\mathbf{A}, \mathbf{B} matrices
Cross product	$A \times B$	A, B sets
Matrix dimensions	$n \times m$	n, m integers

Boolean matrix multiplication example

$$\mathbf{A} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \mathbf{B} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\begin{aligned} c_{11} &= \bigvee_{k=1}^m (a_{1k} \wedge b_{k1}) = (a_{11} \wedge b_{11}) \vee (a_{12} \wedge b_{21}) \vee (a_{13} \wedge b_{31}) \\ &= (1 \wedge 1) \vee (1 \wedge 1) \vee (0 \wedge 0) = 1 \vee 1 \vee 0 = 1 \end{aligned}$$

$$\begin{aligned} c_{31} &= \bigvee_{k=1}^m (a_{3k} \wedge b_{k1}) = (a_{31} \wedge b_{11}) \vee (a_{32} \wedge b_{21}) \vee (a_{33} \wedge b_{31}) \\ &= (0 \wedge 1) \vee (0 \wedge 1) \vee (1 \wedge 0) = 0 \vee 0 \vee 0 = 0 \end{aligned}$$

$$\mathbf{A} \times \mathbf{B} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

Example 75

Regular vs boolean matrix multiplication

$$\mathbf{A} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \mathbf{B} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\mathbf{A} \times \mathbf{B} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

Boolean matrix multiplication

$$\mathbf{A} \cdot \mathbf{B} = \begin{bmatrix} 2 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

Regular matrix multiplication

In general $\mathbf{A} \times \mathbf{B} \neq \mathbf{A} \cdot \mathbf{B}$.

Section 5.7 homework assignment

See homework list for specific exercises.



End

