# COMP9020 Week 3
# Relations

- [RW] - Ch. 1, Ch. 3
- [LLM] - Section 4.4

# Relations and Functions

**Relations** are an abstraction used to capture the idea that the objects from certain domains (often the same domain for several objects) are *related*. These objects may

- influence one another (each other for binary relations; self(?) for unary)
- share some common properties
- correspond to each other precisely when some constraints are satisfied

**Functions** capture the idea of transforming *inputs* into *outputs*.

In general, functions and relations formalise the concept of interaction among objects from various domains; however, there must be a specified domain for each type of objects.

# Applications in Computer Science

- Relations are the building blocks of nearly all Computer Science structures
- Databases are collections of relations
- Any ordering is a relation
- Common data structures (e.g. graphs) are relations
- Functions/procedures/programs compute relations between their input and output

# Applications in Computer Science

Many binary relations (i.e. relationships between two entities) that appear in CS fall into two broad categories:

Equivalence relations (generalizing "equality"):

- Programs that exhibit the same behaviour
- Logically equivalent statements
- The `.equals()` method in Java

Partial orders (generalizing "less than or equal to"):

- Object inheritance
- Simulation
- Requirement specifications
- The `.compareTo()` method in Java

# Outline

- Definition and examples
- Defining relations
- Functions and composition
- Binary relations
- Equivalence relations, classes, and partitions
- Orderings

# Outline

- Definition and examples
- Defining relations
- Functions and composition
- Binary relations
- Equivalence relations, classes, and partitions
- Orderings

# Relations

## Definition

An **n-ary relation** is a subset of the cartesian product of $n$ sets.

$$R \subseteq S_1 \times S_2 \times \ldots \times S_n$$

To show tuples related by $R$ we write:

$$(x_1, x_2, \ldots, x_n) \in R \quad \text{or} \quad R(x_1, x_2, \ldots, x_n)$$

If $n = 2$ we have a **binary** relation $R \subseteq S \times T$ and to show pairs related by $R$ we write:

$$(x, y) \in R \quad \text{or} \quad R(x, y) \quad \text{or} \quad xRy$$

# Examples

## Examples

- Equality: $=$
- Inequality: $\leq$, $\geq$, $<$, $>$, $\neq$
- Divides relation: $|$
- Element of: $\in$
- Subset, superset: $\subseteq$, $\subset$, $\supseteq$, $\supset$
- Congruence modulo $n$: $m = p \pmod{n}$

# Database Examples

**Example (Course enrolments)**

$S$ = set of CSE students
($S$ can be a subset of the set of all students)
$C$ = set of CSE courses
(likewise)
$E$ = enrolments = $\{\ (s, c) : s \text{ takes } c\ \}$

$$E \subseteq S \times C$$

In practice, almost always there are various 'onto' (nonemptiness) and 1–1 (uniqueness) constraints on database relations.

**Example (Class schedule)**

$C$ = CSE courses
$T$ = starting time (hour & day)
$R$ = lecture rooms
$S$ = schedule =

$$\{\,(c,t,r) : c \text{ is at } t \text{ in } r\,\} \subseteq C \times T \times R$$

**Example (sport stats)**

$$R \subseteq \text{competitions} \times \text{results} \times \text{years} \times \text{athletes}$$

# Outline

- Definition and examples
- Defining relations
- Functions and composition
- Binary relations
- Equivalence relations, classes, and partitions
- Orderings

# Defining Relations

Just as with sets $R$ can be defined by

- explicit enumeration of interrelated $k$-tuples (ordered pairs in case of binary relations);
- properties that identify relevant tuples within the entire $S_1 \times S_2 \times \ldots \times S_k$;
- construction from other relations.

# Relation $R$ as Correspondence From $S$ to $T$

Given $R \subseteq S \times T$, $A \subseteq S$, and $B \subseteq T$.

- Relational image of $A$, $R(A)$:

$$R(A) \stackrel{\text{def}}{=} \{t \in T \ : \ (s, t) \in R \text{ for some } s \in A\}$$

- Converse relation $R^{\leftarrow} \subseteq T \times S$:

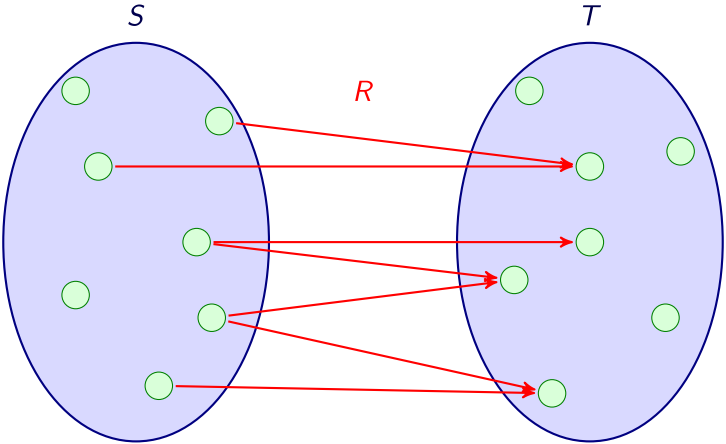
$$R^{\leftarrow} \stackrel{\text{def}}{=} \{(t, s) \in T \times S \ : \ (s, t) \in R\}$$

- Relational pre-image of $B$, $R^{\leftarrow}(B)$:

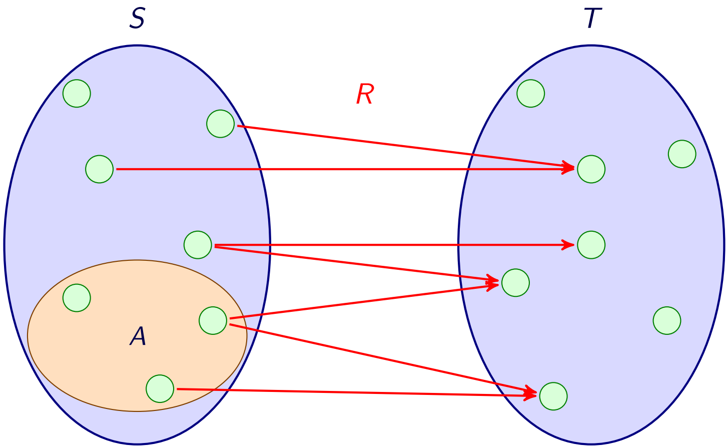
$$R^{\leftarrow}(B) \stackrel{\text{def}}{=} \{s \in S \ : \ (s, t) \in R \text{ for some } t \in B\}$$

Observe that $(R^{\leftarrow})^{\leftarrow} = R$.

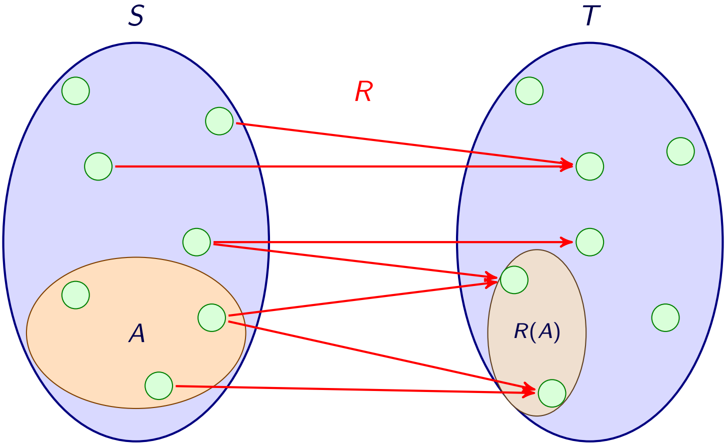
# Binary relation: Graphical representation



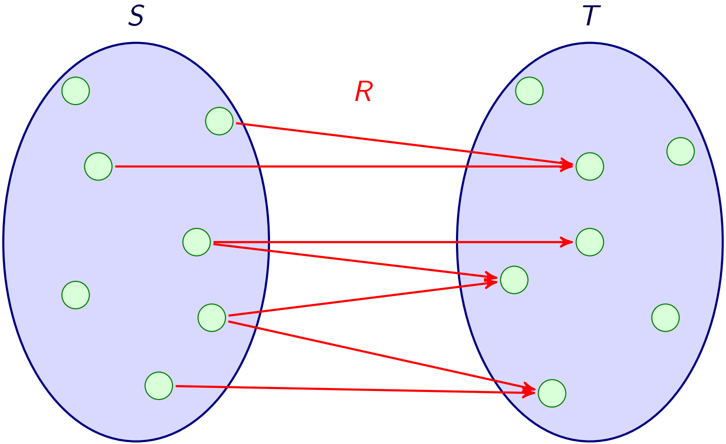
# Binary relation: Graphical representation



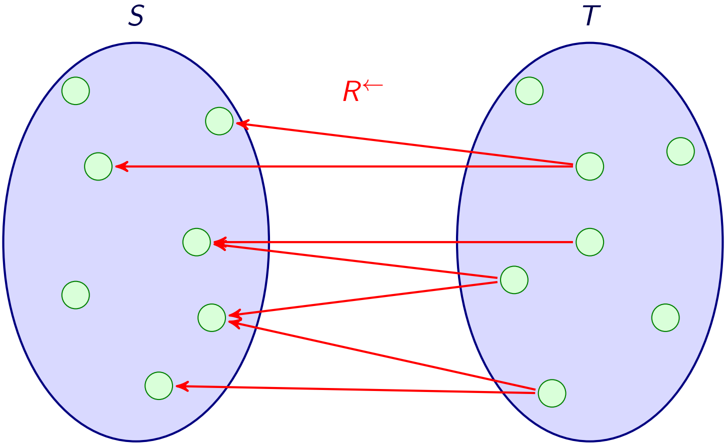
# Binary relation: Graphical representation



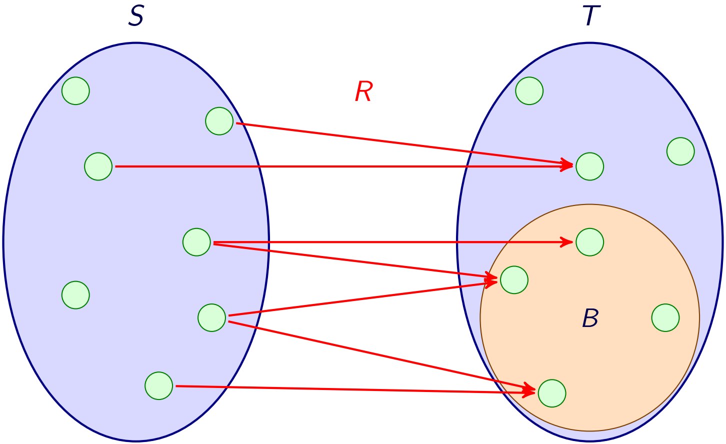
# Binary relation: Graphical representation



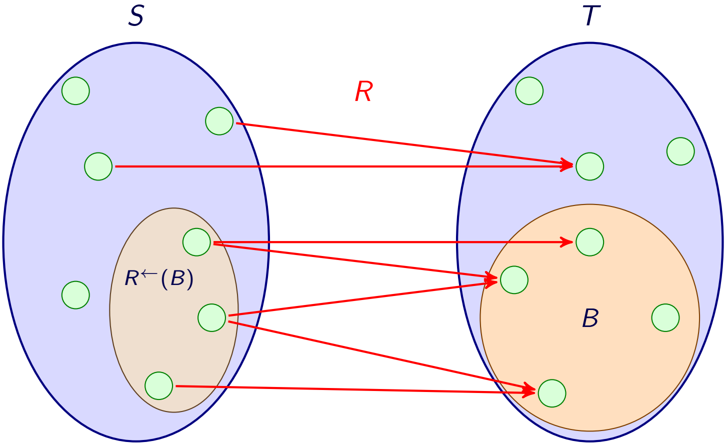
# Binary relation: Graphical representation



# Binary relation: Graphical representation



# Binary relation: Graphical representation



# Exercises

**Exercises**

Let $A = \{1,2\}$, $B = \{2,3\}$, $C = \{3,4\}$, $X = [1,4]$

- $\mid$ on $X$:
- $\in$ on $X \times \{A, B, C\}$:
- $\subseteq^{\leftarrow}$ on $\{A, B, C, X\}$:
- $<$ (2) (on $X$):

# Exercises

## Exercises

Let $A = \{1, 2\}$, $B = \{2, 3\}$, $C = \{3, 4\}$, $X = [1, 4]$

- $|$ on $X$: ?
- $\in$ on $X \times \{A, B, C\}$:
- $\subseteq^{\leftarrow}$ on $\{A, B, C, X\}$:
- $<$ (2) (on $X$):

# Exercises

**Exercises**

Let $A = \{1, 2\}$, $B = \{2, 3\}$, $C = \{3, 4\}$, $X = [1, 4]$

- $\mid$ on $X$: ?
- $\in$ on $X \times \{A, B, C\}$: ?
- $\subseteq^{\leftarrow}$ on $\{A, B, C, X\}$:
- $<$ (2) (on $X$):

# Exercises

**Exercises**

Let $A = \{1, 2\}$, $B = \{2, 3\}$, $C = \{3, 4\}$, $X = [1, 4]$

- $|$ on $X$:   ?
- $\in$ on $X \times \{A, B, C\}$:   ?
- $\subseteq^{\leftarrow}$ on $\{A, B, C, X\}$:   ?
- $<$ (2) (on $X$):

# Exercises

**Exercises**

Let $A = \{1, 2\}$, $B = \{2, 3\}$, $C = \{3, 4\}$, $X = [1, 4]$

- $\mid$ on $X$: ?
- $\in$ on $X \times \{A, B, C\}$: ?
- $\subseteq^{\leftarrow}$ on $\{A, B, C, X\}$: ?
- $<$ (2) (on $X$): ?

# Outline

- Definition and examples
- Defining relations
- Functions and composition
- Binary relations
- Equivalence relations, classes, and partitions
- Orderings

# Functions

**Definition**

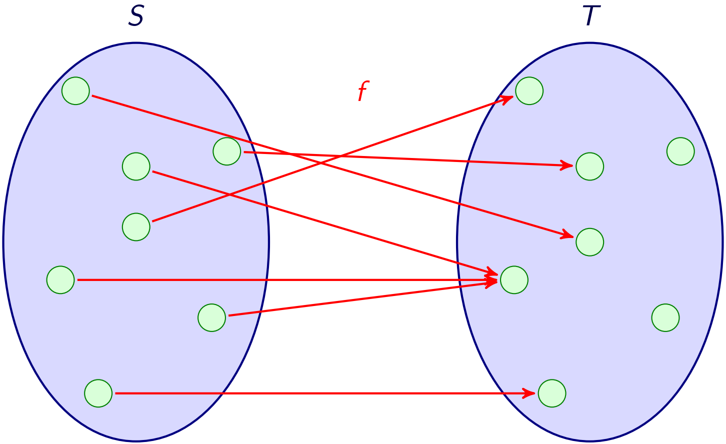
A **function**, $f : S \to T$, is a binary relation $f \subseteq S \times T$ such that for all $s \in S$ there is *exactly one* $t \in T$ such that $(s, t) \in f$.

We write $f(s)$ for the unique element related to $s$.

We write $T^S$ for the set of all functions from $S$ to $T$.

A **partial function** $f : S \nrightarrow T$ is a binary relation $f \subseteq S \times T$ such that for all $s \in S$ there is *at most one* $t \in T$ such that $(s, t) \in f$.
That is, it is a function $f : S' \longrightarrow T$ for $S' \subseteq S$

# Graphical representation



# Functions

$f : S \longrightarrow T$ describes pairing of the sets: it means that $f$ assigns to every element $s \in S$ a unique element $t \in T$. To emphasise where a specific element is sent, we can write $f : x \mapsto y$, which means the same as $f(x) = y$

| | | Symbol | |
|---|---|---|---|
| $S$ | **domain** of $f$ | $\mathrm{Dom}(f)$ | (inputs) |
| $T$ | **co-domain** of $f$ | $\mathrm{Codom}(f)$ | (*possible* outputs) |
| $f(S)$ | **image** of $f$ | $\mathrm{Im}(f)$ | (*actual* outputs) |
| $= \{ f(x) : x \in \mathrm{Dom}(f) \}$ | | | |

**Important!**

The domain and co-domain are critical aspects of a function's definition.

$$f : \mathbb{N} \to \mathbb{Z} \quad \text{given by} \quad f(x) \mapsto x^2$$

and

$$g : \mathbb{N} \to \mathbb{N} \quad \text{given by} \quad g(x) \mapsto x^2$$

are different functions even though they have the same behaviour!

# Composition of Functions

Composition of functions is described as

$$g \circ f : x \mapsto g(f(x)), \quad \text{requiring } \operatorname{Im}(f) \subseteq \operatorname{Dom}(g)$$

Composition is associative

$$h \circ (g \circ f) = (h \circ g) \circ f, \quad \text{can write } h \circ g \circ f$$

# Composition of Functions

If a function maps a set into itself, i.e. when $\mathrm{Dom}(f) = \mathrm{Codom}(f)$ (and thus $\mathrm{Im}(f) \subseteq \mathrm{Dom}(f)$), the function can be composed with itself — **iterated**

$$f \circ f, f \circ f \circ f, \ldots, \quad \text{also written } f^2, f^3, \ldots$$

**Identity** function on $S$

$$\mathrm{Id}_S(x) = x, x \in S; \mathrm{Dom}(\mathrm{Id}_S) = \mathrm{Codom}(\mathrm{Id}_S) = \mathrm{Im}(\mathrm{Id}_S) = S$$

For $g : S \longrightarrow T \quad g \circ \mathrm{Id}_S = g, \; \mathrm{Id}_T \circ g = g$

# Extension: Composition of Binary Relations

If $R_1 \subseteq S \times T$ and $R_2 \subseteq T \times U$ then the composition of $R_1$ and $R_2$ is the relation:

$$\begin{aligned} R_1; R_2 := \{(a, c) : \quad & \text{there is a } b \in T \text{ such that} \\ & (a, b) \in R_1 \text{ and } (b, c) \in R_2\}. \end{aligned}$$

Note that if $f : S \to T$ and $g : T \to S$ are functions then $f; g = g \circ f$.

# Exercises

## Exercises

Let $f, g : \mathbb{Z} \to \mathbb{Z}$ be given by $f(n) = n^2 + 3$ and $g(n) = 5n - 11$. What is:

- $f \circ g(n) =$
- $g \circ f(n) =$
- $g^2(n) =$

# Exercises

## Exercises

Let $f, g : \mathbb{Z} \to \mathbb{Z}$ be given by $f(n) = n^2 + 3$ and $g(n) = 5n - 11$. What is:

- $f \circ g(n) = ?$
- $g \circ f(n) = ?$
- $g^2(n) = ?$

# Outline

# Binary relations

A **binary relation between** $S$ **and** $T$ is a subset of $S \times T$: i.e. a set of ordered pairs.
Also: over $S$ and $T$; from $S$ to $T$; on $S$ (if $S = T$).

**Example (Special (Trivial) Relations)**

**Identity** (diagonal, equality) $I = \{ (x, x) : x \in S \}$

**Empty** $\emptyset$

**Universal** $U = S \times S$

# Defining binary relations: Set-based definitions

Defining a relation $R \subseteq S \times T$:

- Explicitly listing tuples: e.g. $\{(1,1),(2,3),(3,2)\}$
- Set comprehension: $\{(x,y) \in [1,3] \times [1,3] : 5|xy-1\}$
- Construction from other relations: $\{(1,1)\} \cup \{(2,3)\} \cup \{(2,3)\}^{\leftarrow}$

# Defining binary relations: Matrix representation

Defining a relation $R \subseteq S \times T$:

Rows enumerated by elements of $S$, columns by elements of $T$:

### Examples

- The relation $\{(1,1),(2,3),(3,2)\} \subseteq [1,3] \times [1,3]$:

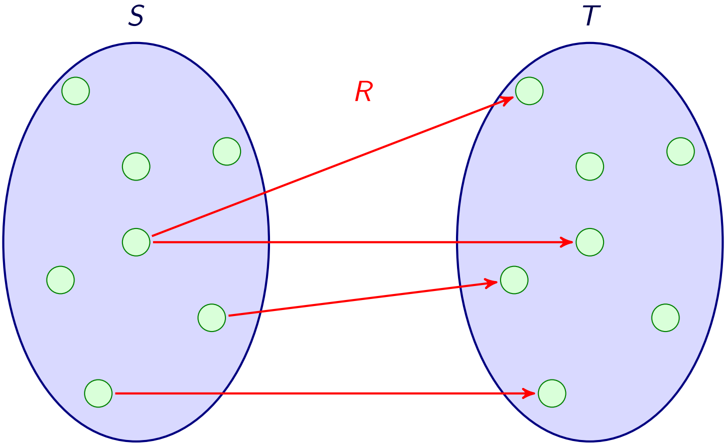
$$\begin{bmatrix} \bullet & \circ & \circ \\ \circ & \circ & \bullet \\ \circ & \bullet & \circ \end{bmatrix}$$

- The relation $\{(1,1),(1,2),(1,3),(1,4),(2,2),(3,2)\} \subseteq [1,3] \times [1,4]$:

$$\begin{bmatrix} \bullet & \bullet & \bullet & \bullet \\ \circ & \bullet & \circ & \circ \\ \circ & \bullet & \circ & \circ \end{bmatrix}$$

## Defining binary relations: Graphical representation

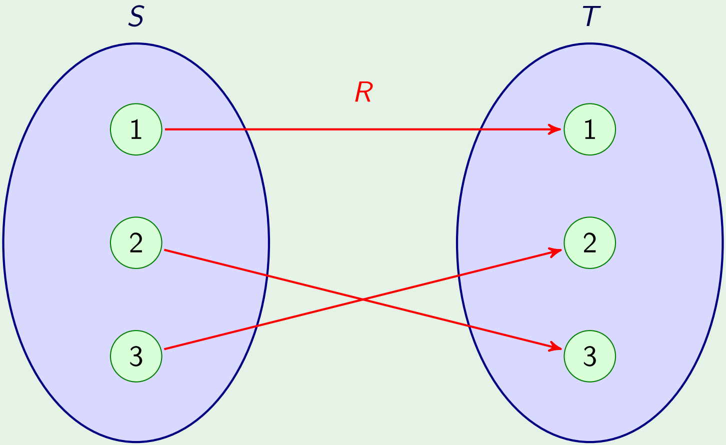
Defining a relation $R \subseteq S \times T$:



# Defining binary relations: Graphical representation

**Example**

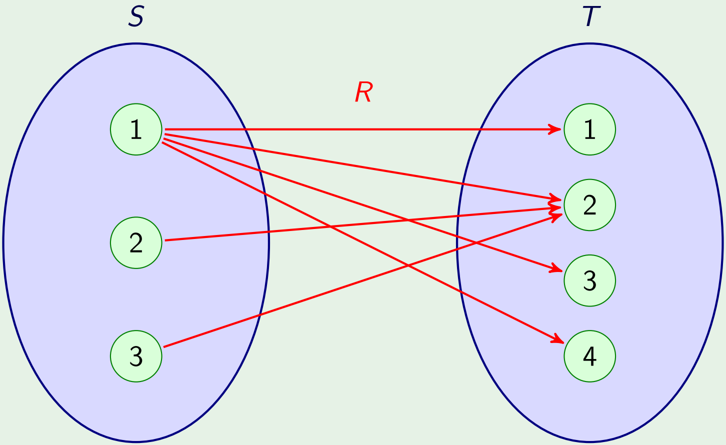
$R = \{(1,1),(2,3),(3,2)\} \subseteq [1,3] \times [1,3]$:



# Defining binary relations: Graphical representation

**Example**

$\{(1,1),(1,2),(1,3),(1,4),(2,2),(3,2)\} \subseteq [1,3] \times [1,4]$:



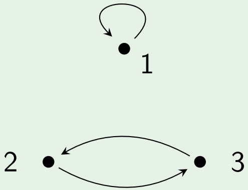
# Defining binary relations: Graph representation

If $S = T$ we can define $R \subseteq S \times S$ as a **directed graph** (week 5).

- Nodes: Elements of $S$
- Edges: Elements of $R$

**Example**

$R = \{(1,1),(2,3),(3,2)\} \subseteq [1,3] \times [1,3]$:



# Outline

# Properties of Binary Relations $R \subseteq S \times S$

## Definition

| | | |
|---|---|---|
| (R) | reflexive | For all $x \in S$: $(x, x) \in R$ |
| (AR) | antireflexive | For all $x \in S$: $(x, x) \notin R$ |
| (S) | symmetric | For all $x, y \in S$: If $(x, y) \in R$ then $(y, x) \in R$ |
| (AS) | antisymmetric | For all $x, y \in S$: If $(x, y)$ and $(y, x) \in R$ then $x = y$ |
| (T) | transitive | For all $x, y, z \in S$: If $(x, y)$ and $(y, z) \in R$ then $(x, z) \in R$ |

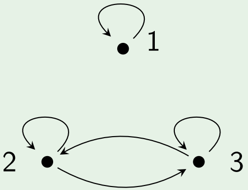
## NB

- *Properties have to hold for all elements*
- *(S), (AS), (T) are conditional statements – they will hold if there is nothing which satisfies the 'if' part*

# Relation properties: Examples

## Examples

**(R)** Reflexivity: $(x, x) \in R$ for all $x$



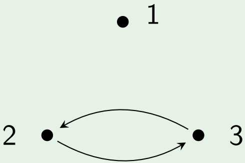

$$\begin{bmatrix} \bullet & \circ & \circ \\ \circ & \bullet & \bullet \\ \circ & \bullet & \bullet \end{bmatrix}$$

# Relation properties: Examples

## Examples

**(R)** Reflexivity: $(x, x) \in R$ for all $x$

**(AR)** Antireflexivity: $(x, x) \notin R$ for all $x$




$$\begin{bmatrix} \circ & \circ & \circ \\ \circ & \circ & \bullet \\ \circ & \bullet & \circ \end{bmatrix}$$

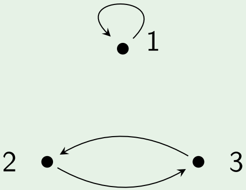
# Relation properties: Examples

## Examples

**(R)** Reflexivity: $(x, x) \in R$ for all $x$

**(AR)** Antireflexivity: $(x, x) \notin R$ for all $x$

**(S)** Symmetry: If $(x, y) \in R$ then $(y, x) \in R$ for all $x$, $y$




$$\begin{bmatrix} \bullet & \circ & \circ \\ \circ & \circ & \bullet \\ \circ & \bullet & \circ \end{bmatrix}$$

# Relation properties: Examples

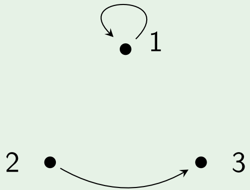
## Examples

**(R)** Reflexivity: $(x, x) \in R$ for all $x$

**(AR)** Antireflexivity: $(x, x) \notin R$ for all $x$

**(S)** Symmetry: If $(x, y) \in R$ then $(y, x) \in R$ for all $x$, $y$

**(AS)** Antisymmetry: $(x, y) \in R$ and $(y, x) \in R$ implies $x = y$ for all $x$, $y$

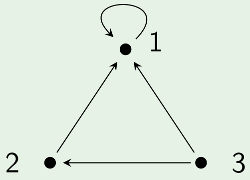



$$\begin{bmatrix} \bullet & \circ & \circ \\ \circ & \circ & \bullet \\ \circ & \circ & \circ \end{bmatrix}$$

# Relation properties: Examples

## Examples

- **(R)** Reflexivity: $(x, x) \in R$ for all $x$
- **(AR)** Antireflexivity: $(x, x) \notin R$ for all $x$
- **(S)** Symmetry: If $(x, y) \in R$ then $(y, x) \in R$ for all $x$, $y$
- **(AS)** Antisymmetry: $(x, y) \in R$ and $(y, x) \in R$ implies $x = y$ for all $x$, $y$
- **(T)** Transitivity: $(x, y) \in R$ and $(y, z) \in R$ implies $(x, z) \in R$ for all $x$, $y$, $z$.




$$\begin{bmatrix} \bullet & \circ & \circ \\ \bullet & \circ & \circ \\ \bullet & \bullet & \circ \end{bmatrix}$$

# Interaction of Properties

A relation *can* be both symmetric and antisymmetric. Namely, when $R$ consists only of some pairs $(x, x), x \in S$.
A relation *cannot* be simultaneously reflexive and antireflexive (unless $S = \emptyset$).

**NB**

$$\left.\begin{array}{r} \textit{nonreflexive} \\ \textit{nonsymmetric} \end{array}\right\} \textit{ is not the same as } \left\{\begin{array}{l} \textit{antireflexive/irreflexive} \\ \textit{antisymmetric} \end{array}\right.$$

# Exercises

## Exercises

$\boxed{\text{RW: 3.1.1}}$ The following relations are on $S = \{1, 2, 3\}$. Which of the properties (R), (AR), (S), (AS), (T) does each satisfy?

(a) $(m, n) \in R$ if $m + n = 3$?

(e) $(m, n) \in R$ if $\max\{m, n\} = 3$?

# Exercises

## Exercises

$\boxed{\text{RW: 3.1.1}}$ The following relations are on $S = \{1, 2, 3\}$. Which of the properties (R), (AR), (S), (AS), (T) does each satisfy?

(a) $(m, n) \in R$ if $m + n = 3$? ?

(e) $(m, n) \in R$ if $\max\{m, n\} = 3$? ?

# Exercises

### Exercises

$\boxed{\text{RW: 3.1.10}}$ Give examples of relations with specified properties.

(a) (AS), (T), not (R)

(b) (S), not (R), not (T)

# Exercises

## Exercises

$\boxed{\text{RW: 3.1.10}}$ Give examples of relations with specified properties.

(a) (AS), (T), not (R)

?

(b) (S), not (R), not (T)

?

# Exercises

## Exercises

$\boxed{\text{RW: 3.6.10 (supp)}}$

$R$ is a relation on $\mathbb{N} \times \mathbb{N}$, i.e. it is a subset of $\mathbb{N}^2 \times \mathbb{N}^2$
$(m, n)\, R\, (p, q)$ if $m = p \pmod 3$ or $n = q \pmod 5$.

(a) Is $R$ reflexive?

(b) Is $R$ symmetric?

(c) Is $R$ transitive?

# Exercises

## Exercises

$\boxed{\text{RW: 3.6.10 (supp)}}$

$R$ is a relation on $\mathbb{N} \times \mathbb{N}$, i.e. it is a subset of $\mathbb{N}^2 \times \mathbb{N}^2$
$(m, n)\, R\, (p, q)$ if $m = p \pmod 3$ or $n = q \pmod 5$.

(a) Is $R$ reflexive? ?

(b) Is $R$ symmetric? ?

(c) Is $R$ transitive? ?

# Exercises

## Exercises

Complete the following table of common relations (over $\mathbb{Z}$) and their properties:

| | $(R)$ | $(AR)$ | $(S)$ | $(AS)$ | $(T)$ |
|---|---|---|---|---|---|
| $=$ | | | | | |
| $\leq$ | | | | | |
| $<$ | | | | | |
| $\emptyset$ | | | | | |
| $\mathcal{U} = \mathbb{Z} \times \mathbb{Z}$ | | | | | |
| $\mid$ | | | | | |
| $= \pmod 3$ | | | | | |

## Exercises

Complete the following table of common relations (over $\mathbb{Z}$) and their properties:

| | $(R)$ | $(AR)$ | $(S)$ | $(AS)$ | $(T)$ |
|---|---|---|---|---|---|
| $=$ | ? | | | | |
| $\leq$ | | | | | |
| $<$ | | | | | |
| $\emptyset$ | | | | | |
| $\mathcal{U} = \mathbb{Z} \times \mathbb{Z}$ | | | | | |
| $\mid$ | | | | | |
| $= \pmod 3$ | | | | | |

# Exercises

## Exercises

Complete the following table of common relations (over $\mathbb{Z}$) and their properties:

| | $(R)$ | $(AR)$ | $(S)$ | $(AS)$ | $(T)$ |
|---|---|---|---|---|---|
| $=$ | ? | | | | |
| $\leq$ | ? | | | | |
| $<$ | | | | | |
| $\emptyset$ | | | | | |
| $\mathcal{U} = \mathbb{Z} \times \mathbb{Z}$ | | | | | |
| $\mid$ | | | | | |
| $\equiv \pmod 3$ | | | | | |

# Exercises

## Exercises

Complete the following table of common relations (over $\mathbb{Z}$) and their properties:

| | $(R)$ | $(AR)$ | $(S)$ | $(AS)$ | $(T)$ |
|---|---|---|---|---|---|
| $=$ | ? | | | | |
| $\leq$ | ? | | | | |
| $<$ | ? | | | | |
| $\emptyset$ | | | | | |
| $\mathcal{U} = \mathbb{Z} \times \mathbb{Z}$ | | | | | |
| $\mid$ | | | | | |
| $\equiv \pmod 3$ | | | | | |

# Exercises

## Exercises

Complete the following table of common relations (over $\mathbb{Z}$) and their properties:

| | $(R)$ | $(AR)$ | $(S)$ | $(AS)$ | $(T)$ |
|---|---|---|---|---|---|
| $=$ | ? | | | | |
| $\leq$ | ? | | | | |
| $<$ | ? | | | | |
| $\emptyset$ | ? | | | | |
| $\mathcal{U} = \mathbb{Z} \times \mathbb{Z}$ | | | | | |
| $\mid$ | | | | | |
| $= \pmod 3$ | | | | | |

# Exercises

## Exercises

Complete the following table of common relations (over $\mathbb{Z}$) and their properties:

| | $(R)$ | $(AR)$ | $(S)$ | $(AS)$ | $(T)$ |
|---|---|---|---|---|---|
| $=$ | ? | | | | |
| $\leq$ | ? | | | | |
| $<$ | ? | | | | |
| $\emptyset$ | ? | | | | |
| $\mathcal{U} = \mathbb{Z} \times \mathbb{Z}$ | ? | | | | |
| $\mid$ | | | | | |
| $= \pmod{3}$ | | | | | |

# Exercises

## Exercises

Complete the following table of common relations (over $\mathbb{Z}$) and their properties:

| | $(R)$ | $(AR)$ | $(S)$ | $(AS)$ | $(T)$ |
|---|---|---|---|---|---|
| $=$ | ? | | | | |
| $\leq$ | ? | | | | |
| $<$ | ? | | | | |
| $\emptyset$ | ? | | | | |
| $\mathcal{U} = \mathbb{Z} \times \mathbb{Z}$ | ? | | | | |
| $\mid$ | ? | | | | |
| $= \pmod{3}$ | | | | | |

# Exercises

## Exercises

Complete the following table of common relations (over $\mathbb{Z}$) and their properties:

| | $(R)$ | $(AR)$ | $(S)$ | $(AS)$ | $(T)$ |
|---|---|---|---|---|---|
| $=$ | ? | | | | |
| $\leq$ | ? | | | | |
| $<$ | ? | | | | |
| $\emptyset$ | ? | | | | |
| $\mathcal{U} = \mathbb{Z} \times \mathbb{Z}$ | ? | | | | |
| $\mid$ | ? | | | | |
| $\equiv \pmod 3$ | ? | | | | |

# Outline

- Definition and examples
- Defining relations
- Functions and composition
- Binary relations
- Equivalence relations, classes, and partitions
- Orderings

# Equivalence relations

Equivalence relations capture a general notion of "equality". They are relations which are:

- Reflexive (R): Every object should be "equal" to itself
- Symmetric (S): If $x$ is "equal" to $y$, then $y$ should be "equal" to $x$
- Transitive (T): If $x$ is "equal" to $y$ and $y$ is "equal" to $z$, then $x$ should be "equal" to $z$.

# Equivalence relations

Equivalence relations capture a general notion of "equality". They are relations which are:

- Reflexive (R): Every object should be "equal" to itself
- Symmetric (S): If $x$ is "equal" to $y$, then $y$ should be "equal" to $x$
- Transitive (T): If $x$ is "equal" to $y$ and $y$ is "equal" to $z$, then $x$ should be "equal" to $z$.

**Definition**

A binary relation $R \subseteq S \times S$ is *equivalence relation* if it satisfies (R), (S), (T).

**Example**

Partition of $\mathbb{Z}$ into classes of numbers with the same remainder on division by $p$; it is particularly important for $p$ prime

$$\mathbb{Z}(p) = \mathbb{Z}_p = \{0, 1, \ldots, p - 1\}$$

One can define all four arithmetic operations (with the usual properties) on $\mathbb{Z}_p$ for a prime $p$; division has to be restricted when $p$ is not prime.

**NB**

$(\mathbb{Z}_p, +, \cdot, 0, 1)$ *are fundamental algebraic structures known as* **rings**. *These structures are very important in coding theory and cryptography.*

# Equivalence Classes and Partitions

Suppose $R \subseteq S \times S$ is an equivalence relation
The **equivalence class** $[s]$ (w.r.t. $R$) of an element $s \in S$ is

$$[s] = \{t : t \in S \text{ and } sRt\}$$

**Fact**

*$s\,R\,t$ if and only if $[s] = [t]$.*

# Equivalence classes: Proof example

**Proof**

Suppose $[s] = [t]$. Recall $[s] = \{x \in S : (s, x) \in R\}$. We will show that $(s, t) \in R$.

Because $R$ is reflexive, $(t, t) \in R$.

Therefore $t \in [t]$.

Because $[t] = [s]$, it follows that $t \in [s]$.

But then $(s, t) \in R$ by the definition of $[s]$.

# Equivalence classes: Proof example

**Proof**

Now suppose $(s, t) \in R$. We will show $[s] = [t]$ by showing $[s] \subseteq [t]$ and $[t] \subseteq [s]$.

Take any $x \in [s]$.

By the definition of $[s]$, $(s, x) \in R$.

Since $R$ is symmetric $(x, s) \in R$.

Since $R$ is transitive and $(s, t) \in R$ we have that $(x, t) \in R$.

Since $R$ is symmetric $(t, x) \in R$.

Therefore, $x \in [t]$.

Therefore $[s] \subseteq [t]$.

# Equivalence classes: Proof example

**Proof**

Now suppose $(s, t) \in R$. We will show $[s] = [t]$ by showing $[s] \subseteq [t]$ and $[t] \subseteq [s]$.

Take any $x \in [t]$.

By the definition of $[t]$, $(t, x) \in R$.

Since $R$ is transitive and $(s, t) \in R$ we have that $(s, x) \in R$.

Therefore $x \in [s]$.

Therefore $[t] \subseteq [s]$. $\square$

# Partitions

## Definition

A **partition** of a set $S$ is a collection of sets $S_1, \ldots, S_k$ such that

- $S_i$ and $S_j$ are disjoint (for $i \neq j$)
- $S = S_1 \cup S_2 \cup \cdots \cup S_k = \bigcup_{i=1}^{k} S_i$

The collection of all equivalence classes $\{[s] : s \in S\}$ forms a partition of $S$

In the opposite direction, a partition of a set defines the equivalence relation on that set. If $S = S_1 \cup \cdots \cup S_k$, then we can define $\sim \subseteq S \times S$ as:

$$s \sim t \text{ exactly when } s \text{ and } t \text{ belong to the same } S_i.$$

# Exercises

**Exercises**

$\boxed{\text{RW: 3.6.6 (supp)}}$

(d) Show that $m \sim n$ iff $m^2 = n^2 \pmod 5$ is an equivalence on $S = \{1, \ldots, 7\}$.

Find all the equivalence classes.

# Exercises

## Exercises

$\boxed{\text{RW: 3.6.6 (supp)}}$

(d) Show that $m \sim n$ iff $m^2 = n^2 \pmod 5$ is an equivalence on $S = \{1, \dots, 7\}$.

?

Find all the equivalence classes.

?

# Outline

- Definition and examples
- Defining relations
- Functions and composition
- Binary relations
- Equivalence relations, classes, and partitions
- Orderings

# Partial Order

A **partial order** $\preceq$ on $S$ satisfies (R), (AS), (T).
We call $(S, \preceq)$ a **poset** — partially ordered set

### Examples

Posets:

- $(\mathbb{Z}, \leq)$
- $(\mathrm{Pow}(X), \subseteq)$ for some set $X$
- $(\mathbb{N}, |)$

Not posets:

- $(\mathbb{Z}, <)$
- $(\mathbb{Z}, |)$

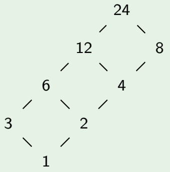
# Hasse diagram

Every finite poset $(S, \preceq)$ can be represented with a **Hasse diagram**:

- Nodes are elements of $S$
- An edge is drawn *upward* from $x$ to $y$ if $x \prec y$ and there is no $z$ such that $x \prec z \prec y$

## Example

Hasse diagram for positive divisors of 24 ordered by $|$:



# Ordering Concepts

## Definition

Let $(S, \preceq)$ be a poset.

- **Minimal** element: $x$ such that there is no $y$ with $y \preceq x$
- **Maximal** element: $x$ such that there is no $y$ with $x \preceq y$
- **Minimum (least)** element: $x$ such that $x \preceq y$ for all $y \in S$
- **Maximum (greatest)** element: $x$ such that $y \preceq x$ for all $y \in S$

## NB

- *There may be multiple minimal/maximal elements.*
- *Minimum/maximum elements are the unique minimal/maximal elements if they exist.*
- *Minimal/maximal elements always exist in finite posets, but not necessarily in infinite posets.*

# Examples

## Examples

- $\text{Pow}(\{a, b, c\})$ with the order $\subseteq$
  $\emptyset$ is minimum; $\{a, b, c\}$ is maximum
- $\text{Pow}(\{a, b, c\}) \setminus \{\{a, b, c\}\}$ (proper subsets of $\{a, b, c\}$)
  Each two-element subset $\{a, b\}, \{a, c\}, \{b, c\}$ is maximal.
    - But there is no maximum

# Ordering Concepts

## Definition

Let $(S, \preceq)$ be a poset.

- $x$ is an **upper bound** for $A$ if $a \preceq x$ for all $a \in A$
- $x$ is a **lower bound** for $A$ if $x \preceq a$ for all $a \in A$
- The **set of upper bounds** for $A$ is defined as $\mathrm{ub}(A) = \{x : a \preceq x \text{ for all } a \in A\}$
- The **set of lower bounds** for $A$ is defined as $\mathrm{lb}(A) = \{x : x \preceq a \text{ for all } a \in A\}$
- The **least upper bound** of $A$, $\mathrm{lub}(A)$, is the minimum of $\mathrm{ub}(A)$ (if it exists)
- The **greatest lower bound** of $A$, $\mathrm{glb}(A)$ is the maximum of $\mathrm{lb}(A)$ (if it exists)

# glb and lub

To show $x$ is $\mathrm{glb}(A)$ you need to show:

- $x$ is a lower bound: $x \preceq a$ for all $a \in A$.
- $x$ is the greatest of all lower bounds: If $y \preceq a$ for all $a \in A$ then $y \preceq x$.

**Example**

$\mathrm{Pow}(X)$ ordered by $\subseteq$.

- $\mathrm{glb}(A, B) = A \cap B$
- $\mathrm{lub}(A, B) = A \cup B$

# Ordering Concepts

**Definition**

Let $(S, \preceq)$ be a poset.

- $(S, \preceq)$ is a **lattice** if $\text{lub}(x, y)$ and $\text{glb}(x, y)$ exist for every pair of elements $x, y \in S$.
- $(S, \preceq)$ is a **complete lattice** if $\text{lub}(A)$ and $\text{glb}(A)$ exist for every subset $A \subseteq S$.

**NB**

*A finite lattice is always a complete lattice.*

# Examples

## Examples

- $\{1, 2, 3, 4, 6, 8, 12, 24\}$ partially ordered by divisibility is a lattice
  - e.g. $\text{lub}(\{4, 6\}) = 12$; $\text{glb}(\{4, 6\}) = 2$
- $\{1, 2, 3\}$ partially ordered by divisibility is not a lattice
  - $\{2, 3\}$ has no lub
- $\{2, 3, 6\}$ partially ordered by divisibility
  - $\{2, 3\}$ has no glb
- $\{1, 2, 3, 12, 18, 36\}$ partially ordered by divisibility
  - $\{2, 3\}$ has no lub ($12, 18$ are minimal upper bounds)

## NB

*An infinite lattice need not have a lub (or no glb) for an arbitrary infinite subset of its elements, in particular no such bound may exist for* **all** *its elements.*

## Examples

- $(\mathbb{Z}, \leq)$: neither $\mathsf{lub}(\mathbb{Z})$ nor $\mathsf{glb}(\mathbb{Z})$ exist
- $(\mathcal{F}(\mathbb{N}), \subseteq)$ [all finite subsets of $\mathbb{N}$]: lub exists for pairs of elements but not generally for (infinite) sets of elements. glb exists for any set of elements: intersection of a set of finite sets is finite.
- $(\mathcal{I}(\mathbb{N}), \subseteq)$ [all infinite subsets of $\mathbb{N}$]: glb does not exist for some pairs of elements (e.g. odds and evens). lub exists for any set of elements: union of a set of infinte sets is always infinte.

# Exercises

## Exercises

$\boxed{\text{RW: 11.1.5}}$ Consider poset $(\mathbb{R}, \leq)$

(a) Is this a lattice?

(b) Give an example of a non-empty subset of $\mathbb{R}$ that has no upper bound.

(c) Find $\text{lub}(\{ x \in \mathbb{R} : x < 73 \})$

(d) Find $\text{lub}(\{ x \in \mathbb{R} : x \leq 73 \})$

(e) Find $\text{lub}(\{ x : x^2 < 73 \})$

(f) Find $\text{glb}(\{ x : x^2 < 73 \})$

# Exercises

## Exercises

$\boxed{\text{RW: 11.1.5}}$ Consider poset $(\mathbb{R}, \leq)$

(a) Is this a lattice? ?

(b) Give an example of a non-empty ?
subset of $\mathbb{R}$ that has no upper bound. ?

(c) Find $\mathrm{lub}(\{ x \in \mathbb{R} : x < 73 \})$ ?

(d) Find $\mathrm{lub}(\{ x \in \mathbb{R} : x \leq 73 \})$ ?

(e) Find $\mathrm{lub}(\{ x : x^2 < 73 \})$ ?

(f) Find $\mathrm{glb}(\{ x : x^2 < 73 \})$ ?

# Total orders

## Definition

A **total order** is a partial order that also satisfies:

(L) *Linearity* (any two elements are comparable):

$$\text{For all } x, y \text{ either: } x \leq y \text{ or } y \leq x \text{ (or both if } x = y)$$

## NB

*On a finite set all total orders are "isomorphic"*
*On an infinite set there is quite a variety of possibilities.*

# Examples

## Examples

- $\mathbb{Z}$ with $\leq$:
  (no minimum/maximum element)
- $\mathbb{Z}$ with $\{(x, y) : x < 0 \leq y \text{ or } |x| \leq |y|\}$:
  (no maximum element, minimum element is -1)
- $\mathbb{Z}$ with $\{(x, y) : x < 0 \leq y, \text{ or } x \geq y \text{ and } xy \geq 0\}$:
  (minimum element -1, maximum element 0)

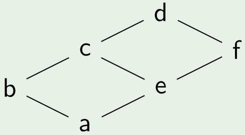
# Ordering of a Poset — Topological Sort

## Definition

For a poset $(S, \preceq)$ any total order $\leq$ that is consistent with $\preceq$ (if $a \preceq b$ then $a \leq b$) is called a **topological sort**.

## Example

Consider




The following all are topological sorts:
$a \leq b \leq e \leq c \leq f \leq d$
$a \leq e \leq b \leq f \leq c \leq d$
$a \leq e \leq f \leq b \leq c \leq d$

# Well-Ordered Sets

**Definition**

A *well-ordered set* is a poset where every subset has a least element.

**NB**

*The greatest element is not required.*

**Examples**

- $\mathbb{N} = \{0, 1, \ldots\}$
- $\mathbb{N}_1 \dot\cup \mathbb{N}_2 \dot\cup \mathbb{N}_3 \dot\cup \ldots$, where each $\mathbb{N}_i \simeq \mathbb{N}$ and $\mathbb{N}_1 < \mathbb{N}_2 < \mathbb{N}_3 \cdots$

**NB**

*Well-ordered sets are an important mathematical tool to prove termination of programs.*

# Combining Orders

**Product order** — can combine any partial orders. In general, it is only a *partial order*, even if combining total orders.
For $s, s' \in S$ and $t, t' \in T$ define

$$(s, t) \preceq (s', t') \quad \text{if } s \preceq s' \text{ and } t \preceq t'$$

# Practical Orderings

They are, effectively, *total* orders on the *product* of ordered sets.

- **Lexicographic order** — defined on all of $\Sigma^*$. It extends a total order already assumed to exist on $\Sigma$.
- **Lenlex** — the order on (potentially) the entire $\Sigma^*$, where the elements are ordered first by length.
  $\Sigma^{(1)} \prec \Sigma^{(2)} \prec \Sigma^{(3)} \prec \cdots$, then lexicographically within each $\Sigma^{(k)}$. In practice it is applied only to the finite subsets of $\Sigma^*$.
- **Filing order** — lexicographic order confined to the strings of the same length.
  It defines total orders on $\Sigma^i$, separately for each $i$.

# Example

## Example

$\boxed{\text{RW: 11.2.5}}$ Let $\mathbb{B} = \{0, 1\}$ with the usual order $0 < 1$. List the elements $101, 010, 11, 000, 10, 0010, 1000$ of $\mathbb{B}^*$ in the

(a) Lexicographic order

(b) Lenlex order

$\boxed{\text{RW: 11.2.8}}$ When are the lexicographic order and *lenlex* on $\Sigma^*$ the same?

# Example

## Example

$\boxed{\text{RW: 11.2.5}}$ Let $\mathbb{B} = \{0, 1\}$ with the usual order $0 < 1$. List the elements $101, 010, 11, 000, 10, 0010, 1000$ of $\mathbb{B}^*$ in the

(a) Lexicographic order

$000, 0010, 010, 10, 1000, 101, 11$

(b) Lenlex order

$10, 11, 000, 010, 101, 0010, 1000$

$\boxed{\text{RW: 11.2.8}}$ When are the lexicographic order and *lenlex* on $\Sigma^*$ the same?

Only when $|\Sigma| = 1$.

# Exercises

## Exercises

RW: 11.6.6 True or false?

(a) If a set $\Sigma$ is totally ordered, then the corresponding lexicographic partial order on $\Sigma^*$ also must be totally ordered.

(b) If a set $\Sigma$ is totally ordered, then the corresponding lenlex order on $\Sigma^*$ also must be totally ordered.

(c) Every finite poset has a Hasse diagram.

(d) Every finite poset has a topological sorting.

(e) Every finite poset has a minimum element.

(f) Every finite totally ordered set has a maximum element.

(g) An infinite poset cannot have a maximum element.

# Exercises

## Exercises

RW: 11.6.6 True or false?

(a) If a set $\Sigma$ is totally ordered, then the corresponding lexicographic partial order on $\Sigma^*$ also must be totally ordered. ?

(b) If a set $\Sigma$ is totally ordered, then the corresponding lenlex order on $\Sigma^*$ also must be totally ordered.

(c) Every finite poset has a Hasse diagram.

(d) Every finite poset has a topological sorting.

(e) Every finite poset has a minimum element.

(f) Every finite totally ordered set has a maximum element.

(g) An infinite poset cannot have a maximum element.

# Exercises

## Exercises

$\boxed{\text{RW: 11.6.6}}$ True or false?

(a) If a set $\Sigma$ is totally ordered, then the corresponding lexicographic partial order on $\Sigma^*$ also must be totally ordered. ?

(b) If a set $\Sigma$ is totally ordered, then the corresponding lenlex order on $\Sigma^*$ also must be totally ordered. ?

(c) Every finite poset has a Hasse diagram.

(d) Every finite poset has a topological sorting.

(e) Every finite poset has a minimum element.

(f) Every finite totally ordered set has a maximum element.

(g) An infinite poset cannot have a maximum element.

# Exercises

## Exercises

RW: 11.6.6 True or false?

(a) If a set $\Sigma$ is totally ordered, then the corresponding lexicographic partial order on $\Sigma^*$ also must be totally ordered. ?

(b) If a set $\Sigma$ is totally ordered, then the corresponding lenlex order on $\Sigma^*$ also must be totally ordered. ?

(c) Every finite poset has a Hasse diagram. ?

(d) Every finite poset has a topological sorting.

(e) Every finite poset has a minimum element.

(f) Every finite totally ordered set has a maximum element.

(g) An infinite poset cannot have a maximum element.

# Exercises

## Exercises

RW: 11.6.6 True or false?

(a) If a set $\Sigma$ is totally ordered, then the corresponding lexicographic partial order on $\Sigma^*$ also must be totally ordered. ?

(b) If a set $\Sigma$ is totally ordered, then the corresponding lenlex order on $\Sigma^*$ also must be totally ordered. ?

(c) Every finite poset has a Hasse diagram. ?

(d) Every finite poset has a topological sorting. ?

(e) Every finite poset has a minimum element.

(f) Every finite totally ordered set has a maximum element.

(g) An infinite poset cannot have a maximum element.

# Exercises

## Exercises

$\boxed{\text{RW: 11.6.6}}$ True or false?

(a) If a set $\Sigma$ is totally ordered, then the corresponding lexicographic partial order on $\Sigma^*$ also must be totally ordered. ?

(b) If a set $\Sigma$ is totally ordered, then the corresponding lenlex order on $\Sigma^*$ also must be totally ordered. ?

(c) Every finite poset has a Hasse diagram. ?

(d) Every finite poset has a topological sorting. ?

(e) Every finite poset has a minimum element. ?

(f) Every finite totally ordered set has a maximum element.

(g) An infinite poset cannot have a maximum element.

# Exercises

## Exercises

$\boxed{\text{RW: 11.6.6}}$ True or false?

(a) If a set $\Sigma$ is totally ordered, then the corresponding lexicographic partial order on $\Sigma^*$ also must be totally ordered. ?

(b) If a set $\Sigma$ is totally ordered, then the corresponding lenlex order on $\Sigma^*$ also must be totally ordered. ?

(c) Every finite poset has a Hasse diagram. ?

(d) Every finite poset has a topological sorting. ?

(e) Every finite poset has a minimum element. ?

(f) Every finite totally ordered set has a maximum element. ?

(g) An infinite poset cannot have a maximum element.

# Exercises

## Exercises

RW: 11.6.6 True or false?

(a) If a set $\Sigma$ is totally ordered, then the corresponding lexicographic partial order on $\Sigma^*$ also must be totally ordered. ?

(b) If a set $\Sigma$ is totally ordered, then the corresponding lenlex order on $\Sigma^*$ also must be totally ordered. ?

(c) Every finite poset has a Hasse diagram. ?

(d) Every finite poset has a topological sorting. ?

(e) Every finite poset has a minimum element. ?

(f) Every finite totally ordered set has a maximum element. ?

(g) An infinite poset cannot have a maximum element. ?