COMP9020 Lecture 4-5
Session 1, 2017
Functions and Relations

- Textbook - Ch. 3, Sec. 3.1, 3.3–3.4; Ch. 11, Sec. 11.1–11.2
- Problem sets 4 and 5
- Supplementary Exercises Ch. 3 and 11 (R & W)

NB

Mid-session test: Friday, 7 April, 2:30pm (1hr)

Properties of Functions

Recall:

$f : S \longrightarrow T$

S — **domain** of f, symbol: $\mathrm{Dom}(f)$

T — **codomain** of f, symbol: $\mathrm{Codom}(f)$

$\{ f(x) : x \in \mathrm{Dom}(f) \}$ — **image** of f, symbol: $\mathrm{Im}(f)$

Function is called **onto** (or **surjective**) if every element of the codomain is mapped to by at least on x in the domain, i.e.

$$\mathrm{Im}(f) = T$$

Examples (of functions that are not onto)

- $f : \mathbb{N} \longrightarrow \mathbb{N}$ with $f(x) \mapsto x^2$
- $f : \{a, \ldots, z\}^* \longrightarrow \{a, \ldots, z\}^*$ with $f(\omega) \mapsto a\omega e$

1-1 Functions

Function is called **1–1** (**one-to-one**) or **injective** if different x implies different $f(x)$, i.e.

$$f(x) = f(y) \Rightarrow x = y$$

Examples (of functions that are not 1–1)

- absolute value
- floor, ceiling
- length of a word

Inverse Functions

Inverse function — $f^{-1} : T \longrightarrow S$;
for a given $f : S \longrightarrow T$ exists exactly
when f is both 1–1 and onto.
Image of a subdomain A under a function

$$f(A) = \{ f(s) : s \in A \} = \{ t \in T : t = f(s) \text{ for some } s \in A \}$$

Inverse image — $f^{\leftarrow}(B) = \{ s \in S : f(s) \in B \} \subseteq S$;
it is defined for every f
If f^{-1} exists then $f^{\leftarrow}(B) = f^{-1}(B)$

$f(\emptyset) = \emptyset, f^{\leftarrow}(\emptyset) = \emptyset$

Examples

$\boxed{1.7.5}$ f and g are 'shift' functions $\mathbb{N} \longrightarrow \mathbb{N}$ defined by $f(n) = n + 1$, and $g(n) = \max(0, n - 1)$

(c) Is f 1–1? onto?
(d) Is g 1-1? onto?
(e) Do f and g commute, i.e. $\forall n\,((f \circ g)(n) = (g \circ f)(n))$?

Examples

$\boxed{1.7.5}$ f and g are 'shift' functions $\mathbb{N} \longrightarrow \mathbb{N}$ defined by
$f(n) = n + 1$, and $g(n) = \max(0, n - 1)$

(c) f is 1–1, not onto: $f(\mathbb{N}) = \mathbb{N} \setminus \{0\} = \mathbb{P}$

(d) g is onto, not 1–1: $g(0) = g(1)$

(e) f and g do not commute:
$g \circ f : n \mapsto (n + 1) - 1 = n$, thus $g \circ f = \mathrm{Id}_{\mathbb{N}}$
$f \circ g : 0 \mapsto 1$, hence $f \circ g \neq \mathrm{Id}_{\mathbb{N}}$

NB

$f \circ g$ is the identity when restricted to $\mathbb{P}$

NB

For a **finite** *set* S *and* $f : S \longrightarrow S$ *the properties*

1. *onto, and*
2. *1–1*

are equivalent. (Proof suggestion?)

Examples

$\boxed{1.7.6}$ $\Sigma = \{a, b, c\}$

(c) Is length : $\Sigma^* \longrightarrow \mathbb{N}$ onto?

(d) $\text{length}^{\leftarrow}(2) \stackrel{?}{=}$

Examples

$\boxed{1.7.12}$ Verify that $f : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R} \times \mathbb{R}$ defined by $f(x, y) = (x + y, x - y)$ is invertible.

Examples

$\boxed{1.7.6}$ $\Sigma = \{a, b, c\}$

(c) Is length : $\Sigma^* \longrightarrow \mathbb{N}$ onto?

Yes: $\text{length}^{\leftarrow}(\{n\}) = \Sigma^n \neq \emptyset$

(d) $\text{length}^{\leftarrow}(2) = \{aa, ab, ac, bb, \ldots, cc\}$

Examples

$\boxed{1.7.12}$ Verify that $f : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R} \times \mathbb{R}$ defined by $f(x, y) = (x + y, x - y)$ is invertible.

The inverse is $f^{-1}(a, b) = (\frac{a+b}{2}, \frac{a-b}{2})$; substituting shows that $f \circ f^{-1} = \mathrm{Id}_{\mathbb{R}\times\mathbb{R}}$

Examples

$\boxed{1.7.6}$ $\Sigma = \{a, b, c\}$
(c) Is length : $\Sigma^* \longrightarrow \mathbb{N}$ onto?
Yes: $\text{length}^{\leftarrow}(\{n\}) = \Sigma^n \neq \emptyset$
(d) $\text{length}^{\leftarrow}(2) = \{aa, ab, ac, bb, \ldots, cc\}$

Examples

$\boxed{1.7.12}$ Verify that $f : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R} \times \mathbb{R}$ defined by $f(x, y) = (x + y, x - y)$ is invertible.
The inverse is $f^{-1}(a, b) = (\frac{a+b}{2}, \frac{a-b}{2})$; substituting shows that $f \circ f^{-1} = \text{Id}_{\mathbb{R}\times\mathbb{R}}$

Supplementary Exercises [cont'd]

$\boxed{1.8.16}$ $\Sigma = \{a, b\}$; relate it to Σ^*

(a) Is there an onto $\Sigma \longrightarrow \Sigma^*$?

(b) Is there an onto $\Sigma^* \longrightarrow \Sigma$?

Supplementary Exercises [cont'd]

$\boxed{1.8.16}$ $\Sigma = \{a, b\}$; relate it to Σ^*
(a) Is there an onto $\Sigma \longrightarrow \Sigma^*$? No: $|\Sigma| = 2, |\Sigma^*| = \infty$.
(b) Is there an onto $\Sigma^* \longrightarrow \Sigma$? Yes, eg $f(\omega) = a$ when $\text{length}(\omega)$ is odd, $f(\omega) = b$ when $\text{length}(\omega)$ is even.
The following is **not** completely correct $f : \omega \mapsto \langle\text{first letter of } \omega\rangle$
Reason: $f(\lambda)$ is not defined.

Matrices

An $\mathbf{m} \times \mathbf{n}$ **matrix** is a rectangular array with m horizontal rows and n vertical columns.

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

NB

Matrices are important objects in Computer Science, e.g. for

- *optimisation*
- *graphics and computer vision*
- *cryptography*
- *information retrieval and web search*
- *machine learning*

Basic Matrix Operations

The **transpose** $\mathbf{A}^\mathsf{T}$ of an $m \times n$ matrix $\mathbf{A} = [a_{ij}]$ is the $n \times m$ matrix whose entry in the ith row and jth column is a_{ji}.

Example

$$\mathbf{A} = \begin{bmatrix} 2 & -1 & 0 & 4 \\ 3 & 2 & -1 & 2 \\ 4 & 0 & 1 & 3 \end{bmatrix} \qquad \mathbf{A}^\mathsf{T} = \begin{bmatrix} 2 & 3 & 4 \\ -1 & 2 & 0 \\ 0 & -1 & 1 \\ 4 & 2 & 3 \end{bmatrix}$$

NB

A matrix $\mathbf{M}$ *is called symmetric if* $\mathbf{M}^\mathsf{T} = \mathbf{M}$

The **sum** of two $m \times n$ matrices $\mathbf{A} = [a_{ij}]$ and $\mathbf{B} = [b_{ij}]$ is the $m \times n$ matrix whose entry in the ith row and jth column is $a_{ij} + b_{ij}$.

Example

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

$$\mathbf{A} + \mathbf{B} = \begin{bmatrix} 3 & -1 & 5 & 7 \\ 5 & 5 & -3 & 3 \\ 8 & -2 & 1 & 5 \end{bmatrix}$$

Fact

$$\mathbf{A} + \mathbf{B} = \mathbf{B} + \mathbf{A} \quad \textit{and} \quad (\mathbf{A} + \mathbf{B}) + \mathbf{C} = \mathbf{A} + (\mathbf{B} + \mathbf{C})$$

Given $m \times n$ matrix $\mathbf{A} = [a_{ij}]$ and $c \in \mathbb{R}$, the **scalar product** $c\mathbf{A}$ is the $m \times n$ matrix whose entry in the ith row and jth column is $c \cdot a_{ij}$.

Example

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

The **product** of an $m \times n$ matrix $\mathbf{A} = [a_{ij}]$ and an $n \times p$ matrix $\mathbf{B} = [b_{jk}]$ is the $m \times p$ matrix $\mathbf{C} = [c_{ik}]$ defined by

$$c_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk} \qquad \text{for } 1 \leq i \leq m \text{ and } 1 \leq k \leq p$$

Example

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \cdot \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} = \begin{bmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{bmatrix}$$

NB

The rows of $\mathbf{A}$ *must have the same number of entries as the columns of* $\mathbf{B}$.
The product of a $1 \times n$ *matrix and an* $n \times 1$ *matrix is usually called the* **inner product** *of two* **n-dimensional vectors.**

Example

Consider

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

Calculate $\mathbf{AB}$, $\mathbf{BA}$

$$\mathbf{AB} = \begin{bmatrix} -10 & 5 \\ -20 & 10 \end{bmatrix} \qquad \mathbf{BA} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

NB

In general, $\mathbf{A} \cdot \mathbf{B} \neq \mathbf{B} \cdot \mathbf{A}$

Example

Consider

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

Calculate **AB**, **BA**

$$\mathbf{AB} = \begin{bmatrix} -10 & 5 \\ -20 & 10 \end{bmatrix} \qquad \mathbf{BA} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

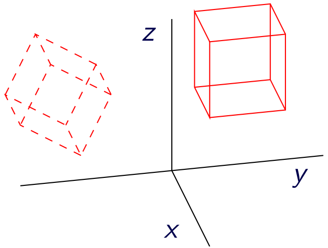
NB

In general, $\mathbf{A} \cdot \mathbf{B} \neq \mathbf{B} \cdot \mathbf{A}$

Example: Computer Graphics

Rotating an object w.r.t. the x axis by degree α:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\alpha & -\sin\alpha \\ 0 & \sin\alpha & \cos\alpha \end{bmatrix} \begin{bmatrix} 5 & 5 & 7 & 7 & 5 & 7 & 5 & 7 \\ 1 & 1 & 1 & 1 & 3 & 3 & 3 & 3 \\ 9 & 7 & 7 & 9 & 7 & 7 & 9 & 9 \end{bmatrix}$$



Relations and their Representation

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

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

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

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

$$x \in R \Rightarrow x = (x_1, x_2, \ldots x_n) \text{ where each } x_i \in S_i$$

If $n = 2$ we have a **binary** relation $\mathcal{R} \subseteq S \times T$.
(mostly we consider binary relations)
equivalent notations: $(x_1, x_2, \ldots x_n) \in R \iff R(x_1, x_2, \ldots x_n)$
for binary relations: $(x, y) \in R \iff R(x, y) \iff xRy$.

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)

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

Applications

Relations are ubiquitous in Computer Science

- Databases are collections of relations
- Common data structures (e.g. graphs) are relations
- Any ordering is a relation
- Functions/procedures/programs compute relations between their input and output

Relations are therefore used in most problem specifications and to describe formal properties of programs.
For this reason, studying relations and their properties helps with formalisation, implementation and verification of programs.

n-ary Relations

Relations can be defined linking $k \geq 1$ domains $D_1, \ldots, D_k$ simultaneously.
In database situations one also allows for *unary* $(n = 1)$ relations.
Most common are **binary** relations

$$\mathcal{R} \subseteq S \times T; \quad \mathcal{R} = \{(s,t) | \text{ "some property that links } s, t\text{"}\}$$

For related s, t we can write $(s,t) \in \mathcal{R}$ or $s\mathcal{R}t$; for unrelated items either $(s,t) \notin \mathcal{R}$ or $s \not{\mathcal{R}} t$.
$\mathcal{R}$ 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 $D_1 \times D_2 \times \ldots \times D_k$;
- construction from other relations.

Functions as Relations

Any function $f : S \longrightarrow T$ can be viewed as a binary relation

$$\{ (s, f(s)) : s \in S \} \subseteq S \times T$$

If a subset of $S \times T$ corresponds to a function, it must satisfy certain conditions w.r.t. S and T (which?)

Binary Relations

A binary relation, say $\mathcal{R} \subseteq S \times T$, can be presented as a matrix with rows enumerated by (the elements of) S and the columns by T; eg. for $S = \{s_1, s_2, s_3\}$ and $T = \{t_1, t_2, t_3, t_4\}$ we may have

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

Example

$\boxed{\text{3.1.2(e)}}$ Write the following relation on $A = \{0, 1, 2\}$ as a matrix.

$(m, n) \in R$ if $m \cdot n = m$

$$\begin{array}{cc} & \begin{array}{ccc} 0 & 1 & 2 \end{array} \\ \begin{array}{c} 0 \\ 1 \\ 2 \end{array} & \begin{bmatrix} \bullet & \bullet & \bullet \\ \circ & \bullet & \circ \\ \circ & \bullet & \circ \end{bmatrix} \end{array}$$

Example

$\boxed{\text{3.1.2(e)}}$ Write the following relation on $A = \{0, 1, 2\}$ as a matrix.

$(m, n) \in R$ if $m \cdot n = m$

$$\begin{array}{cc} & \begin{array}{ccc} 0 & 1 & 2 \end{array} \\ \begin{array}{c} 0 \\ 1 \\ 2 \end{array} & \begin{bmatrix} \bullet & \bullet & \bullet \\ \circ & \bullet & \circ \\ \circ & \bullet & \circ \end{bmatrix} \end{array}$$

Relations on a Single Domain

Particularly important are binary relationships between the elements of the same set. We say that '$\mathcal{R}$ is a relation on S' if

$$\mathcal{R} \subseteq S \times S$$

Special (Trivial) Relations

(all w.r.t. set S)

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

Empty $\emptyset$

Universal $U = S \times S$

Important Properties of Binary Relations $\mathcal{R} \subseteq S \times S$

(R)	reflexive	$(x, x) \in \mathcal{R}$	$\forall x \in S$
(AR)	antireflexive	$(x, x) \notin \mathcal{R}$	$\forall x \in S$
(S)	symmetric	$(x, y) \in \mathcal{R} \Rightarrow (y, x) \in \mathcal{R}$	$\forall x, y \in S$
(AS)	antisymmetric	$(x, y), (y, x) \in \mathcal{R} \Rightarrow x = y$	$\forall x, y \in S$
(T)	transitive	$(x, y), (y, z) \in \mathcal{R} \Rightarrow (x, z) \in \mathcal{R}$	$\forall x, y, z \in S$

NB

An object, notion etc. is considered to satisfy a property if none of its instances violates any defining statement of that property.

Examples

(R) reflexive $(x,x) \in \mathcal{R}$ for all $x \in S$ $\begin{bmatrix} \bullet & \bullet & \circ \\ \circ & \bullet & \circ \\ \bullet & \circ & \bullet \end{bmatrix}$

(AR) antireflexive $(x,x) \notin \mathcal{R}$ $\begin{bmatrix} \circ & \bullet & \bullet \\ \circ & \circ & \circ \\ \bullet & \circ & \circ \end{bmatrix}$

(S) symmetric $(x,y) \in \mathcal{R} \Rightarrow (y,x) \in \mathcal{R}$ $\begin{bmatrix} \bullet & \circ & \bullet \\ \circ & \circ & \bullet \\ \bullet & \bullet & \circ \end{bmatrix}$

(AS) antisymmetric $(x,y),\ (y,x) \in \mathcal{R} \Rightarrow x = y$
$\begin{bmatrix} \bullet & \bullet & \circ \\ \circ & \circ & \bullet \\ \bullet & \circ & \circ \end{bmatrix}$

(T) transitive $(x,y),\ (y,z) \in \mathcal{R} \Rightarrow (x,z) \in \mathcal{R}$
$\begin{bmatrix} \circ & \circ & \bullet \\ \bullet & \bullet & \bullet \\ \circ & \circ & \circ \end{bmatrix}$

Example

$\boxed{3.1.1}$ 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 $m + n = 3$

(AR) and (S)

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

(S)

$\boxed{3.1.2(b)}$ $(m, n) \in R$ if $m < n$

(AR), (AS), (T)

Example

$\boxed{3.1.1}$ 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 $m + n = 3$
(AR) and (S)

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

$\boxed{3.1.2(b)}$ $(m, n) \in R$ if $m < n$
(AR), (AS), (T)

Interaction of Properties

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

NB

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

Most important kinds of relations on S

- total order $\begin{bmatrix} \bullet & \bullet & \bullet \\ \circ & \bullet & \bullet \\ \circ & \circ & \bullet \end{bmatrix}$
- partial order $\begin{bmatrix} \bullet & \bullet & \bullet \\ \circ & \bullet & \circ \\ \circ & \circ & \bullet \end{bmatrix}$, $\begin{bmatrix} \bullet & \bullet & \circ \\ \circ & \bullet & \circ \\ \circ & \circ & \bullet \end{bmatrix}$
- equivalence $\begin{bmatrix} \bullet & \bullet & \circ \\ \bullet & \bullet & \circ \\ \circ & \circ & \bullet \end{bmatrix}$
- identity $\begin{bmatrix} \bullet & \circ & \circ \\ \circ & \bullet & \circ \\ \circ & \circ & \bullet \end{bmatrix}$

NB

Some of those are special cases of the others, eg. 'total order' of a 'partial order', 'identity' of an 'equivalence'.

Relation $\mathcal{R}$ as Correspondence From S to T

$\mathcal{R}(A) \stackrel{\text{def}}{=} \{t \in T | (s,t) \in \mathcal{R} \text{ for some } s \in A \subseteq S\}$
$\mathcal{R}^{\leftarrow}(B) \stackrel{\text{def}}{=} \{s \in S | (s,t) \in \mathcal{R} \text{ for some } t \in B \subseteq T\}$
Converse relation $\mathcal{R}^{\leftarrow}$

$$\mathcal{R}^{\leftarrow} = \{(t,s) \in T \times S | (s,t) \in \mathcal{R}\}$$

Note that $\mathcal{R}^{\leftarrow} \subseteq T \times S$.
Observe that $(\mathcal{R}^{\leftarrow})^{\leftarrow} = \mathcal{R}$.

NB

Viewed this way $\mathcal{R}$ becomes a function from $Pow(S)$ to $Pow(T)$. However, not every $g : Pow(S) \longrightarrow Pow(T)$ can be matched to a relation.

(Using a small domain like $S = \{a, b\}$ provide an example of a function $g : \text{Pow}(S) \longrightarrow \text{Pow}(S)$ which does not correspond to any relation on S. Can you do it with $S' = \{a\}$?)

NB

The order of axes – S and T – is important. For $\mathcal{R} \subseteq S \times S$, its converse $\mathcal{R}^{\leftarrow}$ is usually quite different from $\mathcal{R}$.

Example: divisibility relation on $\mathbb{P}$

$$\begin{aligned} D &\stackrel{\text{def}}{=} \{\ (p, q) : p|q\ \} = \{(1,1), (1,2), \ldots, (2,2), (2,4), \ldots\} \\ D^{\leftarrow} &= \{\ (p, q) : p \in q\mathbb{P}\ \} \\ &= \{(1,1), (2,1), (2,2), (3,1), (3,3), (4,1), (4,2), \ldots\} \end{aligned}$$

For every $n \in \mathbb{P}$, $D(\{n\})$ is infinite, $D^{\leftarrow}(\{n\})$ is finite.

Question

$f^{\leftarrow}$ is a relation; when is it a function?

Question

$f^{\leftarrow}$ is a relation; when is it a function?

Answer

When f is 1-1 and onto.

Example

$\boxed{3.1.9}$ Find the properties of the *empty relation* $\emptyset \subset S \times S$ and the *universal relation* $U = S \times S$. Assume that S is a nonempty domain.

(a) $\emptyset$ is (AR), (S), (AS), (T); if $S = \emptyset$ itself then $\emptyset$ is also (R).

(b) U is (R), (S), (T); if $|S| \leq 1$ then also (AS)

Example

$\boxed{3.1.9}$ Find the properties of the *empty relation* $\emptyset \subset S \times S$ and the *universal relation* $U = S \times S$. Assume that S is a nonempty domain.

(a) $\emptyset$ is (AR), (S), (AS), (T); if $S = \emptyset$ itself then $\emptyset$ is also (R).

(b) U is (R), (S), (T); if $|S| \leq 1$ then also (AS)

Example

$\boxed{\text{3.1.10(a)}}$ Give examples of relations with specified properties.
(AS), (T), $\neg$(R).

Examples over $\mathbb{N}$, Pow($\mathbb{N}$)

- strict order of numbers $x < y$
- simple (weak) order, but with some pairs (x, x) removed from $\mathcal{R}$
- being a prime divisor
  $(p, n) \in \mathcal{R}$ iff p is prime and $p|n$
  - not reflexive: $(1, 1) \notin \mathcal{R}, (4, 4) \notin \mathcal{R}, (6, 6) \notin \mathcal{R}$
  - transitivity is meaningful only for the pairs $(p, p), (p, n)$, $p|n$ for p prime

Example

$\boxed{\text{3.1.10(a)}}$ Give examples of relations with specified properties.
(AS), (T), $\neg$(R).

Examples over $\mathbb{N}$, $\mathrm{Pow}(\mathbb{N})$

- strict order of numbers $x < y$
- simple (weak) order, but with some pairs (x, x) removed from $\mathcal{R}$
- being a prime divisor
  $(p, n) \in \mathcal{R}$ iff p is prime and $p|n$
  - not reflexive: $(1, 1) \notin \mathcal{R}, (4, 4) \notin \mathcal{R}, (6, 6) \notin \mathcal{R}$
  - transitivity is meaningful only for the pairs $(p, p), (p, n)$, $p|n$ for p prime

Example

$\boxed{\text{3.1.10(b)}}$ Give examples of relations with specified properties.
(S), $\neg$(R), $\neg$(T).

Easiest examples - inequality

- $\mathcal{R} = \{(x, y) | x \neq y,\ x, y \in \mathbb{N}\}$
- $\mathcal{R} = \{(A, B) | A \neq B,\ A, B \subseteq S\}$

Example

$\boxed{\text{3.1.10(b)}}$ Give examples of relations with specified properties.
(S), ¬(R), ¬(T).

Easiest examples - inequality

- $\mathcal{R} = \{(x, y) | x \neq y,\ \ x, y \in \mathbb{N}\}$
- $\mathcal{R} = \{(A, B) | A \neq B,\ \ A, B \subseteq S\}$

Example

$\boxed{3.1.14}$ Which properties carry from individual relations to their union?

(a) $\mathcal{R}_1, \mathcal{R}_2 \in (\mathrm{R}) \Rightarrow \mathcal{R}_1 \cup \mathcal{R}_2 \in (\mathrm{R})$

(b) $\mathcal{R}_1, \mathcal{R}_2 \in (\mathrm{S}) \Rightarrow \mathcal{R}_1 \cup \mathcal{R}_2 \in (\mathrm{S})$

(c) $\mathcal{R}_1, \mathcal{R}_2 \in (\mathrm{T}) \not\Rightarrow \mathcal{R}_1 \cup \mathcal{R}_2 \in (\mathrm{T})$

Eg. $S = \{a, b, c\}, a\mathcal{R}_1 b, b\mathcal{R}_2 c$

and no other relationships

Example

$\boxed{3.1.14}$ Which properties carry from individual relations to their union?

(a) $\mathcal{R}_1, \mathcal{R}_2 \in$ (R) $\Rightarrow \mathcal{R}_1 \cup \mathcal{R}_2 \in$ (R)
(b) $\mathcal{R}_1, \mathcal{R}_2 \in$ (S) $\Rightarrow \mathcal{R}_1 \cup \mathcal{R}_2 \in$ (S)
(c) $\mathcal{R}_1, \mathcal{R}_2 \in$ (T) $\not\Rightarrow \mathcal{R}_1 \cup \mathcal{R}_2 \in$ (T)
Eg. $S = \{a, b, c\}, a\mathcal{R}_1 b, b\mathcal{R}_2 c$
and no other relationships

Equivalence Relations and Partitions

Relation $\mathcal{R}$ is called an *equivalence* relation if it satisfies (R), (S), (T). Every equivalence $\mathcal{R}$ defines *equivalence classes* on its domain S.
The equivalence class $[s]$ (w.r.t. $\mathcal{R}$) of an element $s \in S$ is

$$[s] = \{ \, t \in S : t\mathcal{R}s \, \}$$

This notion is well defined only for $\mathcal{R}$ which is an equivalence relation. Collection of all equivalence classes $[S]_{\mathcal{R}} = \{ \, [s] : s \in S \, \}$ is a partition of S

$$S = \bigcup_{s \in S} [s]$$

Thus the equivalence classes are disjoint and jointly cover the entire domain. It means that every element belongs to one (and only one) equivalence class.

We call $s_1, s_2, \ldots$ *representatives* of (different) equivalence classes

For $s, t \in S$ either $[s] = [t]$, when $s\mathcal{R}t$, or $[s] \cap [t] = \emptyset$, when $s \not{\mathcal{R}} t$.

We commonly write $s \sim_{\mathcal{R}} t$ when s, t are in the same equivalence class.

In the opposite direction, a partition of a set defines the equivalence relation on that set. If $S = S_1 \dot{\cup} \ldots \dot{\cup} S_k$, then we specify $s \sim t$ exactly when s and t belong to the same S_i.

If the relation $\sim$ is an equivalence on S and $[S]$ the corresponding partition, then

$$\nu : S \longrightarrow [S], \quad \nu : s \mapsto [s] = \{\, x \in S : x \sim s \,\}$$

is called the *natural* map. It is always onto.

Question

When is ν also 1–1 ?

If the relation $\sim$ is an equivalence on S and $[S]$ the corresponding partition, then

$$\nu : S \longrightarrow [S], \quad \nu : s \mapsto [s] = \{ x \in S : x \sim s \}$$

is called the *natural* map. It is always onto.

Question

When is ν also 1–1 ?

Answer

When $\sim$ is the identity on S.

A function $f : S \longrightarrow T$ defines an equivalence relation on S by

$$s_1 \sim s_2 \quad \text{iff} \quad f(s_1) = f(s_2)$$

These sets $f^{\leftarrow}(t)$, $t \in T$ that are nonempty form the corresponding partition

$$S = \bigcup_{t \in T} f^{\leftarrow}(t)$$

Question

When are all $f^{\leftarrow}(t) \neq \emptyset$?

A function $f : S \longrightarrow T$ defines an equivalence relation on S by

$$s_1 \sim s_2 \quad \text{iff} \quad f(s_1) = f(s_2)$$

These sets $f^{\leftarrow}(t)$, $t \in T$ that are nonempty form the corresponding partition

$$S = \bigcup_{t \in T} f^{\leftarrow}(t)$$

Question

When are all $f^{\leftarrow}(t) \neq \emptyset$?

Answer

When f is onto.

Example

Partition of $\mathbb{Z}$ into classes of numbers with the same remainder $\pmod{p}$; 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.

Standard notation:
$m = n \pmod{p}$ stands for: $m \bmod p = n \bmod p$

Example

$\boxed{3.6.6}$ Show that $m \sim n$ when $m^2 = n^2 \pmod 5$ is an equivalence on $S = \{1, \ldots, 7\}$. Find all the equivalence classes.

(a) It just means that $m = n \pmod 5$ or $m = -n \pmod 5$, e.g. $1 = -4 \pmod 5$. This satisfies (R), (S), (T).

(b) We have
$[0] = \{0, 5\}$
$[1] = \{1, 4, 6\}$
$[2] = \{2, 3, 7\}$

Supplementary Exercises

$\boxed{3.6.10}$

$\mathcal{R}$ is a relation on $\mathbb{N} \times \mathbb{N}$, i.e. it is a subset of $\mathbb{N}^4$
$(m, n) \sim (p, q)$ if $m = p \pmod 3$ or $n = q \pmod 5$.
(a) $\mathcal{R} \in$ (R)?
Yes: $(m, n) \sim (m, n)$ iff $m = m \pmod 3$ or $n = n \pmod 5$ iff true or true.
(b) $\mathcal{R} \in$ (S)?
Yes: by symmetry of $. = . \pmod n$.
(c) $\mathcal{R} \in$ (T)?
No — for arbitrary two pairs (m_1, n_1) and (m_2, n_2) one can create a chain $(m_1, n_1)\mathcal{R}(m_2, n_1)$ and $(m_2, n_1)\mathcal{R}(m_2, n_2)$, but not all pairs are related.

Supplementary Exercises

$\boxed{3.6.10}$

$\mathcal{R}$ is a relation on $\mathbb{N} \times \mathbb{N}$, i.e. it is a subset of $\mathbb{N}^4$

$(m, n) \sim (p, q)$ if $m = p \pmod 3$ or $n = q \pmod 5$.

(a) $\mathcal{R} \in$ (R)?

Yes: $(m, n) \sim (m, n)$ iff $m = m \pmod 3$ or $n = n \pmod 5$ iff true or true.

(b) $\mathcal{R} \in$ (S)?

Yes: by symmetry of $. = . \pmod n$.

(c) $\mathcal{R} \in$ (T)?

No — for arbitrary two pairs (m_1, n_1) and (m_2, n_2) one can create a chain $(m_1, n_1)\mathcal{R}(m_2, n_1)$ and $(m_2, n_1)\mathcal{R}(m_2, n_2)$, but not all pairs are related.

Supplementary Exercises

$\boxed{3.6.10}$

$\mathcal{R}$ is a relation on $\mathbb{N} \times \mathbb{N}$, i.e. it is a subset of $\mathbb{N}^4$
$(m, n) \sim (p, q)$ if $m = p \pmod 3$ or $n = q \pmod 5$.
(a) $\mathcal{R} \in$ (R)?
Yes: $(m, n) \sim (m, n)$ iff $m = m \pmod 3$ or $n = n \pmod 5$ iff true or true.
(b) $\mathcal{R} \in$ (S)?
Yes: by symmetry of $. = . \pmod n$.
(c) $\mathcal{R} \in$ (T)?
No — for arbitrary two pairs (m_1, n_1) and (m_2, n_2) one can create a chain $(m_1, n_1)\mathcal{R}(m_2, n_1)$ and $(m_2, n_1)\mathcal{R}(m_2, n_2)$, but not all pairs are related.

Supplementary Exercises

$\boxed{3.6.10}$

$\mathcal{R}$ is a relation on $\mathbb{N} \times \mathbb{N}$, i.e. it is a subset of $\mathbb{N}^4$
$(m, n) \sim (p, q)$ if $m = p \pmod 3$ or $n = q \pmod 5$.
(a) $\mathcal{R} \in$ (R)?
Yes: $(m, n) \sim (m, n)$ iff $m = m \pmod 3$ or $n = n \pmod 5$ iff true or true.
(b) $\mathcal{R} \in$ (S)?
Yes: by symmetry of $. = . \pmod n$.
(c) $\mathcal{R} \in$ (T)?
No — for arbitrary two pairs (m_1, n_1) and (m_2, n_2) one can create a chain $(m_1, n_1)\mathcal{R}(m_2, n_1)$ and $(m_2, n_1)\mathcal{R}(m_2, n_2)$, but not all pairs are related.

Order Relations

Total order $\leq$ on S
(R) $x \leq x$ for all $x \in S$
(AS) $x \leq y, y \leq x \Rightarrow x = y$
(T) $x \leq y, y \leq z \Rightarrow x \leq z$
(L) *Linearity* — any two elements are comparable:
for all x, y either $x \leq y$ or $y \leq x$ (and both if $x = y$)

On a finite set all total orders are isomorphic

$$x_1 \leq x_2 \leq \cdots \leq x_n$$

On an infinite set there is quite a variety of possibilities.

Examples

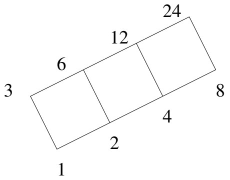
- discrete with a least element, e.g. $\mathbb{N} = \{0, 1, 2, \ldots\}$
- discrete without a least element, e.g. $\mathbb{Z} = \{\ldots, 0, 1, 2, \ldots\}$
- various dense/locally dense orders
  - rational numbers $\mathbb{Q}$: $\quad p < q \Rightarrow \exists_r p < r < q$
  - $S = [a, b]$ — both least and greatest elements
  - $S = (a, b]$ — no least element
  - $S = [a, b)$ — no greatest element
  - other $[0, 1] \cup [2, 3] \cup [4, 5] \cup \ldots$

Partial Order

A **partial order** $\preceq$ on S satisfies (R), (AS), (T); need not be (L)
We call $(S, \preceq)$ a **poset** — partially ordered set

Finite posets can be represented as so-called **Hasse diagrams**

$\boxed{\text{11.1.1(a)}}$ Hasse diagram for positive divisors of 24



Ordering Concepts

- *Minimal* and *maximal* elements (they always exist in every finite poset)
- *Minimum* and *maximum* — unique minimal and maximal element
- *lub* (least upper bound) and *glb* (greatest lower bound) of a subset $A \subseteq S$ of elements
  $\text{lub}(A)$ — smallest element $x \in S$ s.t. $x \succeq a$ for all $a \in A$
  $\text{glb}(A)$ — greatest element $x \in S$ s.t. $x \preceq a$ for all $a \in A$
- *Lattice* — a poset where lub and glb exist for every pair of elements
  (by induction, they then exist for every *finite* subset of elements)

Examples

- $\mathsf{Pow}(\{a, b, c\})$ with the order $\subseteq$
  $\emptyset$ is minimum; $\{a, b, c\}$ is maximum
- $\boxed{11.1.4}$
  $\mathsf{Pow}(\{a, b, c\}) \setminus \{\{a, b, c\}\}$ (proper subsets of $\{a, b, c\}$)
  Each two-element subset $\{a, b\}, \{a, c\}, \{b, c\}$ is maximal.
    - But there is no maximum
- $\{1, 2, 3, 4, 6, 8, 12, 24\}$ partially ordered by divisibility is a lattice
    - e.g. $\mathsf{lub}(\{4, 6\}) = 12$; $\mathsf{glb}(\{4, 6\}) = 2$
- $\{1, 2, 3\}$ partially ordered by divisibility is not a lattice
    - $\{2, 3\}$ has no lub
- $\{2, 3, 6\}$ partially ordered by divisibility is not a lattice
    - $\{2, 3\}$ has no glb
- $\{1, 2, 3, 12, 18, 36\}$ partially ordered by divisibility is not a lattice
    - $\{2, 3\}$ 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

- $\mathbb{Z}$ — neither lub nor glb;
- $\mathbb{F}(\mathbb{N})$ — all finite subsets, has no *arbitrary* lub property; glb exists, it is the intersection, hence always finite;
- $\mathbb{I}(\mathbb{N})$ — all infinite subsets, may not have an arbitrary glb; lub exists, it is the union, which is always infinite.

Example

$\boxed{11.1.5}$ 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 $\operatorname{lub}(\{\, x \in \mathbb{R} : x < 73 \,\})$

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

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

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

Example

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

(a) It is a lattice.

(b) subset with no upper bound: $\mathbb{R}_{>0} = \{\ r \in \mathbb{R} : r > 0\ \}$

(c) and (d) $\text{lub}(\{\ x : x < 73\ \}) = \text{lub}(\{\ x : x \leq 73\ \}) = 73$

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

(f) $\text{glb}(\{\ x : x^2 < 73\ \}) = -\sqrt{73}$

Example

$\boxed{11.1.13}$ $\mathbb{F}(\mathbb{N})$ — collection of all *finite* subsets of $\mathbb{N}$

(a) Does it have a maximal element?

(b) Does it have a minimal element?

(c) Given $A, B \in \mathbb{F}(\mathbb{N})$, does $\{A, B\}$ have a lub in $\mathbb{F}(\mathbb{N})$?

(d) Given $A, B \in \mathbb{F}(\mathbb{N})$, does $\{A, B\}$ have a glb in $\mathbb{F}(\mathbb{N})$?

(e) Is $\mathbb{F}(\mathbb{N})$ a lattice?

Example

$\boxed{11.1.13}$ $\mathbb{F}(\mathbb{N})$ — collection of all *finite* subsets of $\mathbb{N}$
(a) No maximal elements
(b) $\emptyset$ is the minimum
(c) $\mathrm{lub}(A, B) = A \cup B$
(d) $\mathrm{glb}(A, B) = A \cap B$
(e) $\mathbb{F}(\mathbb{N})$ is a lattice — is has *finite* union and intersection properties.

Example

$\boxed{11.1.14}$ $\mathbb{I}(\mathbb{N}) = \mathrm{Pow}(\mathbb{N}) \setminus \mathbb{F}(\mathbb{N})$ — collection of all *infinite* subsets of $\mathbb{N}$

(a) Does it have a maximal element?

(b) Does it have a minimal element?

(c) Given $A, B \in \mathbb{I}(\mathbb{N})$, does $\{A, B\}$ have a lub in $\mathbb{I}(\mathbb{N})$?

(d) Given $A, B \in \mathbb{I}(\mathbb{N})$, does $\{A, B\}$ have a glb in $\mathbb{I}(\mathbb{N})$?

(e) Is $\mathbb{I}(\mathbb{N})$ a lattice?

Example

$\boxed{11.1.14}$ $\mathbb{I}(\mathbb{N}) = \text{Pow}(\mathbb{N}) \setminus \mathbb{F}(\mathbb{N})$ — collection of all *infinite* subsets of $\mathbb{N}$

(a) $\mathbb{N}$ is the maximum

(b) No minimum element ($\emptyset$ is not in $\mathbb{I}(\mathbb{N})$)

(c) $\text{lub}(A, B) = A \cup B$

(d) $\text{glb}(A, B) = A \cap B$ *if it exists*; it does not exist when $A \cap B$ is finite, eg. when empty.

(e) $\mathbb{I}(\mathbb{N})$ is not a lattice — it has finite union but not finite intersection property; eg. sets $2\mathbb{N}$ and $2\mathbb{N} + 1$ have the empty intersection.

Well-Ordered Sets

Well-ordered set: 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 $\mathbb{N}_i \sim \mathbb{N}$ and $\mathbb{N}_1 < \mathbb{N}_2 < \mathbb{N}_3 \cdots$

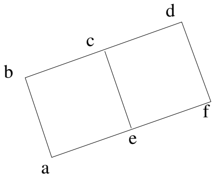
NB

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

Ordering of a Poset — Topological Sort

For a poset $(S, \preceq)$ any linear order $\leq$ that is consistent with $\preceq$ is called **topological sort**. Consistency means that $a \preceq b \Rightarrow a \leq b$.

Consider



Various possible topological sortings

The following all are topological sorts:

$a \leq b \leq e \leq c \leq f \leq d$

$a \leq e \leq b \leq f \leq c \leq d$

. . . . . .

$a \leq e \leq f \leq b \leq c \leq d$

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 Σ^*. It extends a total order already assumed to exist on Σ.
- **Lenlex** — the order on (potentially) the entire Σ^*, 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 Σ^*.
- **Filing order** — lexicographic order confined to the strings of the same length.
  It defines total orders on Σ^i, separately for each i.

Example

$\boxed{11.2.5}$ 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

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

$\boxed{11.2.8}$ When are the lexicographic order and *lenlex* on Σ^* the same?

Only when $|\Sigma| = 1$.

Example

$\boxed{11.2.5}$ 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

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

$\boxed{11.2.8}$ When are the lexicographic order and *lenlex* on Σ^* the same?

Only when $|\Sigma| = 1$.

Supplementary Exercises

$\boxed{11.6.6}$ True or false?

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

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

(c) Every finite partially ordered set has a Hasse diagram.

(d) Every finite partially ordered set has a topological sorting.

(e) Every finite partially ordered set has a smallest element.

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

(g) An infinite partially ordered set cannot have a largest element.

Supplementary Exercises

$\boxed{11.6.6}$

(a) and (b) – True; this is the idea behind various lex-sorts

(c) Yes.

(d) Yes.

(e) False – consider a two-element set with the identity as p.o.

(f) True – due to the finiteness

(g) False, eg. $\mathbb{Z}_{<0}$

Summary

- Properties of functions: onto, 1-1; f^{-1}, $f^{\leftarrow}$
- Properties of binary relations: (R), (AR); (S), (AS); (T)
- Matrix operations: transposition, sum, scalar product, product
- Equivalence relations $\sim$, equivalence classes $[S]$, example $\mathbb{Z}_p$
- Ordering concepts: total, partial, lub, glb, lattice, topological sort
- Orderings: product, lexicographic, lenlex, filing