COMP9020 20T1
Week 4
Equivalence and Order Relations

- Textbook (R & W) - Ch. 3, Sec. 3.4-3.5
  Ch. 11, Sec. 11.1-11.2
- Problem set 4 + quiz

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

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

This notion is well defined only for $\mathcal{R}$ which is an equivalence relation. Collection of all equivalence classes is a *partition* of S:

$$S = \dot{\bigcup}_{s \in S} [s]_{\mathcal{R}} \qquad (\dot{\cup} \text{ denotes a } \textit{disjoint union})$$

Example

$\mathcal{R} = \{(m, n) \in \mathbb{Z} : m \mod 2 = n \mod 2\}$
$[0] = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$ (same as $[-2]$, $[2]$, $\ldots$)
$[1] = \{\ldots, -3, -1, 1, 3, 5, \ldots\}$

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.

Example

$\mathbb{Z} = \{\ldots, -3, 0, 3, \ldots\} \dot\cup \{\ldots, -2, 1, 4, \ldots\} \dot\cup \{\ldots, -1, 2, 5, \ldots\}$

$m \sim n$ if, and only if, $m \mod 3 = n \mod 3$

$[0] = [3] = [6] = \ldots \qquad [0] \cap [1] = \emptyset = [0] \cap [2]$

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.

Exercise

When is ν also 1–1 ?

Only when $\sim$ is the identity on S.

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.

Exercise

When is ν also 1–1 ?

Only 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

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

Exercise

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

When f is onto.

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

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

Exercise

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

When f is onto.

Example: Congruence Relations

$\mathbb{Z} \longrightarrow \mathbb{Z}_p$: 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: $\mathbf{m} \equiv \mathbf{n} \pmod{\mathbf{p}}$
$\stackrel{\text{def}}{=}$ remainder of dividing m by p = remainder of dividing n by p

NB

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

Modular Arithmetic

Example

$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

n	$-n$
0	0
1	4
2	3
3	2
4	1

$*_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

n	n^{-1}
0	–
1	1
2	3
3	2
4	4

Exercise

$\boxed{3.5.6}$ Calculate the following in $\mathbb{Z}_7$.

(b) $5 + 6 = 4$

(c) $4 * 4 = 2$

(d) for any $k \in \mathbb{Z}_7$, $0 + k = k$

(e) for any $k \in \mathbb{Z}_7$, $1 * k = k$

Exercise

$\boxed{3.5.6}$ Calculate the following in $\mathbb{Z}_7$.

(b) $5 + 6 = 4$

(c) $4 * 4 = 2$

(d) for any $k \in \mathbb{Z}_7$, $0 + k = k$

(e) for any $k \in \mathbb{Z}_7$, $1 * k = k$

Exercise

Solve the following for x in $\mathbb{Z}_5$.

(a) $2 + x = 1$ $\quad \Rightarrow x = 4$

(b) $2 * x = 1$ $\quad \Rightarrow x = 2^{-1} = 3$

(c) $2 * x = 3$ $\quad \Rightarrow x = 3 * 2^{-1} = 3 * 3 = 4$

Exercise

Solve the following for x in $\mathbb{Z}_6$.

(d) $5 + x = 1$

(e) $5 * x = 1$

(e) $2 * x = 1$

Exercise

Solve the following for x in $\mathbb{Z}_5$.

(a) $2 + x = 1 \quad \Rightarrow x = 4$

(b) $2 * x = 1 \quad \Rightarrow x = 2^{-1} = 3$

(c) $2 * x = 3 \quad \Rightarrow x = 3 * 2^{-1} = 3 * 3 = 4$

Exercise

Solve the following for x in $\mathbb{Z}_6$.

(d) $5 + x = 1 \quad \Rightarrow x = 2$

(e) $5 * x = 1 \quad \Rightarrow x = 5 \quad (\text{since } 25 \mod 6 = 1)$

(e) $2 * x = 1 \quad \text{undefined} \quad (\text{since } 2 \cdot k \mod 6 \neq 1 \text{ for all } k \in \mathbb{Z}_6)$

Exercise

Solve the following for x in $\mathbb{Z}_5$.

(a) $2 + x = 1 \quad \Rightarrow x = 4$

(b) $2 * x = 1 \quad \Rightarrow x = 2^{-1} = 3$

(c) $2 * x = 3 \quad \Rightarrow x = 3 * 2^{-1} = 3 * 3 = 4$

Exercise

Solve the following for x in $\mathbb{Z}_6$.

(d) $5 + x = 1 \quad \Rightarrow x = 2$

(e) $5 * x = 1 \quad \Rightarrow x = 5 \quad (\text{since } 25 \mod 6 = 1)$

(e) $2 * x = 1$ undefined $\quad (\text{since } 2 \cdot k \mod 6 \neq 1 \text{ for all } k \in \mathbb{Z}_6)$

Supplementary Exercise

Exercise

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

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

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

Supplementary Exercise

Exercise

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

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

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

It is often necessary to define a function on $[S]$ by describing it on the individual representatives $t \in [s]$ for each equivalence class $[s]$. If $\phi : [S] \longrightarrow X$ is to be defined in this way, one must

- define $\phi(t)$ for all $t \in S$, making sure that $\phi(t) \in X$
- make sure that $\phi(t_1) = \phi(t_2)$ whenever $t_1 \sim t_2$, ie. when $[t_1] = [t_2]$
- define $\phi([s]) \stackrel{\text{def}}{=} \phi(s)$.

The second condition is critical for ϕ to be well-defined.

Example

$[S] = \{0, 4, 8, \ldots\} \,\dot{\cup}\, \{1, 5, 9, \ldots\} \,\dot{\cup}\, \{2, 6, 10, \ldots\} \,\dot{\cup}\, \{3, 7, 11, \ldots\}$

$\phi : [S] \longrightarrow \mathbb{Z}_2$ defined by $\phi(n) = n \bmod 2$

$\phi(0) = 0 = \phi(4) = \phi(8) = \ldots$

Example

Example of a not well-defined 'function' on equivalence classes:

$$\phi : \{0, 3, 6, \dots\} \,\dot{\cup}\, \{1, 4, 7, \dots\} \,\dot{\cup}\, \{2, 5, 8, \dots\} \longrightarrow \mathbb{Z}_5$$
$$\phi(n) \stackrel{?}{=} n \bmod 5$$

Problem: $[0] = [3] = [6] = \dots$ in $\mathbb{Z}_3$; however,
$0 \bmod 5 = 0,\ 3 \bmod 5 = 3,\ 6 \bmod 5 = 1\ \dots$

Supplementary Exercise

Exercise

$\boxed{3.6.10}$

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

$(m, n)\,\mathcal{R}\,(p, q)$ if $m \equiv p \pmod 3$ or $n \equiv q \pmod 5$.

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

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

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

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

(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 $(m_1, n_1) \not\mathcal{R} (m_2, n_2)$.

Supplementary Exercise

Exercise

$\boxed{3.6.10}$

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

$(m,n)\,\mathcal{R}\,(p,q)$ if $m \equiv p \pmod 3$ or $n \equiv q \pmod 5$.

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

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

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

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

(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 $(m_1, n_1) \not\mathcal{R} (m_2, n_2)$.

Supplementary Exercise

Exercise

$\boxed{3.6.10}$

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

$(m, n)\,\mathcal{R}\,(p, q)$ if $m \equiv p \pmod 3$ or $n \equiv q \pmod 5$.

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

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

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

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

(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 $(m_1, n_1)\,\not\mathcal{R}(m_2, n_2)$.

Supplementary Exercise

Exercise

$\boxed{3.6.10}$

$\mathcal{R}$ is a binary relation on $\mathbb{N} \times \mathbb{N}$, i.e. it is a subset of $\mathbb{N}^4$
$(m,n)\,\mathcal{R}\,(p,q)$ if $m \equiv p \pmod 3$ or $n \equiv q \pmod 5$.
(a) $\mathcal{R} \in$ (R)?
Yes: $(m,n) \sim (m,n)$ iff $m \equiv m \pmod 3$ or $n \equiv n \pmod 5$ iff true or true.
(b) $\mathcal{R} \in$ (S)?
Yes: by symmetry of $. \equiv . \pmod n$.
(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 $(m_1, n_1) \not\mathcal{R} (m_2, n_2)$.

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 $\mathbb{Q} : \forall p, q \in \mathbb{Q}\,(p < q \Rightarrow \exists r \in \mathbb{Q}\,(p < r < q))$
  - $S = [a, b]$ — 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

To each (partial) order one can associate a unique **quasi-order**

$$x \prec y \text{ iff } x \preceq y \text{ and } x \neq y$$

It satisfies (AS) and (T); it satisfies (L) if it corresponds to a total order (we could call it a total quasi-order); it does not satisfy (R) for any pair x, y.

Example

Exercise

$\boxed{11.1.8}$ For $\omega_1, \omega_2 \in \Sigma^*$ define $\omega_1 \preceq \omega_2$ when $\omega_2 = \nu\omega_1\nu'$ for some ν, ν'.
Is this a partial order?

Yes.
Relation $\preceq$ means being a substring; it is a partial order:

(R) $\omega = \lambda\omega\lambda$, hence $\omega \preceq \omega$
(AS) if $\omega_1 = \nu\omega_2\nu'$ and $\omega_2 = \chi\omega_1\chi'$ for some ν, ν', χ, χ' then $\nu = \nu' = \chi = \chi' = \lambda$, hence $\omega_1 = \omega_2$
(T) if $\omega_1 = \nu\omega_2\nu'$ and $\omega_2 = \chi\omega_3\chi'$ then $\omega_1 = \nu\chi\omega_3\chi'\nu'$

Example

Exercise

$\boxed{11.1.8}$ For $\omega_1, \omega_2 \in \Sigma^*$ define $\omega_1 \preceq \omega_2$ when $\omega_2 = \nu\omega_1\nu'$ for some ν, ν'.
Is this a partial order?

Yes.
Relation $\preceq$ means being a substring; it is a partial order:

(R) $\omega = \lambda\omega\lambda$, hence $\omega \preceq \omega$
(AS) if $\omega_1 = \nu\omega_2\nu'$ and $\omega_2 = \chi\omega_1\chi'$ for some ν, ν', χ, χ' then $\nu = \nu' = \chi = \chi' = \lambda$, hence $\omega_1 = \omega_2$
(T) if $\omega_1 = \nu\omega_2\nu'$ and $\omega_2 = \chi\omega_3\chi'$ then $\omega_1 = \nu\chi\omega_3\chi'\nu'$

Exercise

$\boxed{11.6.16}$ Properties of four relations defined on $\mathbb{P} = \{1, 2, \ldots\}$?

- $\mathcal{R}_1$ if $m|n$
- $\mathcal{R}_2$ if $|m - n| \leq 2$
- $\mathcal{R}_3$ if $2|m + n$
- $\mathcal{R}_4$ if $3|m + n$

	$\mathcal{R}_1$	$\mathcal{R}_2$	$\mathcal{R}_3$	$\mathcal{R}_4$
(R)				
(S)				
(AS)				
(T)				
Equivalence	?	?	?	?
Partial order	?	?	?	?

Exercise

$\boxed{11.6.16}$ Properties of four relations defined on $\mathbb{P} = \{1, 2, \ldots\}$

- $\mathcal{R}_1$ if $m|n$
- $\mathcal{R}_2$ if $|m - n| \leq 2$
- $\mathcal{R}_3$ if $2|m + n$
- $\mathcal{R}_4$ if $3|m + n$

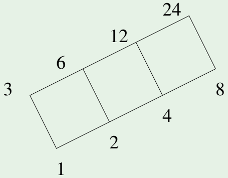
	$\mathcal{R}_1$	$\mathcal{R}_2$	$\mathcal{R}_3$	$\mathcal{R}_4$
(R)	Yes	Yes	Yes	
(S)		Yes	Yes	Yes
(AS)	Yes			
(T)	Yes		Yes	
Equivalence			Yes	
Partial order	Yes			

Hasse Diagram

Every finite poset can be represented as a **Hasse diagram**, where a line is drawn *upward* from x to y if $x \prec y$ and there is no z such that $x \prec z \prec y$

Example

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



$p \preceq q$ if, and only if, $p \mid q$

(Named after mathematician Helmut Hasse (Germany), 1898–1979)

Ordering Concepts

Definition

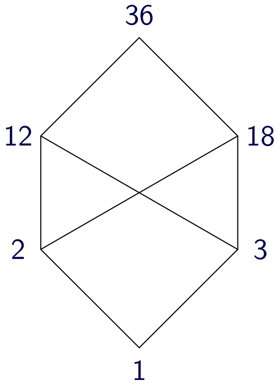
- *Minimal* and *maximal* elements (they always exist in every finite poset)
- *Minimum* and *maximum* — unique minimal and maximal element
- *lub* (least upper bound) and *glb* (greatest lower bound) of a subset $A \subseteq S$ of elements
  $\mathrm{lub}(A)$ — smallest element $x \in S$ s.t. $x \succeq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

- $\mathrm{Pow}(\{a,b,c\})$ with the order $\subseteq$
  $\emptyset$ is minimum; $\{a,b,c\}$ is maximum
- $\boxed{11.1.4}$
  $\mathrm{Pow}(\{a,b,c\}) \setminus \{\{a,b,c\}\}$ (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. $\mathrm{lub}(\{4,6\}) = 12$; $\mathrm{glb}(\{4,6\}) = 2$
- $\{1,2,3\}$ 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

Examples

- $\{1, 2, 3, 12, 18, 36\}$ 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.

Exercise

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

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

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

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

Exercise

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

Exercise

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

(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 $(\mathbb{F}(\mathbb{N}), \subseteq)$ a lattice?

Exercise

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

(a) No maximal elements

(b) $\emptyset$ is the minimum

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

(d) $\operatorname{glb}(A, B) = A \cap B$

(e) $(\mathbb{F}(\mathbb{N}), \subseteq)$ is a lattice — is has *finite* union and intersection properties.

Exercise

$\boxed{11.1.14}$ $\mathbb{I}(\mathbb{N}) = \text{Pow}(\mathbb{N}) \setminus \mathbb{F}(\mathbb{N})$ — 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 $(\mathbb{I}(\mathbb{N}), \subseteq)$ a lattice?

Exercise

$\boxed{11.1.14}$ $\mathbb{I}(\mathbb{N}) = \mathrm{Pow}(\mathbb{N}) \setminus \mathbb{F}(\mathbb{N})$ — all *infinite* subsets of $\mathbb{N}$
(a) $\mathbb{N}$ is the maximum
(b) No minimal elements ($\emptyset$ is not in $\mathbb{I}(\mathbb{N})$)
(c) $\mathrm{lub}(A, B) = A \cup B$
(d) $\mathrm{glb}(A, B) = A \cap B$ *if it exists*; it does not exist when $A \cap B$ is finite, eg. when empty.
(e) $(\mathbb{I}(\mathbb{N}), \subseteq)$ 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 $\mathbb{N}_i \simeq \mathbb{N}$ and $\mathbb{N}_1 < \mathbb{N}_2 < \mathbb{N}_3 \cdots$

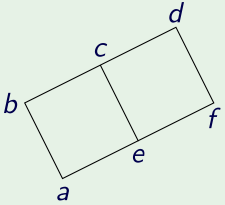
NB

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 $a \preceq b \Rightarrow a \leq b$.

Example



The following all are topological sorts:

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

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

$\ldots\ldots$

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

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

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

Exercise

$\boxed{11.2.1}$ Let $A = \{1, 2, 3, 4\}$ and $S = A \times A$ with the product order.

(a) A chain with seven elements?

(b) A chain with eight elements?

Exercise

$\boxed{11.2.1}$ Let $A = \{1, 2, 3, 4\}$ and $S = A \times A$ with the product order.

(a) A chain with seven elements?

$(1, 1)\,(1, 2)\,(2, 2)\,(2, 3)\,(2, 4)\,(3, 4)\,(4, 4)$ (other solutions exist)

(b) A chain with eight elements?

The above is a maximal chain.

No chains of eight elements.

Example

$\boxed{11.2.4}$ Take $(S, \preceq_1)$, $(T, \preceq_2)$ to be any total orders of more than one element. Then $S \times T$ with the product order is not a total order: for any $s_1 \prec s_2, t_1 \prec t_2$ the pair (s_1, t_2) and (s_2, t_1) are *not* comparable.

Ordering of Functions

T — arbitrary set (no order required)
S — partially ordered set
$M = \{f : T \longrightarrow S\}$ — set of all functions from T to S
It has a natural partial order

$$f \preceq g \quad \text{iff} \quad \forall t \in T \, (f(t) \preceq g(t))$$

It is, in effect, a product order on $S^{|T|}$. In most applications T has a linear ordering; however, it does not affect the order of the functions defined on T (only the order on S matters).

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.

Examples

Exercise

$\boxed{11.2.5}$ 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 $|\Sigma| = 1$.

Examples

Exercise

$\boxed{11.2.5}$ 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?

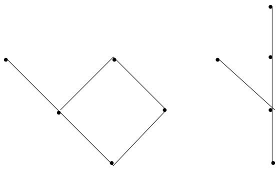
Only when $|\Sigma| = 1$.

Supplementary Exercise

$\boxed{11.6.12}$ Draw a Hasse diagram for a poset with exactly 5 members, 2 of which are maximal and 1 of which is the poset's minimum.

Supplementary Exercise

$\boxed{11.6.12}$ Draw a Hasse diagram for a poset with exactly 5 members, 2 of which are maximal and 1 of which is the poset's minimum.



and more ...

Supplementary Exercise

Exercise

$\boxed{11.6.6}$ 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 minimum.

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

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

Supplementary Exercise

Exercise

$\boxed{11.6.6}$

(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

- Equivalence relations $\sim$, equivalence classes $[S]$
- Special equivalence relations on $\mathbb{Z}_p$; notation $m \equiv n \pmod{p}$
- Ordering concepts:
  total, partial, lub, glb, lattice, topological sort
- Orderings: product, lexicographic, lenlex, filing

Coming up ...

- Ch. 3, Sec. 3.2; Ch. 6, Sec. 6.1-6.5 (Graphs)