CHAPTER 5 RELATIONS

SECTION 5.1

DEFINITION:

Let A, B be sets. A **RELATION** R **FROM** A **TO** B is a subset of $A \times B$.

We write $x\,R\,y$ iff $(x,y) \in R$ and $x \not R\, y$ iff $(x,y) \notin R$.

EXAMPLE

• Let $A = \{0,1,2\}$ and $B = \{1,2,3\}$. Define xRy or $(x,y) \in R$ if $x < y$. Then

$$R = \{(0,1),(0,2),(0,3),(1,2),(1,3),(2,3)\}$$

Thus we have $0\,R\,1$, $0\,R\,2$, etc. and $2 \not R\, 2$. Using ordered pair notation: $(0,1) \in R$, $(0,2) \in R$, $(2,2) \notin R$.

• Let E be the relation on $\mathbb{Z} \times \mathbb{Z}$ defined by

$$E = \{(x,y) : x \equiv y \pmod 2\}.$$

Here we have $2\,E\,6$, $3\,E\,-11$, $2 \not E\, 7$, etc. Using the ordered pair notation, we have $(2,6) \in E$, $(3,-11) \in E$, $(2,7) \notin E$.

• Let A be the set of bit strings of length 6. Define $x\,R\,y$ if the first 4 bits of x and y are identical. Then

$$101000\,R\,101011, \qquad 101111 \not R\, 101011$$

• Let $f : A \to B$ be a function. Recall the graph $\Gamma(f)$ of f

$$\Gamma(f) = \{(a, f(a)) \mid a \in A\}.$$

Then $\Gamma(f)$ is a relation from A to B. This example shows that functions can be thought of as special types of relations.

DEFINITION:

Let R be a relation from A to B. The **DOMAIN** of R is the set

$$\{a \in A \mid \exists b \in B, aRb\}.$$

The **RANGE** of R is the set

$$\{b \in B \mid \exists a \in A, aRb\}.$$

REMARK

When R is the graph $\Gamma(f)$ of a function $f : A \to B$, then the domain of R is exactly the domain of the function f, and the range of R is exactly the range of the function f.

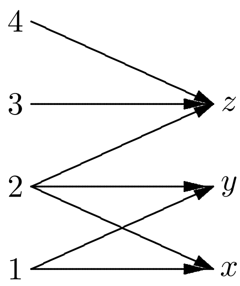
SECTION 5.2 REPRESENTING RELATIONS

ARROW DIAGRAM

A relation R can be represented by an **ARROW DIAGRAM** where there is an arrow from a to b if $(a, b) \in R$. The following is an example.

$R = \{(1, x), (1, y), (2, x), (2, y), (2, z)(3, z), (4, z)\}$

from $A = \{1, 2, 3, 4\}$ to $B = \{x, y, z\}$.



DEFINITION:

Let R be a relation from A to B. Then the **INVERSE of** R, denoted R^{-1}, is the relation from B to A defined by

$$R^{-1} = \{(b, a) \in B \times A \mid arb\}.$$

REMARK

- $\forall a \in A \; \forall b \in B \; (aRb \Leftrightarrow b\, R^{-1}\, a)$.

- The arrow diagram of R^{-1} can be obtained by reversing the arrows in the arrow diagram of R.

- Let $f : A \to B$ be a function. Then $(\Gamma(f))^{-1}$ is a relation from B to A. Furthermore, $(\Gamma(f))^{-1}$ is the graph of a function $g : B \to A$ if and only if f is bijective, if and only if $g = f^{-1}$.

SECTION 5.3 EQUIVALENCE RELATIONS

DEFINITION:

A **RELATION** on a set A is a relation on $A \times A$.

DEFINITION:

Let R be a relation on A.

1. R is **REFLEXIVE** if $\forall x \in A$, $(x, x) \in R$.

2. R is **SYMMETRIC** if $\forall x, y \in A$, $(x, y) \in R \Rightarrow (y, x) \in R$.

3. R is **ANTISYMMETRIC** if $\forall x, y \in A$, $(x, y) \in R$ and $(y, x) \in R$ imply $x = y$. (This means that at most one of the pairs (x, y) and (y, x) can be in R.)

3. R is **TRANSITIVE** if $\forall x, y, z \in A$, $(x, y) \in R, (y, z) \in R \Rightarrow (x, z) \in R$.

EXAMPLE

• The equality relation on $\mathbb{R}$, where

$$(x, y) \in R \quad \text{if} \quad x = y$$

is reflexive, symmetric, antisymmetric and transitive.

• The $\leq$ relation on $\mathbb{R}$, where

$$(x, y) \in R \quad \text{if} \quad x \leq y$$

is reflexive, antisymmetric and transitive but is not symmetric.

• The $<$ relation on $\mathbb{R}$, where

$$(x, y) \in R \quad \text{if} \quad x < y$$

is not reflexive, not symmetric but is antisymmetric and transitive.

• The congruence mod 3 relation on $\mathbb{Z}$, where

$$(x, y) \in R \quad \text{if} \quad x \equiv y \pmod 3$$

is reflexive, symmetric and transitive but is not antisymmetric.

• The "divides" relation D on $\mathbb{N}$ where $(x, y) \in D$ iff $x \mid y$ is reflexive, antisymmetric and transitive but is not symmetric.

• The "subset" relation on a collection of sets where $(A, B) \in R$ if $A \subseteq B$, is reflexive, antisymmetric and transitive but is not symmetric.

DEFINITION:

A relation R on a set A is an **EQUIVALENCE RELATION** if it is reflexive, symmetric and transitive.

If R is an equivalence relation and $(a, b) \in R$, we say a is **EQUIVALENT** to b.

DEFINITION:

Suppose R is an equivalence relation on A. For each $a \in A$, the **EQUIVALENCE CLASS** of a, denoted by $[a]$, is the set of all elements of A related to a, i.e.,

$$[a]_R = \{x \in A \mid (a, x) \in R\}.$$

When there is no danger of confusion, we drop the subscript and simply write $[a]$.

Define A/R to be the **SET OF ALL EQUIVALENCE CLASSES**, i.e.,

$$A/R = \{[a]_R \mid a \in A\}.$$

- $[a]_R$ consists of all elements related to a.
- $A/R \subseteq P(A)$.

EXAMPLE

- Let S be the relation on $\mathbb{R}$ where $(a, b) \in S$ if $a - b \in \mathbb{Z}$. Is S an equivalence relation?

SOLN: Since $a - a = 0 \in \mathbb{Z}$, $(a, a) \in S$ for all $a \in \mathbb{R}$, S is reflexive.

Since $a - b \in \mathbb{Z}$ implies that $b - a \in \mathbb{Z}$, we have $(a, b) \in S$ implies $(b, a) \in S$. Thus S is symmetric.

Since $a - b \in \mathbb{Z}$, and $b - c \in \mathbb{Z}$ implies $(a - b) + (b - c) = a - c \in \mathbb{Z}$, we have $(a, b) \in S$, $(b, c) \in S$ imply $(a, c) \in S$. Thus S is transitive.

Therefore S is an equivalence relation.

- In the equivalence relation S, $[a] = \{n + a \mid n \in \mathbb{Z}\}$.
- $S/\mathbb{R} = \{[a] \mid 0 \leq a < 1\}$.
- **CONGRUENCE MODULO** m Let m be an integer > 1. The relation

$$R = \{(a, b) \mid a \equiv b \pmod{m}\}$$

is an equivalence relation.

PROOF: Recall that $a \equiv b \pmod{m}$ iff $m \mid (a - b)$.

REFLEXIVE: Since $m \mid (a - a)$, $(a, a) \in R$.

SYMMETRIC: If $m \mid (a-b)$, then $m \mid (b-a)$. Thus $(a,b) \in R \Rightarrow (b,a) \in R$.

TRANSITIVE: If $m \mid (a-b)$ and $m \mid (b-c)$, then $m \mid (a-b)+(b-c) = a-c$. Thus $(a,b) \in R$ and $(b,c) \in R$ imply $(a,c) \in R$.

Therefore R is an equivalence relation.

• In the equivalence relation R, $[n] = \{n + km \mid k \in \mathbb{Z}\} = [r]$, where $r = n$ **mod** m. There are only m equivalent classes: $[0], [1], \ldots, [m-1]$. Therefore, $\mathbb{Z}/R = \{[0], [1], \ldots, [m-1]\}$.

Thus when $m = 2$, there are 2 equivalence classes

$$\begin{aligned} [0] &= \{2k \mid k \in \mathbb{Z}\} && \text{(the even numbers)} \\ [1] &= \{1 + 2k \mid k \in \mathbb{Z}\} && \text{(the odd numbers)} \end{aligned}$$

When $m = 3$, there are 3 equivalence classes:

$$\begin{aligned} [0] &= \{3k \mid k \in \mathbb{Z}\} \\ [1] &= \{3k+1 \mid k \in \mathbb{Z}\} \\ [2] &= \{3k+2 \mid k \in \mathbb{Z}\} \end{aligned}$$

• The "Divides" relation on $\mathbb{Z}$, i.e., $(a,b) \in R$ iff $a \mid b$ is not an equivalence relation because it is not symmetric.

• Let $n \in \mathbb{N}$ and R_n be the relation on the set of finite bitstrings defined as follows $(s,t) \in R_n$ if (i) $s = t$ or (ii) s, t are both of length at least n and the first n bits of s and t are equal. Prove that R_n is an equivalence relation.

SOLN: We modify the bit strings as follows: If s is of length $m < n$, we append $n-m$ copies of x at the end s to get s'. If a bitstring t is of length $\geq n$, then $t' = t$. We define a relation R' on the modified strings by $(s', t') \in R'$ if the first n bits of s', t' are equal. Then $(s', t') \in R'$ iff $(s,t) \in R_n$.

We shall prove that R' is an equivalence relation which in turn will imply that R_n is an equivalence relation.

It is obvious that R' is an equivalence relation. (Think about it.)

• In R_n, $[a] = \{a\}$ if the length of a is $\leq n$. If the length of a is $> n$, let b the first n bits of a, then $[a] = \{bx \mid x \text{ is a bitstring}\}$.

EQUIVALENCE CLASSES & PARTITIONS

DEFINITION:

A collection of nonempty subsets $A_1, A_2 \ldots,$ of S is a **PARTITION** of S if

- $A_1 \cup A_2 \cdots = S$; and
- $A_1, A_2 \ldots,$ are mutually disjoint.

EXAMPLE

- The set of prime numbers, the set of composite numbers and the set $\{1\}$ is a partition $\mathbb{N}$.
- The set $A = \{1, 2, 3\}$ has the following partitions:

$$\begin{gathered}\{\{1\},\{2\},\{3\}\}\\ \{\{1\},\{2,3\}\}\\ \{\{2\},\{1,3\}\}\\ \{\{3\},\{1,2\}\}\\ \{A\}\end{gathered}$$

THEOREM:

Let R be an equivalence relation on a set A. The following statements for elements a, b of A are equivalent:

(i) $(a, b) \in R$, (ii) $[a] = [b]$, (iii) $[a] \cap [b] \neq \emptyset$.

PROOF: We need to prove that (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (i).

(i) $\Rightarrow$ (ii): From (i), we have $(a, b) \in R$ which implies $(b, a) \in R$ (R is symmetric). Now let $x \in [a]$. Then $(a, x) \in R$. But $(b, a) \in R$. Hence $(b, x) \in R$ (R is transitive), consequently $x \in [b]$. Thus $[a] \subseteq [b]$. Reversing the role of a, b, we get $[b] \subseteq [a]$. Thus $[a] = [b]$.

(ii) $\Rightarrow$ (iii): This is obvious as $[a] \cap [b] = [a]$.

(iii) $\Rightarrow$ (i): Let $x \in [a] \cap [b]$ (x exists because of (iii)). Then $x \in [a]$ implies that $(a, x) \in R$, and $x \in [b]$ implies that $(x, b) \in R$. Thus, by transitivity, $(a, b) \in R$ which is (i).

The following is a corollary.

THEOREM:

Let R be an equivalence relation on a set A. If $a, b \in A$, then either

$$[a] = [b] \quad \text{or} \quad [a] \cap [b] = \emptyset.$$

THEOREM:

Let R be an equivalence relation on a set S. Then the distinct equivalence classes form a partition of S. That is, S/R is a partition of S.

Conversely, let $\{A_i \mid i \in I\}$ be a partition of the set S. Then there is an equivalence relation T on S that has the sets A_i, $i \in I$ as its equivalence classes.

PROOF: For any $x \in S$, since $x \in [x]$, we see that x is in some equivalence class. Thus the union of the distinct equivalence classes is A. But distinct equivalence classes are pairwise disjoint. Thus we get a partition.

For the second part, define T as follows: $(x, y) \in T$ $\exists i \in I$ such that $x, y \in A_i$. It is clear T is symmetric. Let $w \in S$. Since the collection is a partition, $\exists k \in I$ such that $w \in A_k$. Thus $(w, w) \in T$ and this proves that T is reflexive. Now we prove transitivity. Let $(x, y) \in T$ and $(y, z) \in T$. Then $\exists i \in I$ such that $x, y \in A_i$ and $\exists j \in I$ such that $y, z \in A_j$. Since $y \in A_i$ and $y \in A_j$, and the collection is a partition, we have $i = j$. Thus $x, z \in A_i$ and therefore $(x, z) \in T$. If $x \in A_i$, then it is related to all the elements of A_i and not to other elements. Thus $[x] = A_i$. Hence the equivalence classes are members of the partition.

SECTION 5.4 PARTIAL ORDERINGS

DEFINITION:

A relation R on a set A is a **PARTIAL ORDER** if it is reflexive, antisymmetric and transitive.

We call (A, R) a **PARTIALLY ORDERED SET** or **POSET**.

EXAMPLE

- $(A, \leq)$, where $A \subseteq \mathbb{R}$ and $x\,R\,y$ if $x \leq y$, is a poset.
- $(S, |)$, where $S \subseteq \mathbb{N}$ and $m\,R\,n$ if $m \mid n$, is a poset.
- $(A, \subseteq)$, where A is a collection of sets and $S\,R\,T$ if $S \subseteq T$, is a poset.
- If R is a partial order on A, then R^{-1} is also a partial order on A.

NOTATION

In the above examples, we have used $\leq, \subseteq, |$, etc., to denote partial order. However, we often need to discuss partial order in an arbitrary poset and the symbol $\preceq$ is adopted. We read $a \preceq b$ as a IS less than or equal to b, or equivalently, b is greater than or equal to a, just as in $\leq$. However, the two must not be confused. Also when $a \preceq b$ and $a \neq b$, we write $a \prec b$.

In a poset $(P, \preceq)$, if $a, b \in P$ it is not necessary that either $a \preceq b$ or $b \preceq a$. For example in the poset $(\mathbb{N}, |)$, $2 \nmid 3$ and $3 \nmid 2$, i.e., $2 \not\preceq 3$ and $3 \not\preceq 2$.

DEFINITION:

Let A be a poset. Elements $a, b \in A$ are **COMPARABLE** if either $a \preceq b$ or $b \preceq a$. Otherwise, they are **NONCOMPARABLE**

EXAMPLE

- Consider the partial order $\leq$ on $\mathbb{R}$. Every two real numbers are comparable.
- Consider the partial order $\subseteq$. Let $A = \{a\}$ and $B = \{b\}$, with $a \neq b$. Then $A \not\subseteq B$ and $B \not\subseteq A$. Thus A, B are noncomparable.

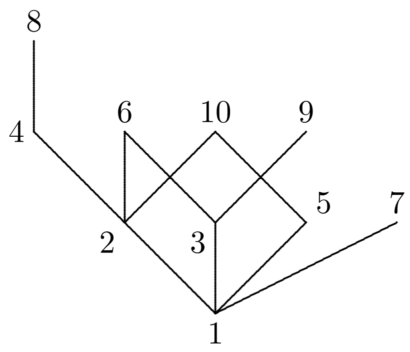
DEFINITION:

Let A be a subset of a poset.

1. $a \in A$ is a **MAXIMAL ELEMENT** of A, if $\sim (\exists c \in A$ such that $a \prec c)$.
2. $a \in A$ is a **MINIMAL ELEMENT** of A, if $\sim (\exists c \in A$ such that $c \prec a)$.
3. $a \in A$ is a **LARGEST (or GREATEST or MAXIMUM) ELEMENT** of A, if $\forall b \in A$, $b \preceq a$.
4. $a \in A$ is a **SMALLEST (or LEAST or MINIMUM) ELEMENT** of A, if $\forall b \in A$, $a \preceq b$.

EXAMPLE

Let $A = \{1, 2, \ldots, 10\}$ with the partial order $|$. Then



- 6, 7, 8, 9, 10 are maximal elements.
- No greatest element
- 1 is the least element and also a minimal element

THEOREM:

Every nonempty finite poset S has a minimal element and a maximal element.

PROOF: Let $a_1 \in S$. If a_1 is not minimal, then $\exists a_2 \in S$ such that $a_2 \prec a_1$. Continue this process, so that if a_n is not minimal, $\exists a_{n+1} \in S$ such that $a_{n+1} \prec a_n$. Since S is finite, this process must end with a minimal element.

The maximal element case is similar.

THEOREM:

Every nonempty poset S has at most one largest element and one smallest element.

PROOF: If both x and y are smallest, then $x \preceq y$ (since x is smallest), and $y \preceq x$ (since y is smallest), so that $x = y$ by anti-symmetricity of $\preceq$.

Similar proof if both x and y are largest.

REMARK

It is possible to have no largest or smallest element. It is also possible to have more than one maximal element, and/or more than one minimal element.

HASSE DIAGRAM

DEFINITION:

Let $(A, \preceq)$ be a poset. The corresponding **HASSE DIAGRAM** is constructed as follows. If $x \prec y$ and there is no z such that $x \prec z \prec y$, then place x below y and draw a line joining x to y.

• From the Hasse diagram, one can determine if $x \prec y$ by checking if we can get from x to y by using lines going upwards.

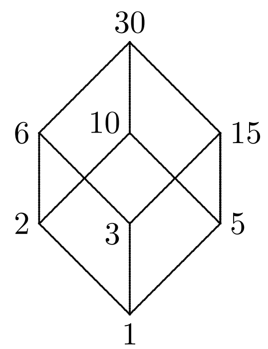
• The minimal (resp. maximal) elements can be easily determined from the Hasse diagram, as they correspond to those elements having no lines going downwards (resp. upwards).

EXAMPLE

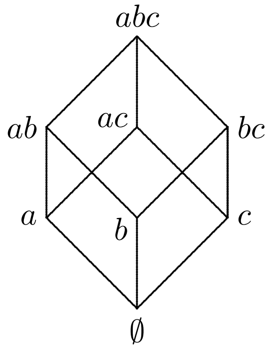
• Consider the "divides" relation, i.e. $x \preceq y$ if $x \mid y$, on the set

$$\{1, 2, 3, 5, 6, 10, 15, 30\},$$

the Hasse diagram is as follows:



• Consider the power set $P(S)$, where $S = \{a, b, c\}$ with the partial order $\subseteq$. Draw its Hasse diagram.



DEFINITION:

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

The partial order $\preceq$ is called a **TOTAL ORDER** if $\forall a, b \in P$, a, b are comparable.

Such a poset $(P, \preceq)$ is called a **TOTALLY ORDERED SET**.

A subset Q of P is a **CHAIN** if $\forall a, b \in Q$, a, b are comparable (that is, if $(Q, \preceq)$ is a totally ordered set).

EXAMPLE

• $(\mathbb{R}, \leq)$ is a totally ordered set.

• On the Hasse diagram, a chain is a subset consisting of elements that lie on a single ascending (or descending) line.

• The set of English words W with the alphabetical order is a totally ordered set. (This order is called **LEXICOGRAPHIC (or DICTIONARY) ORDER**. Note that

$$\begin{array}{rl} discreet \prec discrete & \text{(because the first difference occurs in the } 7^{\text{th}} \text{ letter and } e \prec t) \\ discreetness \prec discretion & \text{(because the first difference occurs in the } 7^{\text{th}} \text{ letter and } e \prec t) \\ discreet \prec discreetness & \text{(because the first word is a subword of the second)} \end{array}$$

.

• The way that we order the set of positive integers is also a lexicographic order. (Here when we compare two integers, we need to append 0's at the left end of the shorter integer so that the two integers are of the same length.) Thus

$$001 < 101, \quad 2234 < 2239, \quad 000201 < 100000.$$

• **PRODUCT ORDER**: $(x_1, x_2, \ldots, x_n) \preceq (y_1, y_2, \ldots, y_n)$ if and only if $x_i \preceq y_i$ for all i. For example, $(1, 2, 3) \preceq (2, 3, 4)$, but $(1, 2, 3) \not\preceq (2, 3, 1)$.

- Product order is a subset of lexicographic order.
- Lexicographic order is total, but product order is not total.

DEFINITION:

Let $(P, \preceq)$ be a total order.

The partial order $\preceq$ is called a **WELL ORDER** if every nonempty subset of P has the smallest element.

EXAMPLE

- $(\mathbb{Z}^+, \leq)$ is a well order.
- $(\mathbb{Z}, \leq)$ is not a well order.

INFOMRATION FLOW

The flow of information from one person to another is often restricted via security clearance. An example is the *multilevel security policy* used in government and military systems. Each piece of information is assigned a security class (A, C) where A is the *authority level* and C is a *category*. Usually each category represents some areas of interests. Information can flow from (A, C) to (A', C') iff $A \preceq A'$ and $C \subseteq C'$, i.e., the security level of A is lower than or equal to that of A' and the areas of interests of C is subset of those of C'. This ordering, $(A, C) \preceq (A', C')$, is a partial order.

TOPOLOGICAL SORTING

Suppose a project is made up of 20 different tasks to be executed in a sequence. Certain task, say a, cannot be performed until another task, say b, has been completed. This give rise to a partial order $b \preceq a$. Thus we need to order the 20 tasks in such a way that this partial ordering is adhered to.

DEFINITION:

A total order $\preceq$ is said to be **COMPATIBLE** with the partial order R if aRb implies $a \preceq b$.

The construction of such a total order is called **TOPOLOGICAL SORTING**

THEOREM:

Given a finite poset S with partial order R, a total ordering compatible with R exists.

PROOF: $S = S_1$ has a minimal element a_1. $S_2 = S - \{a_1\}$ has a minimal element a_2. In general, $S_n = S - \{a_1, \ldots, a_{n-1}\}$ has a minimal element a_n. The order $a_i \prec a_j$ iff $i \leq j$ is a total order. If $a_i R a_j$, and $a_i \neq a_j$, then $a_i \notin S_j$, otherwise a_j is not a minimal element of S_j. Thus $i < j$ and $a_i \prec a_j$. So $\preceq$ is compatible with R.

$\boxed{\textbf{EXAMPLE}}$

Consider the "divides" relation on the set $S = \{1, 2, 3, 5, 6, 10, 15, 30\}$. A compatible total ordering can be found as follows:

1 is the only minimal element. Therefore $a_1 = 1$.

2, 3, 5 are the minimal elements of S_2. Pick $a_2 = 3$.

2, 5 are the minimal elements of S_3. Pick $a_3 = 2$.

5 is the only minimal element of S_4. Therefore $a_4 = 5$.

6, 10, 15 are the minimal elements of S_5. Pick $a_5 = 6$.

10, 15 are the minimal elements of S_6. Pick $a_6 = 15$.

10 is the only minimal element of S_7. Therefore $a_7 = 10$.

30 is the only element of S_8. Therefore $a_8 = 30$.

The total order is

$$1 \prec 3 \prec 2 \prec 5 \prec 6 \prec 15 \prec 10 \prec 30.$$