Discrete Mathematics with Applications

Dr Liew How Hui

May 2021

Outline

Set

Informally, a set is any well-defined list, collection, or class of objects. The objects comprising the set are called its *elements* or *members*. The statement "p is an element of A" is written "$p \in A$".

The operations associated with sets A and B are defined below.

Definition 3.3.1:

1. A is a *subset* of B, $A \subset B$: if $x \in A$ then $x \in B$.
2. *power set* of A, $\mathscr{P}(A)$: the family of all the subsets of any set A. E.g. When $A = \{1, 2, 3\}$, $\mathscr{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

Set (cont)

Definition 3.3.2:

1. *union* of A and B, $A \cup B := \{x : x \in A \vee x \in B\}$
2. *intersection* of A and B, $A \cap B := \{x : x \in A \wedge x \in B\}$
3. *difference* of A and B, $A \setminus B := \{x : x \in A \wedge x \notin B\}$
4. *(Cartesian) product* of A and B, $A \times B$: the ordered pairs of A and B, i.e. $\{(a, b) : a \in A, b \in B\}$. E.g. When $A = \{1, 2, 3\}$, $B = \{a, b\}$, $A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$.

   The product can be generalised to the case of n sets $A_1, \cdots, A_n$: the *n-ary Cartesian product over sets* $A_1, \cdots, A_n$ is $A_1 \times \cdots \times A_n := (((A_1 \times A_2) \times A_3) \times \cdots A_n) = \{((x_1, x_2), \cdots, x_n) : x_i \in A_i\}$.

Set (cont)

Let A and B be two sets. $A \times B = \emptyset$ iff $A = \emptyset$ or $B = \emptyset$.

Proof by Contraposition

$\Leftarrow$: If $A \times B \neq \emptyset$, then $\exists z \in A \times B$, $z = (z_1, z_2)$, $z_1 \in A$ and $z_2 \in B$, hence $A \neq \emptyset$ and $B \neq \emptyset$.
$\Rightarrow$: If $A \neq \emptyset$ and $B \neq \emptyset$, $\exists x \in A$ and $\exists y \in B$ such that $(x, y) \in A \times B$. This implies $A \times B \neq \emptyset$.

Relation

The notion of a *(binary) relation* between two sets of objects is common and important.

For human being, throughout life, we experience a wide variety of personal relationships. The words such as “father of”, “son of”, “husband of”, “friend of”, etc. are about relationships between two persons.

For two objects, typical comparisons using such words as “bigger than”, “better than”, “faster than”, etc.

A relation is a set of ordered pairs ‘relating’ entities from a **domain** to a **range**.

The theory of *relational database language* SQL is based on the *manipulation of set relations*.

Relation (cont)

Definition 3.3.4

Let A and B be two nonempty sets and let $a \in A$, $b \in B$. A *(binary) relation R from A to B* is a subset of $A \times B$, i.e. $R \subset A \times B$. A *(binary) relation R on A* is a subset of $A \times A$, i.e. $R \subset A \times A$.

Definition 3.3.5

Given an ordered pair $(a, b) \in A \times B$, *a is related to b by R*, written aRb, if $(a, b) \in R$. If *a is not related to b by R*, we denote it as $a \not R\, b$ or $(a, b) \notin R$.

Relation (cont)

Definition 3.3.6

Let $R \subset A \times B$ be a relation from A to B. The *domain of* R, $\text{Dom}(R) = \{a \in A | \exists b \in B, aRb\}$. The range of R, $\text{range}(R) = \{b \in B | \exists a \in A, aRb\}$.

Definition 3.3.7

A *function* f *from* A *to* B is a relation from A to B such that for every $x \in \text{Dom}(f)$, there is a unique value y such that xfy or what we usually write $y = f(x)$. It is normally written as $f : A \to B$, $x \mapsto y$.

Relation (cont)

Example 3.3.9: Let $A = \{3, 4, 5, 6, 7\}$ and let R be the relation $<$ (less than) on A. List the elements of R.

Solution

Since $aRb = a < b$,
$R = \{(3, 4), (3, 5), (3, 6), (3, 7), (4, 5), (4, 6), (4, 7), (5, 6), (5, 7), (6, 7)\}$.

Relation (cont)

Example 3.3.10: Let R be a relation on $A = \{1, 2, 3, 4\}$ defined by: $xRy = x$ divides y and $x < y$. List all elements in R.

Class discussion.

Relation (cont)

Example 3.3.11: The domain and range of the following relations R

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

is

$$\text{Dom}(R) = \{a, b, d\}, \quad \text{range}(R) = \{a, b, c, e\}.$$

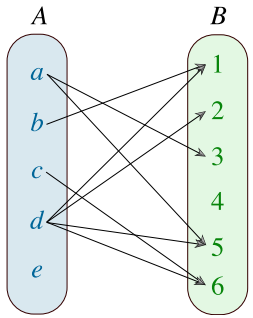
Example 3.3.12: Given $A = \{-3, -2, -1, 0, 1, 2, 3, 4\}$, $B = \{0, 1, 4\}$ and define the relation R from A to B as $R = \{(x, y) : y = x^2\}$. Determine the domain and range of R.

Class Discussion.

Relation (cont)

There are many ways to specify and represent binary relations:

- Listing Tuples (Roster Notation). Example 3.3.11's R.
- Set Builder Notation. Example 3.3.12's $\{(x, y) : y = x^2\}$
- Relation as a Cartesian Plane Graph. Only useful for relation between numbers.
- Relation as an Arrow Diagram:



- Relation as a Directed Graph: Only for range=domain.
- Relation as a Matrix (next section)

Outline

Matrix

Relation from a finite set A to a finite set B has a "Boolean" (or binary or logical) matrix representation.

Definition

A rectangular array

$$A = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{bmatrix}$$

of $m \times n$ numbers a_{ij} is called a *matrix of m rows and n columns* or $m \times n$-matrix.

Relation (cont)

A matrix representation of relation R from a finite set A to a finite set B is stated below.

Definition 3.3.15

Let $A = \{a_1, a_2, \cdots, a_m\}$ and $B = \{b_1, b_2, \cdots, b_n\}$ and let R be a relation from A to B. Then R can be represented by an $m \times n$ Boolean matrix (or 0-1 matrix) $M_R = [m_{ij}]$, called the *matrix representation of* R, where

$$m_{ij} = \begin{cases} 1 \text{ or } T, & \text{if } (a_i, b_j) \in R, \\ 0 \text{ or } F, & \text{if } (a_i, b_j) \notin R. \end{cases}$$

The logical connectives $\wedge$ and $\vee$ can be applied to the Boolean matrix.

Relation (cont)

Example 3.3.16: Let $A = \{a, b, c, d, e, f\}$, $B = \{1, 2, 4, 5, 6\}$ and let $R = \{(a, 2), (a, 5), (b, 5), (b, 6), (c, 1), (c, 4), (e, 5), (f, 6)\}$ be the relation from A to B. Find the matrix representation of R.

Matrix representation

$$M_R = \begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 4 & 5 & 6 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Relation (cont)

Example 3.3.17: Let $M_R = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$ be the matrix representation of a relation R from $A = \{a, b, c\}$ to $B = \{1, 2, 3, 4\}$. Write down the set R.

Class Discussion.

Relation (cont)

Let $M_A = [a_{ij}]$ and $M_B = [b_{ij}]$ be an $m \times n$ Boolean matrices. Let $M_C = [c_{jk}]$ be an $n \times k$ Boolean matrix.

- The **meet** of M_A and M_B, $M_A \wedge M_B = [a_{ij} \wedge b_{ij}]$;
- The **join** of M_A and M_B, $M_A \vee M_B = [a_{ij} \vee b_{ij}]$;
- The **product** of M_A and M_C, $M_A \odot M_C = [\bigvee_j (a_{ij} \wedge c_{jk})]$

Note that $0 \wedge 0 = 0$, $0 \wedge 1 = 0$, $1 \wedge 0 = 0$, $1 \wedge 1 = 1$; $0 \vee 0 = 0$, $0 \vee 1 = 1$, $1 \vee 0 = 1$, $1 \vee 1 = 1$. We can regard $0 = F$, $1 = T$.

Relation (cont)

Let $R_1, R_2 \subset A \times B$, $R_3 \subset B \times C$.

- The matrix representation of $R_1 \cap R_2$, $M_{R_1 \cap R_2} = M_{R_1} \wedge M_{R_2}$;
- The matrix representation of $R_1 \cup R_2$, $M_{R_1 \cup R_2} = M_{R_1} \vee M_{R_2}$;
- The matrix representation of $R = \{(a, c) : \exists b(aR_1b \wedge bR_3c)\} \subset A \times C$, $M_R = M_{R_1} \odot M_{R_3}$;

Relation (cont)

When $A = B = S$, a relation $R \subset S \times S$ becomes a binary relation on the set S. The **directed graph (or digraph) representation** of R is a pair (S, R) where S is the set of **vertices** and R is the set of **edges**.

A generalisation is the **distance (or cost) matrix** contains information about distances of the edges. These concepts can be applied to websites connected by hyperlinks or cities connected by roads etc., in which case (unless the connection network is extremely dense) the matrices tend to be sparse, that is, contain few nonzero entries. Therefore, specifically tailored matrix algorithms can be used in network theory.

Properties of a Relation (cont)

A binary relation R on a set S has some properties which are abstracted from the equality and inequality properties of integers — reflexive, irreflexive, symmetric, asymmetric, antisymmetric and transitive.

Recall the properties of equality:

- reflexive: $x = x$;
- symmetric: if $x = y$ then $y = x$;
- transitive: if $x = y$ and $y = z$ then $x = z$.

Definition 3.3.18

A relation R on a set A is called *reflexive* if $(a, a) \in R$ (or aRa) for every $a \in A$.
A relation R on a set A is called *irreflexive* if $(a, a) \notin R$ for every $a \in A$.

Properties (cont)

Example 3.3.20: Let $A = \{1, 2, 3, 4, 5, 6\}$. Determine whether the following relations are reflexive and irreflexive.

1. $R_1 = \{(1, 1), (1, 2), (2, 2), (3, 3), (4, 4), (5, 5), (5, 6), (6, 6)\}$
2. $R_2 = \{(x, y) \in A \times A | x > y\}$
3. $R_3 = \{(1, 1), (1, 3), (2, 2)\}$

Class Discussion (using Excel? Python?).

Properties (cont)

Definition 3.3.21

Given a relation R on a set A.

1. R is called *symmetric* if when $(a, b) \in R$, $(b, a) \in R$.
2. R is called *asymmetric* if when $(a, b) \in R$, $(b, a) \notin R$.
3. R is called *antisymmetric* if when $(a, b) \in R$ and $(b, a) \in R$, $a = b$.

Remark: For a relation R on a set A, if R is symmetric, then M_R is a symmetric matrix. If R is asymmetric, then M_R is not symmetric about diagonal and its diagonal contains all 0's. If R is antisymmetric, then M_R is not symmetric about diagonal. Beware that not symmetric does not mean asymmetric or antisymmetric. However, asymmetric implies antisymmetric but not vice versa.

Properties (cont)

Example 3.3.23: Let $A = \{1, 2, 3, 4, 5, 6\}$. Determine whether the following relations are symmetric, asymmetric and anti-symmetric.

- $R_0 = \emptyset$
- $R_1 = \{(1, 2), (2, 1), (2, 3), (3, 2), (3, 4), (5, 5)\}$.
- $R_2 = \{(1, 2), (2, 1), (2, 4), (3, 4), (4, 2), (4, 3), (5, 6), (6, 5), (6, 6)\}$.
- $R_3 = \{(a, b) \in A \times A : a > b\}$.

Class Discussion (using Excel? Python?).

Properties (cont)

Definition 3.3.24

A relation on R on a set A is *transitive* if whenever $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$.

A relation R on a set A is *not transitive* if there exist $a, b, c \in A$ such that $(a, b) \in R$ and $(b, c) \in R$ but $(a, c) \notin R$.

If R is transitive, then the matrix representation M_R has the property if $m_{ij} = 1$ and $m_{jk} = 1$ then $m_{ik} = 1$. An easy way to identify transitive property is to calculate M_R^2: If every non-zero element in the matrix $M_R^2 = M_R \odot M_R$ $(m_{ij} = 1 \wedge m_{jk} = 1)$ corresponds to a non-zero element in M_R $(m_{ik} = 1)$, then R is transitive.

Properties (cont)

Example 3.3.26: Let $A = \{1, 2, 3, 4, 5\}$ and R_i, $i = 1, 2, 3, 4$ be relations on A. Determine whether the following relations are transitive.

- $R_1 = \{(1, 1), (1, 2), (2, 1), (3, 4), (3, 5), (4, 5)\}$

Solution

By definition: R_1 is *not transitive* since $(2, 1) \in R_1$ and $(1, 2) \in R_1$ but $(2, 2) \notin R_1$.

By matrix representation:

$$M_{R_1} = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{pmatrix} 1 & \boxed{1} & 0 & 0 & 0 \\ 1 & \boxed{0} & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array} \quad M_{R_1}^2 = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{pmatrix} 2 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array} = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{pmatrix} 1 & \boxed{1} & 0 & 0 & 0 \\ 1 & \boxed{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

Properties (cont)

Example 3.3.26 (cont):

- $R_2 = \{(1,2),(3,4)\}$

Solution

R_2 is transitive since there are no elements a, b and c in A such that $(a,b) \in R_2$ and $(b,c) \in R_2$, but $(a,c) \notin R_3$.

We can also show this by comparing $M^2_{R_2}$ to M_{R_2}:

$$M_{R_2} = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array} \quad M^2_{R_2} = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}.$$

Since there is no non-zero element in $M^2_{R_2}$ corresponding to the non-zero element in M_{R_2}, R_2 is transitive.

Properties (cont)

Example 3.3.26 (cont):

- $R_3 = \{(1,2),(1,3),(1,4),(4,4)\}$
- $R_4 = \{(1,2),(2,1),(2,2),(2,3),(3,2)\}$

Class Discussion (using Python? Octave? Julia?).

Outline

Closures of Binary Relations (cont)

For a set $A = \{1, 2, 3\}$, if we are considering the addition on A, we find that $1 + 3$ gives 4, which not inside A.

This kind of situation is said to be **not closed**.

By adding enough elements into A, we can form $\overline{A} = \{1, 2, 3, 4, \cdots\}$ which is closed for addition. Any two numbers adding together is still in A.

With the same logic, we wish to turn some relations which are not "closed" with respect to the properties mentioned earlier such as reflexive, symmetric etc. to have a "closed" binary relation.

Closures of Binary Relations

A binary relation R may not be symmetric, but R is always contained in some symmetric relation R^{sym}. This is because we can add symmetric elements into R until we get the **smallest** relation R^{sym} is symmetric closure.

Again, a binary relation R may not be transitive but it is always contained in some transitive relation R^{tr}, which the smallest R^{tr} is called the **transitive closure**.

Closures of Binary Relations (cont)

In the theory of rewriting systems (https://en.wikipedia.org/wiki/Rewriting), one often uses more wordy notions such as the reflexive transitive closure R^* — the smallest preorder containing R, or the reflexive transitive symmetric closure $R^{\equiv}$ — the smallest equivalence relation containing R, and therefore also known as the **equivalence closure**.

When considering a particular term algebra (https://en.wikipedia.org/wiki/Term_algebra), an equivalence relation that is compatible with all operations of the algebra is called a congruence relation. The **congruence closure** of R is defined as the smallest congruence relation containing R.

Closures of Binary Relations (cont)

For arbitrary property P and relation R, the P **closure of** R **need not exist**.
The properties reflexivity, transitivity and symmetry are **closed under arbitrary intersections**. In such cases, the P closure can be directly defined as the intersection of all sets with property P containing the relation R.

Closures of Binary Relations (cont)

Some important particular closures can be constructively obtained as follows:

- $cl_{ref}(R) = R \cup \{(x, x) : x \in S\}$ is the reflexive closure of R,
- $cl_{sym}(R) = R \cup \{(y, x) : (x, y) \in R\}$ is its symmetric closure,
- $cl_{trn}(R) = R \cup \{(x_1, x_n) : n > 1 \wedge (x_1, x_2), \ldots, (x_{n-1}, x_n) \in R\} = \bigcup_{i=1}^{n} R^i$ is its transitive closure,
- $cl_{emb,\Sigma}(R) = R \cup \{\langle f(x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n), f(x_1, \ldots, x_{i-1}, y, x_{i+1}, \ldots, x_n)\rangle : \langle x_i, y\rangle \in R \wedge f \in \Sigma n\text{-ary} \wedge 1 \leq i \leq n \wedge x_1, \ldots, x_n \in S\}$ is its embedding closure with respect to a given set Σ of operations on S, each with a fixed arity.

The relation R is said to **have closure under some** cl_{xxx}, if $R = cl_{xxx}(R)$; for example R is called symmetric if $R = cl_{sym}(R)$.

Closures of Binary Relations (cont)

Any of the four closures preserves symmetry, i.e., if R is symmetric, so is any $cl_{xxx}(R)$. Similarly, all four preserve reflexivity. Moreover, cl_{trn} preserves closure under $cl_{emb,\Sigma}$ for arbitrary Σ. As a consequence, the equivalence closure of an arbitrary binary relation R can be obtained as

$$cl_{trn}(cl_{sym}(cl_{ref}(R))),$$

and the congruence closure with respect to some Σ can be obtained as

$$cl_{trn}(cl_{emb,\Sigma}(cl_{sym}(cl_{ref}(R)))).$$

Closures of Binary Relations (cont)

In the latter case, the nesting order does matter; e.g. if S is the set of terms over $\Sigma = \{a, b, c, f\}$ and $R = \{\langle a, b\rangle, \langle f(b), c\rangle\}$, then the pair $\langle f(a), c\rangle$ is contained in the congruence closure $cl_{trn}(cl_{emb,\Sigma}(cl_{sym}(cl_{ref}(R))))$ of R, but not in the relation $cl_{emb,\Sigma}(cl_{trn}(cl_{sym}(cl_{ref}(R))))$.

Transitive Closure

The **intersection** of two transitive relations is transitive.

The **union** of two transitive relations need not be transitive. To preserve transitivity, one must take the transitive closure. This occurs, for example, when taking the union of two equivalence relations or two preorders. To obtain a new equivalence relation or preorder one must take the transitive closure (reflexivity and symmetry — in the case of equivalence relations — are automatic).

Transitive Closure (cont)

In computer science, the concept of transitive closure can be thought of as constructing a data structure that makes it possible to answer reachability questions. That is, can one get from node a to node d in one or more hops? A binary relation tells you only that node a is connected to node b, and that node b is connected to node c, etc. After the transitive closure is constructed, in an $O(1)$ operation one may determine that node d is reachable from node a. The data structure is typically stored as a matrix $M_R^2 \vee M_R^3 \vee \cdots$.

The transitive closure of the adjacency relation of a directed acyclic graph (DAG) is the reachability relation of the DAG and a strict partial order.

Transitive Closure (cont)

In logic, the transitive closure of a binary relation cannot solely be expressed in first-order logic (FO). This means that one cannot write a formula using predicate symbols R and T that will be satisfied in any model iff T is the transitive closure of R. In finite model theory, first-order logic (FO) extended with a transitive closure operator is usually called transitive closure logic, and abbreviated FO(TC) or just TC. TC is a sub-type of fixpoint logics. The fact that FO(TC) is strictly more expressive than FO was discovered by Ronald Fagin in 1974; the result was then rediscovered by Alfred Aho and Jeffrey Ullman in 1979, who proposed to use fixpoint logic as a database query language.

Transitive Closure (cont)

Efficient transitive closure computation has been recognised as a significant sub-problem in evaluating recursive database queries, since almost all practical recursive queries are transitive.

According to https://en.wikipedia.org/wiki/Transitive_closure, since the 1980s Oracle Database has implemented a proprietary SQL extension CONNECT BY... START WITH that allows the computation of a transitive closure as part of a declarative query. The SQL 3 (1999) standard added a more general WITH RECURSIVE construct also allowing transitive closures to be computed inside the query processor; as of 2011 the latter is implemented in IBM DB2, Microsoft SQL Server, Oracle, and PostgreSQL.

Datalog (mentioned in Logic) also implements transitive closure computations.

Transitive Closure (cont)

Naïve Algorithm

Let A be the the matrix representation of the binary relation R of a finite set S of n elements. The matrix representation of the transitive closure is

$$A^+ = A \vee A^2 \vee \cdots \vee A^n.$$

However, this is very computationally inefficient.

The Warshall's algorithm is a more efficient algorithm.

Transitive Closure (cont)

Warshall's Algorithm

Let n be the number of elements in the set A and M_R be the matrix representation of the relation R.

- Create a copy of the original matrix: $M := M_R$
- for k=1,...,n
  - for i=1,...,n
    - if $i \neq k$ and $M_{ik} \neq 0$:
      $M_{ij} := M_{ij} \vee M_{kj}$

Transitive Closure (cont)

Example 4.1.13: Given $S = \{1, 2, 3, 4\}$ and $R = \{(1, 2), (2, 1), (2, 3), (3, 4)\}$. Find the transitive closure of R.

Solution

The matrix representation of R is

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Transitive Closure (cont)

Solution of Example 4.1.13:

Step 1:
$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Step 2:
$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Transitive Closure (cont)

Solution of Example 4.1.13 cont

Step 3:

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Step 4:

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Transitive Closure (cont)

Given a set $S = \{1, 2, 3, 4, 5\}$ and a relation $R = \{(1,1), (1,2), (2,1), (2,2), (3,3), (3,4), (4,3), (4,4), (4,5), (5,4), (5,5)\}$ on R. Find $cl_{trn}(R)$ using the Warshall's Algorithm.

Answer

$$M_{cl_{trn}(R)} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Exercise: Let see if we can get the answer.

Outline

Equivalence Relations

Equivalence relation is the **generalisation** of the equality (recall the three properties of equality mentioned in Slide 21).

Definition 3.3.27

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

Question: Is the inequality relation "$<$" an equivalence relation on A? Justify your answer.

Equivalence Relations (cont)

Definition 3.3.30

Let R be an equivalence relation on a set A and let $a \in A$. The set of all elements that related to a, is called the *equivalence class of* a. It is denoted as

$$[a] \text{ or } \overline{a} = \{x \in A | (x, a) \in R\}.$$

The set of all the distinct equivalence classes of R form a set A/R, called the ***quotient*** *set of* A or the *partition* of A.

Relation (cont)

Example (Finite Set): Let $A = \{a, b, c, d, e, f, g\}$ and $R = \{(a, a), (a, b), (b, a), (b, b), (c, c), (c, d), (d, c), (d, d), (e, e), (e, f), (e, g), (f, e), (f, f), (f, g), (g, e), (g, f), (g, g)\}$. Find the equivalence class of each element in A and the quotient set A/R.

Solution

The equivalence class of

- a, b is $\{a, b\}$
- c, d is $\{c, d\}$
- e, f, g is $\{e, f, g\}$

The quotient set $A/R = \{\{a, b\}, \{c, d\}, \{e, f, g\}\}$

Equivalence Relations (cont)

Example 3.3.31: Let $A = \{1, 2, 3, 4\}$ and $R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (4, 4)\}$ be an equivalence relation on A. Find the equivalence class of each element in A and the quotient set A/R.

Class Discussion.

Equivalence Relations (cont)

Example 3.3.29: Let $A = \mathbb{Z}$ and R be the relation on A defined by $aRb = a + b$ is even. Show that R is an equivalence relation.

Proof: To prove equivalence, we need to show all THREE properties are satisfied

- $a + a = 2a$ is even, so $(a, a) \in R$. R is reflexive.
- If $a + b$ is even then $b + a$ is also even. Thus $(a, b) \in R \Rightarrow (b, a) \in R$. So R is symmetric.
- Let $a, b, c \in A$. Let $(a, b) \in R$ and $(b, c) \in R$, then $a + b = 2k_1$ and $b + c = 2k_2$ for some integer k_1 and k_2. Then $a + c = 2k_1 + 2k_2 - 2b = 2(k_1 + k_2 - b)$ is even. So R is transitive.

Hence R is an equivalence relation.

Equivalence Relations (cont)

Example 3.3.29 (cont): Very abstract.

To make it more concrete, we have introduce R on $A = \mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$.

0R0, 0R2, 0R4, ...
Unfolding: It just means 0+0 is even, 0+2 is even, 0+4 is even, ...
Similarly for the following cases:
0R(-2), 0R(-4), ...

1R1, 1R3, 1R5, ...
1R(-1), 1R(-3), 1R(-5), ...

The quotient

$$A/R = \{[0],\ [1]\} = \{\{0, \pm 2, \pm 4, \dots\},\ \{\pm 1, \pm 3, \pm 5, \dots\}\}$$

Equivalence Relations (cont)

Example 3.4.6: Let $A = \mathbb{Z}^+$ and R be the relation on A defined by

$$R = \{(x, y) \in A \times A | x - y \mod 3 = 0\}.$$

Find the equivalence class (called the "modulus" or "modular numbers") of each element in A and the quotient set of A.

Solution

1. Since
   - for all $x, y \in \{1, 4, 7, 10, \cdots\}$, $x - y \mod 3 = 0$;
   - for all $x, y \in \{2, 5, 8, 11, \cdots\}$, $x - y \mod 3 = 0$;
   - for all $x, y \in \{3, 6, 9, 12, \cdots\}$, $x - y \mod 3 = 0$;

Equivalence Relations (cont)

Example 3.4.6 (cont):

Solution

1. we have

$$[1] = \{1, 4, 7, 10, \cdots\} = [4] = [7] = \cdots = [3k - 2]$$
$$[2] = \{2, 5, 8, 11, \cdots\} = [5] = [8] = \cdots = [3k - 1]$$
$$[3] = \{3, 6, 9, 12, \cdots\} = [6] = [9] = \cdots = [3k]$$

   where $k = 1, 2, \cdots$.

2. So there are only three distinct equivalent classes of R, and hence $A/R = \{[1], [2], [3]\}$.

Alternative answer: $A/R = \{[0], [1], [2]\}$.

Equivalence Relations (cont)

Remark: Example 3.4.6 is just a special case of the fact that the congruence modulo n (Topic 2) is an equivalence relation.

- reflexive: For any $x \in \mathbb{Z}$, $x \equiv x \pmod{n}$;
- symmetric: For any $x, y \in \mathbb{Z}$, if $x \equiv y \pmod{n}$, then $y \equiv x \pmod{n}$;
- transitive: For any $x, y, z \in \mathbb{Z}$, if $x \equiv y \pmod{n}$ and $y \equiv z \pmod{n}$, then $x \equiv z \pmod{n}$.

The quotient $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\equiv_n$ is $\{[0], [1], \cdots, [n-1]\}$
or more concretely

$$
\begin{aligned}
[0] &= \{0, \pm n, \pm 2n, \cdots\} = n\mathbb{Z} \\
[1] &= \{1, \pm n + 1, \pm 2n + 1, \cdots\} = n\mathbb{Z} + 1 \\
&\cdots \\
[n-1] &= \{n-1, \pm n + (n-1), \pm 2n + (n-1), \cdots\} = n\mathbb{Z} + (n-1)
\end{aligned}
$$

Equivalence Relations (cont)

Q: How do mathematicians construct new mathematical objects from know mathematical objects?

A: Mostly using **set product** (Slide 4), **set quotient** (Slide 49), **subset** and **set union**.

Q: How is the set of integers $\mathbb{Z}$ constructed?

A: Assume we have a natural number set $\mathbb{N}$. The integer set $\mathbb{Z}$ is defined as the quotient set $(\mathbb{N} \times \mathbb{N})/\sim$ with

$$(m_1, n_1) \sim (m_2, n_2) \equiv m_1 + n_2 = m_2 + n_1$$

where $m_1, m_2, n_1, n_2 \in \mathbb{N}$. So $0 = \{(i, i) : i \in \mathbb{N}\}$, $1 = \{(i+1, i) : i \in \mathbb{N}\}$, $-1 = \{(i, i+1) : i \in \mathbb{N}\}$, etc.

Equivalence Relations (cont)

Q: How do mathematicians construct the set of rational numbers $\mathbb{Q}$?

A: $\mathbb{Q} = \mathbb{Z} \times \mathbb{Z}/\sim$ where

$$(p_1, q_1) \sim (p_2, q_2) \equiv p_1 q_2 = p_2 q_1.$$

So $0 = \{(0, i) : i \in \mathbb{Z}$, $\frac{1}{2} = \{(i, 2i) : i \in \mathbb{Z}$, etc.

Q: How do mathematicians construct the set of real numbers $\mathbb{R}$?

A: Complicated. Refer to `https://en.wikipedia.org/wiki/Construction_of_the_real_numbers`

1. Equivalent Cauchy sequence
2. Dedekind cuts
3. ... less popular.

Equivalence Relations (cont)

Q: How do we construct $\mathbb{R}^n$?
A: By set product $\mathbb{R}^n = \mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R}$.

Q: How do we construct something complex, like a circle?
A: By taking subset. E.g.
$S^1 = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 - 1 = 0\}$. In general,
$S = \{(x_1, ..., x_n) \in \mathbb{R}^n : f_j(x_1, \cdots, x_n) = 0, j = 1, ..., m\}$.

Equivalence Relations (cont)

There is a group of mathematicians called the topologists, who use equivalence relation on various sets to **glue** points together. A little bit like how a sculptor makes sculptures.

If X is a topological space, gluing the points x and y in X means considering the quotient space obtained from the equivalence relation $a \sim b$ iff $a = b$ or $a = x, b = y$ (or $a = y, b = x$).

Consider $[0, 1]$ and the equivalence relation $\sim$ such that $0 \sim 1$ while $x \sim x$ for $0 < x < 1$, then $[0, 1]/\sim$ is homeomorphic to the circle S^1.

Equivalence Relations (cont)

Consider the unit square $I^2 = [0,1] \times [0,1]$ and the equivalence relation $\sim$ generated by the requirement that all boundary points be equivalent, thus identifying all boundary points to a single equivalence class. Then $I^2/\sim$ is homeomorphic to the sphere S^2.

More generally, suppose X is a space and A is a subspace of X. One can identify all points in A to a single equivalence class and leave points outside of A equivalent only to themselves. The resulting quotient space is denoted X/A (as an abbreviation of X/R).

Equivalence Relations (cont)

Consider the set $\mathbb{R}$ of real numbers with the ordinary topology, and write $x \sim y$ iff $x - y \in \mathbb{Z}$. Then the quotient space $X/\sim$ is homeomorphic to the unit circle S^1 via the homeomorphism which sends the equivalence class of x to $\exp(2\pi ix)$.

A generalisation of the previous example is the following: Suppose a topological group G acts continuously on a space X. One can form an equivalence relation on X by saying points are equivalent iff they lie in the same orbit. The quotient space under this relation is called the **orbit space**, denoted X/G.

Equivalence Relations (cont)

Remark: I have skipped the "topology" of the set X which are fundamental. Refer to `https://en.wikipedia.org/wiki/Topological_space` for details.

There are YouTube videos on these, but mostly boring mathematics. It is difficult to create pretty video explaining how to use set product, set quotient, etc. to create new mathematical objects called manifolds.

https://www.youtube.com/watch?v=lmcT2mP2bfE
(These changed how I think about higher dimensions)

Equivalence Relations (cont)

There are many equivalence relations which are "impossible" to visualise.

Example: https://en.wikipedia.org/wiki/Projective_space

A **projective space** $\mathbb{P}(\mathbb{R}^n)$ of dimension n is the quotient set of $\mathbb{R}^{n+1} \setminus \{0\}$ by the equivalence relation "being on the same vector line", i.e. $x \sim y$ if there is a nonzero element $\lambda \in \mathbb{R}$ such that $x = \lambda y$.

A generalisation of projective space is the Grassmannian $Gr(k, \mathbb{R}^n)$ which is a set that parameterises all k-dimensional linear subspaces of the n-dimensional vector space $\mathbb{R}^n$. When $k = 1$, $Gr(1, \mathbb{R}^n)$ is the projective space $\mathbb{P}(\mathbb{R}^{n-1})$

Equivalence Relations (cont)

There are many equivalence relations where the quotient is **impossible** to describe such as the logical equivalence relation: Let ϕ, ψ, ξ be any propositions.

- $\phi \leftrightarrow \phi$, therefore $\phi \equiv \phi$ and $\equiv$ is reflexive;
- If $\phi \equiv \psi$, then $\phi \leftrightarrow \psi$ is a tautology, then $\phi \leftrightarrow \psi$ is a tautology, therefore $\psi \equiv \phi$ and $\equiv$ is symmetric.
- If $\phi \equiv \psi$ and $\psi \equiv \xi$, then $\phi \rightarrow \psi$, $\phi \leftarrow \psi$, $\psi \rightarrow \xi$, $\psi \leftarrow \xi$ are tautologies, then $\phi \rightarrow \xi$ and $\phi \leftarrow \xi$ by modus ponens and $\phi \leftrightarrow \xi$ is a tautology, therefore $\phi \equiv \xi$ and $\equiv$ is transitive.

However, the quotient of all propositions under logical equivalence is **too complex** to describe.

Outline

Partial Order Relations

The partial order relation is a **generalisation** of the **inequality** $\leq$, which satisfies the following three properties:

- reflexive: $x \leq x$;
- anti-symmetric: if $x \leq y$ and $y \leq x$ then $x = y$;
- transitive: if $x \leq y$ and $y \leq z$ then $x \leq z$.

Definition 3.3.32

A relation R on a set A is called a ***partial order*** if R is reflexive, anti-symmetric and transitive.
The set A together with the partial order R, (A, R), is called a ***partially ordered set***, or ***poset***. Note that a poset is often denoted as $(A, \preceq)$. Here, $\preceq$ are used to denote partial order relation.

Partial Order Relations (cont)

Typical examples of partial order relation and posets:

- $\subset$ and $(P(S), \subset)$
- $\leq$ and $(\{1, 2, 3\}, \leq)$
- $\geq$ and $(\{1, 2, 3\}, \geq)$
- $\leq$ and $(\mathbb{Z}, \leq)$
- $\geq$ and $(\mathbb{Z}, \geq)$
- $\leq$ and $(\mathbb{R}, \leq)$
- $\geq$ and $(\mathbb{R}, \geq)$

Note: $(\mathbb{Z}, <)$ and $(\mathbb{Z}, >)$ are **not** posets since the relations "$<$" and "$>$" are not reflexive: $1 \not< 1$ and $1 \not> 1$.

Partial Order Relations (cont)

The 'integral divisibility' is also a partial order relation.

Example 3.3.35: Show that $(\mathbb{Z}^+, |)$ a poset.

Proof

- The relation $|$ is reflexive because any positive integer divides itself.
- Note that if $a|b$ and $b|a$ then $a = \pm b$. Since $a, b \in \mathbb{Z}^+$, the negative sign will not happen and $a = b$. So the relation $|$ is antisymmetric.
- The relation $|$ is transitive because $a|b \Rightarrow b = k_1 a$, $b|c \Rightarrow c = k_2 b$, therefore $c = k_2 k_1 a \Rightarrow a|c$.

Hence the relation of divisibility $|$ is a partial order and $(\mathbb{Z}^+, |)$ is a poset.

Partial Order Relations (cont)

Observations on Example 3.3.35: In $(\mathbb{Z}^+, |)$, $\preceq$ is $|$:

- $2|4$, therefore $2 \preceq 4$
- $2|6$, therefore $2 \preceq 6$
- $4 \nmid 6$, therefore $4 \not\preceq 6$
- $6 \nmid 4$, therefore $6 \not\preceq 4$

Note that **neither** $4 \preceq 6$ **nor** $6 \preceq 4$, we say that 4 and 6 are **incomparable** in $(\mathbb{Z}^+, \preceq)$.

Definition

In a poset $(A, \preceq)$, for any $a, b \in A$, if neither $a \preceq b$ nor $b \preceq a$, then a and b are said to be **incomparable**.

Partial Order Relations (cont)

Definition

We say $a \prec b$ if $a \preceq b$ and $a \neq b$. Similarly, $a \succ b$ if $a \succeq b$ and $a \neq b$.

Definition

Given a poset $(A, \preceq)$. For $a \in A$,

- If there is no $b \in A$ such that $b \prec a$, we say that a is a **minimal element of** A.
- There is some $b \in A$ so that $b \prec a$ and there is no $c \in A$ so that $b \prec c \prec a$. We say that b is an **immediate predecessor of** a.
- If there is no $b \in A$ such that $a \prec b$, we say that a is a **maximal element (of** A**)**.
- There is some $b \in A$ so that $a \prec b$ and there is no $c \in A$ so that $a \prec c \prec b$. We say that b is an **immediate successor of** a.

Partial Order Relations (cont)

Again, observations on Example 3.3.35: In $(\mathbb{Z}^+, |)$:

- 1 is the minimal element of $\mathbb{Z}^+$ because $1|a$, $a \in \mathbb{Z}^+$.
- 1 is the immediate predecessor of any prime number
- 2 is the immediate predecessor of 4, 6 but not 8 because $2 \prec 4 \prec 8$; 4 is the immediate successor of 2, 6 is the immediate successor of 2 and 3, etc.
- There is not maximal element in $\mathbb{Z}^+$

There are posets special elements mentioned in the previous slide, E.g. in $(\mathbb{Q}, \leq)$, there is no min, max and any $a \in \mathbb{Q}$ does not have immediate predecessor or successor.

Partial Order Relations (cont)

A special case of poset is chain.

Definition 3.3.36

A *total order* or *linear order* is a binary relation (here denoted by infix $\preceq$) on some set A which is transitive, antisymmetric, and total, i.e. for all $x, y, z \in A$:

- If $x \preceq y$ and $y \preceq x$ then $x = y$ (antisymmetry);
- If $x \preceq y$ and $y \preceq z$ then $x \preceq z$ (transitivity);
- $x \preceq y$ or $y \preceq x$ (totality).

A set paired with a total order (A, R) is called a *totally ordered set*, a *linearly ordered set*, or a *chain*.

Example 3.3.37: $(\mathbb{Z}, \leq)$ and $(\mathbb{Z}, \geq)$ are chains.

Partial Order Relations (cont)

Partial orders form a natural setting for increasing and decreasing functions.

Definition

Given two posets $(A, \preceq_A)$ and $(B, \preceq_B)$, a function, $f : A \to B$, is

- **increasing** (, monotonic or order-preserving) if for all $a, b \in A$, $a \preceq_A b \Rightarrow f(a) \preceq_B f(b)$.

  When $\preceq$ is changed to $\prec$, we call f **strictly increasing**.

- **decreasing** if for all $a, b \in A$, $a \preceq_A b \Rightarrow f(b) \preceq_B f(a)$.

  When $\preceq$ is changed to $\prec$, we call f **strictly decreasing**.

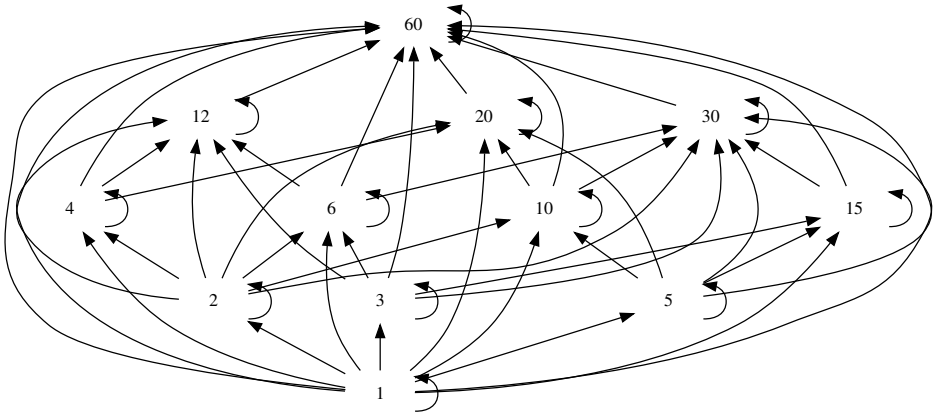
Partial Order Relations (cont)

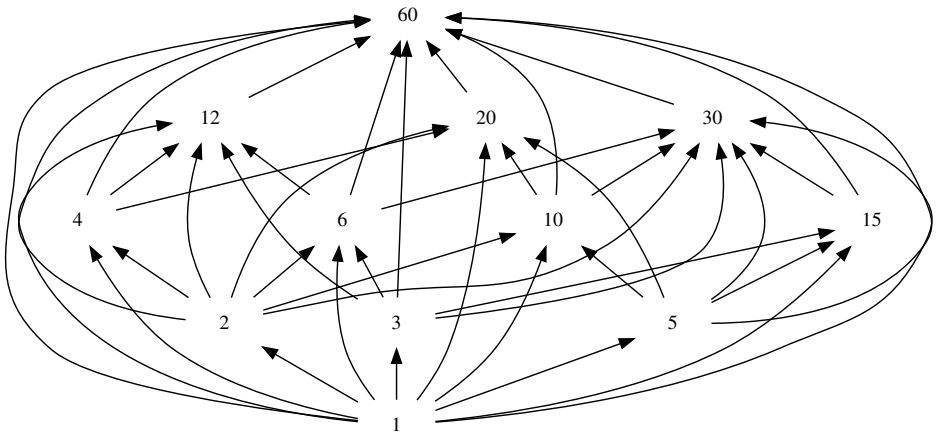
A digraph (Slide 20) that contains no sequence of edges leading back to its starting point is called a **directed acyclic graph** or **DAG**.

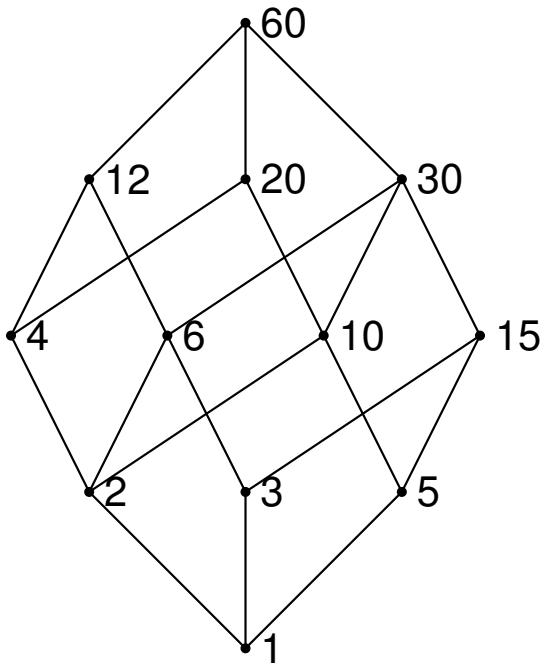
A **Hasse diagram** is a "reduced" DAG to represent the **transitive reduction**. For a finite poset $(S, \preceq)$, one represents each element of S as a vertex in the plane and draws a line segment or curve that goes upward from x to y whenever $x \preceq y$ and there is no z such that $x \preceq z \preceq y$. These curves may cross each other but must not touch any vertices other than their endpoints. Such a diagram, with labelled vertices, uniquely determines its partial order.

Partial Order Relations (cont)

Example: (Set of divisors of 60, division) is a poset. Sketch the digraph representation, DAG and Hasse diagram.





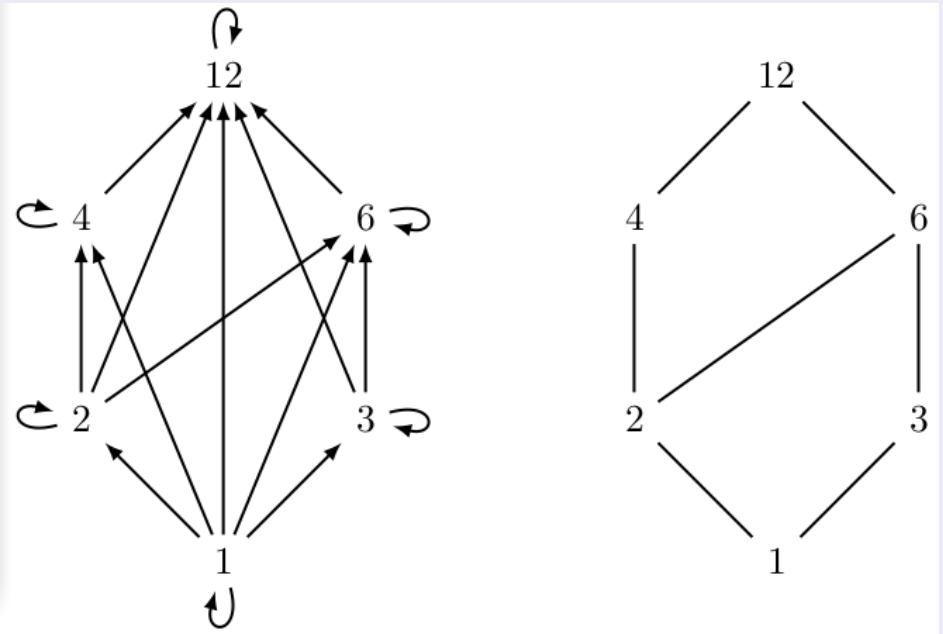


Partial Order Relations (cont)

Example: (Set of divisors of 12, division), i.e. $(\{1, 2, 3, 4, 6, 12\}, |)$ is a poset. Sketch the digraph representation and the Hasse diagram.

Solution

$| = \{(1,1), (1,2), (1,3), (1,4), (1,6), (1,12), (2,2), (2,4), (2,6), (2,12), (3,3), (3,6), (3,12), (4,4), (4,12), (6,6), (6,12), (12,12)\}$



Partial Order Relations (cont)

Example (Abstract from English dictionary?): Let Σ be some **alphabet** and consider the set

$$\Sigma^* = \Sigma^0 \cup \Sigma^1 \cup \Sigma^2 \cup \cdots$$

of all **finite words** drawn from Σ.
Given two words x and y, we define

$$x \preceq y \equiv x \text{ is a prefix of } y,$$

i.e. if there is some word z such that $xz = y$.
$(\Sigma^*, \preceq)$ can be proved to be a poset.

Partial Order Relations (cont)

Method 1 of constructing new poset from two posets $(A, \preceq_A)$ and $(B, \preceq_B)$.

Define $\preceq$ on $A \times B$ to be

$$(a, b) \preceq (a', b') \equiv a \preceq_A a' \text{ and } b \preceq_B b'.$$

It can be proved that $\preceq$ is a partial order. The poset $(A \times B, \preceq)$ defined in this way is called the **product poset** of A and B.

Partial Order Relations (cont)

Method 2 of constructing new poset from two posets $(A, \preceq_A)$ and $(B, \preceq_B)$.
Define $\preceq$ on $A \times B$ to be

$$(a, b) \preceq (a', b') \equiv (a \preceq_A a') \vee (a = a' \wedge b \preceq_B b).$$

It is a partial order on $A \times B$ called the **lexicographic order**.
The useful property of lexicographic order (lex order for short) is that if the original partial orders are total, so is the lex order: this is why dictionary-makers use it. This also gives a source of very difficult-to-visualise total orders, like lex order on $\mathbb{R} \times \mathbb{R}$, which looks like the classic real number line where every point is replaced by an entire copy of the reals.

Outline

General Overview

Q: Why do we need to learn logic?

A: To build a structured knowledge, which **starts** from 'simple', 'basic' formal characterisation of mathematical objects to obtain **advanced** description of mathematical objects.

General Overview

In this course, we have covered the following mathematical objects:

- FOL formulas such as $\forall x P(x, y)$ and FOL sentences (quantified statements) $\exists x \exists y (Q(x, y) \wedge R(x, y))$
- $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}/\equiv_n$: the advanced description is 'unique factorisation theorem' for $\mathbb{Z}$ & $\sqrt{2}$ is irrational. Note: Early mathematicians believed all numbers are rational.
- Set operations are similar to logic in many ways: $\cap$ vs $\wedge$, $\cup$ vs $\vee$, - vs $\sim$.

General Overview (cont)

Q: Is logic the core of mathematics?

A: No! Mathematics = logic reasoning + mathematical object characterisation.

Q: Why is logic reasoning important?
A: Because naive set theory has a serius flaw: All sets can be described by some predicate $P(x)$:

$$S = \{x : P(x)\}.$$

Example: $S = \{x : x is an even integer.\} = \{0, \pm 2, \pm 4, ...\}$
Bertrand Russell consider the following set:

$$S = \{x : x \notin x\}$$

General Overview (cont)

Q: Is $S \in S$?

Bertrand Russell discovered that

- For any proposition p, $p \vee \sim p \equiv T$ and $p \wedge \sim p \equiv F$, $\sim\sim p \equiv p$ (we learned them in the first topic).
- Let p be the proposition '$S \in S$'.
- By $\sim\sim p \equiv p$, either $S \in S$ (Case 1) or $S \notin S$ (Case 2) but not both.
- Let $P(x)$ be '$x \notin x$'.
  - Case 1: $S \in S \Rightarrow P(S) \Rightarrow S \notin S$
  - Case 2: $S \notin S \Rightarrow P(S) \Rightarrow S \in S$

  In either case, we have $T \rightarrow F$. Naive set theory is contradicting!

General Overview (cont)

The Russell's paradox which arrises in naïve set theory leads to the development of "Axiomatic Set Theory" with

- Zermelo-Fraenkel Set Theory (with/without Axiom of Choice)

as the standard. The following are some variations:

- von Neumann-Gödel-Bernays-Gödel (NBG) class theory
- Tarski-Grothendieck set theory
- Constructive Set Theory

General Overview (cont)

The ZFC axioms governing how sets are constructed:

1. Axiom of extensionality: Two sets are equal (are the same set) if they have the same elements.

$$\forall x \forall y [\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y].$$

2. Axiom of regularity (or axiom of foundation): Every non-empty set x contains a member y such that x and y are disjoint sets.

$$\forall x [\exists a (a \in x) \rightarrow \exists y (y \in x \wedge \neg \exists z (z \in y \wedge z \in x))].$$

General Overview (cont)

The ZFC axioms (cont):

3. Axiom schema of specification (also called the axiom schema of separation or of restricted comprehension): Let ϕ be any formula in the language of ZFC with all free variables among $x, z, w_1, \ldots, w_n$ (y is not free in ϕ). Then:

$$\forall z \forall w_1 \forall w_2 \ldots \forall w_n \exists y \forall x [x \in y \Leftrightarrow ((x \in z) \wedge \phi)].$$

4. Axiom of pairing: If x and y are sets, then there exists a set which contains x and y as elements.

$$\forall x \forall y \exists z ((x \in z) \wedge (y \in z)).$$

General Overview (cont)

The ZFC axioms (cont):

5. Axiom of union: The union over the elements of a set exists.

$$\forall \mathcal{F}\, \exists A\, \forall Y\, \forall x[(x \in Y \wedge Y \in \mathcal{F}) \Rightarrow x \in A].$$

6. Axiom schema of replacement: The image of a set under any definable function will also fall inside a set. Let ϕ be any formula in the language of ZFC whose free variables are among $x, y, A, w_1, \ldots, w_n$, so that in particular B is not free in ϕ. Then:

$$\forall A \forall w_1 \forall w_2 \ldots \forall w_n \Big[\forall x(x \in A \Rightarrow \exists! y\, \phi) \rightarrow$$
$$\exists B\, \forall x\Big(x \in A \Rightarrow \exists y(y \in B \wedge \phi)\Big)\Big].$$

General Overview (cont)

The ZFC axioms (cont):

7. Axiom of infinity: Let $S(w)$ abbreviate $w \cup \{w\}$, where w is some set. Then there exists a set X such that the empty set $\varnothing$ is a member of X and, whenever a set y is a member of X then $S(y)$ is also a member of X.

$$\exists X \left[\varnothing \in X \wedge \forall y(y \in X \Rightarrow S(y) \in X)\right].$$

8. Axiom of power set: for any set x, there is a set y that contains every subset of x:

$$\forall x \exists y \forall z[z \subseteq x \Rightarrow z \in y].$$

General Overview (cont)

The ZFC axioms (cont):

9. Well-ordering theorem: For any set X, there is a binary relation R which well-orders X. This means R is a linear order on X such that every nonempty subset of X has a member which is minimal under R.

Given axioms 1–8, there are many statements provably equivalent to axiom 9 (well-ordering theorem), the best known of which is the axiom of choice (AC), which goes as follows. Let X be a set whose members are all nonempty. Then there exists a function f from X to the union of the members of X, called a "choice function", such that for all $Y \in X$ one has $f(Y) \in Y$. Since the existence of a choice function when X is a finite set is easily proved from axioms 1–8, AC only matters for certain infinite sets. AC is characterised as nonconstructive because it asserts the existence of a choice set but says nothing about how the choice set is to be "constructed".

General Overview (cont)

Important mathematical objects and the modern mathematics:

- Finite sets and relations on finite sets leads to combinatorics (partitioning and counting) and graph theory.
- Any sets & operations & mapping between sets lead to modern (abstract) algebra
- $\mathbb{N}$, $\mathbb{Z}$ and $f : \mathbb{N} \to \mathbb{N}$ leads to Number Theory
- $\mathbb{R}$ and $f : \mathbb{R} \to \mathbb{R}$ leads to Calculus, ODE, PDE
- $\mathbb{C}$ and $f : \mathbb{C} \to \mathbb{C}$ leads to complex analysis
- Let $\mathscr{F}$ be the set of functions $f : \mathbb{R} \to \mathbb{R}$. $\mathscr{F}$ and $L : \mathscr{F} \to \mathbb{R}$ leads to linear functional analysis.
- Probability space & statistics