MA2185 Discrete Mathematics

1.1 Propositional Logic

Negation ¬p, Conjunction p ∧ q, Disjunction p ∨ q, Exclusive or p ⊕ q

Conditional statement p → q

p is called the **hypothesis** (or antecedent or premise) 假設/前提

q is called the **conclusion** (or consequence) 結論/結果

Biconditional statement p ↔ q

1.3 Propositional Equivalences

Always true, **tautology (重言式)** Always false, **contradiction(矛盾式)**

Neither a tautology nor contradiction, **contingency(可能式)**

Logically equivalent, p ≡ q, if p ↔ q is a tautology

De Morgan's Laws

$\neg(p \land q) \equiv \neg p \lor \neg q$

$\neg(p \lor q) \equiv \neg p \land \neg q$

1.4 Predicates and Quantifiers

Universal quantifier ∀, Existential quantification ∃

Counterexample 反例

$\neg \forall x P(x) \equiv \exists x \neg P(x)$

$\neg \exists x Q(x) \equiv \forall x \neg Q(x)$

1.6 Rules of Inference

命題邏輯 Logical Equivalences 邏輯等價, Rules of Inference 推理規則

2.1 Sets

a is element of set A, a ∈ A

$N = \{0, 1, 2, 3, ...\}$, *the set of natural numbers* 自然數

$Z = \{..., -2, -1, 0, 1, 2, ...\}$, *the set of integers* 整數

$Q = \{p/q \mid p \in Z,\ q \in Z,\ and\ q = 0\}$, *the set of rational numbers* 有理數

R, *the set of real numbers* 實數

C, *the set of complex numbers* 虛數

Closed interval $[a, b]$, open interval (a, b)

A and B are **equal** if and only if $\forall x(x \in A \leftrightarrow x \in B)$

Set A is **subset** of set B, $A \subseteq B$, $\forall x(x \in A \to x \in B)$

A ⊆ B and B ⊆ A, then A = B

For every set S, $\emptyset \subseteq S$ *and* $S \subseteq S$

S is **finite set**, n distinct elements, n is **cardinality (基數)** of |S|

Power set of S is the set of all subsets of the set S. denoted P(S)

e.g. $P(\{0, 1, 2\}) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}\}$

Cartesian product (笛卡爾積), $A \times B = \{(a, b) \mid a \in A \land b \in B\}$

Truth set, $\{x \in D \mid P\ (x)\}$

2.2 Set Operations

Union A ∪ B, Intersection A ∩ B, Difference A − B, Complement $\overline{A}$

$|A \cup B| = |A| + |B| - |A \cap B|$

Two sets are called disjoint if their intersection is the empty set.

2.3 Functions

[One-to-one, Injunction]

$f(a) = f(b)$ implies that a = b for all a and b in the domain of f.

$\forall a \forall b(f(a) = f(b) \rightarrow a = b),\ \forall a \forall b(a \neq b \rightarrow f(a) = f(b))$

[Onto, Surjection]

For every element b ∈ B there an element a ∈ A with $f(a) = b$

$\forall y \exists x(f(x) = y)$, where x is the domain and y is the codomain

[One-to-one correspondence, Bijection] Both one-to-one and onto

[Increasing] $f(x) \leq f(y)$, **[Strictly increasing]** $f(x) < f(y)$

[Decreasing] $f(x) \geq f(y)$, **[Strictly decreasing]** $f(x) > f(y)$

[Composition of functions] $(f \circ g)(a) = f(g(a))$

If f and g are injective/surjective, then f ∘ g is injective/surjective.

[Identity functions] $Id_A(a) = a$

[Inverse functions] $f : A \rightarrow B,\ f^{-1} : B \rightarrow A$

f is injective, $g \circ f = Id_A$, f is surjective, $f \circ g = Id_B$

f is bijective, $g \circ f = Id_A \ and \ f \circ g = Id_B$

Let f be a function from the set A to the set B. The **graph** of the function f is the set of ordered pairs {(a, b) | a ∈ A and f (a) = b}.

A **partial function** f from set A to set B is an assignment to each element a in a subset of A, called the domain of definition of f , of a unique element b in B. The sets A and B are called the **domain** and **codomain** of f , respectively. We say that f is undefined for elements in A that are not in the domain of definition of f . When the domain of definition of f equals A, we say that f is a **total function**

9.1 Relations and Their Properties

Let A and B be sets. A **binary relation** from A to B is a subset of A × B.

A **relation** on a set A is a relation from A to A

[Reflexive]

(a, a) ∈ R for every element a ∈ A,

$\forall a((a,\ a) \in R)$, where the universe of discourse is the set of all elements in A.

[Symmetric]

$(b,\ a) \in R$ whenever(a, b) ∈ R, for all a, b ∈ A

$\forall a \forall b((a,\ b) \in R \rightarrow (b,\ a) \in R)$

[Antisymmetric]

For all a, b ∈ A, if (a, b) ∈ R with a ≠ b, then (b, a) not ∈ R

if (a, b) ∈ R and (b, a) ∈ R, then a = b

$\forall a \forall b(((a,\ b) \in R \land (b,\ a) \in R) \rightarrow (a\ =\ b))$

[Transitive]

(a, b) ∈ R and (b, c) ∈ R, then (a, c) ∈ R, for all a, b, c ∈ A.

$\forall a \forall b \forall c(((a,\ b) \in R \land (b,\ c) \in R) \rightarrow (a,\ c) \in R)$

[Composite]

Let R is A to B and S is B to C. The composite of R and S is the relation consisting of ordered pairs (a, c), where a ∈ A, c ∈ C, and for which there exists an element b ∈ B such that (a, b) ∈ R and (b, c) ∈ S. We denote the composite of R and S by S ∘ R

$$R\ =\ \{(1,\ 1),\ (1,\ 4),\ (2,\ 3),\ (3,\ 1),\ (3,\ 4)\}$$
$$S\ =\ \{(1,\ 0),\ (2,\ 0),\ (3,\ 1),\ (3,\ 2),\ (4,\ 1)\}$$
$$S \circ R\ =\ \{(1,\ 0),\ (1,\ 1),\ (2,\ 1),\ (2,\ 2),\ (3,\ 0),\ (3,\ 1)\}$$

9.3 Representing Relations

matrix $M_R = [m_{ij}]$

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

R is symmetric if and only if $M_R = (M_R)^t$

R is antisymmetric relation that $m_{ij} = 0 \; or \; m_{ji} = 0 \; when \; i \neq j$

$$\mathbf{M}_{R_1 \cup R_2} = \mathbf{M}_{R_1} \vee \mathbf{M}_{R_2} \quad \text{and} \quad \mathbf{M}_{R_1 \cap R_2} = \mathbf{M}_{R_1} \wedge \mathbf{M}_{R_2}.$$

$$\mathbf{M}_{S \circ R} = \mathbf{M}_R \odot \mathbf{M}_S.$$

$$\mathbf{M}_{R^n} = \mathbf{M}_R^{[n]},$$

A **directed graph**, or **digraph**, consists of a set V of **vertices** (or **nodes**) together with a set E of ordered pairs of elements of V called **edges** (or **arcs**). The vertex a is called the **initial vertex** of the edge (a, b), and the vertex b is called the **terminal vertex** of this edge.

Symmetric: every edge we also have the reverse edge

Antisymmetric: which is not a loop, then we don’t have the reverse edge

Transitive: if two consecutive edges, then we also have“combination”

9.5 Equivalence Relations

[Equivalence] Reflexive, symmetric, and transitive

[Equivalent] Two elements a, b related by equivalence relation, denote a ~ b

[Equivalence Class]

The set of all elements that are related to an element a of A is called the equivalence class of a. Denoted by $[a]_R$

$[a]_R = \{ s \mid (a, s) \in R \}$

[Representative]

If $b \in [a]_R$, then b is called a representative of this equivalence class.

9.6 Partial Orderings

[Partial ordering] Reflexive, antisymmetric, and transitive

[Partially ordered set, Poset]

Set S with partial ordering R called partially ordered set, or poset, denoted (S, R)

<= denote relation in any poset, When a and b are elements of the poset (S, <=), it is not necessary that either a <= b or b <= a.

Elements a, b of poset (S, <=) called **comparable** if either a <= b or b <= a.

a and b are called **incomparable,** neither a <= b nor b <= a

When every two elements in set are comparable, relation called **total ordering**

If (S, <=) is poset and every two elements of S are comparable, S is called a **totally ordered** or **linearly ordered set**, and <= is called a **total order** or a **linear order**. A totally ordered set also called **chain**.

(S, <=) is **well-ordered set** if it is poset that <= is a total ordering and every nonempty subset of S has a least element.

[THE PRINCIPLE OF WELL-ORDERED INDUCTION]

S is a well-ordered set. Then P (x) is true for all x ∈ S, if

INDUCTIVE STEP: For every y ∈ S, if P(x) true for all x ∈ S with x ≺ y, then P(y) true

[Lexicographic Order]

$(a_1,\ a_2,\ ...,\ a_n) \prec (b_1,\ b_2,\ ...,b_n)\ \ if\ a_1\ =\ b_1\ ...\ a_n\ \ =\ \ b_n,\ and\ a_{i+1}\ \prec_{i+1}\ b_{i+1}$

[Hasse Diagrams]

1. Remove all loops since partial ordering is reflexive, a loop (a, a) is present at every vertex a.
2. Remove all edges (x, y) since there an element z ∈ S such that x ≺ z and z ≺ x
3. Arrange each edge that initial vertex below terminal vertex
4. Remove all the arrows on the directed edges

Let (S, ≺=) be poset. element y ∈ S **covers** element x ∈ S if x ≺ y and no element z ∈ S that x ≺ z ≺ y. The pairs (x, y) that y covers x called **covering relation** of (S, ≺=)

[Maximal] a is maximal in the poset (S, ≺=) if there is no b ∈ S such that a ≺ b

[Minimal] a is minimal if there is no element b ∈ S such that b ≺ a

[Greatest element] greater than every other element in poset

[Least element] less than all other elements in poset

[Upper bound]

If u is element of S that a <= u for all elements a ∈ A, u is called upper bound of A

[Lower bound]

If l is element of S that l <= a for all elements a ∈ A, l is called lower bound of A

[Least upper bound] Less than every other upper bound

[Greatest lower bound] Greater than every other lower bound

[Lattice] both a least upper bound and a greatest lower bound

[Topological Sorting]

Total ordering <= is **compatible** with partial ordering R if a <= b whenever aRb. Constructing compatible total ordering from partial ordering called topological sorting

5.1 Mathematical Induction

Prove P(n) is true for all positive integers n, where P (n) is a propositional function

BASIS STEP: We verify that P (1) is true.

INDUCTIVE STEP: Show that conditional statement P (k) → P (k + 1) is true for all positive integers k.

Assume that P (k) is true and show under this assumption, P (k + 1) be true

Example: Let $P(n)$ be $1^3 + 2^3 + \cdots + n^3 = (n(n+1)/2)^2$ for positive integer n

$$P(1):\ 1 = (1(1+1)/2)^2$$

$$RHS : (1(1+1)/2)^2 = 1 = LHS$$

So $P(1)$ is true

Assume that $P(k)$ is true,

$$1^3 + 2^3 + ... + k^3 = (k(k+1)/2)^2$$

Note that $P(k+1)$ is

$$1^3 + 2^3 + \ldots + k^3 + (k+1)^3 = ((k+1)(k+2)/2)^2$$

and then

$$\begin{aligned}
1^3 + 2^3 + \ldots + k^3 + (k+1)^3 &= (k(k+1)/2)^2 + (k+1)^3 \\
&= k^2(k+1)^2/4 + (k+1)^3 \\
&= (k+1)^2(k^2/4 + (k+1)) \\
&= (k+1)^2(k+2)^2/4 \\
&= ((k+1)(k+2)/2)^2 \\
&= P(k+1)
\end{aligned}$$

It shows $P(k+1)$ is true when $P(k)$ is true

By mathematical induction, $P(n)$ is true for all positive integers n

5.3 Recursive Definitions and Structural Induction

Define function with set of nonnegative integers domain:

BASIS STEP: Specify value of function at zero

RECURSIVE STEP: Give a rule for finding its value at an integer from its values at smaller integers

It is called **recursive** or **inductive definition**

[Arithmetic sequence] $a_n = a_{n-1} + d \qquad a_n = a_0 + nd$

[Geometric sequence] $a_n = c\, a_{n-1} \qquad a_n = c^n\, a_0$

[Compound interest] $P_n = r^n P_0$

8.2 Solving Linear Recurrence Relations

Linear homogeneous recurrence relation of degree k with constant coefficients

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k}$$

where $c_1, c_2, \ldots, c_k$ are real numbers with $c_k \neq 0$

[Linear] a_k power by 1

[Homogeneous] all arguments multiple by some a_k

[Degree k] a_n depends on the kth preceding term

[Constant coefficients] all coefficients are constants

[Characteristic equation]

$$r^k - c_1 r^{k-1} - c_2 r^{k-2} \ldots c_{k-1} r - c_k = 0$$

[Characteristic roots] roots of characteristic equation

Solution of degree two:

$a_n = c_1 a_{n-1} + c_2 a_{n-2}$

$r^2 - c_1 r - c_2 = 0,\ we\ have\ r_1,\ r_2\ (r_1 \neq r_2)$

$a_n = a_1 r_1^n + a_2 r_2^n$

Solution of degree two with same r root:

$r^2 - c_1 r - c_2 = 0,\ we\ have\ r_0$

$a_n = a_1 r_0^n + a_2 n r_0^n$

Solution of degree k with distinct r roots:

$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k}$

$r^k - c_1 r^{k-1} - \ldots - c_k = 0,\ we\ have\ r_1,\ r_2,\ \ldots,\ r_k (distinct\ roots)$

$a_n = a_1 r_1^n + a_n r_2^n + \ldots + a_k r_k^n$

General solution of linear homogeneous recurrence relations with constant coefficients:

$r^k - c_1 r^{k-1} - ... - c_k = 0,\ we\ have\ t\ distinct\ roots$

$the\ root\ multiply\ by\ m_1,\ m_2,\ ...,\ m_t\ times$

$m_1 + m_2 + ... + m_t = k$

$$a_n = (a_{1,0} + a_{1,1}n + ... + a_{1,m_1-1}n^{m_1-1})r_1^n + (a_{2,0} + a_{2,1}n + ... + a_{2,m_2-1}n^{m_2-1})r_2^n\ +$$

$$+\ ...\ +\ (a_{t,0} + a_{t,1}n + ... + a_{t,m_t-1}n^{m_t-1})r_t^n$$

$where\ a_{i,j} are\ 1\ \le i \le t\ \ and\ 0 \le j \le m_j - 1$

$$a_n = \sum_{i=0}^{t}(\sum_{j=0}^{m_t-1} a_{i,j}n^j)r_t^n$$

Nonhomogeneous linear recurrence relation with constant coefficients

$a_n\ =\ c_1 a_{n-1}\ +\ c_2 a_{n-2}\ +\ ...\ +\ c_k\ a_{n-k}\ + F(n)$

$\{a_n^{(p)}\}$ is a particular solution of the nonhomogeneous linear recurrence relation with constant coefficients

$\{a_n^{(h)}\}$ is a solution of the associated homogeneous recurrence relation

$a_n = a_n^{(p)} + a_n^{(h)}$

Format of F(n): $F(n)\ =\ (b_t n^t + b_{t-1}n^{t-1} + ... + b_1 n + b_0)s^n$

When s is not a root of the characteristic equation of the associated linear homogeneous recurrence relation, there is a particular solution of the form

$a_n^{(p)} = (p_t n^t + p_{t-1}n^{t-1} + ... + p_1 n + p_0)s^n$

When s is a root of this characteristic equation and its multiplicity is m, there is a particular solution of the form

$a_n^{(p)} = n^m(p_t n^t + p_{t-1}n^{t-1} + ... + p_1 n + p_0)s^n$

6.1 The Basics of Counting

A_k is set of ways

There are $n_1,\ n_2,\ ...,\ n_k$, n is number of ways, k is number of task

[Product rule] $|A_1 \times A_2 \times ... \times A_k| \ = \ |A_1|\,|A_2|\ ...\ |A_k| \ = n_1 n_2 ... n_k$

[Sum rule] $|A_1 \cup A_2 \cup ... \cup A_k| \ = \ |A_1| + |A_2| + ... + |A_k| \ = \ n_1 + n_2 + ... + n_k$

[Subtraction Rule] $|\,A_1 \cup A_2\,| = |A_1| + |A_2| - |\,A_1 \cap A_2\,|$

[Division Rule] If finite set A is the union of n pairwise disjoint subsets each with d elements, then n = |A| / d

Counting problems can solved by **tree diagrams**

[Pigeonhole principle]

Assume that

pigeons: n + 1 objects are placed into

pigeonholes: n boxes

At least one box contains two or more objects

6.3 Permutations and Combinations

$$P(n,\ r) \ = \ \frac{n!}{(n-r)!}$$

$$C(n,\ r) \ = \ \frac{n!}{(n-r)!r!}$$

$$\binom{n}{r} = \binom{n}{n-r}$$

6.4 Binomial Coefficients and Identities

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

$$\sum_{j=0}^{n} (-1)^j \binom{n}{j} = 0$$

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$