Mathematical reasoning

Logic and Proofs

Propositional Logic

- a proposition: a declarative sentence that is either true or false
- compound propositions $\neg$. $\wedge$. $\vee$. $\oplus$. $\rightarrow$. $\leftrightarrow$
  - conjunction: $p \wedge q$
  - disjunction: $p \vee q$
  - The connective or
    - inclusive or $p \vee q$
    - exclusive or $p \oplus q$
  - implication $p \rightarrow q$ (p: hypothesis, antecedent, premise ; q: consequence, conclusion)
    - ↳ expressing. q unless $\neg p$ p only if q
      q whenever p q when p
      q follows from p p is sufficent for q q is necessary for p
  - $p \rightarrow q$
  - converse. $q \rightarrow p$
  - inverse: $\neg p \rightarrow \neg q$
  - contrapositive: $\neg q \rightarrow \neg p$ + equivalent: when two compound propositions always have the same truth value.
  - Biconditional: $p \leftrightarrow q$ (p iff q)
- Precedence: $\neg > \wedge > \vee > \rightarrow > \leftrightarrow$
- Bitwise Operations. OR. AND. XOR
- Consistent System Specifications: consistent if it's possible to assign truth values so each is true

Propositional Equivalences

- tautology → a proposition which is always true
- contradiction → false
- Contingency → neither a tautology nor a contradiction
- Logically equivalent. if $p \leftrightarrow q$ is a tautology
  $(p \Leftrightarrow q)$
  - show $p \equiv q$
    - truth table
    - already-proved equivalences
  - De Morgan's Laws
    - $\neg(p \wedge q) \equiv \neg p \vee \neg q$
    - $\neg(p \vee q) \equiv \neg p \wedge \neg q$
- Key Logical Equivalences
  - Identity Laws: $p \wedge T \equiv p$, $p \vee F \equiv p$
  - Domination Laws: $p \vee T \equiv T$, $p \wedge F \equiv F$
  - Idempotent Laws: $p \vee p \equiv p$. $p \wedge p \equiv p$
  - Double Negation Laws: $\neg(\neg p) \equiv p$
  - Negation Laws: $p \vee \neg p \equiv T$
    $p \wedge \neg p \equiv F$
  - Commutative Laws: $p \wedge q \equiv q \wedge p$
    $p \vee q \equiv q \vee p$
  - Associative Laws: $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
    $(p \vee q) \vee r \equiv p \vee (q \vee r)$
  - Distributive Laws: $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
    $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
  - Absorption Laws. $p \vee (p \wedge q) \equiv p$
    $p \wedge (p \vee q) \equiv p$

Dual { contains only the ∨. ∧. ¬. T. F.
| $s \Leftrightarrow t$ if and only if $s^* \Leftrightarrow t^*$

p NOR q: $p \downarrow q$ is true when both p and q are false

p NAND q: $p \mid q$ is false when both p and q are true

Propositional Satisfiablity { an assignment of truth values → make it true
| unsatisfiable iff it's a contradiction

Propositional Normal Forms

- Propositional Formula { each propositional variable is a formula.
  - if A is a formula. then $\neg A$
  - if A, B is a formula. then $A \vee B$, $A \wedge B$, $A \to B$, $A \leftrightarrow B$
- Normal Forms { literal: a variable or its negation
  - DNF (disjunctive normal forms): it's written as a disjunction in which all terms are conjunction of literals
  - Clauses { conjunctive clause (basic product)
    - disjunctive clause (basic addition)
- minterms { each minterm is true for exactly one assignment
  - The conjunction of two different is always false
  - The disjunction of all minterm is T
- full disjuctive form { a Boolean function is expressed as a disjunction of minterms
  - find full disjunctive form: { truth table
    - change clause to minterm
- Conjunctive normal form   maxterm $M_i = \neg m_i$

Predicates and Quantifiers

variables: x, y, z.

Predicates: $P(x), M(x)$ ..

propositional functions $\xrightarrow{\text{variable} \leftarrow \text{value}}$ propositions

Quantifiers
- universal Quantifier: $\forall$ $\quad \forall x P(x)$
- existential Quantifier: $\exists$ $\quad \exists x P(x)$
- uniqueness Quantifier: $\exists! x P(x)$ one and only one
  $(\exists x (P(x) \land \forall y (P(y) \to y = x))$
- Precedence: $\forall, \exists$ have higher precedence than all the logical operators.

* $\forall x (S(x) \to J(x))$ $\quad \exists x (S(x) \land J(x))$

$\forall x P(x) \lor A \equiv \forall x (P(x) \lor A)$ $\qquad \forall x (A \to P(x)) \equiv A \to \forall x P(x)$

$\forall x P(x) \land A \equiv \forall x (P(x) \land A)$ $\qquad \exists x (A \to P(x)) \equiv A \to \exists x P(x)$

$\exists x P(x) \lor A \equiv \exists x (P(x) \lor A)$ $\qquad \forall x (P(x) \to A) \equiv \exists x P(x) \to A$

$\exists x P(x) \land A \equiv \exists x (P(x) \land A)$ $\qquad \exists x (P(x) \to A) \equiv \forall x P(x) \to A$

Neste Quantifiers

Basic Structures

Sets

- an unordered collection of objects
- ① elements / members, contain its elements
- ② universal set 全集
  empty set 空集 $\emptyset$ $\quad \emptyset \neq \{\emptyset\}$
- ③ subsets $A \subseteq B$
- ④ proper subsets 真子集 $\forall x(x\in A \rightarrow x\in B) \land \exists x(x\in B \land x\notin A)$
- ⑤ Set Cardinality
  - finite
  - infinite
  - cardinality → the number of elements in A $|A|$
- ⑥ Power Sets: the set of all subsets of a set A
- ⑦ tuples: orderd n-tuple $(a_1, \cdots, a_n)$
  (a_1, a_2) → ordered pairs

Cartesian Product. $A\times B = \{(a,b) \mid a\in A \land b\in B\}$

⑧ a subset R of the Cartesian product $A\times B$ is called a relation from A to B

⑨ Truth Set of Quantifiers $\{x\in D \mid P(x)\}$

Set Operations

- Union $\{x \mid x\in A \lor x\in B\}$
- Intersection $\{x \mid x\in A \land x\in B\}$ if empty → A and B are disjoint
- complement (补集) $\overline{A} = \{x\in U \mid x\notin A\}$ (A^c)
- difference. $A - B = \{x \mid x\in A \land x\notin B\} = A\cap\overline{B}$
- Inclusion-Exclusion: $|A\cup B| = |A| + |B| - |A\cap B|$
- Symmetric Difference. $A\oplus B = (A-B)\cup(B-A)$

Functions

- $f: A \to B$ an assignment of each element of A to exactly one element of B

  $\forall a\,[a \in A \to \exists!\, b\,(b \in B \wedge f(a) = b)]$
- $f: A \to B$ can also be defined as a subset of $A \times B$ (a relation)

  $\forall x\,[x \in A \to \exists y\,[y \in B \wedge (x,y) \in f]]$

  and $\forall x, y_1, y_2\,[(x,y_1) \in f \wedge (x,y_2) \in f] \to y_1 = y_2]$
- $f: A \to B$
  - f maps A to B
  - $A \to$ domain of f
  - $B \to$ codomain of f
  - $f(a) = b$: b: image a: preimage

    $\Downarrow$

    range.

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

$$\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}$$

- injection (one-to-one)

  surjection (onto)

  bijection (one-to-one correspondence)

  inverse functions $f^{-1}(y) = x$ iff $f(x) = y$

  composition $f \circ g\,(x) = f(g(x))$
- floor function $f(x) = \lfloor x \rfloor$ $\lfloor x + n \rfloor = \lfloor x \rfloor + n$

  ceiling function $f(x) = \lceil x \rceil$ $\lceil x + n \rceil = \lceil x \rceil + n$

Cardinality of Sets

The cardinality of A is equal to B. iff there is a one-to-one correspondence from A to B

- if one-to-one function from A to B $\to |A| \leq |B|$
- countable: A set that is either finite or has the same cardinality as Z^+

  * R is uncountable

  * countably infinite: $\aleph_0$ $|S| = \aleph_0$
- Benstien Theorem: if $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$

rational number (有理数) $\to$ countable (positive)

* There're the same number of positive rational numbers and positive integers

  Q is countable infinite

- Cantor Diagonalization Argument

To infinity And Beyond

Bijections

Cardinality ① example: $\mathbb{Z}$ and $\mathbb{N}$. $f(x) = \begin{cases} \frac{x}{2} & x \text{ is even} \\ -\frac{x+1}{2} & x \text{ is odd.} \end{cases}$

$$\begin{array}{cccccc} 0 & 1 & 2 & 3 & 4 & \cdots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ 0 & -1 & 1 & -2 & 2 & \cdots \end{array}$$

S is countable if there is a bijection between S and $\mathbb{N}$ or some subset of $\mathbb{N}$.

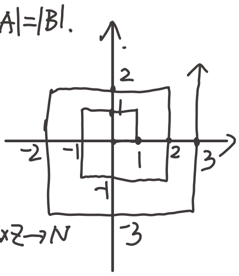
① Cantor-Bernstein theorm: $|A| \le |B|$. $|B| \le |A| \Rightarrow |A| = |B|$.

*example: obviously $|\mathbb{N}| \le |\mathbb{Q}|$

$|\mathbb{Q}| \le |\mathbb{N}|$: injection $f: \mathbb{Q} \to \mathbb{N}$

$\frac{a}{b}$ written as (a,b) $(\mathbb{Z} \times \mathbb{Z})$

$\Rightarrow$ come up with an injection from $\mathbb{Z} \times \mathbb{Z} \to \mathbb{N}$



$(0,0) \to 0$ $(1,0) \to 1$, $(1,1) \to 2$, $(0,1) \to 3$ ...

*example: the set of all binary strings (of any finite length) $\{0,1\}^*$

$\varepsilon, 0, 1, 00, 01, 10, 11, 000, \ldots$ (lextcographic order)

$f: \{0,1\}^* \to \mathbb{N}$: $f(n)$ to be the nth strings in $\{0,1\}^*$

*example: polynomials with natural number coefficients.

① Cantor's Diagonalization

Theorm: The real interval $\mathbb{R}[0,1]$ is uncountable

Proof. suppose towards a contradiction. bijection $f: \mathbb{N} \to \mathbb{R}[0,1]$

$r_1 = 0.d_{11}d_{12}d_{13}d_{14}\ldots$

$r_2 = 0.d_{21}d_{22}d_{23}d_{24}\ldots$

$\vdots$

$d_{ij} \in \{0,1,2,3,\ldots,8,9\}$.

form a new number $r = 0.d_1d_2d_3d_4\ldots$ $d_i = \begin{cases} 4 & \text{if } d_{ii} \ne 4 \\ 5 & \text{if } d_{ii} = 4 \end{cases}$ r not in lise

① The Cantor Set

uncountable: $[0,1] \Leftrightarrow \{0,1,2\}$

f: C: $\{x \in [0,1]$: x has a ternary representation consisting only of 0 and 2$\}$

f: $C \to [0,1]$ is onto

① Power Set:

Theorem: $|\mathcal{P}(\mathbb{N})| > |\mathbb{N}|$

	0	1	2	3	4	5	
0	1	0	0	0	0	0	...
1	0	0	0	0	0	0	...
2	1	0	1	0	0	0	...
⋮							

Algorithms

The growth of functions

Big-O Notation : $f(x)$ is $O(g(x))$ iff there are constants C, k such that $|f(x)| \le C|g(x)|$ whenever $x>k$.

* g asymptotically dominates f
* the C, k are called witnesses to the relationship $f(x)$ is $O(g(x))$

* $1+2+\cdots+n \le n+\cdots+n = n^2$ is $O(n^2)$ taking $C=1, k=1$.

$f(n)=n! \le n^n$. $n!$ is $O(n^n)$

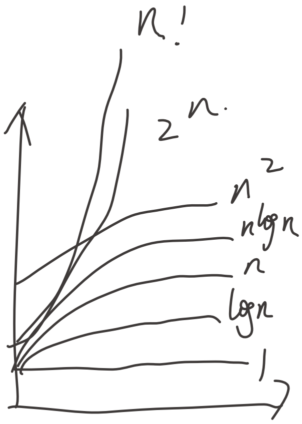
$\log n!$ is $O(n\log n)$ taking $C=1, k=1$

① $d>c>1$: n^c is $O(n^d)$, n^d is not $O(n^c)$

$b>1$, $c,d \to$ positive: $(\log_b n)^c$ is $O(n^d)$, n^d is not $O((\log_b n)^c)$

if $b>1$, $d \to$ positive. n^d is $O(b^n)$, b^n is not $O(n^d)$

if $c>b>1$: b^n is $O(c^n)$, c^n is not $O(b^n)$



$(f_1+f_2)(x)$ is $O(\max\{g_1(x), g_2(x)\})$

$(f_1f_2)(x)$ is $O(g_1(x)g_2(x))$

若 $f_1(x)$ is $O(g(x))$ $f_2(x)$ is $O(g(x)) \Rightarrow (f_1+f_2)(x)$ is $O(g(x))$

① Big-Omega Notation

f is $\Omega(g(x))$ if $|f(x)| \ge C|g(x)|$ when $x>k$

* $f(x)$ is $\Omega(g(x))$ iff $g(x)$ is $O(f(x))$

① Big-Theta Notation

$f(x)$ is $\Theta(g(x))$ if $f(x)$ is $O(g(x))$ and $f(x)$ is $\Omega(g(x))$ $\quad C_1g(x) < f(x) < C_2g(x)$ if $x>k$

($f(x)$ is of order $g(x)$, $f(x)$ and $g(x)$ are of the same order)

* $1+2+\cdots+n \ge \lceil \frac{n}{2} \rceil + (\lceil \frac{n}{2} \rceil + 1) + \cdots + n$
$\ge \lceil \frac{n}{2} \rceil + \lceil \frac{n}{2} \rceil + \cdots + \lceil \frac{n}{2} \rceil \ge \frac{n^2}{4}$

When $f(x)$ is $\Theta(g(x)) \Rightarrow g(x)$ is $\Theta(f(x))$

⊙ $f(x)=a_nx^n+\cdots+a_1x+a_0$. $f(x)$ is $\Theta(x^n)$

Number Theory and Cryptography

Divisibility and Modular Arithmetic

Division

Division Algorithm: $a=dq+r$ d: divisor, q: quotient, r: remainder

$q=a \text{ div } d$, $r=a \bmod d$

Congruence Relation: a is congruence to b modulo m if $m \mid a-b$

Theorem: $a\equiv b \pmod m$ iff $a=b+km$

Theorem: $a\equiv b \pmod m$ iff $a \bmod m = b \bmod m$

Corollary. $(a+b) \pmod m = ((a \bmod m)+(b \bmod m)) \bmod m$

$ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$

Arithmetic Modulo m.

Z_m: $\{0,1,\cdots,m-1\}$

$+_m$: $a+_m b=(a+b) \bmod m$

$a\cdot_m b=(ab) \bmod m$

Representations of Integers

Base b Representations

$n=a_k b^k+\cdots+a_1 b+a_0$ $(a_i<b)$

↳ base b expansion of n, denoted by $(a_k a_{k-1}\cdots a_1 a_0)_b$

Binary / Octal / Hexadecimal Expansions

*Base Conversion

*Conversion Between Binary, Octal, Hexadecimal Expansions

eg: $(11\ 1110\ 1011\ 1100)_2$

二进制运算 ???

Primes and GCD

The fundamental Theorem of Arithmetic

The Sieve of Erastosthenes

Infinitude of Primes

Mersenne Primes : 2^P-1 (p is prime)

Prime Number Theorem: The ratio of the number of primes not exceeding x and $\frac{x}{\ln x} \to 1$ as x grows without bound

Greatest Common Divisor

$gcd(a,b)$

relatively prime: $gcd(a,b)=1$

pairwise relatively prime. $gcd(a_i,a_j)=1$. $a_1,a_2,\cdots,a_n$

$a=p_1^{a_1}\cdots p_n^{a_n}$, $b=p_1^{b_1}\cdots p_n^{b_n}$

$gcd(a,b)=p_1^{min(a_1,b_1)}\cdots p_n^{min(a_n,b_n)}$

Least Common Multiple

$lcm(a,b)=p_1^{max(a_1,b_1)}\cdots p_n^{max(a_n,b_n)}$

$ab=gcd(a,b)\cdot lcm(a,b)$

Euclidean Algorithm

$gcd(a,b)=gcd(b,r)$ $a=bq+r$

gcds as Linear Combinations

$gcd(a,b)=sa+tb$ (Bézout's identity)

$s,t \to$ Bézout's coefficients

if $gcd(a,b)=1$, $a|bc$ then $a|c$

if p is prime, $p|a_1a_2\cdots a_n$, then $p|a_i$ for some i

Theorem: if $ac\equiv bc \pmod m$ and $gcd(c,m)=1$, then $a\equiv b \pmod m$

Linear Congruences

$ax\equiv b \pmod m$

An integer $\bar{a}$ such that $\bar{a}a\equiv 1 \pmod m$ $\Rightarrow$ be an inverse of a modulo m

Theorem 1 If $gcd(a,m)=1$, then an inverse of a modulo m exists and unique

$sa+tm=1$. $s\to$ inverse

The Chinese Remainder Theorem

Let $m_1,\cdots,m_n$ be pairwise relatively prime positive integers greater than one

$x\equiv a_1 \pmod{m_1}$

$\vdots$ $\Rightarrow$ has a unique modulo $m=m_1m_2\cdots m_n$

$x\equiv a_n \pmod{m_n}$

Counting

The Basics of Counting

- The Product Rule
  - Counting Functions: from a set with m elements to n: n^m
  - Counting Subsets of a Finite Set (using product rule)
- The Sum Rule
- Subtraction Rule (the principle of inclusion-exclusion)
- Division Rule
- Tree Diagrams

eg. Choose three different numbers from the integers between 1 to 300 such that the sum of three integers can be d divisible by 3. $3 \times C_{100}^{3} + C_{100}^{1} \times C_{100}^{1} \times C_{100}^{1}$

例 21 4 个人坐在一个圆桌旁边，有多少种坐法？如果每个人左右相邻的人都相同就认为是同一种坐法。

$24/4 = 6$

results, such as that given in Example 4.

Show that for every integer n there is a multiple of n that has only 0s and 1s in its decimal expansion.

Solution: Let n be a positive integer. Consider the $n+1$ integers 1, 11, 111, …, 11 … 1 (where the last integer in this list is the integer with $n+1$ 1s in its decimal expansion). Note that there are n possible remainders when an integer is divided by n. Because there are $n+1$ integers in this list, by the pigeonhole principle there must be two with the same remainder when divided by n. The larger of these integers less the smaller one is a multiple of n, which has a decimal expansion consisting entirely of 0s and 1s.

The Pigeonhole Principle (Dirichlet Drawer Principle)

① Corollary 1: A function f from a set with $k+1$ elements to a set with k elements is not one-to-one

eg. Among any group of 11 integers, there are two integers a and b such that $10 \mid a-b$
(the possible remainders when an integer is divided by $10 \to 10$)

The Generalized Pigeonhole Principle

If N objects are placed into k boxes, then there is at least one box containing at least $\lceil N/k \rceil$ objects

例 10 在 30 天的一个月里，某棒球队一天至少打一场比赛，但至多打 45 场。证明一定有连续的若干天内这个队恰好打了 14 场。

eg. Suppose there are n arbitrary integers $x_1, x_2, \dots, x_n$. Show that there exist some consecutive integers such that the sum of these integers is the multiple of n

例 11 证明在不超过 $2n$ 的任意 $n+1$ 个正整数中一定存在一个正整数被另一个正整数整除。

x_n $\quad a_i = \sum_{k=1}^{i} x_k$

$x_1, x_1+x_2, \dots, x_1+\dots+x_n$

$a_1, \dots, a_n$

①Every sequence of n^2+1 distinct integers contains a subsequence of length $n+1$ that is either strictly increasing or strictly decreasing

$a_1, a_2, \cdots, a_{n^2+1}$

Associate (x_k, y_k) to a_k: $\begin{cases} x_k: \text{the length of the longest increasing subsequence starting at } a_k \\ y_k: \text{decreasing} \end{cases}$

Suppose no $n+1$: $1 \le x_k \le n$, $1 \le y_k \le n$

there are n^2 pairs (x_k, y_k), 又 $a_i \ne a_j$ $\Rightarrow$ contradiction

Ramsey Theory

$R(m,n) = R(n,m)$, $\quad R(n,2) = n$

The **Ramsey number** $R(m, n)$, where m and n are positive integers greater than or equal to 2, denotes the minimum number of people at a party such that there are either m mutual friends or n mutual enemies, assuming that every pair of people at the party are friends or enemies. Example 13 shows that $R(3, 3) \le 6$. We conclude that $R(3, 3) = 6$ because in a group of five people where every two people are friends or enemies, there may not be three mutual friends or three mutual enemies (see Exercise 28).

Permutations and Combinations

- r-permutation $P(n,r) = n(n-1)\cdots(n-r+1) = \dfrac{n!}{(n-r)!}$
- Combinations. $C(n, r)$ $\binom{n}{r} = \dfrac{n!}{(n-r)!\,r!}$

  $C(n, r) = C(n, n-r)$
- Combinatorial Proofs
  - A double counting proof
  - A bijective proof

Binomial Coefficients and Identities

Binomial Theorem: $(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j = \binom{n}{0} x^n + \cdots + \binom{n}{n-1} x y^{n-1} + \binom{n}{n} y^n$

Corollary 1: $\sum_{k=0}^{n} \binom{n}{k} = 2^n$

Corollary 2: $\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$ $\quad \binom{n}{0} + \binom{n}{2} + \cdots = \binom{n}{1} + \binom{n}{3} + \cdots$

Pascal's Identity $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$

(combinatorial proof)

* Pascal's Triangle

$$\begin{matrix} & & \binom{0}{0} & & \\ & \binom{1}{0} & & \binom{1}{1} & \\ \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} \\ & & \vdots & & \end{matrix}$$

Vandermonde's Identity $\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{r-k} \binom{n}{k}$

Corollary 4: $\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2$

Theorem 4: $\binom{n+1}{r+1} = \sum_{j=r}^{n} \binom{j}{r}$ (Proof).

Generalized Permutations and Combinations

2 There are $C(n+r-1, r) = C(n+r-1, n-1)$ r-combinations from a set with n elements when repetition of elements is allowed.

Generating Permutations and Combinations

① The permutation $a_1 a_2 \cdots a_n$ precedes $b_1 b_2 \cdots b_n$, if for some k, $a_1 = b_1, \ldots a_{k-1} = b_{k-1}$, $a_k < b_k$

Algorithm
- Find the integers a_j, a_{j+1} with $a_j < a_{j+1}$ and $a_{j+1} > a_{j+2} > \cdots > a_n$
- Put in the jth position the least integer among $a_{j+1}, \cdots, a_n$ that is greater than a_j
- List in increasing order the rest of integers

② Generating Combinations

- Strat with bit string $00 \cdots 00$ n zeros
- Then find the next larger expansion until $11 \cdots 11$ is obtained

Advanced Counting Techniques

Recurrence Relations

The degree of a recurrence relation: $a_n = a_{n-1} + a_{n-8}$ degree 8

*Counting Bit Strings

Linear Homogeneous Recurrence Relations

$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$ degree k $(c_k \neq 0)$

* $H_n = 2H_{n-1} + 1$: not homogeneous

* Solving Linear Homogeneous Recurrence Relations of Degree Two

Theorem 1: $r^2 - c_1 r - c_2 = 0$ has two distinct roots r_1, r_2.

$a_n = c_1 a_{n-1} + c_2 a_{n-2}$ iff $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$

Theorem 2. $r^2 - c_1 r - c_2 = 0$. one repeated root r_0

$a_n = c_1 a_{n-1} + c_2 a_{n-2}$ iff $a_n = \alpha_1 r_0^n + \alpha_2 n r_0^n = (\alpha_1 + n\alpha_2) r_0^n$

Theorem 3. $r^k - c_1 r^{k-1} - \cdots - c_k = 0$: k distinct roots $r_1, r_2, \cdots, r_k$.

$a_n = c_1 a_{n-1} + \cdots + c_k a_{n-k}$ iff $a_n = \alpha_1 r_1^n + \cdots + \alpha_k r_k^n$

Theorem 4: $r^k - c_1 r^{k-1} - \cdots - c_k = 0$, t distinct roots $r_1, \cdots r_t$ with multiplicities $m_1, m_2, \cdots, m_t$

$a_n = c_1 a_{n-1} + \cdots + c_k a_{n-k}$: $a_n = (\alpha_{10} + \alpha_{11} n + \cdots + \alpha_{1,m_1-1} n^{m_1-1}) r_1^n + \cdots + (\alpha_{t0} + \cdots + \alpha_{t,m_t-1} n^{m_t-1}) r_t^n$

$$= \sum_{i=1}^{t} \left(\sum_{j=0}^{m_i-1} a_{ij} n^j \right) r_i^n$$

Linear Nonhomogeneous Recurrence Relations

$\underline{a_n = c_1 a_{n-1} + \cdots + c_k a_{n-k}} + F(n)$

↳ associated homogeneous recurrence relation

Theorem 5. $a_n = c_1 a_{n-1} + \cdots + c_k a_{n-k} + F(n)$

$F(n) = (b_t n^t + \cdots + b_1 n + b_0) s^n$

- s 不是相伴根时. $(p_t n^t + p_{t-1} n^{t-1} + \cdots + p_0) s^n$
- s 相伴根,重数 m $n^m (p_t n^t + \cdots + p_0) s^n$

Generating Functions

The generating function for the sequence $a_0, a_1, \dots, a_k, \dots$ of real numbers: infinite series $G(x) = a_0 + a_1x + \dots + a_kx^k + \dots$

$$= \sum_{k=0}^{\infty} a_k x^k$$

for finite sequences: set $a_{n+1}=0,\ a_{n+2}=0 \dots$

Counting Problems

$f(x)=\sum_{k=0}^{\infty} a_k x^k$, $g(x)=\sum_{k=0}^{\infty} b_k x^k \Rightarrow f(x)g(x)=\sum_{k=0}^{\infty}\left(\sum_{j=0}^{k} a_j b_{k-j}\right)x^k$

eg: $a_0, a_1, \dots, a_n \dots \rightarrow G(x)$. $\quad a_k \leftrightarrow G(x),\ C_k=1$

$b_k=\sum_{i=0}^{k} a_i$, generating function: $b_k=\sum_{i=0}^{k} a_i = \sum_{i=0}^{k} a_i C_{k-i}$

$\therefore F(x) = G(x)\cdot\frac{1}{1-x}$

$\frac{1}{1-x} = 1+x+x^2+\dots$

The extended binomial coefficient

$$\binom{u}{k} = \begin{cases} \dfrac{u(u-1)\cdots(u-k+1)}{k!} & (k>0) \\ 1 & k=0 \end{cases}$$

The extended Binomial Theorem $|x|<1$: $(1+x)^u = \sum_{k=0}^{\infty}\binom{u}{k}x^k$

$\binom{-n}{k} = (-1)^k C(n+k-1, k)$

eg Find the number of solutions of

$$e_1 + e_2 + e_3 = 17,$$

where e_1, e_2, and e_3 are nonnegative integers with $2 \le e_1 \le 5$, $3 \le e_2 \le 6$, and $4 \le e_3 \le 7$.

Solution: The number of solutions with the indicated constraints is the coefficient of x^{17} in the expansion of

$$(x^2 + x^3 + x^4 + x^5)(x^3 + x^4 + x^5 + x^6)(x^4 + x^5 + x^6 + x^7).$$

This follows because we obtain a term equal to x^{17} in the product by picking a term in the first sum x^{e_1}, a term in the second sum x^{e_2}, and a term in the third sum x^{e_3}, where the exponents e_1, e_2, and e_3 satisfy the equation $e_1 + e_2 + e_3 = 17$ and the given constraints.

It is not hard to see that the coefficient of x^{17} in this product is 3. Hence, there are three solutions. (Note that the calculating of this coefficient involves about as much work as enumerating all the solutions of the equation with the given constraints. However, the method that this illustrates often can be used to solve wide classes of counting problems with special formulae, as we will see. Furthermore, a computer algebra system can be used to do such computations.) ◀

? Use generating functions to determine the number of ways to insert tokens worth \$1, \$2, and \$5 into a vending machine to pay for an item that costs r dollars in both the cases when the order in which the tokens are inserted does not matter and when the order does matter. (For example, there are two ways to pay for an item that costs \$3 when the order in which the tokens are inserted does not matter: inserting three \$1 tokens or one \$1 token and a \$2 token. When the order matters, there are three ways: inserting three \$1 tokens, inserting a \$1 token and then a \$2 token, or inserting a \$2 token and then a \$1 token.)

TABLE 1 Useful Generating Functions.

$G(x)$	a_k
$(1+x)^n = \sum_{k=0}^{n} C(n,k)x^k = 1 + C(n,1)x + C(n,2)x^2 + \cdots + x^n$	$C(n,k)$
$(1+ax)^n = \sum_{k=0}^{n} C(n,k)a^kx^k = 1 + C(n,1)ax + C(n,2)a^2x^2 + \cdots + a^nx^n$	$C(n,k)a^k$
$(1+x^r)^n = \sum_{k=0}^{n} C(n,k)x^{rk} = 1 + C(n,1)x^r + C(n,2)x^{2r} + \cdots + x^{rn}$	$C(n,k/r)$ if $r \mid k$; 0 otherwise
$\frac{1-x^{n+1}}{1-x} = \sum_{k=0}^{n} x^k = 1 + x + x^2 + \cdots + x^n$	1 if $k \le n$; 0 otherwise
$\frac{1}{1-x} = \sum_{k=0}^{\infty} x^k = 1 + x + x^2 + \cdots$	1
$\frac{1}{1-ax} = \sum_{k=0}^{\infty} a^kx^k = 1 + ax + a^2x^2 + \cdots$	a^k
$\frac{1}{1-x^r} = \sum_{k=0}^{\infty} x^{rk} = 1 + x^r + x^{2r} + \cdots$	1 if $r \mid k$; 0 otherwise
$\frac{1}{(1-x)^2} = \sum_{k=0}^{\infty} (k+1)x^k = 1 + 2x + 3x^2 + \cdots$	$k+1$
$\frac{1}{(1-x)^n} = \sum_{k=0}^{\infty} C(n+k-1,k)x^k = 1 + C(n,1)x + C(n+1,2)x^2 + \cdots$	$C(n+k-1,k) = C(n+k-1,n-1)$
$\frac{1}{(1+x)^n} = \sum_{k=0}^{\infty} C(n+k-1,k)(-1)^kx^k = 1 - C(n,1)x + C(n+1,2)x^2 - \cdots$	$(-1)^kC(n+k-1,k) = (-1)^kC(n+k-1,n-1)$
$\frac{1}{(1-ax)^n} = \sum_{k=0}^{\infty} C(n+k-1,k)a^kx^k = 1 + C(n,1)ax + C(n+1,2)a^2x^2 + \cdots$	$C(n+k-1,k)a^k = C(n+k-1,n-1)a^k$
$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots$	$1/k!$
$\ln(1+x) = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k}x^k = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots$	$(-1)^{k+1}/k$

Note: The series for the last two generating functions can be found in most calculus books when power series are discussed.

Q. Use generating functions to find the number of r-combinations from a set with n elements when repetition of elements is allowed.

Inclusion-Exclusion

① Principle of Inclusion-Exclusion

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{1\le i\le n}|A_i| - \sum_{1\le i<j\le n}|A_i\cap A_j| + \sum_{1\le i<j<k\le n}|A_i\cap A_j\cap A_k| - \cdots + (-1)^{n+1}|A_1\cap A_2\cap\cdots\cap A_n|$$

Applications

① An Alternative form of inclusion-exclusion

② The number of onto functions

Let m and n be positive integers with $m \ge n$

There are $n^m - C_n^1(n-1)^m + C_n^2(n-2)^m - \cdots + (-1)^{n-1}C_n^{n-1}\cdot 1^m$ onto functions

③ Derangements

*a permutation of objects that leaves no object in the original position

The number of derangements of a set with n elements: $D_n = n!\left[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n\frac{1}{n!}\right]$

Relations

Relations and Their Properties

- Binary Relations R: from a set A to a set B is a subset $R \subseteq A \times B$
- A binary relation R on a set A is a subset of $A \times A$ or a relation from A to A.

  There're $2^{|A|^2}$ relations on a set A

- Reflexive (自反) Relations

  R is reflexive iff $(a,a) \in R$ for every element $a \in A$

  $\forall x : (x \in U \to (x,x) \in R)$

- Symmetric Relations. $(b,a) \in R$ whenever $(a,b) \in R$.

  $\forall x \forall y \, [(x,y) \in R \to (y,x) \in R]$

- Antisymmetric Relations

  if $(a,b) \in R$, $(b,a) \in R$ then $a=b$ $\to$ anti symmetric

  $\forall x \forall y \, [(x,y) \in R \land (y,x) \in R \to x=y]$

eg: n元素集合上的自反关系 / 反自反

$\begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}$ n^2-n个元素可选0/1.

2^{n^2-n}

对称关系

两部分 $\begin{cases} (x,y),(y,x) \; x \neq y \to \frac{n^2-n}{2} \\ \text{对角}: n \end{cases} \Rightarrow 2^{\frac{n^2+n}{2}}$

反对称关系 $\frac{n^2-n}{2}$个 (x,y)

要么 (x,y), (y,x), ϕ. $\Rightarrow 3^{\frac{n^2-n}{2}}$

对角: 2^n $\therefore$ 共 $2^n \times 3^{\frac{n^2-n}{2}}$

自反且对称 $2^{\frac{n^2-n}{2}}$

- Transitive Relations

  $(a,b) \in R$, $(b,c) \in R \Rightarrow (a,c) \in R$.

- Combining Relations
- Composition $R_2 \circ R_1$
- Powers of a Relation R^n defined by $\begin{cases} \text{Basis Step } R^1 = R. \\ \text{Inductive Step } R^{n+1} = R^n \circ R \end{cases}$

Theorem 1. The relation R on a set A is transitive iff $R^n \subseteq R$,

- Inverse Relation: $R^{-1} = \{(a,b) \mid (b,a) \in R\}$

Representing Relations

- A relation between finite sets can be represented using a zero-one matrix

  $M_R = [m_{ij}]$ $\quad m_{ij} = \begin{cases} 1 & \text{if } (a_i,b_j) \in R \\ 0 & (a_i,b_j) \notin R \end{cases}$

- R: reflexive $\begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}$

R: $\begin{cases} \text{symmetric } m_{ij}=1 \text{ whenever } m_{ji}=1 \\ \text{antisymmetric iff } m_{ij}=0 \text{ or } m_{ji}=0 \text{ when } i \neq j \end{cases}$

- Using Digraphs
  - A directed graph (digraph) vertices + ordered pairs of V (edges)

    (a,b): $a \to$ initial vertex, b: terminal vertex

    - Reflexivity: A loop must be present at all vertices in the graph
    - Symmetry: if (x,y) is an edge, so is (y,x)
    - Antisymmetry: if (x,y) $(x \neq y)$ is an edge, then (y,x) is not a edge
    - Transitivity: If (x,y) (y,z) are edges, so is (x,z)

To Get inverse $\begin{cases} \text{reverse all the arcs in the digraph.} \\ \text{Take the } M_R^T \end{cases}$

Properties: $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$ $\quad (A \times B)^{-1} = B \times A$ $\quad (\overline{R})^{-1} = \overline{R^{-1}}$

$(R \cap S)^{-1} = R^{-1} \cap S^{-1}$ $\quad (R - S)^{-1} = R^{-1} - S^{-1}$

Closures of Relations

① The closure of a relation R with respect to property P is the relation obtained by adding the minimum number of ordered pairs to R to obtain property P.

① Reflexive Closure $r(R) = R \cup \Delta$

① Symmetric Closure $S(R) = R \cup R^{-1}$

① Transitive Closure

1. A path from a to b in the digraph G is a sequence of one or more edges $(x_0, x_1), (x_1, x_2) \cdots (x_{n-1}, x_n)$ in G where $x_0 = a$, $x_n = b$

if $a=b$, the path is called circuit or cycle

Theorem 1: Let R be the relation on a set A, there is a path of length n from a to b iff $(a,b) \in R^n$

Proof: ① Inductive basis. $n=1$. $R^1 = R$. ✓

② Inductive Step $(a,x) \in R$, $(x,b) \in R^n \Rightarrow (a,b) \in R^{n+1}$

The connectivity relation of R: R^*: consists of (a,b) such that there is path from a to b

$$R^* = \bigcup_{n=1}^{\infty} R^n$$

Theorem 2: the transitive closure of a relation R equals the connectivity R^*

$$R^* = \bigcup_{n=1}^{\infty} R^n = t(R)$$

Proof: ① $R \subseteq R^*$ by definition

② R^* is transitive: If $(a,b) \in R^*$, $(b,c) \in R^* \Rightarrow (a,c) \in R^*$

③ R^* is minimum: If S is also a transitive relation $S \supseteq R^*$.

① S transitive: $S^n \subseteq S$, $S^* = \bigcup_{n=1}^{\infty} S^n \subseteq S$ & $S \subseteq S^* \Rightarrow S = S^*$

② Since $R \subseteq S$, then $R^* \subseteq S^* \Rightarrow R^* \subseteq S$.

Lemma 1 A is a set containing n elements. R is relation on A. If there is a path from a to b, then there is such path with length not exceeding n. if $a \neq b$, there is such path with length not exceeding $n-1$.

∴ from this Lemma: $t(R) = \bigcup_1^n R^i$

Theorem 3. $M_{R^*} = M_R \vee M_{R^2} \vee \cdots \vee M_{R^n}$.

① Warshall's algorithm

Interior vertices of a path: $a, x_1, x_2, \cdots, x_{m-1}, b$. $x_1, x_2, \cdots, x_{m-1}$ are interior vertices

Matrices: $M_R = W_0$, $W_1, W_2, \cdots, W_n$, $W_n = M_{R^*}$

We can compute W_k from W_{k-1} $\begin{cases} \text{There is a path from } v_i \text{ to } v_j \text{ with its interior vertices among the first } k-1 \text{ vertices.} & w_{ij}^{(k-1)} = 1 \\ \text{There are paths from } v_i \text{ to } v_k \text{ and from } v_k \text{ to } v_j & w_{ik}^{(k-1)} = 1.\ w_{kj}^{(k-1)} = 1 \end{cases}$

Lemma 2 $w_{ij}^{(k)} = w_{ij}^{(k-1)} \vee \left(w_{ik}^{(k-1)} \wedge w_{kj}^{(k-1)} \right)$

求$t(R)$: $M = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$

$k=1$: 第1列为1的行与第一行逻辑加

$$M_R = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \to \underbrace{\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}}_{M_{R^3}} \to \underbrace{\begin{pmatrix} \quad \end{pmatrix}}_{M_{R^*}}$$

Equivalence Relations

- equivalence if it's reflexive, symmetric, and transitive
- notion $a \sim b$
- **Equivalence Classes** $[a]_R$

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

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

* congruence classes modulo m: $[a]_m = \{\cdots, a-m, a, a+m, a+2m, \cdots\}$

Theorem 1 R: equivalence relation

equivalent statements
$$\begin{cases} \text{(i) } aRb \\ \text{(ii) } [a]=[b] \\ \text{(iii) } [a]\cap[b] \neq \phi \end{cases}$$

$R_1 \cap R_2 \rightarrow$ equivalence

$R_1 \cup R_2 \rightarrow$ Not! : transitive

$(R_1 \cup R_2)^* \rightarrow$ equivalence

- **Partition of a Set**

a collection of disjoint nonempty subsets of S that have S as their union.

i.e. the collection of subsets A_i, where $i \in I$, forms a partition of S iff
$$\begin{cases} A_i \neq \phi \\ A_i \cap A_j = \phi \quad (i \neq j) \\ \bigcup_i A_i = S \end{cases}$$

notation: $pr(A) = \{A_i \mid i \in I\}$

Theorem 2 R: an equivalence relation

Then the equivalence classes of R form a partition of S.

Conversely, given a partition $\{A_i\}$ of the set S, there is an equivalence relation R that has the sets A_i as its equivalence classes.

Partial Orderings

- partial ordering if it's reflexive, antisymmetric, transitive.

* A set together with a partial ordering R is called a partially ordered set, or poset. denoted by (S,R).

- **Comparability**

Definition. The elements a and b of a poset $(S, \preccurlyeq)$ are comparable if either $a \preccurlyeq b$ or $b \preccurlyeq a$

* symbol $\preccurlyeq$ is used to denote the relation in any poset

Definition: if $(S, \preccurlyeq)$ is a poset and every two elements of S are comparable, S is called a totally ordered or linearly ordered set.

$\preccurlyeq$ is called a total order / linear order. chain

- $(S, \preccurlyeq)$ is well-ordered if it's a poset such that $\preccurlyeq$ is a total ordering and every nonempty subset of S has a least element.

- **Lexicographic Order**

Given two posets $(A_1, \preccurlyeq_1)$ and $(A_2, \preccurlyeq_2)$, the lexicographic ordering on $A_1 \times A_2$ is defined by specifying that (a_1, a_2) is less than (b_1, b_2)

$\Rightarrow (a_1,a_2) \prec (b_1,b_2)$ either if $a_1 \prec_1 b_1$ or if $a_1 = b_1$ and $a_2 \prec_2 b_2$

Hasse Diagrams

- a visual representation of a partial ordering that leaves out edges that must be present because of reflexive and transitive properties

- **Terminology**

$(S, \preccurlyeq)$: poset
$$\begin{cases} a \text{ is maximal in } (S,\preccurlyeq) \text{ if there is no } b \in S \text{ such that } a \preccurlyeq b \text{ (top of the Hasse diagram)} \\ a \text{ is minimal in } (S,\preccurlyeq) \text{ if there is no } b \in S \text{ such that } b \preccurlyeq a \text{ (bottom} \cdots) \\ a \text{ is greatest element} \\ \quad\ \text{least element} \end{cases}$$

Theorem. The greatest and least element of the poset $(A, \preccurlyeq)$ are unique when they exist.

- upper / lower bound, least upper bound, greatest lower bound

- lattices. every pair of elements has both a least upper bound and greatest lower bound

* Every totally ordered set is a lattice.

Topological Sorting

- A total ordering $\preceq$ is said to be compatible with the partial ordering R if $a \preceq b$ whenever aRb

Topological Sorting: constructing a compatible total ordering from a partial ordering

Lemma 1: Every finite nonempty poset $(S, \preceq)$ has at least one minimal element

Graphs

Graphs and Graph Models

① $G=(V,E)$, consist of { V: a nonempty set of vertices
E: a set of edges }

Each edge has either one or two vertices associated with it → endpoints

An edge is said to connect its endpoints

② Simple Graph { each edge connects two different vertices
no two edges connect the same pair of vertices }

Multigraph: have multiple edges connecting the same vertices

Pseudograph: may include loops and possibly multiple edges connecting the same pair of vertices

③ A direct graph (digraph) (V,E) { a nonempty set of vertices V
a set of directed edges E (associated with an ordered pair of vertices) } (u,v): start at u and end at v

{ Simple directed graph
directed multigraph: multiple directed edges from a vertex to a second vertex (possibly the same) }

Graph Terminology

Undirected Graphs $G=(V,E)$

{ vertex, edge
If $\{u,v\}$ is an edge in an undirected graph G, they are called adjacent (or neighbours) in G
An edge e connecting u and v is called incident with vertices u and v
loop
The degree of a vertex: the number of edges incident with it, except that a loop at a vertex contributes twice to the degree of that vertex. }

$\deg(v)$. if $\deg(v)=0$, v is called isolated If $\deg(v)=1$ → pendant

Theorem 1. (The Handshaking Theorem)

$G=(V,E)$ be an undirected graph with e edges. Then $\sum_{v\in V}\deg(v)=2e$

Theorem 2. An undirected graph has an even number of vertices of odd degree

Directed Graphs $G=(V,E)$

{ (u,v) be an edge in G. Then u is an initial vertex and is adjacent to v and v is a terminal vertex and is adjacent from u
In degree of a vertex v, denoted $\deg(v)$ is the number of edges which terminate at v $\deg^-(v)$
Out degree of v .... initiate $\deg^+(v)$ }

Theorem 3

Let $G=(V,E)$ be a graph with direct edges Then $\sum_{v\in V} d^+(v)=\sum_{v\in V} d^-(v)=|E|$

Some Special Simple Graphs

1° Complete Graphs - K_n: simple graph with { n vertices
exactly one edge between every pair of distinct vertices }

2° Cycle C_n $(n\geq 3)$ 

3° Wheel W_n $(n\geq 3)$ 

4° n-Cubes Q_n $(n\geq 0)$ { graph with 2^n vertices representing bit strings of length n
An edge exists between two vertices that differ in exactly one bit position }

Bipartite Graphs

A simple graph G is bipartite if V can be partitioned into two disjoint subsets V_1 and V_2 such that every edge connects a vertex in V_1 and a vertex in V_2

* There are no edges which connect vertices in V_1 or in V_2

◎ The complete bipartite graph: V_1 and V_2, every vertex in V_1 is connected to every vertex in V_2, denoted by $K_{m,n}$, $m=|V_1|$, $n=|V_2|$

Theorem 4

A simple graph is bipartite iff it's possible to assign one of two different colors to each vertex of the graph so that no two adjacent vertices are are assigned the same color.

◎ Regular graph. every vertex of this graph has the same degree

n-regular

Bipartite Graphs and Matchings

◎ A matching M in a simple graph $G=(V,E)$: a subset of E such that no two edges are incident with the same vertex

◎ A vertex that is the endpoint of an edge of a matching M is said to be matched in M.

A maximum matching → with the largest number of edges

◎ A matching M in a bipartite graph $G=(V,E)$ with bipartition (V_1,V_2) a complete matching from V_1 to V_2 if every vertex in V_1 is the endpoint of an edge in the matching

Theorem 5 (Hall's marriage theorem)

The bipartite graph $G=(V,E)$ with bipartition (V_1, V_2) has a complete matching from V_1 to V_2 iff $|N(A)|\geq|A|$ for all $A\subseteq V_1$

◎ New Graphs from Old

$G=(V,E)$, $H=(W,F)$.

H is a subgraph of G if $W\subseteq V$, $F\subseteq E$

Subgraph H is a proper subgraph of G if $H\neq G$

H is a spanning subgraph of G if $W=V$, $F\subseteq E$.

Representing Graphs and Graph Isomorphism

Representing Graphs

{Graphs

Adjacency lists → lists that specify all the vertices that are adjacent to each vertex.

◎ Adjacency Matrices

* Adjacency matrices of undirected graphs are always symmetric.

◎ The adjacency matrix of a multigraph or pseudograph

⇒ matrices of nonnegative integers

◎ The adjacency matrix of a directed graph

◎ Incidence Matrices

Isomorphism of Graphs

Graphs with the same structure are said to be isomorphic.

⇒ one-to-one correspondence between vertices of the two graphs that preserves the adjacency relationship.

Connectivity

Paths

A path of length n in a simple graph is a sequence of vertices $v_0, v_1, \dots, v_n$ such that $\{v_0, v_1\} \cdots \{v_{n-1}, v_n\}$

The path is a circuit if it begins and ends at the same vertex (length greater than 0)

A path is simple if it does not contain the same edge more than once.

* A path of length zero consists of a single vertex.

Path in directed graph.

Counting paths between vertices

→ using its adjacency matrix

Theorem 2:

The number of different paths of length r from v_i to v_j is equal to the (i,j)th entry of A^r.

A → adjaceny matrix representing the graph consisting of $v_1, \dots, v_n$ (standard power of A)

Connectedness in undirected graphs

An undirected graph is called connected if there is a path between every pair of distinct vertices of the graph.

Theorem 1.

There is a simple path between every pair of distinct vertices of a connected undirected graph

The maximally connected subgraphs of G are called the connected components

A vertex is a cut vertex (or articulation point) if removing it and all edges incident with it results in more connected components than in the original graph.

* a cut edge / bridge

Connectedness in directed graphs

A directed graph is strongly connected if there is a path from a to b and from b to a for all vertices

Weakly connected → underlying undirected graph is connected.

* Strongly connected components → the maximal strongly connected subgraphs

Paths and Isomorphism

Euler Paths

Konigsberg Seven Bridge Problem

Terminologies: Euler Path. a simple path containing every edge of G
Euler Circuit. a simple circuit - - -
Euler Graph: A graph contains an Euler circuit

Theorem 1: A connected multigraph has an Euler circuit iff each of its vertices has an even degree

Proof: Necessary: a: begins with
intermediate vertices

Sufficient: construct ...

Theorem 2. A connected multigraph has an Euler path but not an Euler circuit iff it has exactly two vertices of odd degree.

Euler circuit and paths in directed graphs

A directed multigraph having no isolated vertices
- has an Euler circuit iff weakly connected, $\deg^+ = \deg^-$ for each vertex
- has an Euler path iff weakly connected, $\deg^+ = \deg^-$ for all but two vertices: one $\deg^- = \deg^+ + 1$, one $\deg^+ = \deg^- + 1$

Hamilton paths and circuit

A Hamilton path in a graph G is a path which visits every vertex in G exactly once.

A Hamilton circuit (or Hamilton cycle) is a cycle which visits every vertex exactly once, except for the first vertex, which is also visited at the end of the cycle.

If a connected graph G has a Hamilton circuit $\rightarrow$ G is called a Hamilton graph.

The sufficient condition for the existence of Hamilton path and Hamilton circuit.

Theorem 3 DIRAC' Theorem

If G is a simple graph with n vertices with $n \geq 3$ such that the degree of every vertex in G is at least $\frac{n}{2}$, then G is a Hamilton circuit

Theorem 4. ORE' Theorem

If G is a simple graph with n vertices with $n \geq 3$ such that $deg(u)+deg(v) \geq n$ for every pair of nonadjacent vertices u and v in G then G has a Hamilton circuit

The necessary condition

For undirected graph
- G is connected
- There are at most 2 vertices whose degree are less than 2

The degree of each vertex is larger than 1

Properties
- If a vertex in the graph has degree two, $\rightarrow$ both edges that are incident with this vertex must be part of any Hamilton circuit.
- When a Halmilton circuit is being constructed and this circuit has passed through a vertex, all the other can be removed.

① G is a Hamilton graph, for any nonempty subset S of set V, the number of connected components in $G-S \leq |S|$

Shortest Path Problems

① Weighted graph $G=(V,E,W)$: assign weights to the edges of graphs

② Length of a path in a weighted graph : the sum of the weights of the edges of this path

A Shortest path algorithm

Dijkstra's Algorithm (undirected graph with positive weights)

① Proceed by forming a distinguished set of vertices iteratively

Let S_k denote this set of vertices after k iterations of labeling procedure.

Step 1: Label a with 0 and other with ∞ $L_0(a)=0$, $L_0(v)=\infty$, $S_0=\phi$

Step 2: S_k is formed from S_{k-1} by adding a vertex u not in S_{k-1} with the smallest label.

Once u is added to S_k, we update the labels of all vertices not in S_k, so that $L_k(v)$ is the length of the shortest path from a to v that contain vertices only in S_k

$L_k(v) = \min\{L_{k-1}(v), L_{k-1}(u)+w(u,v)\}$

Theorem 1: Dijkstra's algorithm finds the length of a shortest path between two vertices in a connected simple undirected positive weighted graph

Theorem 2. Dijkstra's algorithm uses $O(n^2)$ operations (additions and comparisons)

Planar Graphs

◎ If it can be drawn in the plane without any edges crossing.

* Such a drawing is called a planar representation of the graph.

◎ Euler's Formula

region: A region is a part of the plane completely disconnected off from other parts of the plane by the edges of the graph.

{ Bounded region
{ Unbounded region

* There is one unbounded region in a planar graph

Theorem 1: Euler's formula

Let G be a connected planar simple graph with e edges and v vertices. Let r be the number of regions in a planar representation of G. Then $r = e - v + 2$ (Proof)

* Note: The Euler's formula is a necessary condition

◎ Suppose R is a region of a connected planar simple graph, the number of the edges on the boundary of R is called the Degree of R.

$Deg(R)$

Corollary 1 If G is a connected planar simple graph with e edges and v vertices where $v \geq 3$, then $e \leq 3v - 6$

* The equality holds iff every region has exactly three edges

* For unconnected planar simple graph, $e \leq 3v - 6$ also holds

Corollary 2. If G is a connected planar simple graph, then G has a vertex of degree not exceeding five.

Corollary 3. If a connected planar simple graph has e edges and v vertices, with $v \geq 3$ and no circuit of length 3, $e \leq 2v - 4$

◎ Kuratowski's Theorem

Elementary subdivision

Homeomorphic. $G_1 = (V_1, E_1)$, $G_2 = (V_2, E_2)$ are called homeomorphic if they can be obtained from the same graph by a sequence of elementary subdivision

Theorem 2: A graph is nonplanar iff it contains a subgraph homeomorphic to $K_{3,3}$ or K_5

Graph Coloring

◎ The dual graph of the map
{ Each region of the map is represented by a vertex
{ An edge connect two vertices if the regions represented by these vertices have a common border
{ Two regions that touch at only one point are not considered adjacent.

Terminologies. Coloring: A coloring of a simple graph is the assignment of a color to each vertex so that no two adjacent vertices are assigned the same color.

{ The chromatic number of a graph → the least number of colors needed for a coloring of graph.
$\chi(G)$

Theorem 1 The chromatic number of a planar graph is no greater than four

* $\chi(G)$ $K_n = n$.
{ A simple graph with a chromatic number of 2: bipartite

Applications

Trees

① Definition 1: A tree is a connected undirected graph with no simple circuits

* Forest: an undirected graph with no simple circuits. (不一定 connected)

Any tree must be a simple graph

Each connected components of forest is tree

Theorem 1: An undirected graph is a tree iff there is a unique simple path between any two of its vertices

Rooted Tree

① a particular vertex of a tree → designated as the root

→ direct each edge away from the root.

* Terminology: Parent: v → the unique vertex u with a directed edge from u to v.

Child: v → the child of u

Vertices with the same parent are called siblings.

Ancestors: The ancestors of a non-root vertex are all the vertices in the path from root to this vertex

Descendants

Leaf: A vertex is called a leaf if it has no children.

Internal vertex: has children

Subtree

Binary Tree

① A rooted tree is called a m-ary tree if every internal vertex has no more than m children.

It's a binary tree if $m=2$

full m-ary tree: every internal vertex has exactly m children.

Ordered rooted tree

a rooted tree where the children of each internal vertex are ordered

The tree rooted at the left child → left subtree. right subtree

Tree Properties

Theorem 2 A tree with n vertices has $n-1$ edges

Theorem 3 A full m-ary tree with i internal vertices contains $n=mi+1$ vertices

Theorem 4 A full m-ary tree with ($n=mi+1$, $n=i+l$)

n vertices has $i=\frac{n-1}{m}$ internal vertices and $l=\frac{[(m-1)n+1]}{m}$ leaves

i internal vertices has $n=mi+1$ vertices and $l=(m-1)i+1$ leaves

l leaves has ...

level: the length of the unique path from the root to v.

height: maximum of the levels of its vertices

Balanced: all its leaves are at levels h or $h-1$

Theorem 5: There're at most m^h leaves in an m-ary tree of height h

If an m-ary tree of height h has l leaves. $h \geq \lceil \log_m l \rceil$

full and balanced ⇒ $h=\lceil \log_m l \rceil$

11.2 Applications of Trees

Binary Search Trees

Concepts
- used to store items in its vertices
- Binary Search Tree.
  - An ordered rooted binary tree
  - Each vertex contains a distinct key value
  - key values can be compared using "greater than" "less than"
  - key value of each vertex → less than every key value in its right subtree
    - greater than ... left ..

Construct the binary search tree

Decision Trees

Prefix Codes
- Definition
- construct prefix codes
  - Using a binary tree
    - left edge at each internal vertex → 0
    - right ... → 1
  - Huffman Coding

11.3 Tree Traversal

① Traversal Algorithms : systematically visiting every vertex of an ordered rooted tree

Preorder traversal root → left subtree → right subtree

Inorder traversal left subtree → root → right subtree

Postorder traversal left subtree → right subtree → root

② Infix. prefix. postfix notation

A binary Expression Tree
- Each leaf node contains a single operand
- nonleaf node contains a single operator

* the fully parenthesized expression obtained by an inorder traversal of the binary tree is said to be in infix form

* prefix form (Polish notation)

* postfix form (reverse polish notation)

11.4 Spanning Trees

① Definition: A spanning tree of G (simple graph) is a subgraph of G that is a tree containing every vertex of G

Theorem 1: A simple graph is connected iff it has a spanning tree

Depth-first search (back tracking)

Breath-first search

11.5. Minimum Spanning Trees

① Definition: a spanning tree that has the smallest sum of weights of its edges

Prim's algorithm

Kruskal's algorithm

Network Flow

◎Definitions:

Flowgraph: Directed graph with distinguished vertices s (source 源点) ant t (sink, 收点/汇点)

Capacities on the edges: $c(e) >= 0$

◎Problem: assign flows $f(e)$ to the edges such that $\begin{cases} 0 <= f(e) \le c(e) \\ \text{Flow is conserved at vertices other than } s, t. \end{cases}$

优化目标: The flow leaving the source is as large as possible

Flows.

An s-t flow (可行流) is a function that satisfies:

$\begin{cases} \text{For each edge } e \in E, \quad 0 \le f(e) \le c(e) & \text{[capacity]} \\ \text{For each } v \in V - \{s,t\}: \sum_{in} f(e) = \sum_{out} f(e) & \text{[conservation]} \end{cases}$

特例: 零流

The value of a flow f: $v(f) = \sum_{e \text{ out of } s} f(e)$

Max flow problem: Find s-t flow of maximum value

Cuts in a graph

Cut: Partition of V into disjoint sets S, T with s in S and t in T

$Cap(S,T)$: sum of the capacities of edges from S to T

$Flow(S,T)$: net flow out of S (out of minus into)

$Flow(S,T) \le Cap(S,T)$

Cuts $\begin{cases} \text{An s-t cut} \to \text{a partition } (A,B) \text{ of } V \text{ with } s \in A, t \in B \\ \text{The capacity of a cut } (A,B): \sum_{e \text{ out of } A} c(e) \end{cases}$

Minimum Cut Problem

→ Find an s-t cut of minimum capacity

Flows and Cuts

Flow value lemma. $\sum_{e \text{ out of } A} f(e) - \sum_{e \text{ into } A} f(e) = v(f)$

Let f be any flow, and let (A,B) be any s-t cut. Then, the net flow sent across the cut is equal to the amount leaving s

* The value of the flow is at most the capacity of the cut

* $v(f) \le cap(A,B)$. $\left[v(f) = \sum_{e \text{ out of } A} - \sum_{e \text{ into } A} \le \sum_{e \text{ out of } A} f(e) \le \sum_{e \text{ out of } A} c(e) = cap(A,B) \right]$

◎ **Corollary**: If $v(f) = cap(A,B)$ → f is a max flow and (A,B) is a min cut

Towards a Max Flow Algorithm

Greedy Algorithm. $\begin{cases} \text{Start with } f(e) = 0 \text{ for all edges } e \in E \\ \text{Find an s-t path } P \text{ where each edge has } f(e) < c(e) \\ \text{Augment flow along } P \\ \text{Repeat until got stuck} \end{cases}$

Residual Graph

- Flow graph showing the remaining capacity

Augmenting Path Algorithm

Augmenting Path

- Vertices $v_1, \cdots, v_k$
- $v_1 = s$, $v_k = t$.
- possible to add b units of flow between v_j and v_{j+1}

↳ 所有正向边: $f(u,v) < c(u,v)$
所有逆向边: $f(u,v) > 0$
⇒ 可增加流量

Ford-Fulkerson Algorithm

Max-Flow Min-Cut Theorem

Augmenting path theorem: Flow f is a max flow iff there are no augmenting paths

Max-flow min-cut theorem. The value of the max flow is equal to the value of the min cut.

↳ finds a flow where the residual graph is disconnected. hence FF finds a maximum flow.