1.1~1.3

proposition

whether T or F → $\underbrace{\text{T or F}}$ truth table

proposition → logic operators (connectives):
- $\neg p$ (propositional variables)
- $p \wedge q$
- $p \vee q$
- $p \oplus q$
- $p \downarrow q$ ($F \downarrow F \equiv T$)
- $\boxed{p \to q}$ → conditional statement

p: hypothesis, antecedent, premise
q: conclusion, consequence

converse: $q \to p$
inverse: $\neg p \to \neg q$
contrapositive: $\neg q \to \neg p$

contrapositive — equivalent — $p \to q$

if p, then q if p, q p implies q p only if q	q when/whenever p q unless $\neg p$ q follows from p q if p
a necessary condition for p is q	a sufficient condition for q is p
p is sufficient for q	q is necessary for p q provided that p

↓

biconditional statement: $p \leftrightarrow q$ →
- p is necessary and sufficient for q
- if p then q, and conversely
- p iff q
- p exactly when q

translating sentence:

s1. define propositional variables
s2. use connectives to combine them

- Truth Table
- Precedence:

column ↓ , row →

$\neg$	1
$\wedge$	2
$\vee$	3
$\to$	4
$\leftrightarrow$	5

$\forall, \exists$ higher than all of them

- Bit Operations ($T \to 1$, $F \to 0$)
  - bitwise OR
  - bitwise AND
  - bitwise XOR

bit string: a sequence of zero or more bits

consistent: → a list of propositions
→ have a possible truth value of variables for all propositions to be true

- logic puzzles
  (define p, q and find to judge p, q's truth value)
- judge, find

classification
- tautology → $p \leftrightarrow q$ is a tautology ⇒ logically equivalent → $p \equiv q$, $p \Leftrightarrow q$
  - show: ① truth table ② already-proved equivalences
- contradiction
- contingency

not logical equivalent: find a counterexample

① $p \wedge T \equiv p$	$p \vee F \equiv p$
② $p \vee T \equiv T$	$p \wedge F \equiv F$
③ $p \vee p \equiv p$	$p \wedge p \equiv p$
④ $\neg(\neg p) \equiv p$	
⑤ $p \vee q \equiv q \vee p$	$p \wedge q \equiv q \wedge p$
⑥ $(p \vee q) \vee r \equiv p \vee (q \vee r)$	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
⑦ $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
⑧ $\neg(p \wedge q) \equiv \neg p \vee \neg q$	$\neg(p \vee q) \equiv \neg p \wedge \neg q$
⑨ $p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
⑩ $p \vee \neg p \equiv T$	$p \wedge \neg p \equiv F$
⑪ $p \to q \equiv \neg p \vee q$	
⑫ $p \leftrightarrow q = (p \to q) \wedge (q \to p)$	

- satisfiable
- unsatisfiable: negation is a tautology

*Sudoku problem:

$\bigwedge_{i=1}^{9} \bigwedge_{n=1}^{9} \bigvee_{j=1}^{9} p(i,j,n)$ every row contains every number

$\bigwedge_{j=1}^{9} \bigwedge_{n=1}^{9} \bigvee_{i=1}^{9} p(i,j,n)$ every column contains every number

$\bigwedge_{r=0}^{2} \bigwedge_{s=0}^{2} \bigwedge_{n=1}^{9} \bigvee_{i=1}^{3} \bigvee_{j=1}^{3} p(3r+i, 3s+j, n)$ every 3x3 blocks ...

$p(i,j,n) \to \neg p(i,j,n')$ no cell contains more than one number

1.4~1.5

predicate ⟶ $P(x_1, x_2, \dots, x_n)$: n-place (n-ary) predicate — predicate logic (calculus)

quantifiers

- universal quantification $\forall x P(x)$ (↳ universal quantifier) ($\equiv P(x_1)\wedge P(x_2) \wedge \dots \wedge P(x_n)$)
  - counterexample $P(x)\equiv F$
  - domain: range of x
  - ways to express: For all / every / each / arbitrary / any
    - All of / Given any
  - when express, don't forget define the domain
- existensial quantification $\exists x P(x)$ ($\equiv P(x_1) \vee P(x_2) \vee \dots \vee P(x_n)$)
  - ↳ existential quantification
  - $\exists_1 P(x)$ / $\exists ! P(x)$: exist a unique x such that P(x) is true

bound variable ⟷ **free variable**

↑ all variables in a propositional function ← when translating, it must be checked

logically equivalent (have the same truth value)

$\forall x(A(x)\wedge B(x)) \equiv \forall x A(x) \wedge \forall x B(x)$ $\qquad$ $\forall x(A(x)\vee B(x)) \not\Leftrightarrow \forall x A(x) \vee \forall x B(x)$

$\exists x(A(x)\vee B(x)) \equiv \exists x A(x) \vee \exists x B(x)$ $\qquad$ $\exists x(A(x)\wedge B(x)) \not\Leftrightarrow \exists x A(x) \wedge \exists x B(x)$

De Morgan's laws: $\neg\forall x P(x) \equiv \exists x \neg P(x)$ $\qquad$ $\neg\exists x P(x) \equiv \forall x \neg P(x)$

x not occurring in A:

$\forall x P(x) \vee A \equiv \forall x (P(x) \vee A)$ $\qquad$ $\forall x P(x) \wedge A \equiv \forall x (P(x) \wedge A)$

$\exists x P(x) \vee A \equiv \exists x (P(x) \vee A)$ $\qquad$ $\exists x P(x) \wedge A \equiv \exists x (P(x) \wedge A)$

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

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

Order matters: $\forall x \forall y P(x,y) \equiv \forall y \forall x P(x,y)$ $\qquad$ $\exists x \forall y P(x,y) \not\Leftrightarrow \forall y \exists x P(x,y)$

translating tips:
- All $S(x)$ are $O(x)$: $\forall x (S(x) \to O(x))$
- No $S(x)$ are $O(x)$: $\forall x (S(x) \to \neg O(x))$
- Some $S(x)$'s are $O(x)$: $\exists x (S(x) \wedge O(x))$
- Some $S(x)$ are not $O(x)$: $\exists x (S(x) \wedge \neg O(x))$

nested quantifiers (multiple variables)

functionally complete logically equivalent to sth. involving only $\wedge, \vee, \neg$ / $\vee(\wedge), \neg$ → functionally complete

- literal P, $\neg P$
- clause
  - disjunctive clause
  - conjunctive clause
- CNF $(A_{11} \vee \dots \vee A_{1n_1}) \wedge \dots \wedge (A_{k1} \vee \dots \vee A_{kn_k})$
- DNF $(A_{11} \wedge \dots \wedge A_{1n_1}) \vee \dots \vee (A_{k1} \wedge \dots \wedge A_{kn_k})$ → FDNF disjunction of minterms
  - ① DNF
  - ② use laws to add all variables

Prenex Normal Form $Q_1x_1 Q_2x_2 \cdots Q_nx_n B$ → quantifier free

translating step:
- s1. $\to$, $\leftrightarrow$
- s2. move in all '$\neg$'
- s3 rename the variables
- s4. move all quantifiers front

1.6

argument — premises → conclusion

⇓ whenever all premises are true, the conclusion is also true

valid → prove: s1. assume the premises are true
s2. determine conclusion is true

*if conclusion is $p \to q$, we can:

$p_1 \wedge p_2 \wedge \dots \wedge p_n \to (p \to q) \Rightarrow p_1 \wedge p_2 \wedge \dots \wedge p_n \wedge p \to q$

(logically equivalent)

addition premise

rules of inference:

p, $p \to q$, $\therefore q$ Modus Ponens	$p \to q$, $q \to r$, $\therefore p \to r$ Hypothetical syllogism	p, $\therefore p \vee q$ Addition	p, q, $\therefore p \wedge q$ conjunction
$\neg q$, $p \to q$, $\therefore \neg p$ Modus Tollens	$p \vee q$, $\neg p$, $\therefore q$ Disjunctive Syllogism	$p \wedge q$, $\therefore p$ simplification	$p \vee q$, $\neg p \vee r$, $q \vee r$ resolution

resolution → write the premise and conclusion as clauses (using '$\vee$')

for quantified statements

$\forall x P(x)$, $\therefore P(c)$ u.i	$\exists x P(x)$, $\therefore P(c)$ for some element c E.i
$P(c)$ for an arbitrary c, $\therefore \forall x P(x)$ u.g.	$P(c)$ for some element c, $\therefore \exists x P(x)$ E.g

Universal modus ponens:

$\forall x (P(x) \to Q(x))$

$P(a)$, where a is a particular element in the domain

$\therefore Q(a)$

Universal modus tollens

$\forall x (P(x) \to Q(x))$

$\neg Q(a)$, where a is a particular element in the domain

$\therefore \neg P(a)$

1.7~1.8

proof methods:

direct proofs

proof by contraposition $P \to Q \equiv \neg Q \to \neg P$

vacuous proof $P \to Q$ (P is F)

trivial proof $P \to Q$ (Q is T)

proof p by contradiction assume p is false Additional hypothesis $\neg(s \vee r) \Rightarrow$ contradiction $\Rightarrow s \vee r$

proofs of equivalence $p_1 \leftrightarrow p_2 \leftrightarrow \dots \leftrightarrow p_n \equiv [(p_1 \to p_2) \wedge (p_2 \to p_3) \wedge \dots \wedge (p_n \to p_1)] \Rightarrow p_1, p_2, \dots, p_n$ are equivalent

proof by cases

existence proof — constructive existence proof find $P(c)$
— nonconstructive existence proof derive contradiction if $\neg \exists c$

uniqueness proof $\exists x (P(x) \wedge \forall y (y \neq x \to \neg P(y)))$ — existence, uniqueness

forward reasoning

backward reasoning

2.1~2.2

cartesian product $A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \dots, a_n) \mid a_i \in A_i, \text{for } i=1 \text{ to } n\}$

ordered n-tuple $(a_1, a_2, \dots, a_n) = (b_1, b_2, \dots, b_n) \Leftrightarrow a_i = b_i$

2-tuples → ordered pairs

unordered

set $\xrightarrow{\text{contain}}$ elements/members $\xrightarrow{\text{exactly/distinct}}$ finite – cardinality / infinite

$\emptyset$ void set / null set / empty set

subset ⟶ power set (2^n)

equal

proper subset

truth set the truth set of $P = \{x \in D \mid P(x)\}$

union $A \cup B$ (the cardinality of $A \cup B$: $|A \cup B| = |A| + |B| - |A \cap B|$) ⟹ Generalized Unions and Intersections

$A_1 \cup A_2 \cdots \cup A_n = \bigcup_{i=1}^{n} A_i$

$A_1 \cap A_2 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i$

⇓ bitwise

intersection $A \cap B$ → disjoint $A \cap B = \emptyset$

difference of A and B $A - B = \{x \mid x \in A \wedge x \notin B\}$ > $A - B = A \cap \bar{B}$

the complement of a set $\bar{A} = \{x \mid x \notin A, x \in U\}$

symmetric difference $A \oplus B = (A \cup B) - (A \cap B)$

⇓

set indentities

$A \cup \emptyset = A$, $A \cap U = A$ $A \cup U = U$, $A \cap \emptyset = \emptyset$ $A \cup A = A$, $A \cap A = A$ $\bar{\bar{A}} = A$ $A \cup B = B \cup A$, $A \cap B = B \cap A$ $A \cup (B \cup C) = (A \cup B) \cup C$, $A \cap (B \cap C) = (A \cap B) \cap C$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $\overline{A \cup B} = \bar{A} \cap \bar{B}$ $\overline{A \cap B} = \bar{A} \cup \bar{B}$

* ways to prove set identities:

① $A \subseteq B$ & $A \supseteq B$ $\forall x \in B \Rightarrow (a, b)$ turn A into $A = \{x \mid x \in A\}$ use logical equivalence

② logical equivalence

③ membership table

④ previously proven identities

→ prove $\emptyset$: suppose to the contrary

don't try to express all the elements because not all sets are finite

2.3

function / mapping / transformations $f: A \to B$ (f maps A to B; A: domain, B: codomain) $\forall a (a \in A \to \exists! b (b \in B \wedge f(a) = b))$ (a: preimage, b: image, range) ⟹ graph: $\{(a, b) \mid a \in A \wedge f(a) = b\}$

$(f_1 + f_2)(x) = f_1(x) + f_2(x)$

$(f_1 f_2)(x) = f_1(x) f_2(x)$

$f(S) = \{f(s) \mid s \in S\}$ (S: a subset of A) ⟹
- $f(\emptyset) = \emptyset$
- $f(\{a\}) = \{f(a)\}$
- $f(A \cup B) = f(A) \cup f(B)$
- $f(A \cap B) \subseteq f(A) \cap f(B)$

one-to-one / injective → injection
$\forall a \forall b (f(a) = f(b) \to a = b)$

onto / surjective → surjection
$\forall b \in B \, \exists a \in A (f(a) = b)$

are used to prove
show not: find a counterexample

> one-to-one correspondence / bijection → same cardinality

only → inverse function $f^{-1}(y) = x$ iff $f(x) = y$

monotonic function f
- monotonically (strictly) increasing: $\forall x \forall y (x < y \to f(x) < f(y))$
- monotonically (strictly) decreasing: $\forall x \forall y (x > y \to f(x) > f(y))$

composition of functions $f \circ g(a) = f(g(a))$ ⟹ the range of $g \subseteq$ the domain of f

floor function $\lfloor x \rfloor$ → real number let $x = n + \varepsilon$

ceiling function $\lceil x \rceil$ let $x = n - \varepsilon$

分成整数和小数部分

2.4

sequence $n \to a_n$ (integer) $\Rightarrow$ notation of sequence $\{a_n\}$
sequence of $\{a_n\}$: $a_1, a_2, \dots, a_n, \dots$
order matters

- geometric progression ar^n
- arithmetic progression $a+nd$
- summations $\sum_{i=m}^{n} a_i = \sum_{i=m}^{n} a_i = \sum_{m \le i \le n} a_i$
  - $\sum_{s \in S} f(s)$

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

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

2.5

$|A|=|B| \Leftrightarrow$ bijection $\longrightarrow$ countable (finite / same cardinality as Z^+), uncountable

$|A| \le |B| \Leftrightarrow$ injection $\xrightarrow[\text{cardinality}]{\text{different}}$ $|A|<|B|$

$|A| \to$ countable infinite
$\parallel$
$|Z^+| \to \aleph_0$ (aleph null)

$\Rightarrow$ the union of a countable number of countable sets is countable.

$*$ important examples: ① Q^+ countable

② $(0,1)$ $\mathbb{R}$ uncountable

③ $[0,1]$ $\mathbb{R}$ same cardinality as $(0,1)$ $\mathbb{R}$

$\boxed{\begin{array}{l} |A| \le |B| \\ |A| \ge |B| \end{array}}$ then $\longrightarrow |A|=|B|$ S-B Theorem

$[0,1)$
$\parallel$
$[\frac{1}{4}, \frac{3}{4}]$

$|P(A)| > |A|$

The Continuum Hypothesis there is no a such that $\aleph_0 < a < \aleph_1$

computerbility
- computable
- uncomputable

chapter 3

algorithm
- input, output
- definiteness, correctness
- finiteness, effectiveness (each step in a finite amount of time)
  - finite number of steps
- generality

Pseudocode

$*$ Halting problem:

那么，如何来证明这个停机问题呢?
反证!假设我们某一天真做出了这么一个极度聪明的万能算法（就叫God_algo吧），你只要给它一段程序（二进制描述），再给它这段程序的输入，它就能告诉你这段程序在这个输入上会不会结束（停机），我们来编写一下我们的这个算法吧:

```
bool God_algo(char* program, char* input)
{
    if(<program> halts on <input>)
        return true;
    return false;
}
```

这里我们假设if的判断语句里面是你天才思考的结晶，它能够像上帝一样洞察一切程序的宿命。现在，我们从这个God_algo出发导出一个新的算法:

```
bool Satan_algo(char* program)
{
if( God_algo(program, program) )
{
     while(1);       // loop forever!
     return false;   // can never get here!
}
else
     return true;
}
```

正如它的名字所暗示的那样，这个算法便是一切邪恶的根源了。当我们把这个算法运用到它自身身上时，会发生什么呢?
Satan_algo(Satan_algo);
我们来分析一下这行简单的调用:
显然，Satan_algo(Satan_algo)这个调用要么能够运行结束返回（停机），要么不能返回（loop forever）。
如果它能够结束，那么Santa_algo算法里面的那个if判断就会成立（因为God_algo(Santa_algo,Santa_algo)将会返回true），从而程序便进入那个包含一个无穷循环while(1);的if分支，于是这个Satan_algo(Satan_algo)调用便永远不会返回（结束）了。
如果不能结束（停机），则if判断就会失败，从而选择另一个if分支并返回true，即Satan_algo(Satan_algo)又能够返回（停机）。
总之，我们有:
Satan_algo(Satan_algo)能够停机=> 它不能停机
Satan_algo(Satan_algo)不能停机=> 它能够停机

① find the maximum

② search — linear search or sequential search
  - binary search

③ sort

$\rightarrow$ Optimization problem
Greedy Algorithms (each step. not the whole)

Big-O Notation

"$f(x)$ is $O(g(x))$" $\Longleftrightarrow \exists C, k$ s.t $\forall x (x>k \to |f(x)| \le C|g(x)|)$
$\in$

proof: ① $f(x) \in O(g(x))$: find a pair of C, k.

② $f(x) \notin O(g(x))$: use $f(x) \le C g(x)$ to work out $x < \_\_$

$o(1) < o(\log^b n) < o(n) < o(n\log n) < o(n^b) < o(b^n) < o(n!)$ ($\log(n!)$?)

① Addition of functions —— $(f_1+f_2)(x) = O(\max(g_1(x), g_2(x)))$

② Multiplication of functions —— $(f_1 f_2)(x) = O(g_1(x) g_2(x))$

$\rightarrow$ Big-Theta

"$f(x)$ is $\Theta(g(x))$" $\Leftrightarrow \exists C_1, C_2, K$
$\forall x (x>k \to 0 \le C_1 g(x) \le f(x) \le C_2 g(x))$

proof: find a pair of C_1, C_2, K

Big-Omega

"$f(x)$ is $\Omega(g(x))$" $\Leftrightarrow \exists C, k$ s.t. $\forall x (x>k \to |f(x)| \ge C|g(x)|)$

- Space Complexity
- Time Complexity —— comparisons ..

chapter 5 the well-ordering property (nonegative integers (nonempty)) → proof ① set a ~~nonempty~~ nonpositive set S ② find the least element and suppose the goal is False ③ work out contradiction (find an element smaller than the "least element")

mathematical induction { basis step $P(1)$; inductive step $\forall k\,(P(k)\to P(k+1))$; conclusion $\therefore \forall n\, P(n)$ } → more general form: $P(b)$, $\forall k\,(k\geq b \to (P(k)\to P(k+1)))$, $\therefore \forall n \geq b\; P(n)$

strong induction $P(n_0) \wedge \forall k \geq n_0 (P(n_0)\wedge P(n_0+1)\wedge \dots \wedge P(k) \longrightarrow P(k+1)) \to \forall n \geq n_0 (P(n))$

↓

polygon (use the interior diagonal)

recursively defined functions { basis step; recursive step } ⟶ more general version (first k nonegative integers)

euclidean algorithm: $a=bq+r \Rightarrow \gcd(a,b)=\gcd(b,r)$

LAME'S Theorem

recursively defined sets { basis step — initial collection of elements; recursive step — rules for forming new elements }

structural induction { basis step; recursive step }

some examples see the "chapter 5" note

	Weak mathematical	Strong Mathematical	Structural
Used for	Usuall formulae	Usual formulae not provable via mathematical induction	Only things defined via recursion
Assumption	Assume P(k)	Assume P(1), P(2), …, P(k)	Assume statement is true for some "old" elements
What to prove	True for P(k+1)	True for P(k+1)	Statement is true for some "new" elements created with "old" elements
Step 1 called	Base case	Base case	Basis step
Step 2 called	Inductive step	Inductive step	Recursive step

chapter 6

{ The sum rule
The product rule
The Inclusion-Exclusion Principle (subtraction rule) { $|A\cup B|=|A|+|B|-|A\cap B|$; $|\bar{A}\cap\bar{B}|=|\overline{A\cup B}|=|U|-|A\cup B|=|U|-(|A|+|B|-|A\cap B|)$ }
Tree diagrams }

The 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

examples: ①

(3) In a party of 2 or more people, there are 2 people with the same number of friends in the party. (Assuming you can't be your own friend and that friendship is mutual.)

Pigeons : the n people (with $n > 1$).

Pigeonholes: the possible number of friends, i.e.

the set {0, 1, 2, 3, …, n-1}

具体问题具体分析：

讨论两鸽巢共存的可能性

②

【Example 3】 Show that among any n+1 positive integers not exceeding 2n there must be an integer that divides one of the other integers.

Solution:

Let n+1 positive integers be $a_1,a_2,\cdots,a_{n+1}(1\leq a_i\leq 2n)$

Write a_i(i=1,2,…,n+1) as $2^{k_i}q_i$, where k_i is a nonnegative integer and q_i is an odd positive integer less than 2n.

Since there are only n odd positive integers less than 2n, by the pigeonhole principle it follows that there exist integers i and j such that q_i=q_j=q,

then $a_i=2^{k_i}q$ and $a_j=2^{k_j}q$

It follows that if $a_i < a_j$, then $a_i \mid a_j$, while if $a_j < a_i$, then $a_j \mid a_i$.

整除问题

① 取公因数 (2^{k_i})

② pigeonhole.

【Example 5】 Suppose that 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.

Solution:

$$a_i=\sum_{k=1}^{i}x_k\,(i=1,2,\dots,n)$$

(1) $\exists i\;(n\mid a_i)$

(2) $\neg\exists i\;(n\mid a_i)$

连续和问题 ⇒ 考虑集合的前 n 项和

consecutive $a_i=\sum_{i=1}^{i}x_i$ $\{a_i\}$ n个元素

则 连续和 p~q = $a_q - a_p$

整除性 余数分类 + 求差 + 鸽巢原理

Division Pigeon hole

③

【Example 6】 Every sequence of n^2+1distinct integers contains a subsequence of length $n+1$ that is either strictly increasing or strictly decreasing.

Proof:

For example, n=2

1,2,3,4,5 ; 4,8,3,6,1; 1,4,5,3,2

Let the sequence be $a_1,a_2,\dots,a_{n^2+1}$

Associate (x_k,y_k) to the term a_k, where x_k is the length of the longest increasing subsequence starting at a_k, and y_k is the length of the longest decreasing subsequence starting at a_k

Suppose that there is no increasing or decreasing subsequence of length n+1.Then

$1\leq x_k\leq n \qquad 1\leq y_k\leq n$

Hence there are $n\times n=n^2$ pairs (x_k,y_k),

Since there are n^2+1 a_k, By the pigeonhole principle, it follows that there exist terms a_i,a_j $(1\leq i<j\leq n^2+1)$ such that $(x_i,y_i)=(x_j,j_j)$

Since $a_i \neq a_j$

It follows that

(1) $a_i < a_j$

(2) $a_i > a_j$

In either case there is a contradiction.

构造 Pair (x_k, y_k)

利用 Pigeon hole

④ 〖Example 4〗 **During 11 weeks football games will be held at least 1 game a day, but at most 12 games be arranged each week. Show that there must be a period of some number of consecutive days during which exactly 21 games must be played.**

Solution:

x_i : the number of football games held on the ith day

$a_i = \sum_{k=1}^{i} x_k \qquad 1 \le a_1 < a_2 \ldots < a_{77} \le 12 \times 11 = 132$

$c_i = a_i + 21 \qquad 22 \le c_1 < c_2 < \ldots < c_{77} \le 132 + 21 = 153$

$A = \{a_1, a_2, \ldots a_{77}, c_1, c_2, \ldots c_{77}\} \qquad B = \{1, 2, \ldots, 153\}$

$\exists i \ne j$ such that $a_i = c_j$

$a_i = a_j + 21$

$a_i - a_j = x_i + x_{i-1} + \ldots + x_{j+1} = 21$

连续Day：

法1. 构造 $c_i = a_i + (\text{games}) \Rightarrow a_i = c_j$

$\downarrow$

加 $a_0 = 0$, $c_0 = (\text{games}) \longrightarrow \begin{cases} a_i = c_0 \ \checkmark \\ a_i = c_j \ \checkmark \end{cases}$

法2. 转换成如②所示连续和问题. 对余数讨论.

⑤ 〖Example 7〗 Assume that in a group of six people, each pair of individuals consists of two friends or two enemies. Show that there are either three mutual friends or three mutual enemies in the group.

Proof:

Let the six people be $a_1, a_2, a_3, a_4, a_5, a_6$

Take a_1 into consideration. Of the five other people in the group, there are either three or more who are friends of a_1, or three or more who are enemies of a_1. This follows from the generalized pigeonhole principle.

(1) Suppose that a_i, a_j, a_k are freinds of a_1

(2) Suppose that a_i, a_j, a_k are enemies of a_1

$R(m, n)$

(i) $\left.\begin{matrix} R(3,3) \le 6 \\ R(3,3) = 5 \times \end{matrix}\right\} R(3,3) = 6$

(ii) $R(n, m) = R(m, n)$

(iii) $R(n, 2) = n$

(iv) $R(4,4) = 18$

(v) $R(5,5) \in [43, 49]$

r-permutation $\quad P(n, r) = \dfrac{n!}{(n-r)!}$

r-combination $\quad C(n, r) = \binom{n}{r} = \dfrac{n!}{r!(n-r)!}$

$\qquad\qquad\qquad \| $

$\qquad\qquad C(n, n-r)$

$B = \{b_1, b_2, \ldots, b_r\}$, $A = \{a_1, a_2, \ldots, a_n\} \qquad f: B \to A$

$A = \{a_1, a_2, \ldots, a_n\}$, $B = \{0, 1\} \qquad f: A \to B$.

$C(n, r) = |\{f \mid f: A \to B \wedge r = |\{a \mid a \in A \wedge f(a) = 1\}|\}|$

combinatorial proof $\begin{cases} \text{double counting proof} \\ \text{bijective proof} \end{cases}$

the binomial theorem $\quad (x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j$

$$\Rightarrow \begin{cases} \sum_{k=0}^{n} \binom{n}{k} = 2^n & (x = y = 1) \\ \sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0 & (x = 1, y = -1) \\ \sum_{k=0}^{n} 2^k \binom{n}{k} = 3^n & (x = 1, y = 2) \end{cases}$$

PASCAL'S Identity $\quad \binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$

Vandermonde's Identity $\quad \binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{r-k} \binom{n}{k} \Rightarrow \binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2$

$\binom{n+1}{r+1} = \sum_{j=r}^{n} \binom{j}{r}$ use bit-string and double counting

The left-hand side counts the bit strings of length n+1 containing r+1 1s.

We show that the right-hand side counts the same objects by considering the cases corresponding to the possible locations of the final 1 in a string with r+1 ones.

$$\sum_{k=r+1}^{n+1} \binom{k-1}{r} = \sum_{j=r}^{n} \binom{j}{r}$$

permutation with repetition $\quad n!/(n_1! n_2! \cdots n_k!)$

r-Circle Permutation $\quad P(n, r)/r$

r-Combination with repetition $\quad C(n+r-1, r)$ (stars and bars)

$\sum_{i=1}^{k} x_i = C \Rightarrow$ ① x_i范围：化成 $x_i \ge 0$，改变 C (本质是自由排列的star数)

② 不等号：添加一个 $x_{i+1} \ge 0$ 化为等号

Distributing objects into boxes:

① distinguishable objects and distinguishable boxes $\quad n!/(n_1! n_2! \ldots n_k!)$

② distinguishable objects and indistinguishable boxes

$S(n, j)$: the number of ways to distribute n distinguishable objects into j indistinguishable boxes so that no boxes is empty ☆

$S(n, j) = \left(\sum_{i=0}^{j-1} (-1)^i C_j^i (j-i)^n\right) / j!$

$\Rightarrow \sum_{j=1}^{k} S(n, j) = \sum_{j=1}^{k} \left(\left(\sum_{i=0}^{j-1} (-1)^i C_j^i (j-i)^n \right) / j! \right)$

$\begin{cases} \text{next larger permutation} \\ \text{next larger combination} \end{cases}$

③ indistinguishable objects and distinguishable boxes $\quad$ use stars and bars

④ indistinguishable objects and indistinguishable boxes $\quad$ 枚举法

chapter 8

recurrence relation $\quad a_n = f(\underbrace{a_0, a_1, a_2, \ldots, a_{n-1}}_{\text{degree} \Rightarrow \text{initial conditions}}) \quad n \geq n_0$

- linear
- constant coefficients
- degree k
- homogeneous (0 = 0, when $a_i = 0$)

how to solve:

【Theorem 5】 Let $\{a_n^{(p)}\}$ be a *particular solution* of the nonhomogeneous linear recurrence relation with constant coefficients $a_n = c_1a_{n-1} + c_2a_{n-2} + \cdots + c_ka_{n-k} + F(n)$
Then every solution is of the form $\{a_n^{(p)} + a_n^{(h)}\}$, where $\{a_n^{(h)}\}$ is a solution of the associated homogeneous recurrence relation.
$a_n = c_1a_{n-1} + c_2a_{n-2} + \cdots + c_ka_{n-k}$.

$a_n^{(p)}$:

【Theorem 6】 Assume a linear nonhomogeneous recurrence equation with constant coefficients with the nonlinear part *F(n)* of the form

$$F(n) = (b_tn^t + b_{t-1}n^{t-1} + \cdots + b_1n + b_0)s^n$$

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

$$(p_tn^t + p_{t-1}n^{t-1} + \cdots + p_1n + p_0)s^n$$

If s is a root of multiplicity m, a particular solutions is of the form

$$n^m\underbrace{(p_tn^t + p_{t-1}n^{t-1} + \cdots + p_1n + p_0)}_{\text{每一项都要遍历}}s^n$$

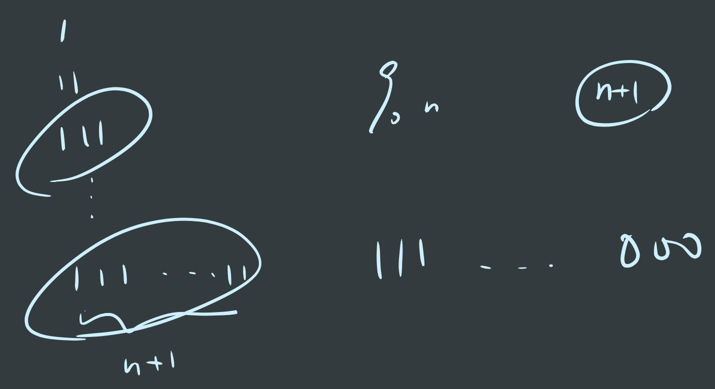
$a_n^{(t)}$:

【Theorem 4】 Let $c_1, c_2, \cdots, c_k$ be real numbers. Suppose that the characteristic equation $r^k - c_1r^{k-1} - \ldots - c_k = 0$ has t distinct roots $r_1, r_2, \cdots, r_t$ with multiplicities $m_1, m_2, \cdots, m_t$, respectively, so that $m_i \geq 1$ *for* $i = 1, 2, \cdots, t$ and $m_1 + m_2 + \cdots + m_t = k$
Then a sequence $\{a_n\}$ is a solution of the recurrence relation $a_n = c_1a_{n-1} + c_2a_{n-2} + \cdots + c_ka_{n-k}$ if and only if

$$a_n = (\alpha_{1,0} + \alpha_{1,1}n + \cdots + \alpha_{1,m_1-1}n^{m_1-1})r_1^n +$$
$$(\alpha_{2,0} + \alpha_{2,1}n + \cdots + \alpha_{2,m_2-1}n^{m_2-1})r_2^n + \cdots +$$
$$(\alpha_{t,0} + \alpha_{t,1}n + \cdots + \alpha_{t,m_t-1}n^{m_t-1})r_t^n$$

for $n = 0, 1, 2, \cdots$ where $\alpha_{i,j}$ are constants for $1 \leq i \leq t, 0 \leq j \leq m_i - 1$

8.4 generating functions



8.5 ~ 8.6 Inclusion - Exclusion

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

$$N(P_1'P_2'\cdots P_n') = N - |A_1\cup A_2\cdots\cup A_n| = N - \sum_{1\le i\le n} N(P_i) + \sum_{1\le i<j\le n} N(P_iP_j) + \dots + (-1)^n N(P_1P_2\cdots P_n)$$

the number of elements in a set that have none of n properties

① $x_1 + x_2 + \dots + x_n = m$

$x_i < k \Rightarrow N(x_1 \ge k, x_2 \ge k, \dots, x_n \ge k)$

② N(prime) of k

i) $\sqrt{k}$'s prime $a_1 \cdots a_i$

ii) $N(a_1'a_2'\cdots a_i') + i$

③ the number of onto functions

$m \longrightarrow n \quad (m \ge n)$

$n^m - C(n,1)(n-1)^m + C(n,2)(n-2)^m - \dots + (-1)^{n-1}C(n,n-1)\cdot 1^m$

④ derangement (错排)

$D_n = n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + (-1)^n\frac{1}{n!}\right)$

chapter 9 relations

9.1 ~ 9.3

【Definition】A *binary relation* **R** from a set **A** to a set **B** is a subset of **A×B.**

Note:

- A *binary relation* **R** is a set.
- $R \subseteq A\times B$
- $R = \{(a,b) \mid a\in A, b\in B, aRb\}$

【Definition】A *relation on the set A* is a relation from **A** to **A**.

Note:

- $R \subseteq A\times A$

【Definition】Let **R** be a relation from

$A = \{a_1, a_2, \cdots, a_m\}, \ to \ B = \{b_1, b_2, \cdots, b_n\}$

An $m\times n$ *connection matrix* $M_R = [m_{ij}]$ for **R** is defined by

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

5. Directed graph/Digraph

【Definition】A *directed graph* or a *digraph*, consists of a set V of *vertices* together with a set E of ordered pairs of elements of V called *edges(or arcs)*.

The *vertices a,b* is called the *initial* and *terminal* vertices of the edge *(a,b)*, respectively.

$\left\{\begin{array}{l}\text{reflexive} \\ \text{irreflexive} \\ \text{symmetric} \\ \text{antisymmetric} — \forall x\forall y\,((x,y)\in R \wedge (y,x)\in R \rightarrow x=y) \\ \text{transitive}\end{array}\right.$

Question:

Symmetric, transitive $\Rightarrow$ reflexive ?

$$\left.\begin{array}{r}(a,b)\in R \\ R\ \ is\ \ symmetric\end{array}\right\} \Rightarrow \left.\begin{array}{r}(b,a)\in R \\ R\ \ is\ \ transitive\end{array}\right\} \Rightarrow (a,a)\in R$$

This argument makes an assumption that $\forall a \exists b (a,b) \in R$

Therefore, symmetry and transitivity are not enough to infer reflexivity

combining relations:

set operation $\cup, \cap, \bar{\ }, -, \oplus$

composition

$R = \{(a,b) \mid a\in A, b\in B, aRb\}, \quad S = \{(b,c) \mid b\in B, c\in C, bSc\}$

The **composite of R and S**: $S\circ R$

$S\circ R = \{(a,c) \mid a\in A \wedge c\in C \wedge \exists b(b\in B \wedge aRb \wedge bSc)\}$

- when using matrix: $M_{S\circ R} = M_R \cdot M_S$
- R^n: $R^1 = R$, $R^{n+1} = R^n \circ R$
- R on a set A is transitive $\Leftrightarrow R^n \subseteq R$ (for n=1,2,...)

mathematical induction

$R^n \subseteq R \Rightarrow R^{n+1} \subseteq R$

$\left.\begin{array}{l}(a,b)\in R^{n+1} \\ R^{n+1} = R^n\circ R\end{array}\right\} \Rightarrow \left.\begin{array}{l}(a,x)\in R, (x,b)\in R^n \subseteq R \\ R \text{ is transitive}\end{array}\right\} \Rightarrow (a,b)\in R$

inverse relation

$R = \{(a,b) \mid a\in A, b\in B, aRb\}$

The *inverse relation* from **B** to **A:** $R^{-1}(R^c)$

$\{(b,a) \mid (a,b)\in R, a\in A, b\in B\}$

the properties of relation operations:

9.4 Closures of Relations

证∀R'满足①②. $R \subseteq R'$

the smallest③ relation with property P① containing R②

reflexive closure $R \cup I_A$ ← the diagonal relation on A. $I_A = \{(x,x) \mid x \in A\}$ $\Rightarrow R = R \cup I_A \leftrightarrow R$ is a reflexive relation

symmetric closure $R \cup R^{-1}$ $\Rightarrow R = R \cup R^{-1} \leftrightarrow R$ is a symmetric relation

transitive closure $\begin{cases} \text{A path of length } n \\ \text{Cycle or Circuit} \end{cases}$ $\Rightarrow$ there is a path of length n from a to b $\leftrightarrow (a,b) \in R^n$

the connectivity relation $R^* = \bigcup_{n=1}^{\infty} R^n \Rightarrow t(R) = R^*$

if $|A| = n$, then any path of length $> n$ must contain a cycle

if $|A| = n$, then $t(R) = R^* = R \cup R^2 \cup \cdots \cup R^n \Rightarrow O(n^4)$

$M_{t(R)} = M_R \vee M_R^{[2]} \vee \cdots \vee M_R^{[n]}$

Warshall's Algorithm

```
W := M_R = [w_ij]_{n×n}
for k :=1 to n
begin
    for i :=1 to n
    begin
        for j :=1 to n
            w_ij = w_ij ∨ (w_ik ∧ w_kj);
    end
end{ W = [w_ij] is M_t(R) }
```

The complexity of algorithm: $2n^3$

【Example 3】 Let $A = \{1,2,3,4,5\}, R = \{(1,1),(1,2),(2,4),(3,5),(4,2)\}, t(R) = ?$

Solution:

$$M = \begin{bmatrix} 1&1&0&0&0\\0&0&0&1&0\\0&0&0&0&1\\0&1&0&0&0\\0&0&0&0&0 \end{bmatrix} \xrightarrow{k=1} \begin{bmatrix} 1&1&0&0&0\\0&0&0&1&0\\0&0&0&0&1\\0&1&0&0&0\\0&0&0&0&0 \end{bmatrix} \xrightarrow{k=2} \begin{bmatrix} 1&1&0&1&0\\0&0&0&1&0\\0&0&0&0&1\\0&1&0&1&0\\0&0&0&0&0 \end{bmatrix}$$

$$\xrightarrow{k=3} \begin{bmatrix} 1&1&0&1&0\\0&0&0&1&0\\0&0&0&0&1\\0&1&0&1&0\\0&0&0&0&0 \end{bmatrix} \xrightarrow{k=4} \begin{bmatrix} 1&1&0&1&0\\0&1&0&1&0\\0&0&0&0&1\\0&1&0&1&0\\0&0&0&0&0 \end{bmatrix} \xrightarrow{k=5} \begin{bmatrix} 1&1&0&1&0\\0&1&0&1&0\\0&0&0&0&1\\0&1&0&1&0\\0&0&0&0&0 \end{bmatrix}$$

9.5 equivalence relations → $\begin{cases} \text{reflexive} \\ \text{symmetric} \\ \text{transitive} \end{cases}$

a and b are equivalent

R is an equivalence relation, and $(a, b) \in R$

Notation: $a \sim b$

(1) aRb
(2) $[a] = [b]$
(3) $[a] \cap [b] \neq \emptyset$
} equivalent

the equivalence class of x

The set of all elements that are related to an element x of A

Notation: $[x]_R$ $[x]$

a representative of the equivalence class $[x]_R$: $b \in [x]_R$

partition of set A

【Definition】A *partition* of set A is a collection of *disjoint nonempty* subsets of A that have A as their union.

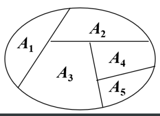
Let $\{A_i \mid i \in I\}$ be a collection of subsets of A. Then the collection forms a *partition* of A if and only if

- $A_i \neq \phi$ for $i \in I$ (I is an index set)
- $A_i \cap A_j = \phi$, when $i \neq j$
- $\forall a \in A, \exists i$ such that $a \in A_i (i = 1,2,\cdots)$

$\bigcup_{i \in I} A_i = A$

Notation:

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

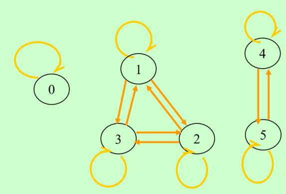


an equivalence relation on a set A
↕
a partition of A.

how to express:

【Example 3】 **Find the partition of the set A from R.**
$A = \{0,1,2,3,4,5\}$,
$R = \{(0,0),(1,1),(2,2),(3,3),(1,2),(1,3),(2,1),(2,3),(3,1),(3,2),(4,4),(4,5),(5,4),(5,5)\}$

Solution:



[0]={0}
[1]={1,2,3}
[4]={4,5}
***pr(A)*={ [0], [1], [4]}**

operations:

【Theorem 3】 If R_1, R_2 are equivalence relations on A, then $R_1 \cap R_2$ is an equivalence relation on A.

【Theorem 4】 If R_1, R_2 are equivalence relations on A, then $R_1 \cup R_2$ is a reflexive and symmetric relation on A.

【Theorem】 If R_1, R_2 are equivalence relations on A, then $(R_1 \cup R_2)^*$ is an equivalence relation on A.

1. logic — language

propositional logic $p \vee q$, $\wedge$, $\oplus$, $\rightarrow$, $\leftrightarrow$

predicate logic $\forall, \exists$

2. sets

- techniques
  - proofs
  - counting
- structures
  - functions
  - relations
  - graphs (trees)

argument form $p_1, p_2, \dots p_n \rightarrow q$

$\Downarrow$

p_1

p_2

$\vdots$

p_n

$\therefore q$

$\uparrow$ valid or not

rules of inference

format: steps

reasons (step numbers)

commonly used prove methods