1. Proposition：命题，必须为truth or false，不能不确定，通常用p,q,r,s表示，大题尽量用多，细的命题

2. 命题操作：逆：$\neg$，异或：$\oplus$，交：$\wedge$，并：$\vee$，implication：$\rightarrow$，biconditional：$\leftrightarrow$，$p\leftrightarrow q$ iff p,q同为true或同为false时返回true

否命题：inverse proposition，逆命题：converse …

3. tautology：恒为true的组合命题；contradiction：恒为false的组合命题

4. p和q are logically equivalent if $p\leftrightarrow q$为tautology，记作$p\equiv q$

5. Associative laws：$(p\vee q)\vee r\equiv p\vee(q\vee r)$，$(p\wedge q)\wedge r\equiv p\wedge(q\wedge r)$。De Morgan's laws：$\neg(p\wedge q)\equiv\neg p\vee\neg q$，$\neg(p\vee q)\equiv\neg p\wedge\neg q$

   Distributive laws：$p\vee(q\wedge r)=(p\vee q)\wedge(p\vee r)$，$p\wedge(q\vee r)\equiv(p\wedge q)\vee(p\wedge r)$。Absorption laws：$p\vee(p\wedge q)\equiv p$，$p\wedge(p\vee q)\equiv p$

   Negation laws：$p\vee\neg p\equiv T$，$p\wedge\neg p\equiv F$　　Useful law：$p\rightarrow q\equiv\neg p\vee q$

6. Predicate Logic：make statements with variables：$P(x)$。如

The intended meaning of the predicate symbol: B ('is a baby'), I ('is illogical'), D ('is despised'), C ('is a crocodile') and M ('can manage'). Domain of x: All human. Domain of y: All animals.

(a) $\forall x(B(x)\rightarrow I(x))$
(b) $\forall x(\exists y(C(y)\wedge M(x,y))\rightarrow\neg D(x))$
(c) $\forall x(I(x)\rightarrow D(x))$
(d) $\forall x(B(x)\rightarrow\exists y(C(y)\wedge\neg M(x,y)))$ or $\exists y(C(y)\wedge\forall x(B(x)\rightarrow\neg M(x,y)))$

7. 全称量词：$\forall$，$\forall x$，对所有x。存在量词：$\exists$，$\exists x$，存在一个x。

8. The argument form with premises前提$p_1,p_2,\dots,p_n$ and conclusion q is valid if $(p_1\wedge p_2\wedge\dots\wedge p_n)\rightarrow q$ is a tautology.

9. Rules of Inference for propositional logic：

Modus ponens：$\dfrac{p \quad p\rightarrow q}{\therefore q}$ | Modus tollens：$\dfrac{\neg q \quad p\rightarrow q}{\therefore \neg p}$ | Hypothetical syllogism：$\dfrac{p\rightarrow q \quad q\rightarrow r}{\therefore p\rightarrow r}$ | Addition：$\dfrac{p}{\therefore p\vee q}$

Disjunctive syllogism：$\dfrac{p\vee q \quad \neg p}{\therefore q}$ | Simplification：$\dfrac{p\wedge q}{\therefore p}$ | Conjunction：$\dfrac{p \quad q}{\therefore p\wedge q}$ | Resolution：$\dfrac{p\vee q \quad \neg p\vee r}{\therefore q\vee r}$

逻辑与证明

10. 证明方法：direct proof，proof by contrapositive证逆否命题，proof by cases：分类讨论，proof of equivalence：证等效命题。

11. set集合：不考虑元素顺序，元素可重复，形如$\{x\mid x$ has property $P\}$

12. Cardinality：集的势，表示集合中不同的元素的数量，记作$|S|$，S为一集合

13. Power set：幂集，the power set of S is the set of all subsets of the set S，记作$P(S)$。

14. Tuple：元组，考虑元素顺序，如$(a_1,a_2,\dots,a_n)$

15. Cartesian Product：笛卡尔乘积 of 集合A,B，记作$A\times B$，$A\times B=\{(a,b)\mid a\in A\wedge b\in B\}$

16. 集合操作：$A\cup B=\{x\mid x\in A\vee x\in B\}$，$A\cap B=\{x\mid x\in A\wedge x\in B\}$，$\bar{A}=\{x\in U\mid x\notin A\}$，$A-B=\{x\mid x\in A\wedge x\notin B\}$。

17. Principle of inclusion-exclusion：$|A\cup B|=|A|+|B|-|A\cap B|$。

18. 函数：Let A and B be two sets. A function from A to B, denoted by $f: A\rightarrow B$, is an assignment of exactly one element of B to each element of A.

- **One-to-one (injective) function**:
  - A function f is called one-to-one or injective if and only if $f(x)=f(y)$ implies $x=y$ for all x,y in the domain of f.
- **Onto (surjective) function**:
  - A function f is called onto or surjective if and only if for every $b\in B$ there is an element $a\in A$ such that $f(a)=b$.
- **One-to-one (bijective) correspondence**
  - One-to-one and onto

Inverse function: Let f be a one-to-one correspondence (bijection) from the set A to the set B. The inverse function of f is the function that assigns to an element b belonging to B the unique element a in A such that $f(a)=b$.

Let f be a function from B to C and let g be a function from A to B. The composition of the functions f and g, denoted by $f\circ g$, is defined by $(f\circ g)(x)=f(g(x))$.

The floor function assigns a real number x the largest integer that is $\le x$, denoted by $\lfloor x\rfloor$. E.g., $\lfloor 3.5\rfloor=3$.

The ceiling function assigns a real number x the smallest integer that is $\ge x$, denoted by $\lceil x\rceil$. E.g., $\lceil 3.5\rceil=4$.

相关证明

Suppose that $f: A\rightarrow B$.

To show that f is injective	Show that if $f(x)=f(y)$ for all $x,y\in A$, then $x=y$
To show that f is not injective	Find specific elements $x,y\in A$ such that $x\neq y$ and $f(x)=f(y)$
To show that f is surjective	Consider an arbitrary element $y\in B$ and find an element $x\in A$ such that $f(x)=y$
To show that f is not surjective	Find a specific element $y\in B$ such that $f(x)\neq y$ for all $x\in A$

数列

A set that is either finite or has the same cardinality as the set of positive integers $\mathbf{Z}^+$ is called countable.

If there is a one-to-one function from A to B, the cardinality of A is less than or equal to the cardinality of B, denoted by $|A|\le|B|$.

Theorem: If there is a one-to-one correspondence between elements in A and B, then the sets A and B have the same cardinality.

Theorem: If A and B are sets with $|A|\le|B|$ and $|B|\le|A|$, then $|A|=|B|$.

A sequence is a function from a subset of the set of integers (typically the set $\{0,1,2,\dots\}$ or $\{1,2,3,\dots\}$) to a set S.

We use the notation a_n to denote the image of the integer n. $\{a_n\}$ represents the ordered list $\{a_1,a_2,a_3,\dots\}$

集合与函数

19. $f(x)$ is $O(g(x))$ if $|f(x)|\le C|g(x)|$ when $x>k$；$f(x)$ is $\Omega(g(x))$ if $|f(x)|\ge C|g(x)|$ when $x>k$

   $f(x)$ is $\Theta(g(x))$ if $f(x)$ is $O(g(x))$ and $f(x)$ is $\Omega(g(x))$

算法复杂度

20. 可除性: Divisibility: We say that a divides b if there is an integer c such that $b = ac$, or equivalently b/a is an integer.

- If a, b, c are integers, where $a \neq 0$, such that $a|b$ and $a|c$, then $a|(mb + nc)$ whenever m and n are integers.

余数计算 **Corollary:** Let m be a positive integer and let a and b be integers. Then,

$$(a + b) \textbf{ mod } m = ((a \textbf{ mod } m) + (b \textbf{ mod } m)) \textbf{ mod } m$$

$$ab \textbf{ mod } m = ((a \textbf{ mod } m)(b \textbf{ mod } m)) \textbf{ mod } m$$

同余关系 Congruence Relation: If a and b are integers and m is a positive integer, then a is congruent to b modulo m if m divides $a - b$, denoted by $a \equiv b \pmod{m}$.

Theorem: Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m}$$

$$ac \equiv bd \pmod{m}$$

The integers a and b are congruent modulo m if and only if there is an integer k such that

$$a = b + km.$$

21. 质数: prime. A integer $p>1$ is a prime if the only positive factors of p are 1 and p.
若n为 composite 复数(非质数), 则n has a prime divisor less than or equal to $\sqrt{n}$.

22. 最大公因数 greatest common divisor: 最大整数d such that $d|a$, $d|b$, 即 $d=\gcd(a,b)$
若 $a=p_1^{a_1}p_2^{a_2}\dots p_n^{a_n}$, $b=p_1^{b_1}p_2^{b_2}\dots p_n^{b_n}$, 则 $\gcd(a,b)=p_1^{\min(a_1,b_1)}p_2^{\min(a_2,b_2)}\dots p_n^{\min(a_n,b_n)}$

23. 最小公倍数 least common multiple: 最小整数d such that $a|d$, $b|d$, 即 $d=\mathrm{lcm}(a,b$
若 $a=p_1^{a_1}p_2^{a_2}\dots p_n^{a_n}$, $b=p_1^{b_1}p_2^{b_2}\dots p_n^{b_n}$, 则 $\mathrm{lcm}(a,b)=p_1^{\max(a_1,b_1)}p_2^{\max(a_2,b_2)}\dots p_n^{\max(a_n,b_n)}$

24. Euclidean Algorithm 欧几里德算法计算gcd:

For two integers 287 and 91, we want to find $\gcd(287, 91)$.

Step 1: $287 = 91 \cdot 3 + 14$

Step 2: $91 = 14 \cdot 6 + 7$

Step 3: $14 = 7 \cdot 2 + 0$

$$\gcd(287, 91) = \gcd(91, 14) = \gcd(14, 7) = 7$$

25. 若 $\gcd(a,b)=1$, 则称 a,b are relatively prime

26. **Bezout'S Theorem**: If a and b are positive integers, then there exist integers s and t such that

$$\gcd(a, b) = sa + tb.$$

Lemma: If a, b, c are positive integers such that $\gcd(a, b) = 1$ and $a|bc$, then $a|c$.

Lemma: If p is prime and $p|a_1a_2...a_n$, then $p|a_i$ for some i.

27. 线性同余: A congruence of the form $ax \equiv b \pmod{m}$, where m is a positive integer, a and b are integers, and x is a variable, is called a linear congruence. → $x \equiv \bar{a}b \pmod{m}$

The solutions to a linear congruence $ax \equiv b \pmod{m}$ are all $\boxed{\text{integers } x}$ that satisfy the congruence.

28. 模逆元: **Modular Inverse**: An integer $\bar{a}$ such that $\bar{a}a \equiv 1 \pmod{m}$ is said to be an inverse of a modulo m.

Solve the congruence $ax \equiv b \pmod{m}$ by multiplying both sides by $\bar{a}$.

$$x \equiv \bar{a}b \pmod{m}.$$

存在条件 When does inverse exist?
Theorem: If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists. The inverse is unique modulo m. That is,

例题

How to find inverses?

Using extended Euclidean algorithm:

Example: Find an inverse of 101 modulo 4620. That is, find $\bar{a}$ such that $\bar{a} \cdot 101 \equiv 1 \pmod{4620}$.

With extended Euclidean algorithm, we obtain $\gcd(a, b) = sa + tb$, i.e., $1 = -35 \cdot 4620 + 1601 \cdot 101$. It tells us that -35 and 1601 are Bezout coefficients of 4620 and 101. We have

$$1 \textbf{ mod } 4620 = 1601 \cdot 101 \textbf{ mod } 4620.$$

Thus, 1601 is an inverse of 101 modulo 4620.

generating functions:

TABLE 1 Useful Generating Functions.

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