离散数学

数论与密码学

群论初步

Group 群

元素集合G与二元运算$\cdot$构成群$\{G,\cdot\}$，如果满足：

- **封闭性**：若$a\in G$且$b\in G$，则$a\cdot b\in G$
- **结合律**：$a\cdot b\cdot c=a\cdot(b\cdot c)$
- **单位元**：存在单位元$e\in G$，使得G中任意元素满足$a\cdot e=e\cdot a=a$
- **逆元**：对G中任意元素a，存在$a'\in G$，满足$a\cdot a'=a'\cdot a=e$

> 在群的基础定义中，不需要满足交换律

一个群G被称为**交换群**（**阿贝尔群**），如果满足：

- **交换律**：$a\cdot b=b\cdot a$

对群G中的指数运算定义如下：

- $a^0=e$
- $a^n=a^{n-1}\cdot a$
- $a^{-n}=(a^{-1})^n$，其中a^{-1}为a的逆元

一个群G被称为**循环群**，如果满足：

- 存在**生成元**g，使得G中任何元素都能表示为$g^k(k\in\mathbb{Z})$

> 无论是有限群还是无限群，循环群总是**交换群**

Rings 环

元素集合R与两个二元运算加法（$+$）和乘法（$\times$）构成环$\{R,+,\times\}$，如果满足：

- $\{R,+\}$是一个**交换群**，单位元为0，a的逆元为$-a$
- **乘法封闭性**：若$a\in R$且$b\in R$，则$a\times b\in R$
- **乘法结合律**：$a\times b\times c=a\times(b\times c)$
- **乘法分配律**：$a\times(b+c)=a\times b+a\times c,(a+b)\times c=a\times c+b\times c$

> 在环的基础定义中，不需要满足**乘法交换律**、不要求存在**乘法单位元**、不要求存在**乘法逆元**，但需要满足**加法交换律**
> $a\times b$可简写为ab

一个环R被称为**交换环**，如果满足：

- **乘法交换律**：$a\times b=b\times a$

一个环R被称为**整环**，如果满足：

- R是一个**交换环**
- **乘法单位元**：存在元素$1\in R$，使得R中任意元素都满足$1\times a=a\times 1=a$
- **无零因子**：若$ab=0$，则$a=0$或$b=0$

Fields 域

一个环$\{F,+,\times\}$被称为域，如果满足：

- F是一个**整环**
- **乘法逆元**：对F中任意元素a，存在$a^{-1}\in F$，满足$a\times a^{-1}=a^{-1}\times a=1$

对域F中的除法定义如下：

- $a/b=a(b^{-1})$

> 由此，一个域F对加、减、乘、除运算封闭

素数

良序原理

公理 非空的自然数集的子集存在最小元

算数基本定理

定理 每一个大于1的整数都可以唯一的表示为素数的积

$$a=\prod_{i=1}^{\infty}p_i^{\alpha_i}$$

最大公约数

定义 能够同时整除不全为零的a和b的最大整数d，记作$\gcd(a,b)$

> $\gcd(-24,-36)=12,\gcd(-17,22)=1$

最小公倍数

定义 能够同时被正整数a和b整除的最小正整数，记作$\operatorname{lcm}(a,b)$
定理 若a,b为正整数，则$\gcd(a,b)\cdot\operatorname{lcm}(a,b)=ab$

贝祖定理

定理 若a,b是正整数，则存在整数s,t使得

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

> 该定理可推广至a,b为任意整数且不全为零，则$\gcd(a,b)$是a,b的整系数线性组合中的最小正元

推论 若$d|a$且$d|b$，则$d|\gcd(a,b)$

定义 正整数a,b的贝祖系数为s,t，如果：$sa+tb=\gcd(a,b)$

素数测试

定理 若a是合数，则a必有小于或等于$\sqrt{a}$的因子

推论 若a是合数，则a必有小于或等于$\sqrt{a}$的素因子

试除法

依次讲$\leq\sqrt{a}$的素数除a来判断a是否为素数

> 时间复杂度：$O(2^{d/2})$，d为输入数据的二进制位数

埃拉托斯特尼筛法

```cpp
#include<bits/stdc++.h>
using namespace std;
#define N 100
bool prime[N+1];
int main(){
    memset(prime,true,sizeof(prime));
    for(int i=2;i<=N;i++){
        if(!prime[i]) continue;
        for(int j=i+i;j<=N;j+=i) prime[j]=false;
    }
    for(int i=2;i<=N;i++)
        if(prime[i]) cout<<i<<' ';
    return 0;
}
```

复杂度比较：在找出$\leq n$的所有素数的条件下

- 筛法复杂度：$O(2^d \log d)$或$O(n \log \log n)$
- 试除法复杂度：$O(2^d \cdot 2^{d/2})$或$O(n \cdot n^{1/2})$

无穷素数

定理 素数的个数是无限的

定义 梅森素数是形如$2^p - 1$的素数，其中p为素数

素数定理

定理 记$\pi(x)$表示不超过x的素数个数，则有

$$\lim_{n \to \infty} \frac{\pi(x) \ln x}{x} = 1$$

威尔逊定理

定理 p是素数当且仅当$(p-1)! \equiv -1 \pmod{p}$

互素

定义 a, b互素如果$gcd(a, b) = 1$
定义 $a_1, a_2, \ldots, a_n$两两互素如果a_i, a_j对任意$1 \leq i < j \leq n$都互素

欧几里得算法

```
int gcd(int a,int b){
    if(b==0) return a;
    return gcd(b,a%b);
}
```

扩展欧几里得算法 求贝祖系数

```
void exgcd(int a,int b,int &d,int &x,int &y){
    if(b==0){
        d=a;
        x=1;
        y=0;
        return;
    }
    exgcd(b,a%b,d,y,x);
    y -= (a/b)*x;
}
```

满足$xa+yb=d=\gcd(a,b)$

> 可用于求解模m下的逆：
> 若$gcd(a,m)=1$，则有$xa+ym=1$，即
>
> $$xa\equiv 1 \pmod{n}$$

列表计算扩展欧几里得算法

核心方程

$$\begin{cases} x=y' \\ y=x'-y'\lfloor a/b \rfloor \end{cases}$$

以计算$\gcd(99,78)$为例

a	b	$\lfloor a/b \rfloor$	x	y
99	78	1	-11	14
78	21	3	3	-11

a	b	$\lfloor a/b \rfloor$	x	y
21	15	1	-2	3
15	6	2	1	-2
6	3	2	0	1
3	0	-	1	0

步骤

- 从上往下计算$a, b, \lfloor a/b \rfloor$列，即辗转相除法
- 最后一行$x = 1, y = 0$
- 从下往上计算x, y列，此时视下面一行为x', y'，上面一行为x, y，注意计算时的a, b要选取与x, y同行的
- 每一行均满足$\gcd(a, b) = xa + yb$

同余除法

定理 若$ac \equiv bc \pmod{m}$，则有

$$a \equiv b \pmod{\frac{m}{\gcd(m, c)}}$$

推论 若m, c互素，则有

$$a \equiv b \pmod{m}$$

同余方程

定义 若$aa^{-1} \equiv 1 \pmod{m}$，则称$a^{-1}$为$a$模$m$的逆
定理 若a, m互素且$m > 1$，则a在模m下有唯一逆元

中国剩余定理

定理 设$m_1, m_2, \ldots, m_n$两两互素且均大于一，$a_1, a_2, \ldots, a_n$是任意整数，则方程组

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \cdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

在模$m = m_1 m_2 \ldots m_n$的意义下有唯一解

$$x \equiv a_1M_1M_1^{-1} + a_2M_2M_2^{-1} + \cdots + a_nM_nM_n^{-1} \pmod{m}$$

其中，$M_i = \frac{m}{m_i}$，M_i^{-1}是M_i在模m_i下的逆

回代法

例 求解同余方程

$$\begin{cases} x \equiv 2 \pmod{3} \cdots\cdots (1) \\ x \equiv 3 \pmod{5} \cdots\cdots (2) \\ x \equiv 2 \pmod{7} \cdots\cdots (3) \end{cases}$$

解
由(1)得

$$x = 3r + 2$$

代入(2)得

$$3r + 2 \equiv 3 \pmod{5}$$

解得

$$r \equiv 2 \pmod{5}$$

此即

$$r = 5s + 2$$

回代得

$$x = 15s + 8$$

代入(3)得

$$15s + 8 \equiv 2 \pmod{7}$$

解得

$$s \equiv 1 \pmod{7}$$

此即

$$s = 7t + 1$$

回代得

$$x = 105t + 23$$

即

$$x \equiv 23 \pmod{105}$$

欧拉函数与欧拉定理

欧拉函数

定义 欧拉函数$\varphi(n)$表示比n小且与n互质的数的个数

- 若p为素数，则$\varphi(p)=p-1$
- 若a,b互素，则$\varphi(ab)=\varphi(a)\varphi(b)$
- 若a,b不互素，则$\varphi(ab)=a\varphi(b)$，其中$a\leq b$
- 若p为素数，则

$$\varphi(p^n)=p^n-p^{n-1}=p^n\left(1-\frac{1}{p}\right)$$

- 对任意正整数n，若其质因数为$p_1,p_2,\ldots,p_k$，则

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

欧拉定理

定理 若$\gcd(a,n)=1$，则有

$$a^{\varphi(n)}\equiv 1 \pmod{n}$$

推论（幂循环） 若$\gcd(a,n)=1$，则有

$$a^x\equiv a^{x \bmod \varphi(n)} \pmod{n}$$

费马小定理 若p为素数且a不被p整除，则

$$a^{p-1}\equiv 1 \pmod{p}$$

伪素数

定义 b是正整数，n是一个合数，n被称为基数b的伪素数，如果：

$$b^{n-1}\equiv 1 \pmod{n}$$

原根

定义 整数r是素数p的原根，如果：

- $r\in\mathbb{Z}_p$
- $\mathbb{Z}_p$中每一个非零元素都是r的幂

> 每个素数都存在一个原根

离散对数

定义 设r为素数p的一个原根，$1 \leq a \leq p-1$。若$r^e \bmod p = a$，且$1 \leq e \leq p-1$，则称e为模p以r为底a的离散对数，记作$e = \log_r a$

密码学

密码系统

定义 一个密码系统是一个五元组(P, C, K, E, D)，其中：

- P是明文字符串的集合
- C是密文字符串的集合
- K是密钥空间
- E是加密函数的集合
- D是解密函数的集合

使用密钥k加密的函数记作E_k，解密函数记作D_k

密码系统的正确性即$D_k(E_k(p)) = p$对所有明文成立

仿射密码

使用如下加密函数

$$f(p) = (ap + b) \bmod m$$

> 当且仅当$\gcd(a, m) = 1$时，f是双射

解密函数

$$f^{-1}(c) = a^{-1}(c - b) \bmod m$$

块密码

置换密码 密钥σ定义为集合$\{1, 2, \ldots, m\}$上的置换。加密时将密文分为大小为m的块，并添加额外的字母补全，对每个块应用σ置换。

RSA密码系统

设p,q是两个不相等的大素数，$n=pq$，w是一个与$\varphi(n)=(p-1)(n-1)$互素的数，d为w模$\varphi(n)$的逆，m是明文且$m<n$

- **加密密钥**：(n,w)
- **解密密钥**：(n,d)
- **保密数据**：$p,q,\varphi(n),d$
- **加密函数**：

$$E_{(n,w)}(m)=m^w \bmod n$$

- **解密函数**：

$$D_{(n,d)}(c)=c^d \bmod n$$

Diffie-Hellman密钥交换协议

Alice和Bob希望共享一个密钥

- 双方选择一个素数p及其原根a
- Alice选择一个整数k_1并发送$a^{k_1} \bmod p$
- Bob选择一个整数k_2并发送$a^{k_2} \bmod p$
- 两人分别计算得到共享密钥

$$k=(a^{k_1})^{k_2} \bmod p=(a^{k_2})^{k_1} \bmod p$$

数字签名

Bob为确保收到的消息来自Alice

- Alice使用解密函数加密，发送$c=D_{(n,d)}(m)$
- Bob使用加密函数解密，得到$m'=E_{(n,w)}(c)$
  若$m'=m$，则可以确信消息来自$Alice$

同态加密

定义 全同态加密指对密文经行操作等价于对明文经行操作，即满足性质

$$E((m_1+m_2)\times m_3)=(E(m_1)+E(m_2))\times E(m_3)$$

部分同态加密即只对某些运算同态

- **加法同态：**

$$E(m_1+m_2)=E(m_1)+E(m_2)$$

- **乘法同态：**

$$E(m_1\times m_2)=E(m_1)\times E(m_2)$$

> RSA密码系统是乘法同态，非加法同态

Schnorr ZKP零知识证明协议

证明者向验证者证明其知晓离散对数，但不透露具体值：
选取一个素数p及其原根g，证明者有私钥$x<p$，公钥$y=g^x \bmod p$，重复n轮以下操作：

- 证明者随机选取一个小于p的整数r，发送$a=g^r \bmod p$
- 验证者发送一个随机值$(e=0$或$1)$
- 证明者发送$s=(r+ex) \bmod (p-1)$
- 验证者验证$g^s=ay^e \bmod p$是否成立

> 重复n轮下，若证明者不知道离散对数，则验证成功率为$\left(\frac{1}{2}\right)^n$

余数系统

定义

利用中国剩余定理，可以将一个大整数表示为元组
定义 大整数x在余数系统下可表示为

$$x=(x_1|x_2|\cdots|x_k)\mathrm{RNS}(p_1|p_2|\cdots|p_k)$$

其中

$$x_i=x \bmod p_i$$

且对任意i,j，有p_i,p_j互素

运算

$$x+y=((x_1+y_1) \bmod p_1|(x_2+y_2) \bmod p_2|\cdots(x_k+y_k) \bmod p_k)$$
$$x\times y=((x_1\times y_1) \bmod p_1|(x_2\times y_2) \bmod p_2|\cdots(x_k\times y_k) \bmod p_k)$$

组合数学基础

鸽巢原理

定理 将$k+1$个物体放入k个盒子中，则至少有一个盒子包含两个或更多物体

广义鸽巢原理 将N个物体放入k个盒子中，则至少有一个盒子包含至少$\lceil N/k \rceil$个物体

排列组合

定义 对于n个不同元素的集合，其r-排列的数量为

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

定义 对于n个不同元素的集合，其r-组合的数量为

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

组合证明

组合证明指使用以下方法之一来证明恒等式：

- **双计数证明**：使用计数论证来证明恒等式两边以不同的方式计算相同的对象
- **双射证明**：展示恒等式两边所计数的对象集合之间存在双射关系

二项式定理

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

负二项式定理

$$(1-x)^{-n}=1+nx+\frac{n(n+1)}{2!}x^2+\cdots=\sum_{k=0}^{\infty}\binom{n+k-1}{k}x^k$$

帕斯卡恒等式

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

广义排列组合

带有重复对象的排列组合

类型	是否允许重复	公式
r-排列	否	$P(n,r)$
r-组合	否	$\binom{n}{r}$
r-排列	是	n^r
r-组合	是	$\binom{n+r-1}{r}$

带有不可区分对象的排列

定理 n个对象分为k类，每类分别有$n_1, n_2, \ldots, n_k$个对象，不同的排列数量是

$$\frac{n!}{n_1!n_2!\cdots n_k!}$$

> 这里的不可区分指的是同一类中的不可区分

将对象分配到盒子中

n物体是否可区分	k盒子是否可区分	公式
是	是	$\frac{n!}{n_1!n_2!\cdots n_k!}$
否	是	$\binom{n+k-1}{k}$
是	否	无简单封闭公式
否	否	无简单封闭公式

> 这里的区分指的是所有物体或盒子之间的区分

母函数

定义 对于序列$a_0, a_1, a_2, \ldots$，函数

$$G(x)=a_0+a_1x+a_2x^2+\cdots$$

称为序列的**母函数**

> 母函数利用多项式乘法的过程来模拟**组合**

母函数是这样一种方法，对于对象k，其母函数的指数为所有可能的选取的个数，各项系数为该选取下对应的方法数。将所有对象的母函数乘起来，得到的描述所有对象做**组合**的状态空间。

例 有8个白球和5个黑球，要求选取偶数个白球和不少于两个黑球，有多少组合方式
解
白球的母函数为

$$G_w(x)=1+x^2+x^4+x^6+x^8$$

黑球的母函数为

$$G_b(x)=x^2+x^3+x^4+x^5+x^6$$

取乘积

$$G=G_w(x)G_b(x)$$

其中x^k的系数即为k个球的组合的方法数

例 若上例中白球不可区分，则有多少组合方式
解
白球母函数改写为

$$G_w(x)=\binom{8}{0}+\binom{8}{2}x^2+\cdots+\binom{8}{8}x^8$$

整数拆分

多项式相乘时指数相加，利用指数来表征整数的组合

无序拆分

例 整数$a_1,a_2,\ldots,a_n$分别有$k_1,k_2,\ldots,k_n$个，求整数N有几种拆分方式
解
整数a_i对应的母函数为

$$G_i(x)=1+x^{a_i}+x^{2a_i}+\cdots+x^{k_ia_i}=\frac{1-x^{(k_i+1)a_i}}{1-x^{a_i}}$$

若a_i有无穷个，则

$$G_i(x)=\frac{1}{1-x^{a_i}}$$

将所有母函数相乘

$$G(x)=\prod_{i=1}^{n}G_i(x)$$

其中x^N的系数即为N的拆分方式数

有序拆分

例（定项拆分） 将N有序拆分为r个非0部分
解
方法1（隔板法） 这相当于在N个球中插入$r-1$个隔板，结果为$\binom{N-1}{r-1}$
方法2（母函数）
每个部分的数对应的母函数为

$$G_i(x)=x+x^2+\cdots=\frac{x}{1-x}$$

相乘得

$$G(x)=x^r(1-x)^{-r}=x^r\sum_{k=0}^{\infty}\binom{r+k-1}{r-1}x^k$$

令$k+r=N$，有

$$G(x)=\sum_{N=r}^{\infty}\binom{N-1}{r-1}x^N$$

例（不定项拆分） 将N有序拆分的方法数
解
只需将N的r-拆分累加即可

$$\sum_{r=1}^{N}\binom{N-1}{r-1}=\sum_{j=0}^{N-1}\binom{N-1}{j}=2^{N-1}$$

例 将N有序拆分为无限个整数$a_1,a_2,\ldots,a_n$的和
解
母函数为

$$G=1+(x^{a_1}+x^{a_2}+\cdots+x^{a_n})+(x^{a_1}+x^{a_2}+\cdots+x^{a_n})^2+\cdots$$

指数型母函数

定义 对于序列$a_0, a_1, a_2, \ldots$，函数

$$G_e(x) = a_0 + \frac{a_1}{1!}x + \frac{a_2}{2!}x^2 + \cdots$$

称为序列的**指数型母函数**

> 用于解决从分为k类的对象中做r-**排列**的问题

例 现有n个元素$a_1, a_2, \ldots, a_n$，分别重复$k_1, k_2, \ldots, k_n$次，对其做r-排列
解
a_i对应的指数型母函数为

$$G_{ei}(x) = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \cdots + \frac{x^{k_i}}{k_i!}$$

若a_i有无穷个，则

$$G_{ei}(x) = e^x$$

其r-排列的母函数为

$$G_e(x) = \prod_{i=1}^{n} G_{ei}(x)$$

其中，$\frac{x^r}{r!}$对应的系数为r-排列的方法数

例 由$1, 2, 3, 4, 5$组成n位数，其中$2, 4$出现偶数次
解
指数型母函数为

$$\begin{aligned} G_e(x) &= \left(1 + \frac{x^2}{2!} + \frac{x^4}{4!} + \cdots\right)^2 \left(1 + \frac{x}{1!} + \frac{x^2}{2!} + \cdots\right)^3 \\ &= \left(\frac{e^x + e^{-x}}{2}\right)^2 e^{3x} \\ &= \frac{1}{4}(e^{5x} + 2e^{3x} + e^x) \\ &= \sum_{n=0}^{\infty} \frac{1}{4}(5^n + 2 \cdot 3^n + 1)\frac{x^n}{n!} \end{aligned}$$

即n位数有$a_n = \frac{1}{4}(5^n + 2 \cdot 3^n + 1)$种可能

高级计数

递归关系（数列递推）

线性递归关系

常系数齐次线性递归关系

定理 对于k阶常系数齐次递归关系

$$c_0a_n+c_1a_{n+1}+c_2a_{n+2}+\cdots+c_ka_{n+k}=0$$

定义其特征方程为

$$c_kr^k+\cdots+c_1r+c_0=0$$

若方程有t个根$r_1,\ldots,r_t$且重数为$\alpha_1,\ldots,\alpha_t$，则数列通项为

$$\begin{aligned}a_n=&(C_{11}+C_{12}n+\cdots+C_{1\alpha_1}n^{\alpha_1-1})r_1^n+\\&(C_{21}+C_{22}n+\cdots+C_{2\alpha_2}n^{\alpha_2-1})r_2^n+\\&\cdots\\&(C_{t1}+C_{t2}n+\cdots+C_{t\alpha_t}n^{\alpha_t-1})r_t^n\\=&\sum_{i=1}^{t}\left(\sum_{j=1}^{\alpha_i}C_{ij}n^{j-1}\right)r_i^n\end{aligned}$$

其中C_{ij}为待定系数

常系数非齐次线性递归关系

定义 形如

$$c_0a_n+c_1a_{n+1}+c_2a_{n+2}+\cdots+c_ka_{n+k}=F(n)$$

的递归关系称为**常系数非齐次线性递归关系**，同时

$$c_0a_n+c_1a_{n+1}+c_2a_{n+2}+\cdots+c_ka_{n+k}=0$$

称为**关联的齐次递归关系**

定理 上述非齐次递归关系的解为

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

其中$a_n^{(h)}$为关联的齐次递归关系的通解，$a_n^{(p)}$为一个特解

分治算法复杂度分析

分治递归关系

定义 假设一个分治算法每次将一个规模为n的问题划分为a个子问题，每个子问题的规模为n/b，合并时的开销为$g(n)$，以$f(n)$表示解决规模为n的问题的开销，则有

$$f(n)=af(n/b)+g(n)$$

主定理

定理 设$f(n)$为一递增函数且满足

$$f(n)=af(n/b)+cn^d$$

则

$$f(n)=\begin{cases}O(n^d), & a<b^d\\ O(n^d\log n), & a=b^d\\ O(n^{\log_b a}), & a>b^d\end{cases}$$

容斥原理

定理 设$A_1,A_2,\dots,A_n$为有限集，则

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

数理逻辑

命题

定义 具有确切真值的陈述句称为**命题**，真值只有“真”和“假”两种。

一般来说，命题可以分为以下两类：

- **原子命题（简单命题）**：不能再分解为更简单命题的命题
- **复合命题**：可以分解为更简单命题的命题

联结词

分类

- **否定式**：“非P”，记作$\neg P$

- **合取式**：“P且Q”，记作$P \wedge Q$
- **析取式**：“P或Q”，记作$P \vee Q$
- **蕴含式**：“若P则Q”，记作$P \to Q$
- **等价式**：“P当且仅当Q”，记作$P \leftrightarrow Q$

真值表

P	Q	$\neg P$	$P \wedge Q$	$P \vee Q$	$P \to Q$	$P \leftrightarrow Q$
1	1	0	1	1	1	1
1	0	0	0	1	0	0
0	1	1	0	1	1	0
0	0	1	0	0	1	1

运算优先级

- 否定>合取>析取>蕴含>等价
- 同级运算从左至右
- 括号优先

命题公式

定义

- 一个特定的命题是一个**常值命题**，它不是0就是1；
- 一个没有赋予具体内容的原子命题是一个**命题变量（命题变元）**，变域是$\{0,1\}$；
- 当原子命题是命题变元时，此复合命题称为**命题公式（真值函数）**。

定义

- 命题变元本身是一个公式
- 若G为公式，则$(\neg G)$也是公式
- 若G,H为公式，则$(G \wedge H),(G \vee H),(G \to H),(G \leftrightarrow H)$也是公式
  命题公式是由有限步上述规则产生的结果

定义 设$P_1,P_2,\ldots,P_n$是出现在公式G中的所有命题变元，指定其一组真值，该真值称为G的一个**解释**，常记为I。若G在解释I下为真，则称I**满足**G；若为假，则称I**弄假**G。

定义 G在所有解释下的真值情况称为G的**真值表**

定义

- G称为**永真公式（重言式）**，如果G在所有解释下都为真
- G称为**永假公式（矛盾式）**，如果G在所有解释下都为假
- G称为**可满足的**，如果G不是永假的

等价

定义 若在任意解释下，G, H真值相同，则称G, H等价，记作$G = H$

定理 $G = H$当且仅当$G \leftrightarrow H$是重言式

基本等价关系如下：

- **结合律**：$G \vee (H \vee S) = (G \vee H) \vee S, G \wedge (H \wedge S) = (G \wedge H) \wedge S$
- **交换律**：$G \vee H = H \vee G, G \wedge H = H \wedge G, G \leftrightarrow H = H \leftrightarrow G$
- **幂等律**：$G \vee G = G, G \wedge G = G$
- **吸收律**：$G \vee (G \wedge H) = G, G \wedge (G \vee H) = G$
- **分配律**：$G \vee (H \wedge S) = (G \vee H) \wedge (G \vee S), G \wedge (H \vee S) = (G \wedge H) \vee (G \wedge S)$
- **同一律**：$G \vee 0 = G, G \wedge 1 = G$
- **零律**：$G \vee 1 = 1, G \wedge 0 = 0$
- **排中律**：$G \vee \neg G = 1$
- **矛盾律**：$G \wedge \neg G = 0$
- **双重否定律**：$\neg(\neg G) = G$
- **德摩根律**：$\neg(G \vee H) = \neg G \wedge \neg H, \neg(G \wedge H) = \neg G \vee \neg H$
- **蕴含式**：$G \to H = \neg G \vee H$
- **等价式**：$G \leftrightarrow H = (G \to H) \wedge (H \to G) = (\neg G \vee H) \wedge (G \vee \neg H)$
- **假言易位**：$G \to H = \neg H \to \neg G$
- **等价否定等式**：$G \leftrightarrow H = \neg G \leftrightarrow \neg H$
- **归谬论**：$(G \to H) \wedge (G \to \neg H) = \neg G$

范式

定义

- 命题变元或命题变元的否定称为**文字**
- 有限个文字的析取称为**子句**
- 有限个文字的合取称为**短语**
- P与$\neg P$称为**互补对**

定义

- 有限个**短语**的析取式称为**析取范式**
- 有限个**子句**的合取式称为**合取范式**

规定

- **单个文字**可以是**子句、短语、析取范式、合取范式**
- **不加括号的子句**$P \vee Q \vee R$同时是**析取范式、合取范式**；**加括号的子句**$(P \vee Q \vee R)$只是**合取范式**
- **不加括号的短语**同时是**析取范式、合取范式**；**加括号的短语**只是**析取范式**

范式的求解

定理 对于任意命题公式，都存在与其等价的析取范式和合取范式

- 利用等价公式替换$\rightarrow$和$\leftrightarrow$
- 利用德摩根律将$\neg$移到命题变元前
- 利用分配律提取$\vee$或$\wedge$

极小项和极大项

定义 在含有n个命题变元的短语（子句）中，若每个命题变元与其否定二者之一出现一次且仅一次，则称该**短语（子句）**为关于该命题变元的一个**极小项（极大项）**

编码
每个极小项（极大项）有且仅有一个成真赋值（成假赋值），不同极小项的成真赋值不同，故可将极小项编码如下

$$m_k, 0 \leq k \leq 2^n - 1$$

将k写为二进制

$$k = (a_1 a_2 \cdots a_n)_2$$

则有

- $a_i = 0$表示P_i在m_i中以**否定**形式出现，在m_i成真赋值中$P_i = 0$
- $a_i = 1$表示P_i在m_i中以**肯定**形式出现，在m_i成真赋值中$P_i = 1$

同理可将极大项编码为

$$M_k, 0 \leq k \leq 2^n - 1$$

并且

- $a_i = 0$表示P_i在M_i中以**肯定**形式出现，在M_i成假赋值中$P_i = 0$
- $a_i = 1$表示P_i在M_i中以**否定**形式出现，在M_i成假赋值中$P_i = 1$

> 编码对应的二进制即为满足极小项、弄假极大项的解释；对于文字形式，极小项中0为否定，极大项中0为肯定

性质

- 任意两个不同极小项的合取必为假；任意两个不同极大项的析取必为真

$$m_i \wedge m_j = 0, M_i \vee M_j = 1, \quad i \neq j$$

- 极大项的否定是极小项；极小项的否定是极大项

$$\neg M_i = m_i$$

- 所有极小项的析取为永真公式；所有极大项的合取是永假公式

$$\bigvee_{i=0}^{2^n-1} m_i = 1, \bigwedge_{i=0}^{2^n-1} M_i = 0$$

主析取范式和主合取范式

定义

- 主析取范式中每个短语都是极小项
- 主合取范式中每个子句都是极大项
- 若一个主析取（合取）范式不包含任何项，则称其为“空”

定理 每个公式都有与之等价的主析取范式和主合取范式

利用等价转换求解主析取、合取范式

- 求出析取范式或合取范式
- 利用幂等律将重复变元消去
- 去除矛盾式和重言式
- 利用矛盾式和重言式以及分配律补足缺失的命题变元，如下

$$Q = (P \vee \neg P) \wedge Q = (P \wedge \neg P) \vee Q$$

- 去除重复的极小项或极大项，整理

利用真值表求解主析取、合取范式

对于公式$G(P_1,P_2,\dots,P_n)$的一个解释I_k，如果

- I_k弄假G，则主析取范式**不包含**m_k，主合取范式**包含**M_k
- I_k满足G，则主析取范式**包含**m_k，主合取范式**不包含**M_k

转换
利用$G=\neg(\neg G)$可以将主合取范式和主析取范式相互转换

应用

定理

- G为重言式当且仅当其合取范式中每个子句都包含至少一个命题变元及其否定
- G为矛盾式当且仅当其析取范式中每个短语都包含至少一个命题变元及其否定
  定理
- G为重言式当且仅当其主析取范式包含所有极小项，主合取范式为空
- G为矛盾式当且仅当其主合取范式包含所有极大项，主析取范式为空
  定理 两个命题公式等价当且仅当其主析取范式相等或主合取范式相等

谓词

个体与谓词

定义 在原子命题中，可以独立存在的客体（主语、宾语等）称为**个体词**，用以刻画客体的性质或客体之间关系的是**谓词**

- 表示**具体或特定**的个体词称为**个体常量**，一般用$a,b,c,\dots$
- 表示**抽象或泛指**的个体词称为**个体变量**，一般用$x,y,z,\dots$
  个体词的取值范围称为**个体域（论域）**，一般用D表示；宇宙间的所有个体域聚集在一起构成的个体域称为**全总个体域**

定义 设D为非空个体域，定义在D^n上取值于$\{0,1\}$的n元函数称为**n元命题函数（n元谓词）**，记为$P(x_1,x_2,\dots,x_n)$

- 一元谓词用于描述个体特性，n元谓词用于描述n个个体之间的关系
- 0元谓词实际上是一般的命题

- 一个n元谓词不是一个命题（真值不确定），但将n个个体变量用具体个体取代后就称为一个命题（真值确定）

量词

定义 称$(\forall x)$为**全称量词**，$(\exists x)$为**存在量词**，其中x称为作用变量。一般将量词加在谓词前，记作$(\forall x)F(x),(\exists x)F(x)$，其中$F(x)$称为量词的辖域

特性谓词

为了解决个体域的声明问题，引入特性谓词
定义 特性谓词是一个刻画个体域特性的一元谓词$U(x):x\in D$

谓词逻辑符号化

- 统一个体域为全总个体域
- 对于**全称量词**，刻画其个体域的特性谓词作为**蕴含式前件**加入

$$(\forall x)(U(x)\to F(x))$$

- 对于**存在量词**，刻画其个体域的特性谓词作为**合取项**加入

$$(\exists x)(U(x)\wedge F(x))$$

- 否定规则：将全称量词和存在量词互换，同时将辖域否定

谓词合式公式

定义

- **常量符号**：用小写英文字母$a,b,c,\cdots$表示，是D中的**某个**元素
- **变量符号**：用小写英文字母$x,y,z,\cdots$表示，是D中的**任意**元素
- **函数符号**：用小写英文字母$f,g,h,\cdots$表示，n元函数符号$f(x_1,x_2,\dots,x_n)$是$D^n\to D$的任意一个函数
- **谓词符号**：用大写英文字母$P,Q,R,\cdots$表示，n元谓词符号$P(x_1,x_2,\dots,x_n)$可以是$D^n\to\{0,1\}$的任意一个谓词

定义 谓词逻辑中的**项**被递归地定义为：

- 任意的常量符号或任意的变量符号是项
- 若$f(x_1,x_2,\dots,x_n)$是n元函数符号，$t_1,t_2,\dots,t_n$是项，则$f(t_1,t_2,\dots,t_n)$是项
- 仅由有限次上述操作产生的符号串才是项

定义 若$P(x_1,x_2,\dots,x_n)$是n元谓词，$t_1,t_2,\dots,t_n$是项，则称$P(t_1,t_2,\dots,t_n)$为**原子谓词公式**，简称**原子公式**

定义 满足下列条件的表达式称为**合式公式**，简称**公式**：

- 原子公式是合式公式
- 若G,H是合式公式，则$(\neg G),(\neg H),(G\vee H),(G\wedge H),(G\to H),(G\leftrightarrow H)$也是合式公式
- 若G是合式公式，x是个体变量，则$(\forall x)G,(\exists x)G$也是合式公式
- 仅由上述操作产生的表达式才是合式公式

自由变元和约束变元

定义 给定合式公式G，若变元x出现在使用变元的量词的辖域之内，则称变元x的出现为**约束出现**，此时x为约束变元；否则x为**自用变元**

定义 量词辖域的确定如下：

- 若量词后有括号，则括号内的子公式就是辖域
- 若量词后无括号，则与量词邻接的子公式为辖域

变换规则

约束变元改名规则

- 将量词中出现的变元以及该量词辖域中此变量的所有约束出现都用新的个体变元替换
- 新的变元一定要有别于改名辖域中的所有其它变量

自由变元代入规则

- 将公式中出现该自由变元的每一处都用新的个体变元替换
- 新变元不允许在原公式中以任何约束形式出现

闭式

定义 设G是任意一个公式，若G中无自由出现的个体变元，则称为**封闭的合式公式**，简称**闭式**

解释

定义 公式G的每一个解释I由以下四个部分组成：

- **非空个体域集合**D
- G中的每个**常量符号**，指定D中某个特定元素
- G中的每个**n元函数符号**，指定$D^n \to D$中的某个函数
- G中的每个**n元谓词符号**，指定$D^n \to \{0,1\}$中的某个特定谓词

分类

定义

- 公式称为**有效公式**，如果它在所有的解释下都为**真**
- 公式称为**矛盾公式**，如果它在所有的解释下都为**假**
- 公式称为**可满足公式**，如果存在解释使其为真

判定问题

定义 **可判定**指的是存在一个有穷算法，能够判定任意公式是否是有效的

定理

- 谓词逻辑是**不可判定的**
- 只含有**一元谓词变项**的公式是可判定的
- **个体域有穷**的公式是可判定的

等价

定义 公式G, H称为**等价的**，记作$G = H$，如果$G \leftrightarrow H$是**有效公式**
定义 设$G(P_1, P_2, \ldots, P_n)$是命题公式，P_i为命题变元，将任意的谓词公式G_i代入P_i后，得到的新公式称为原公式的**代入实例**

谓词演算中的等价关系：

- **改名规则：** $(\forall x)G(x) = (\forall y)G(y), (\exists x)G(x) = (\exists y)G(y)$
- **量词否定：** $\neg(\forall x)G(x) = (\exists x)\neg G(x), \neg(\exists x)G(x) = (\forall x)\neg G(x)$
- **量词辖域的扩张与收律：** $(\forall/\exists x)(G(x) \vee / \wedge S) = (\forall/\exists x)G(x) \vee / \wedge S$
- **量词分配律：**
  $(\forall x)(G(x) \wedge H(x)) = (\forall x)G(x) \wedge (\forall x)H(x), (\exists x)(G(x) \vee H(x)) = (\exists x)G(x) \vee (\exists x)H(x)$
- **改名与收缩：**
  $(\forall x)G(x) \vee (\forall x)H(x) = (\forall x)(\forall y)(G(x) \vee H(y)), (\exists x)G(x) \wedge (\exists x)H(x) = (\exists x)(\exists y)(G(x) \wedge H($

前束范式

定义 称公式G是一个**前束范式**，如果G中**一切量词都位于公式的最前端**（不含否定词）且这些量词的**辖域都延伸到公式的最末端**，形式如下

$$(Q_1x_1)(Q_2x_2)\cdots(Q_nx_n)M(x_1,x_2,\ldots,x_n)$$

其中Q_i为量词$\forall$或$\exists$，M称作公式G的**母式（基式）**，且M中不含量词

转换方法

- 消去公式中包含的$\rightarrow$和$\leftrightarrow$
- 运用德摩根律将$\neg$移到原子谓词公式最前端
- 运用谓词等价公式将所有量词提到公式最前端

Skolem标准型

定义 设公式G是一个**前束范式**，如消去G中所有的存在量词和全称量词，所得到的公式称为**Skolem标准型**。

定理 任意一个公式G都有相应的Skolem标准形存在，但此Skolem标准形**不一定与原公式等值**。

转换方法

- 将公式化为前束范式
- 消去存在量词
  - 若存在量词前没有全称量词，则用Skolem常量替换：

    $$\exists xP(x)\Rightarrow P(a)$$

  - 若存在量词前有全称量词，则用Skolem函数替换，参数为前面所有的全称变元“

    $$\forall x\forall y\exists zP(x,y,z)\Rightarrow\forall x\forall yP(x,y,f(x,y))$$

- 消去所有全称量词

推理与证明技术

命题逻辑的推理理论

有效的推理不一定产生**真实的结论**，有效的推理中可能包含为“假”的前提，而无效的推理却可能得到为“真”的结论。

基本概念

定义 设G, H为公式，对任意解释I，如果I满足G，那么I满足H，则称H是G的**逻辑结果**（G蕴含H），记为$G \Rightarrow H$，称G为**前提**，H为**结论**

定理 $G \Rightarrow H$当且仅当$G \to H$为重言式

定义 设$G_1, G_2, \dots, G_n, H$为公式，称H是$G_1, G_2, \dots, G_n$的逻辑结果，当且仅当H是$G_1 \wedge G_2 \wedge \cdots \wedge G_n$的逻辑结果，记作$G_1, G_2, \dots, G_n \Rightarrow H$，此时称$G_1, G_2, \dots, G_n$为**一组前提**，有时用集合$\Gamma = \{G_1, G_2, \dots, G_n\}$表示，$H$称为**结论**。又称$H$为前提集合$\Gamma$的逻辑结果，记作$\Gamma \Rightarrow H$

定理 $\Gamma \Rightarrow H$当且仅当$G_1 \wedge G_2 \wedge \cdots \wedge G_n \to H$为重言式

判断证明是否有效

真值表技术

列出前提$G_1, G_2, \dots, G_n$和结论H的真值表，如果满足以下条件之一则推理有效：

- 对所有$G_1, G_2, \dots, G_n$都为真的行，H也为真
- 对所有H为假的行，$G_1, G_2, \dots, G_n$至少有一个为假

推理定律

- **简化规则**：$G \wedge H \Rightarrow G, G \wedge H \Rightarrow H$
- **添加规则**：$G \Rightarrow G \vee H, H \Rightarrow G \vee H$
- $\neg G \Rightarrow G \to H, H \Rightarrow G \to H$
- $\neg(G \to H) \Rightarrow G, \neg(G \to H) \Rightarrow \neg H$
- $G, H \Rightarrow G \wedge H$
- **选言三段论**：$\neg G, G \vee H \Rightarrow H, \neg G, G \overline{\vee} H \Rightarrow H$
- **分离规则**：$G, G \to H \Rightarrow H$
- **否定后件式**：$\neg H, G \to H \Rightarrow \neg G$
- **假言三段论**：$G \to H, H \to I \Rightarrow G \to I$
- **二难推论**：$G \vee H, G \to I, H \to I \Rightarrow I$

演绎法

从前提（假设）出发，依据公认的推理规则和推理定律，推导出结论

定义 从前提集合Γ推出结论H的一个**演绎**是构造**命题公式的有限序列**：

$$H_1, H_2, \ldots, H_n$$

其中，H_i要么是Γ中的前提，要么是前序公式的有效结论。如果$H_n = H$，则称H为演绎的有效结论，或称能够从前提Γ演绎出结论H

推理规则

- **规则P（前提引用规则）**：推导过程中可随时引入前提集合中的任意前提
- **规则T（逻辑结果引用规则）**：推导过程中，可随时引入由前序公式推导的逻辑结果S
- **规则CP（附加前提规则）**：如果添加前提P能推导出S，则能从原前提Γ推导出$P \to S$，即$(\Gamma \wedge P) \Rightarrow S$等价于$\Gamma \Rightarrow (P \to S)$

间接证明法（反证法）

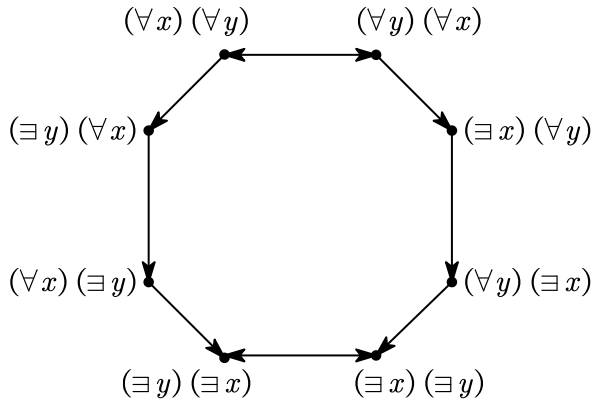
定义 设$G_1, G_2, \ldots, G_n$是一组命题公式，若存在解释I使$G_1 \wedge G_2 \wedge \cdots \wedge G_n$为真，则称公式$G_1, G_2, \ldots, G_n$是**一致的**或**相容的**；若不存在则称$G_1, G_2, \ldots, G_n$是**不一致的**

定理 设前提集合Γ是一致的，则$\Gamma \Rightarrow H$有效当且仅当$\Gamma, \neg H \Rightarrow 0$，即推出矛盾式。

谓词逻辑的推理理论

推理定律

- $(\forall x)G(x) \Rightarrow (\exists x)G(x)$
- $(\forall x)G(x) \vee (\forall x)H(x) \Rightarrow (\forall x)(G(x) \vee H(x))$
- $(\exists x)(G(x) \wedge H(x)) \Rightarrow (\exists x)G(x) \wedge (\exists x)H(x)$
- $(\forall x)(G(x) \to H(x)) \Rightarrow (\forall x)G(x) \to (\forall x)H(x)$
- $(\forall x)(G(x) \to H(x)) \Rightarrow (\exists x)G(x) \to (\exists x)H(x)$
- 二元量词有如下关系（省略$G(x, y)$）：



推理规则

- **US（全称特指规则）**：

    - $(\forall x)G(x) \Rightarrow G(y)$，其中$y$对$x$是**自由的**（即$x$不出现在$y$的辖域内）
    - $(\forall x)G(x) \Rightarrow G(c)$，其中$c$是**任一个体常量**
- **ES（存在特指规则）**：
    - $(\exists x)G(x) \Rightarrow G(c)$，其中$c$为使$G(c)$为真的**特定个体常量**
    - $(\exists x)G(x,y,z) \Rightarrow G(f(y,z),y,z)$，即若$G$中含有除$x$外的自由变量，则需用它们的**函数符号**取代
- **UG（全称推广规则）**：
    - $G(y) \Rightarrow (\forall x)G(x)$，其中$G(y)$对$x$自由且其中不含自由变量$x$
- **EG（存在推广规则）**：
    - $G(c) \Rightarrow (\exists x)G(x)$，其中$G(c)$对$x$自由且其中不含自由变量$x$
    - $G(y) \Rightarrow (\exists x)G(x)$，其中$G(y)$对$x$自由且其中不含自由变量$x$

数学归纳法

普通数学归纳法

定义 若要证明的命题能写成：

$$\forall x \geq n_0, 有P(n)$$

则数学归纳法证明过程如下：

- 验证$P(n_0)$为真
- 假设对于$k \geq n_0$，有$P(k)$为真
- 证明$P(k+1)$为真
  则命题得证

用谓词表示即为

$$P(n_0), (\forall k)((k \geq n_0) \wedge P(k) \rightarrow P(k+1)) \Rightarrow (\forall n)((n \geq n_0) \rightarrow P(n))$$

完全数学归纳法

定义 证明过程如下：

- 验证$P(n_0)$为真
- 假设对于$n \leq k(k \geq n_0)$有$P(n)$为真
- 证明$P(k+1)$为真
  则命题得证

用谓词表示即为

$$P(n_0),(\forall k)((k\geq n_0)\wedge(\forall n)((n\leq k)\rightarrow P(n))\rightarrow P(k+1))\Rightarrow(\forall n)((n\geq n_0)\rightarrow P(n))$$

按定义证明（CP规则证明）

定义 待证明命题含有蕴含式，则可以做如下转换

$$\Gamma\Rightarrow P\rightarrow Q\Leftrightarrow\Gamma,P\Rightarrow Q$$