数学 III

xuyan160322@163.com

2022 年 1 月 13 日

组合数学、数论

- 容斥原理
- 第一反演定理、二项式反演、莫比乌斯反演、子集反演、MinMax 反演等
- 偏序与偏序集
- 卷积
- 前置知识：数论分块（见团队 henrytb “整除分块”）、线性筛

偏序与偏序集

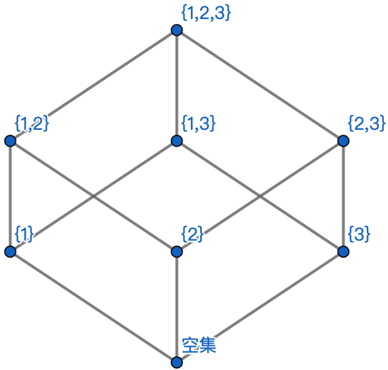
- 关系：X 为集合，关系为 X 的元素的有序对 $X \times X$ 的子集 R。例 $X = \{1, 2, 3, 4, 5, 6\}$
- 属于 R 的有序对 (a, b) 写作 aRb，反之，$a\not{R}b$
- X 中的关系 R 可能具有的特性：
  - 自反：$\forall x \in X, xRx$
  - 反自反：$\forall x \in X, x\not{R}x$
  - 对称：$\forall x, y \in X, xRy \Rightarrow yRx$
  - 反对称：$\forall x \neq y \in X, xRy \Rightarrow y\not{R}x$ $(\forall x, y \in X, xRy \;\&\&\; yRx \Rightarrow x = y)$
  - 传递：$\forall x, y, z \in X, xRy \;\&\&\; yRz \Rightarrow xRz$
- 偏序：自反、反对称、传递，如 $\subseteq, \leqslant, |$
- 集合 X 连同在其上定义的偏序 $\preccurlyeq$ 为偏序集，记作 $(X, \preccurlyeq)$
- 严格偏序：反自反、反对称、传递，如 $\subsetneq, <$（记作 $\prec$）

偏序与偏序集

- 对 X 中的 x 和 y，如果有 xRy 或 yRx，则称 x 和 y 是可比的，否则不可比
- 全序：X 中每一对元素在偏序 R 下都是可比的，如 $\leqslant$
- 偏序集覆盖关系：设 $a, b \in X$，如果 $a \prec b$ 且没有元素 c 能够夹在 a 和 b 之间，称 a 被 b 覆盖（b 覆盖 a），记为 $a \prec_c b$（即不存在 $x \in X$，使得 $a \prec x$ 和 $x \prec b$ 同时成立）。
- 如果 X 有限，由传递性，偏序 $\preccurlyeq$ 由它的覆盖关系唯一确定。

偏序集几何表示（Hasse 图）

- 如 $(\{1,2,3\},\subseteq)$



- 又如 $\{1,2,3,4,5,6,7,8\}$ 和偏序“是……的因子”

容斥原理

- 德摩根定律（De Morgan）
  - $\overline{A \cup B} = \overline{A} \cap \overline{B}$
  - $\overline{A \cap B} = \overline{A} \cup \overline{B}$
  - $\overline{A_1 \cup A_2 \cup \cdots \cup A_n} = \overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n}$
  - $\overline{A_1 \cap A_2 \cap \cdots \cap A_n} = \overline{A_1} \cup \overline{A_2} \cup \cdots \cup \overline{A_n}$
- $P_1, P_2, \ldots, P_m$ 是集合 S 涉及的 m 个性质
- 设 $A_i = \{x | x\ has\ property\ P_i, x \in S\}$，集合 S 中至少具有性质 $P_1, P_2, \ldots, P_m$ 之一的对象个数：

$$\begin{aligned}|\overline{A_1 \cup A_2 \cup \cdots \cup A_m}| = &\sum |A_i| - \sum |A_i \cap A_j| \\ &+ \sum |A_i \cap A_j \cap A_k| - \ldots \\ &+ (-1)^{m+1} |A_1 \cap A_2 \cap \cdots \cap A_m|\end{aligned}$$

- 设 $A = \{A_1, A_2, \ldots, A_m\}$，$\bigcup_{i=1}^{m} A_i = \sum_{B \subseteq A} (-1)^{|B|-1} |\bigcap_{b \in B}|$

证明

- 对于 $x \in \bigcup_{i=1}^{m} A_i$，设其（最多）出现在 k 个不同的集合中，则 x 在容斥原理中出现的次数为

$$
\begin{aligned}
& C_k^1 - C_k^2 + C_k^3 - \cdots + (-1)^{k-1} C_k^k \\
=& 1 - C_k^0 + C_k^1 - C_k^2 + C_k^3 - \cdots + (-1)^{k-1} C_k^k \\
=& 1 - (C_k^0 - C_k^1 + C_k^2 - C_k^3 + \cdots + (-1)^k C_k^k) \\
=& 1 - (1-1)^k \\
=& 1
\end{aligned}
$$

（广义）莫比乌斯反演

- 容斥原理是（广义）莫比乌斯反演（Möbius Inversion）在有限偏序集上的一个实例
- 考虑有限偏序集 $(X, \preccurlyeq)$ 上的二变量函数，设 $\mathcal{F}(X)$ 为只要 $x \not\preccurlyeq y$，就有 $f(x, y) = 0$ 的所有实值函数的（集合），即 $X \times X \to \mathcal{R}$
- 对于 $f, g \in \mathcal{F}(X)$，其卷积 $h = f * g$ 为

$$h(x, y) = \begin{cases} \sum_{\{z: x \preccurlyeq z \preccurlyeq y\}} f(x, z) g(z, y) & \text{if } x \preccurlyeq y \\ 0 & \text{else} \end{cases}$$

- 卷积有结合律：$f * (g * h) = (f * g) * h \ \ (f, g, h \in \mathcal{F}(X))$

$\mathcal{F}(X)$ 中三种特殊的函数

- 第一种：克罗内克 delta 函数（Kronecker delta function）

$$\delta(x,y)=\begin{cases}1 & \text{if } x=y\\ 0 & \text{else}\end{cases}$$

- 第二种：ζ 函数

$$\zeta(x,y)=\begin{cases}1 & \text{if } x\preccurlyeq y\\ 0 & \text{else}\end{cases}$$

逆函数

- $f(x,y)$ 的逆函数：$\forall y \in X, f(y,y) \neq 0$，可定义 $f(x,y)$ 的逆函数 $g(x,y)$，设

$$g(y,y) = \frac{1}{f(y,y)}\ (y \in X)$$

令

$$g(x,y) = -\frac{1}{f(y,y)} \sum_{\{z:x \preccurlyeq z \prec y\}} g(x,z)f(z,y)\ (x \prec y)$$

有

$$\sum_{\{z:x \preccurlyeq z \preccurlyeq y\}} g(x,z)f(z,y) = \delta(x,y)\ (x \preccurlyeq y)$$

即 $g * f = \delta$，g 是 f 关于卷积 $*$ 的左逆函数，也可以类似定义右逆函数 h 使得 $f * h = \delta$，可证得 $g = h$，统称逆函数

第三种：莫比乌斯函数 μ

- ζ 的逆函数为 μ，$\mu * \zeta = \delta$，由逆函数定义

$$\sum_{\{z:x\preccurlyeq z\preccurlyeq y\}} \mu(x,z)\zeta(z,y) = \delta(x,y)\ (x \preccurlyeq y)$$

或等价地，

$$\sum_{\{z:x\preccurlyeq z\preccurlyeq y\}} \mu(x,z) = \delta(x,y)\ (x \preccurlyeq y)$$

因此，$\forall x, \mu(x,x) = 1$，以及

$$\mu(x,y) = -\sum_{\{z:x\preccurlyeq z\prec y\}} \mu(x,z)\ (x \prec y)$$

莫比乌斯反演公式

- 设 $(X, \preccurlyeq)$ 是偏序集且有最小元素 0，设 μ 是它的莫比乌斯函数，设 $F: X \to \mathcal{R}$ 是定义在 X 上的实值函数。设 $G: X \to \mathcal{R}$

$$G(x) = \sum_{\{z: z \preccurlyeq x\}} F(z) \ (x \in X)$$

那么，

$$F(x) = \sum_{\{y: y \preccurlyeq x\}} G(y)\mu(y, x) \ (x \in X)$$

证明

$$
\begin{aligned}
\sum_{\{y:y\preccurlyeq x\}} G(y)\mu(y,x) &= \sum_{\{y:y\preccurlyeq x\}} \sum_{\{z:z\preccurlyeq y\}} F(z)\mu(y,x) \\
&= \sum_{\{y:y\preccurlyeq x\}} \mu(y,x) \sum_{\{z:z\in X\}} \zeta(z,y)F(z) \\
&= \sum_{\{z:z\in X\}} \sum_{\{y:y\preccurlyeq x\}} \zeta(z,y)\mu(y,x)F(z) \\
&= \sum_{\{z:z\in X\}} \Big(\sum_{\{y:z\preccurlyeq y\preccurlyeq x\}} \zeta(z,y)\mu(y,x)\Big)F(z) \\
&= \sum_{\{z:z\in X\}} \delta(z,x)F(z) \\
&= F(x)
\end{aligned}
$$

例：线性有序集的莫比乌斯函数

- 设 $X_n = \{1, 2, \ldots, n\}$，线性有序集 $(X_n, \leqslant), 1 < 2 < \cdots < n$
- $\mu(k, k) = 1, k \in X_n$
- 对 $1 \leqslant l < k \leqslant n$，有 $\mu(k, l) = 0$
- 对 $1 \leqslant k \leqslant n-1$，$\sum_{\{z: k \preccurlyeq j \preccurlyeq k+1\}} \mu(k, j) = \delta(k, k+1) = 0$，则 $\mu(k, k+1) = -1$，类似地 $\mu(k, k+2) = 0$
- 最终

$$\mu(k, l) = \begin{cases} 1 & \text{if } l = k \\ -1 & \text{if } l = k+1 \\ 0 & \text{else} \end{cases}$$

- 反演公式：

$$G(x) = \sum_{\{z: z \leqslant x\}} F(z) \iff F(x) = \begin{cases} G(x) - G(x-1) & \text{if } x \geqslant 2 \\ G(0) & \text{if } x = 1 \end{cases}$$

例：子集反演

- 设 $X_n = \{1, 2, \ldots, n\}$，记 $\mathcal{P}(X_n) = \{x | x \subseteq X_n\}$
- 设 $A, B \in \mathcal{P}(X_n)$ 且 $A \subseteq B$，则 $\mu(A, B) = (-1)^{|B|-|A|}$
  - $A = B$ 时，显然成立
  - $A \neq B$ 时，设 $p = |B - A| = |B| - |A|$，就有

$$\begin{aligned}\mu(A,B) &= -\sum_{\{C: A\subseteq C \subsetneq B\}} \mu(A,C) = -\sum_{\{C: A\subseteq C \subsetneq B\}} (-1)^{|C|-|A|} \\ &= -\sum_{k=0}^{p-1}(-1)^k\binom{p}{k} = (-1)^p\binom{p}{p} - \sum_{k=0}^{p}(-1)^k\binom{p}{k} \\ &= (-1)^p - (1-1)^p = (-1)^{|B|-|A|}\end{aligned}$$

- 设 $F : \mathcal{P}(X_n) \to \mathcal{R}$ 和 $G : \mathcal{P}(X_n) \to \mathcal{R}$，有反演公式：

$$G(K) = \sum_{L\subseteq K} F(L) \iff F(K) = \sum_{L\subseteq K}(-1)^{|K|-|L|}G(L)\ (K \subseteq X_n)$$

子集反演推论——经典容斥原理

- 设 $A_i(i \in X_n)$ 是有限集 S 的子集，对 $K \subseteq X_n$，定义 $F(K)$ 为：S 中恰好在所有 $\overline{A_i}(i \notin K)$ 中的元素的个数，特别地，$F(X_n) = |\bigcap_{i \in X_n} \overline{A_i}|$
- 记 $G(K) = \sum_{L \subseteq K} F(L)$，意为 S 中属于所有 $A_i(i \notin K)$ 的元素的个数，可以发现 $G(X_n) = |S|$。因此

$$G(K) = \begin{cases} |S| & K = X_n \\ |\bigcap\limits_{i \notin K} A_i| & \text{else} \end{cases}$$

$$G(K) = \sum_{L \subseteq K} F(L) \Leftrightarrow F(K) = \sum_{L \subseteq K} (-1)^{|K|-|L|} G(L)$$

取 $K = X_n$，由上式，有

$$F(X_n) = \sum_{L \subseteq K} (-1)^{n-|L|} G(L)$$

子集反演推论——二项式反演

- 反演公式：

$$f(n)=\sum_{i=0}^{n}C_n^i g(i) \Longleftrightarrow g(n)=\sum_{i=0}^{n}(-1)^{n-i}C_n^i f(i)$$

$$f(n)=\sum_{i=0}^{n}(-1)^i C_n^i g(i) \Longleftrightarrow g(n)=\sum_{i=0}^{n}(-1)^i C_n^i f(i)$$

- 证明：子集反演中，设 $F(K)$ 和 $G(K)$ 仅与 $|K|$ 有关

（狭义）莫比乌斯函数与莫比乌斯反演

- 偏序集的直积：设 $(X, \preccurlyeq_1)$ 和 $(Y, \preccurlyeq_2)$ 为两个偏序集，则集合 $X \times Y = \{(x, y) : x \in X, y \in Y\}$ 上定义 $\preccurlyeq$：

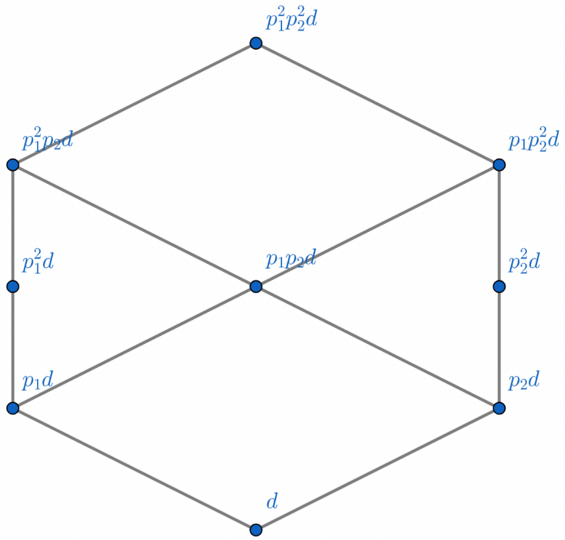
$$(x, y) \preccurlyeq (x', y') \ \textit{iff.}\ x \preccurlyeq_1 x' \ \&\&\ y \preccurlyeq_2 y'$$

- 易证 $(X \times Y, \preccurlyeq)$ 为偏序集
- $(X, \preccurlyeq_1)$ 和 $(Y, \preccurlyeq_2)$ 的莫比乌斯函数为 μ_1 和 μ_2，设 μ 为它们直积的莫比乌斯函数，则

$$\mu((x, y), (x', y')) = \mu_1(x, x')\mu_2(y, y') \quad ((x, y), (x', y') \in X \times Y)$$

- 考虑偏序集 $D_n = (X_n, |)$ 上的莫比乌斯函数 $\mu(a, b)$
- 当 $a|b$ 时，$\mu(a, b) = \mu(1, \frac{a}{b})$（why?），只需考虑 $\mu(1, n)$

D_n 的 Hasse 图



D_n 的莫比乌斯函数

- 对 n 进行质因数分解：$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$，$p_i$ 互不相同，$\alpha_i > 0$
- 可以把 n 视为 $(X_n^i = \{1, p_i, p_i^2, \dots, p_i^{\alpha_i}\}, |)$ 的直积中的元素 $(p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_k^{\alpha_k})$
- X_n^i 为线性有性集，其莫比乌斯函数为：

$$\mu(1, p_i^{\alpha_i}) = \begin{cases} 1 & \alpha_i = 0 \\ -1 & \alpha_i = 1 \\ 0 & \alpha_i \geqslant 2 \end{cases}$$

- 因此

$$\mu(1, n) = \prod_{i=1}^{k} \mu(1, p_i^{\alpha_i}) = \begin{cases} 1 & n = 1 \\ (-1)^k & n \text{ is square free number} \\ 0 & else \end{cases}$$

莫比乌斯反演

- 反演公式：设 F, G 为 N^+ 上的实值函数（记 $\mu(1, n)$ 为 $\mu(n)$）

$$G(n) = \sum_{k:k|n} F(k) \iff F(n) = \sum_{k:k|n} \mu(\frac{n}{k}) G(k) \ (n \in N^+)$$

相关性质（如何理解?）

- $\sum_{d|n} \mu(d) = [n = 1]$
- 积性函数：当 $gcd(p, q) = 1$，$\mu(pq) = \mu(p)\mu(q)$
- 欧拉函数：$\varphi(n) = |S_n|, S_n = \{k : 1 \leqslant k \leqslant n, gcd(k, n) = 1\}$
- $n = \sum_{d|n} \varphi(d)$
- 狄利克雷卷积（Dirichlet Product），对两个数论函数 f 和 g

$$f * g = \sum_{d|n} f(d) g(\frac{n}{d}) = \sum_{d|n} g(d) f(\frac{n}{d})$$

  - 交换律、结合律、分配律；积性函数卷积也是积性函数
  - $e(n) = [n = 1]$，$I(n) = 1$，$id(n) = n$
  - $\mu * I = e$
  - $\varphi * I = id$
  - $\varphi = id * \mu$

杜教筛

- 对 $n > 10^8$ 的数论函数 $f(i)$ 求前缀和 $S(n) = \sum_{i=1}^{n} f(i)$
- 构造一个 g，使得

$$\begin{aligned}\sum_{i=1}^{n}(f*g)(i) &= \sum_{i=1}^{n}\sum_{d|i} f(\frac{i}{d})g(i)\\ &= \sum_{d=1}^{n} g(d)\sum_{i=1}^{n/d} f(i)\\ &= \sum_{d=1}^{n} g(d)S(n/d)\end{aligned}$$

- 因此，$S(n)g(1) = \sum_{i=1}^{n}(f*g)(i) - \sum_{d=2}^{n} g(d)S(n/d)$
- 如果 $f*g$ 可以预处理前缀和，那么可以递归求解 $S(n)$
- 复杂度

线性筛素数、$\varphi(i)$、$\mu(i)$

```
const int N=100000000;
int p[N],q=0,mu[N+5],phi[N+5]; // 根据情况使用long long
bool vis[N];
void init(){
    vis[1]=mu[1]=phi[1]=1;
    for(int i=2;i<=N;i++){
        if(vis[i]==0){
            p[++q]=i;
            mu[i]=-1;
            phi[i]=i-1;
        }
        for(int j=1;j<=q&&p[j]*i<=N;j++){
            vis[i*p[j]]=1;
            if(i%p[j]==0) {
                phi[i*p[j]]=p[j]*phi[i];
                break;
            }
            phi[i*p[j]]=(p[j]-1)*phi[i];
            mu[i*p[j]]=-mu[i];
        }
    }
}
```

杜教筛 $\varphi(i)$ 和 $\mu(i)$ 的前缀和

```
map<LL,LL> f1,f2;
for(int i=1;i<=N-5;i++){
    mu[i]=mu[i-1]+mu[i]; phi[i]=phi[i-1]+phi[i];
}
LL get_phi(LL n){
    if(n<=N-5) return phi[n];
    if(f1[n]!=0) return f1[n];
    LL ans=C2(n); // C(n,2)
    for(LL l=2,r;l<=n;l=r+1){
        r=n/(n/l); ans=ans-(r-l+1)*get_phi(n/l);
    }
    return f1[n]=ans;
}
LL get_mu(LL n){
    if(n<=N-5) return mu[n];
    if(f2[n]!=0) return f2[n];
    LL ans=1;
    for(LL l=2,r;l<=n;l=r+1){
        r=n/(n/l); ans=ans-(r-l+1)*get_mu(n/l);
    }
    return f2[n]=ans;
}
```

应用

- $\sum_{i=1}^{n}\sum_{j=1}^{n}[gcd(i,j)=1]=\sum_{d=1}^{n}\mu(d)\lfloor(n/d)\rfloor\lfloor(n/d)\rfloor$
- $\sum_{i=1}^{n}\sum_{j=1}^{n}gcd(i,j)=\sum_{d=1}^{n}d\sum_{k=1}^{n/d}\mu(k)(\lfloor n/kd\rfloor)^2$
- $\sum_{i=1}^{n}\sum_{j=1}^{n}lcm(i,j)^{gcd(i,j)}$
- P4213 【模板】杜教筛（Sum）
- P2522 [HAOI2011]Problem b
- P3455 [POI2007]ZAP-Queries
- P2257 YY 的 GCD
- P1829 [国家集训队]Crash 的数字表格 / JZPTAB
- P3327 [SDOI2015] 约数个数和
- P3704 [SDOI2017] 数字表格
- P3768 简单的数学题
- SP5971 LCMSUM - LCM Sum
- P3312 [SDOI2014] 数表
- P4449 于神之怒加强版

最后

- 尽信书不如无书
- 大学专业的意义
- 不要太执著两条路中的任意一条（技巧与思想）
- 学习时有些东西一时不理解，只能先接受
- 这只是一个开始