Chapter 3 容斥原理及其推广

目录

1 容斥原理

1.1 容斥原理

我们用一个简单的例子引入本章所讲述的内容.

例 1 某班有100人, 其中会打篮球的有45人, 会打乒乓球的有53人, 会打排球的有55人, 既会打篮球也会打乒乓球的有28人, 既会打篮球也会打排球的有32人, 既会打乒乓球也会打排球的有35人, 三种球都会打的有20人, 问三种球都不会打的有多少人.

解 1 设$E_1 = \left\{\text{此班会打篮球的人}\right\}, E_2 = \left\{\text{此班会打排球的人}\right\}, E_3 = \left\{\text{此班会打乒乓球的人}\right\}$, 则

$$|E_1| = 45, |E_2| = 53, |E_3| = 55, |E_1 \cap E_2| = 28, |E_1 \cap E_3| = 32, |E_2 \cap E_3| = 35, |E_1 \cap E_2 \cap E_3| = 20.$$

我们进行如下计算: 从总人数中减去会打三种球之一的人数, 但此时会打两种球的人数被减了两次, 会打三种球的人数被减了三次; 我们再加上会打两种球的人, 但此时会打三种球的人数又被加了三次; 我们再减去会打三种球的人数, 此时得到的是正确的结果.

结果为22.

解决上述问题的过程体现了容斥原理的思想. 我们下面提出容斥原理.

定理 1 容斥原理 设S为一有限集, $\mathcal{P} = \{P_1, \ldots, P_n\}$为一族性质. 对$[m]$的任一子集$I$, 令$X_I$表示$S$中满足性质$P_i (\forall i \in I)$的那些元素构成的集合. 特别地, 当$I = \{i\}$时简记$X_{\{i\}} = X_i$, 记$\overline{X_I} = S \setminus X_I$, 则集合$S$中不具有$\mathcal{P}$中任何一种性质的元素个数由下式给出.

$$\begin{aligned}\left|\overline{X_1} \cap \overline{X_2} \cap \ldots \cap \overline{X_m}\right| &= |S| - \sum_i |X_i| + \sum_{i<j} \left|X_i \cap X_j\right| + \ldots + (-1)^m |X_1 \cap X_2 \cap \ldots \cap X_m| \\ &= \sum_{I \subseteq [m]} (-1)^{|I|} |X_I|.\end{aligned}$$

证明 1 对任意$x \in S$, 设$J_x = \{i \in [m] \mid x \in X_i\}$. 若$J_x = \varnothing$, 即$x$不在任意一个$X_i$中, 此时$x$对左式贡献为1; 右式中$x$仅对$|S|$贡献1.

若$J_x \neq \varnothing$, 则x在某些X_i中. 设$j = |J_x|$, 则$j > 0$. 此时x对左式贡献为0; 对右式, 注意到$x \in X_i \Leftrightarrow I \subseteq J_x$, 从而$x$对右式贡献为

$$\sum_{I \subseteq J_x} (-1)^{|I|} = \sum_{i=0}^{j} (-1)^i \binom{j}{i} = (1-1)^j = 0.$$

从而有原式成立. 证毕.

1.2 容斥原理的应用

下面是容斥原理的一些简单应用.

例 2 用容斥原理计算n原错位排列(即满足$a_i \neq i$的排列$a_1 \dots a_n$)的个数d_n.

解 2 对n元置换及$1 \leq i \leq n$, 定义性质P_i为i在置换下保持不变(或i为不动点). 定义A_i为n元对称群S_n中所有满足性质P_i的置换组成的子集, 则

$$d_n = \left|\overline{A_1} \cap \dots \cap \overline{A_n}\right|.$$

对任意$1 \leq i_1 < \dots < i_k \leq n$, $\left|A_{i_1} \cap \dots \cap A_{i_k}\right|$ 为S_n中具有不动点$i_1, \dots, i_k$的置换个数, 即为$(n-k)!$. 从而由容斥原理

$$\begin{aligned} d_n &= \left|\overline{A_1} \cap \dots \cap \overline{A_n}\right| = |S_n| - \sum_i |A_i| + \dots + (-1)^n |A_1 \cap \dots \cap A_n| \\ &= n! - (n-1)! + \binom{n}{2}(n-2)! + \dots + (-1)^n \binom{n}{n} = n! - \frac{n!}{1!} + \frac{n!}{2!} + \dots + (-1)^n \frac{n!}{n!} \\ &= n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} \end{aligned}$$

事实上错排数也可通过生成函数的方法求解. 我们留给读者完成.

例 3 从$[n]$到$\{y_1, \dots, y_k\}$的满射有多少个.

解 3 设S为所有从$[n]$到$\{y_1, \dots, y_k\}$的映射的集合, 则$|S| = k^n$. 定义性质P_i为y_i不是映射的像, A_i为满足性质$P_i, 1 \leq i \leq k$的从$[n]$到$\{y_1, \dots, y_k\}$的映射的集合, 则对任意$1 \leq i \leq k$, 有

$$|A_i| = (k-1)^n;$$

对任意$1 \leq i_1 < \dots < i_j \leq k$, 有

$$\left|A_{i_1} \cap \dots \cap A_{i_j}\right| = (k-j)^n.$$

从而满射数为

$$\begin{aligned} \left|\overline{A_1} \cap \dots \cap \overline{A_k}\right| &= |S| - \sum_i |A_i| + \sum_{i<j} \left|A_i \cap A_j\right| + \dots + (-1)^k |A_1 \cap \dots \cap A_k| \\ &= \sum_{j=0}^{k} (-1)^j \binom{k}{j} (k-j)^n = \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} j^n. \end{aligned}$$

这正是第二类Stirling数的通项公式, 我们将在下一章详细讨论. 与容斥原理对偶的等价形式是下述定理:

定理 2 集合S中至少具有$\mathcal{P}$中一种性质的元素个数由下式给出.

$$|X_1 \cup X_2 \cup \ldots \cup X_m| = \sum_i |X_i| - \sum_{i<j} \left|X_i \cap X_j\right| + \ldots + (-1)^{m-1} |X_1 \cap X_2 \cap \ldots \cap X_m|$$

2 偏序集上的Mobius反演

2.1 局部有限偏序集上的环

我们接下来将容斥原理推广至更一般的情况. 在此之前我们先进一步引入一些概念.

定义 1 给定偏序集(X, P), 若对任意$x, y \in X$, 集合$\left[x, y\right] = \{z \in X \mid x \leq z \leq y\}$都是有限集, 则称$(X, P)$为一个**局部有限偏序集**.

例 4 偏序集$(\mathbb{Z}^+, |)$是局部有限偏序集.

例 5 考虑偏序集$P(S) = (S, \subseteq)$, 其中S为一集合. 若S是有限集, 则$P(S)$为局部有限的. 若S为无限集, 则易知$P(S)$不是局部有限的, 但其有限子集之集$P_f(S)$是局部有限的.

给定偏序集(X, P),我们下面考虑这样的函数$f : X \times X \to \mathbb{R}$, 满足

$$x \not\leq y \Rightarrow f(x, y) = 0.$$

令$\mathcal{F}(X)$表示这样的实值函数的集合.

定义 2 给定偏序集(X, P), 对于$\mathcal{F}(X)$中的两个函数f, g, 定义他们的**卷积**$h = f * g$如下:

$$h(x, y) = \begin{cases} \sum_{x \leq z \leq y} f(x, z)\, g(z, y), & x \leq y, \\ 0, & \text{其他}. \end{cases}$$

易知$h \in \mathcal{F}(X)$, 从而卷积是定义在$\mathcal{F}(X)$的一个二元运算.

易验证卷积满足结合律(留给读者), 即对任意$f, g, h \in \mathcal{F}(X)$, 有

$$(f * g) * h = f * (g * h).$$

我们再考虑$\mathcal{F}(x)$中的一个特别的函数.

定义 3 *给定偏序集(X, P), 在$X \times X$上定义函数σ:*

$$\sigma(x, y) = \begin{cases} 1, & x = y; \\ 0, & \text{其他} \end{cases}$$

易知$\forall f \in \mathcal{F}(X) f * \sigma = f$. 在$\mathcal{F}(X)$上定义" + "为函数的加法, 则不难验证$(\mathcal{F}(X), +, *)$构成一有单位元的环, 其单位元为$\sigma$(留给读者证明).

2.2 元素的逆和偏序集上的Mobius函数

我们下面尝试对环内的某些元素求逆.

定义 4 *给定偏序集(X, P), 在$X \times X$上定义函数ζ:*

$$\zeta(x, y) = \begin{cases} 1, & x \leq y; \\ 0, & \text{其他} \end{cases}$$

称ζ为偏序集(X, P)上的ζ-函数.

对于给定的$\mathcal{F}(X)$中的函数f, 若对任意$x \in X$, 均有$f(x, x) \neq 0$, 则可归纳地定义函数$g \in \mathcal{F}(X)$:

$$g(y, y) = \frac{1}{f(y, y)}, \forall y \in X,$$
$$g(x, y) = -\sum_{x \leq z < y} g(x, z) \frac{f(z, y)}{f(y, y)}, \forall x < y, x, y \in X.$$

则当$x = y$时$g * f(y, y) = 1$, 当$x < y$时,

$$\begin{aligned} g * f(x, y) &= \sum_{x \leq z \leq y} g(x, z) f(z, y) = \sum_{x \leq z < y} g(x, z) f(z, y) + g(x, y) f(y, y) \\ &= \sum_{x \leq z < y} g(x, z) f(z, y) + \left(-\sum_{x \leq z < y} g(x, z) f(z, y) \right) = 0 \end{aligned}$$

从而$g * f = \sigma$, 即g是f的左逆. 类似地可证明f存在右逆g'(留给读者完成). 由

$$g' = \sigma * g' = (g * f) * g' = g * (g * g') = g * \sigma = g$$

从而f的左右逆相同, 可定义$g = g'$为f关于$*$的逆.

我们应注意到并非所有$f \in \mathcal{F}$均存在逆, 仅对任意$x \in X f(x, x) \neq 0$的函数满足.

下面给出局部有限偏序集上的Mobius函数的定义.

定义 5 给定偏序集$\mathbf{P} = (X, P)$, 记$\mathbf{P}$上的ζ-函数ζ关于$*$的逆位μ, 称之为$\mathbf{P}$上的***Mobius*函数**, 即

$$\mu(y,y) = \frac{1}{\zeta(y,y)},$$
$$\mu(x,y) = -\sum_{x\leq z<y} \mu(x,z)\frac{\zeta(z,y)}{\zeta(y,y)} = -\sum_{x\leq z<y} \mu(x,z).$$

注意到只有局部有限偏序集上的Mobius函数才有定义, 这是由Mobius函数的定义涉及卷积的定义范围决定的.

我们先用几个直观的例子了解局部有限偏序集上的Mobius函数.

例 6 考虑偏序集$(\mathbb{Z}, |)$, 对任意$x, y \in \mathbb{Z}^+, x|y$, 将$\frac{y}{x}$写成以下素数幂的形式:

$$\frac{y}{x} = \prod_{i=1}^{r} p_i^{a_i}, a_i \geq 1.$$

证明:$(\mathbb{Z}, |)$上的*Mobius*函数为

$$\mu(x,y) = \begin{cases} 1, & x = y \\ (-1)^r, & a_1 = \ldots = a_r = 1, r \geq 1; 0, \quad \max\{a_1, \ldots, a_r\} \geq 2 \vee x \nmid y \end{cases}$$

证明 2 对正整数$\frac{y}{x}$归纳. 当$\frac{y}{x} = 1$时$\mu(x,y) = \mu(x,x) = 1$, 此时命题成立. 设$k \geq 1, x \mid y$且命题对$\frac{y}{x} \leq k$成立, 则当$\frac{y}{x} = k+1 = \prod_{i=1}^{r} p_i^{ai}$时

$$\mu(x,y) = -\sum_{x|z|y, z\neq y} \mu(x,z) = -\sum_{x|z|y, z\neq y} \mu\left(\frac{z}{x}\right) = \mu\left(\frac{y}{x}\right) - \sum_{x|z|y}\mu\left(\frac{z}{x}\right) = \mu\left(\frac{y}{x}\right) - \sum_{t|\frac{y}{x}}\mu(t) = \mu\left(\frac{y}{x}\right)$$

其中$\mu(x)$为经典的*Mobius*函数, 最后一步运用恒等式

$$\sum_{d|n}\mu(d) = 0, \forall n > 1$$

从而命题对$\frac{y}{x} = k+1$成立. 由归纳原理其对一切正整数成立. 证毕.

我们可以看出其与经典的Mobius函数相等, 因此偏序集上的Mobius函数可以看作经典Mobius函数的推广.

例 7 给定集合S, 考虑偏序集$\left(P_f(S), \subseteq\right)$. 证明:其上的*Mobius*函数为

$$\mu(A,b) = (-1)^{|B|-|A|}, A, B \in P_f(S), A \subseteq B.$$

证明 3 对于$A, B \in P_f(S), A \subseteq B$, 设$n = |B| - |A|$. 下面对$n$归纳. 当$n = 0$时$A = B$, 故

$$\mu(A, B) = \mu(A, A) = 1 = (-1)^{|B|-|A|},$$

从而$n = 0$结论成立. 假设对$k \geq 0$, 结论对$n \leq k$时成立, 则当$n = k + 1$时

$$\begin{aligned}\mu(A, B) &= -\sum_{A \subseteq C \subsetneq B} \mu(A, C) = -\sum_{A \subseteq C \subsetneq B} (-1)^{|C|-|A|} = -\sum_{i=0}^{|B|-|A|-1} \binom{|B|-|A|}{i} (-1)^i \\ &= -\left((1-1)^{|B|-|A|} - (-1)^{|B|-|A|}\right) = (-1)^{|B|-|A|}.\end{aligned}$$

从而结论对$n = k + 1$成立. 由归纳原理知结论对一切n成立. 证毕.

2.3 偏序集上的Mobius反演

下面我们介绍偏序集上的Mobius反演.

定理 3 偏序集上的*Mobius*反演公式 设偏序集$(X, \leq)$是满足对任意$x \in X$, $\{z \in X \mid z \leq x\}$都是有限集. 设$\mu(x, y)$是偏序集$(X, \leq)$上的*Mobius*函数(易知其存在), 则对任意定义在X上的实值函数F, G以及任意$x \in X$, 只要

$$G(x) = \sum_{z \leq x} F(z),$$

就有

$$F(x) = \sum_{y \leq x} G(y) \mu(y, x).$$

证明 4 由条件知

$$\sum_{y \leq x} G(y) \mu(y, x) = \sum_{y \leq x} \sum_{z \leq y} F(z) \mu(y, x) = \sum_{z \leq x} F(z) \sum_{z \leq y \leq x} \mu(y, x)$$

注意到

$$\sum_{z \leq y \leq x} \mu(y, x) = \begin{cases} 1, & z = x, \\ 0, & z < x. \end{cases}$$

故

$$\sum_{y \leq x} G(y) \mu(y, x) = F(x).$$

证毕.

2.4 偏序集上的Mobius反演的应用

例 8 给定偏序集$\left(P_f(S), \subseteq\right)$. 设$F, G$为两个定义在$P_f(S)$上的实值函数, 且对任意$A \in P_f(S)$, 满足

$$G(A) = \sum_{B \subseteq A} F(B),$$

证明:

$$F(A) = \sum_{B \subseteq A} (-1)^{|A|-|B|} G(B).$$

证明 5 注意到此时$\mu(B, A) = (-1)^{|A|-|B|}$, 由偏序集上的Mobius反演公式易得上述结果.

在上例中, 我们进一步地规定实值函数F, G, 就得到了我们熟知的结果.

例 9 容斥原理设所考虑性质得集合为

$$\mathcal{P} = \{P_1, \ldots, P_m\}.$$

集合S中满足性质P_i得所有元素集合记为$X_i, 1 \leq i \leq m$. 考虑偏序集$\boldsymbol{P} = (P(\mathcal{P}), \subseteq)$. 其上的实值函数$F, G$定义如下: 对任意$A \subseteq \mathcal{P}, F(A)$为集合$S$中具有$\overline{A}$所有性质但不具有$A$中的任何性质的元素的个数; $G(A)$为集合S中具有$\overline{A}$中所有的性质的元素数. 易知对任意$A \subseteq \mathcal{P}$, 有

$$G(a) = \sum_{b \subseteq A} F(B),$$

从而

$$F(A) = \sum_{B \subseteq A} \mu(B, A) G(B) = \sum_{B \subseteq A} (-1)^{|A|-|B|} G(B).$$

任意给定$B \subseteq \mathcal{P}$, 记$A = \mathcal{P} \setminus B$, 设

$$H(A) = \left|\left\{x \mid x \in S, x\text{具有}A\text{中的所有性质}\right\}\right|.$$

从而

$$F(\mathcal{P}) = \sum_{B \subseteq \mathcal{P}} (-1)^{|\mathcal{P}|-|B|} G(B) = \sum_{A \subseteq \mathcal{P}} (-1)^{|A|} H(A).$$

从而我们可以看出, 容斥原理是偏序集上Mobius反演的特例.

例 10 对于任意正整数n, 确定q元域$\mathbb{F}_q$上n次首一不可约多项式的个数.

解 4 域$\mathbb{F}_q$上n次首一不可约多项式的个数至多为q^n, 是可数的, 故$\mathbb{F}_q$上所有首一不可约多项式可数. 设它们为$f_1(x), \ldots, f_2(x), \ldots$, 次数分别为$d_1, d_2, \ldots$.

对任意正整数n, 令A_n表示$\mathbb{F}_q$上所有n次首一多项式组成的集合,

$$B_n = \left\{ \{i_k\}_{k=1}^{\infty} \mid n = \sum_{j=1}^{\infty} d_j i_j, \{i_k\}_{k=1}^{\infty} \text{为非负整数序列且只有有限项不为} 0 \right\}.$$

任取B_n中的一个数列$\{i_k\}_{k=1}^{\infty}$, 其对应一个多项式

$$f(x) = \prod_{j=1}^{\infty} f_j(x)^{i_j},$$

且$f(x)$是首一的, 次数为$\sum_{j=1}^{\infty} d_j i_j = n$, 从而$f(x) \in A_n$.

反之, 对于A_n中任一n次首一多项式$f(x)$, 其可分解为

$$f(x) = \prod_{j=1}^{\infty} f_j(x)^{i_j},$$

其对应一数列$\{i_k\}_{k=1}^{\infty}$, 其中只有有限项不为0, 且$n = \sum_{j=1}^{\infty} d_j i_j$, 从而$\{i_k\}_{k=1}^{\infty} \in B_n$. 从而存在$A_n$到$B_n$的双射. 故$|A_n| = |B_n|$. 由$|A_n| = q^n$知$\{|A_n|\}_{n=0}^{\infty}$的普通生成函数为

$$1 + qx + q^2x^2 + \ldots = \frac{1}{1 - qx}.$$

$|B_n|$为方程$n = \sum_{j=1}^{\infty} d_j i_j$的非负整数解的个数, 故$\{|B_n|\}_{n=0}^{\infty}$的普通生成函数为

$$\left(1 + x^{d_1} + x^{2d_1} + \ldots\right)\left(1 + x^{d_2} + x^{2d_2} + \ldots\right)\ldots = \prod_{i=1}^{\infty} \frac{1}{1 - x^{d_i}}.$$

因此

$$\frac{1}{1 - qx} = \prod_{i=1}^{\infty} \frac{1}{1 - x^{d_i}}.$$

设N_d为$\mathbb{F}_q$上d次首一不可约多项式的个数, 则

$$\frac{1}{1 - qx} = \prod_{d=1}^{\infty} \left(\frac{1}{1 - x^d}\right)^{N_d}.$$

两端取对数得

$$\ln \frac{1}{1 - qx} = \sum_{d=1}^{\infty} N_d \ln \frac{1}{1 - x^d}.$$

由$\ln\frac{1}{1-z}=\sum_{k=1}^{\infty}\frac{z^k}{k}$得

$$\sum_{n=1}^{\infty}\frac{(qx)^n}{n}=\sum_{d=1}^{\infty}N_d\sum_{j=1}^{\infty}\frac{x^{jd}}{j}.$$

比较上式两端x^n的系数, 有

$$\frac{q^n}{n}=\sum_{d|n}N_d\frac{d}{n}.$$

即$q^n=\sum_{d|n}dN_d$. 由*Mobius*反演公式得到

$$nN_n=\sum_{d|n}\mu(d)\,q^{\frac{n}{d}}.$$

从而

$$N_n=\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d.$$

显然任意1次多项式不可约, 从而$\mathbb{F}_q$上依次首一不可约多项式的个数为q. 设$n\geq 2$, 且其素因子分解为$n=p_1^{a_1}\ldots p_r^{a_r}$, 则有

$$nN_n=q^n-\sum_{i=1}^{r}q^{\frac{n}{p_i}}+\sum_{1\leq i<j\leq r}q^np_ip_j+\ldots+(-1)^r\,q^{\frac{n}{p_1\cdots p_r}}.$$

故nN_n不能被$q^{\frac{n}{p_1\cdots p_r}+1}$整除, 从而$nN_n\neq 0$, 故$N_n>0$, 即任意有限域上的任意次不可约多项式总是存在的. 由此便可证明: 对任意素数幂$q=p^r$, 存在q元有限域.

例 11 欧拉函数$\phi(n)$定义为*:*

$$\phi(n)=\left|\left\{k\mid 1\leq k\leq n,\gcd(k,n)=1\right\}\right|,n\geq 1$$

即$\phi(n)$是不超过n且与n互素的正整数个数. 试求$\phi(n)$的计算公式.

解 5 对正整数n及其正因子d, 设

$$A_d=\left\{k\mid 1\leq k\leq n,\gcd(k,n)=d\right\},$$

则

$$|A_d|=\left|A_d=\left\{k\mid 1\leq k\leq n,\gcd(k,n)=d\right\}\right|=\left|\left\{\frac{k}{d}\mid 1\leq\frac{k}{d}\leq\frac{n}{d},\gcd\left(\frac{k}{d},\frac{n}{d}\right)=1\right\}\right|=\phi\left(\frac{n}{d}\right).$$

易知$\{A_d\}_{d|n}$是$[n]$的一个划分, 故

$$n=\sum_{d|n}|A_d|=\sum_{d|n}\phi\left(\frac{n}{d}\right)=\sum_{d|n}\phi(d).$$

由Mobius反演公式, 得到

$$\phi(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)=\sum_{d|n}\mu(d)\frac{n}{d}.$$

易知$\phi(1)=1$, 当$n\geq 2$是设n的素因子分解为$n=\prod_{i=1}^{r}p_i^{a_i}, a_i\geq 1, 1\leq i\leq r$. 此时

$$\phi(n)=\sum_{d|n}\mu(d)\frac{n}{d}=\sum_{k=0}^{r}\sum_{\{i_1,\ldots,i_k\}\subseteq[r]}(-1)^k\frac{n}{\prod_{j=1}^{k}p_{i_j}}=n\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right).$$

例 12 令$h(n)$表示多重集$S=\{n\cdot t_1,\ldots,n\cdot t_k\}$的$n$-环排列数, 试求$h(n)$.

解 6 每一个环排列τ有一个最小正周期d(即τ可分解为$\frac{n}{d}$个完全一致的长度为d, 周期也为d的线排列, 这里$d\mid n$). 同时每个长度为d的环排列对应d个长度为d, 周期也为d的线排列. 令$f(n)$表示长度为n, 周期也为n的线排列的个数, 则有

$$h(n)=\sum_{d|n}\frac{f(d)}{d}.$$

另一方面, 在所有长度为n的线排列以及所有长度为d, 周期也为d的线排列之间(对所有$d\mid n$)存在一一对应, 故

$$k^n=\sum_{d|n}f(d),$$

从而

$$f(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)k^d$$

因此有

$$\begin{aligned}h(n)&=\sum_{d|n}\frac{f(d)}{d}=\sum_{d|n}\frac{1}{d}\sum_{e|d}\mu\left(\frac{d}{e}\right)k^e=\sum_{e|n}k^e\sum_{e|d|n}\frac{1}{d}\mu\left(\frac{d}{e}\right)=\sum_{e|n}k^e\sum_{b|\frac{n}{e}}\frac{1}{eb}\mu(b)\\&=\sum_{e|n}k^e\frac{1}{n}\left(\sum_{b|\frac{n}{e}}\frac{\frac{n}{e}}{b}\mu(b)\right)=\frac{1}{n}\sum_{e|n}k^e\phi\left(\frac{n}{e}\right).\end{aligned}$$

例 13 证明Mobius反演公式的如下变形: 设两个函数序列

$$\{a_n(x)\}_{n=1}^{\infty}, \{b_n(x)\}_{n=1}^{\infty}$$

满足

$$a_n(x)=\sum_{d|n}b_{\frac{n}{d}}\left(x^d\right), n\geq 1,$$

则

$$b_n(x)=\sum_{d|n}\mu\left(\frac{n}{d}\right)a_d x^{\left(x^{\frac{n}{d}}\right)}, n\geq 1.$$

证明 6

$$\sum_{d|n}\mu\left(\frac{n}{d}\right)a_d\left(x^{\frac{n}{d}}\right)=\sum_{d|n}\mu\left(\frac{n}{d}\right)\sum_{e|d}b_{\frac{d}{e}}\left(x^{\frac{n}{\frac{d}{e}}}\right)=\sum_{q|n}\sum_{e|\frac{n}{q}}\mu\left(\frac{\frac{n}{q}}{e}\right)b_q\left(x^{\frac{n}{q}}\right)\quad (q=\frac{d}{e})$$

$$=\sum_{q|n}b_q\left(x^{\frac{n}{q}}\right)\sum_{e|\frac{n}{q}}\mu\left(\frac{\frac{n}{q}}{e}\right)=b_n\left(x^{\frac{n}{n}}\right)+\sum_{q|n,q\neq n}b_q\left(x^{\frac{n}{q}}\right)\cdot 0=b_n(x).$$

其中最后一步应用了

$$\sum_{d|n}\mu(d)=\begin{cases}1, & n=1,\\ 0, & n>1\end{cases}$$

从而原命题证毕.

3 生成函数与容斥原理的推广

设S为有限集, $\mathcal{P}$为一族性质, 我们下面考虑: S中有多少元素**恰**满足$\mathcal{P}$中的r个性质? 其答案是复杂的. 但我们较容易得知这样的问题的答案:S中有多少元素**至少**满足$\mathcal{P}$中的r个性质? 我们尝试将前者转化为后者.

对$x\in S$, 令$\mathcal{P}(x)$表示x所满足性质的集合, 即$\mathcal{P}(x)=\{P_i\in\mathcal{P}\mid P_i(x)\}$. 设$Q\subseteq\mathcal{P}$是一些性质的集合, 令$G(\supseteq Q)=\{x\in S\mid Q\subseteq\mathcal{P}(x)\}$ 表示S中至少满足Q中所有性质的元素的集合, 再令

$$g_r=\begin{cases}\sum_{|Q|=r}|G(\supseteq Q)|, & r\leq m,\\ 0, & r>m.\end{cases}$$

和

$$e_r=\begin{cases}|\{x\in S\mid |\mathcal{P}(x)|=r\}|, & r\leq m,\\ 0, & r>m.\end{cases}$$

应注意到g_r大于等于S中至少满足$\mathcal{P}$中r个性质的元素个数, 这是因为对不同的Q, $G(\supseteq Q)$中可能有公共元素. e_r为S中所有恰好满足$\mathcal{P}$中r个性质的元素个数. 计算有序对(x,Q)的个数, 其中$x\in S, Q\subseteq\mathcal{P}(x), |Q|=r$, 我们得到

$$g_r=\sum_{|Q|=r}|G(\supseteq Q)|=\sum_{|Q|=r}\sum_{x\in S,Q\subseteq\mathcal{P}(x)}1=\sum_{x\in S}\sum_{|Q|=r,Q\subseteq\mathcal{P}(x)}1=\sum_{x\in S}\binom{|\mathcal{P}(x)|}{r}=\sum_{n=r}^{m}\binom{n}{r}e_n$$

令$G(x)$, $E(x)$分别表示$\{g_n\}_{n=0}^{\infty}$, $\{e_n\}_{n=0}^{\infty}$的普通生成函数, 则有

$$G(x)=\sum_{r\geq 0}g_r x^r=\sum_{r\geq 0}\sum_{n\geq 0}\binom{n}{r}e_n x^r=\sum_{n\geq 0}e_n\sum_{r\geq 0}\binom{n}{r}x^r=\sum_{n\geq 0}e_n(1+x)^n=E(1+x7).$$

也即

$$E(x)=G(x-1).$$

当$n=0$时我们得到容斥原理:

$$e_0=E(0)=G(-1)=\sum_{r=0}^{m}(-1)^r g_r.$$

一般地,对$0\leq n\leq m$, 有

$$e_n=\sum_{r=n}^{m}\binom{r}{n}(-1)^{r-n}g_r.$$

例 14 *对于正整数n, 确定S_n中恰有k个不动点的置换个数e_k和e_k的极限性质, 并求出$\{e_k\}_{k=0}^{\infty}$的普通生成函数(当$k>n$时$e_k=0$).*

解 7 对于$1\leq i\leq n$, 令P_i表示性质:一个置换中i是不动点, $\mathcal{P}=\{P_1,\dots,P_n\}$, 则$S_n$中所有恰好满足$\mathcal{P}$中$k$个性质的元素个数就是$S_n$中恰有$k$个不动点的置换个数$e_k$, 从而

$$\begin{aligned}e_k&=\sum_{r=k}^{n}\binom{r}{k}(-1)^{r-k}g_r=\sum_{r=k}^{n}\binom{r}{k}(r-k)\binom{n}{r}(n-r)!=\sum_{r=k}^{n}\binom{r}{k}(-1)^{r-k}\frac{n!}{r!}\\&=\frac{n!}{k!}\sum_{r=k}^{\infty}\frac{(-1)^{r-k}}{(r-k)!}=\frac{n!}{k!}\sum_{i=0}^{n-k}\frac{(-1)^i}{i!}\to\frac{n!}{k!}\mathrm{e}^{-1}.\end{aligned}$$

其普通生成函数为

$$\begin{aligned}E(x)&=\sum_{k\geq 0}e_k x^k\sum_{k\geq 0}\left(\sum_{r=k}^{n}\binom{r}{k}(-q)^{r-k}\frac{n!}{r!}\right)x^k=n!\sum_{r=0}^{n}\sum_{k=0}^{r}\frac{1}{r!}\binom{r}{k}x^k(-1)^{r-k}\\&=n!\sum_{r=0}^{n}\frac{1}{r!}(x-1)^r\end{aligned}$$

此例中我们可以求出

$$G(x)=E(x+1)=n!\sum_{r=0}^{m}\frac{x^r}{r!}.$$

以及错排数

$$e_0 = E(0) = n! \sum_{r=0}^{\infty} \frac{(-1)^r}{r!} \to \frac{n!}{e}.$$

以及S_n中元素(置换)平均含有的不动点数为

$$\frac{1}{n!} \sum_{k=0}^{n} k e_k = \frac{1}{n!} \sum_{k=0}^{n} \binom{k}{1} e_k = \frac{g_1}{n!} = \frac{n \cdot (n-1)!}{n!} = 1.$$