组合数学

Fiddie

September 2, 2024

Contents

2020-2021 学年孙智伟老师开的《组合数学》课程.

组合数学 (combinatorics) 研究的是有穷数学, 可能没有代数运算, 研究对象有: (1) 组合计数 (如 Lucas 序列); (2) 存在性问题 (如相异代表系, Hall 定理); (3) 组合设计 (存在能否构造, 如 36 军官问题).

组合数学比较直观, 外界可能有误解. 1980 年代西方不歧视组合了, 因为它不简单. 1998 年 Fields 奖给了 W.T.Gowers, 他用组合数学研究泛函分析, 解决了 Banach 的问题.

王兴华、徐利治的《数学分析的方法以及例题选讲》包括了很多组合, 有其他书上没有的东西.

教材: 李乔, 组合数学基础, 高教出版社, 1997.

参考书:

- J.H.van Lint & R.W.Wilson, A course in combinatorics, Cambridge Univ. Press, 2001(有中译本, 组合数学教程, 机械工业出版社), 此书不拖泥带水, 用最快速度让你知道基本概念.
- 具体数学: R.L.Graham, D.E.Knuth, O.Patashnik, Concrete Mathematics, Addison-Wesley, MA, 1994.
- 图论: B.Bollobas, Modern Graph Theory, Springer 1998.
- R. P. Stanley, Enumerate Combinatorics, I. II. (有中译本, 计数组合学, 科学出版社.)

基本符号

符号	含义	所在章节
$\binom{n}{m}$	组合数	§1.1
$(x)_k$	x 向下乘 k 个	§1.1
(a_n)	有序数列 $a_1, a_2, \cdots$	§1.2
$p(n)$	分拆函数	§1.3
S_n	n 元有限集的置换	§1.4, §5.3, §6.4
$s(n,k), \begin{bmatrix} n \\ k \end{bmatrix}$	第一类 Stirling 数	§1.4
$S(n,k), \begin{Bmatrix} n \\ k \end{Bmatrix}$	第二类 Stirling 数	§1.4
C_n	Catalan 数	§1.5
B_n	Bell 数	§1.5
D_n	更列数	§1.5
H_n	调和数	§1.2
$H_n^{(2)}$	二阶调和数	第一章习题
$[x_1^{k_1} \cdots x_n^{k_n}] f(x_1, \cdots, f_n)$	多项式 $f(x_1, \cdots, x_n)$ 中 $x_1^{k_1} \cdots x_n^{k_n}$ 项的系数	§2.2, §6.4
F_n	Fibonacci 数	§2.2
L_n	Lucas 数	§2.2
P_n	Pell 数	§2.2
$T_n(x)$	第一类 Chebyshev 多项式	§2.2
$U_n(x)$	第二类 Chebyshev 多项式	§2.2
B_n	Bernoulli 数	§2.3
$\zeta(s)$	Riemann-Zeta 函数	§2.3
$\varphi(n)$	Euler 函数	§3.1
$\pi(x)$	不超过 x 的素数个数	§3.1
$\mu(n)$	Möbius 函数	§3.2
$\mathscr{D}(X)$	$\{$映射$\alpha : X \times X \to \mathbb{R} \mid x \not\leq y$时$\alpha(x,y) = 0\}$.	§3.2
$R_r(p_1, \cdots, p_n)$	Ramsey 数	§4.2
K_n	n 阶完全图	§4.3
$\rho(\boldsymbol{A})$	$(0,1)$-矩阵 $\boldsymbol{A}$ 的项秩	§5.3
$\lambda(\boldsymbol{A})$	$(0,1)$-矩阵 $\boldsymbol{A}$ 的线秩	§5.3
$\mathrm{per}(\boldsymbol{A})$	矩阵 $\boldsymbol{A}$ 的积和式	§5.3
$A_1 + \cdots + A_n$; nA	和集 $\{a_1 + \cdots + a_n \mid a_i \in A_i, i = 1, 2, \cdots, n\}$	§6.1
$A_1 \dot{+} \cdots \dot{+} A_n$; $n^{\wedge}A$	异元和集 $\{a_1 + \cdots + a_n \mid a_i \in A_i, a_i$两两不同$\}$	§6.1

第 1 章　组合计数

§1.1　排列组合与二项式系数

关于排列的基本定义:

- 设 S 为集合, $x_1,\cdots,x_k\in S$. 把有序 k 元组 $(x_1,\cdots,x_k)$ 叫 S 上的一个 k **元可重排列**或 S 的一个 k**-样本**. 把 S 叫**字母表**, S 中元素叫**字母**, $a_1\cdots a_k(a_i\in S)$ 是基于字母表 S 的长为 k 的**字(word)**.
- **乘法原理**: 设 W 中有序 k 元组 $(x_1,\cdots,x_k)$ 中第一个分量 x_1 有 n_1 种取法, x_1 取定后 x_2 有 n_2 种取法, x_1,x_2 取定后 x_3 有 n_3 种取法, $\cdots$, $x_1,\cdots,x_{k-1}$ 取定后 x_k 有 n_k 种取法, 那么这种有序 k 元组有 $n_1n_2\cdots n_k$ 个.
- 如果元素取自 S 的有序 k 元组 $(x_1,\cdots,x_k)$ 中 $x_1,\cdots,x_k$ 两两不同, 称之为 S 的一个 k**-排列**. n 元集的 n-排列叫**全排列**. n 元集的 k-排列个数是 $p(n,k)=n(n-1)\cdots(n-k+1)$, 也记为 $(n)_k$. 一般地, 定义

$$(x)_0=1,(x)_k=x(x-1)\cdots(x-k+1)(k=1,2,\cdots),x\in\mathbb{R}.$$

- 集合论中, $\{x_1,\cdots,x_k\}=\{x_1,x_1,x_2,\cdots,x_k\}$, 但在组合数学中有可能重复, 定义**可重集合(multi-set)**: 集合中元素允许重复.
- 设 S 为 n 元集, 取 S 的一个**重子集** M, 使得 a_i 在 M 中出现 l_i 次 $(i=1,\cdots,n)$, 称 M 是 $\boldsymbol{a_1^{l_1}a_2^{l_2}\cdots a_n^{l_n}}$ **型**.

以 n 元集 $S=\{a_1,\cdots,a_n\}$ 为字母表, 那么 $a_1^{l_1}a_2^{l_2}\cdots a_n^{l_n}$ 型的字有多少? 其中 $l_1+\cdots+l_n=k$. 我们重写这个字为

$$a_{11},a_{12},\cdots,a_{1l_1},a_{21},a_{22},\cdots,a_{2l_2},\cdots,a_{n1},a_{n2},\cdots,a_{nl_n}.$$

这是长为 k 的字, 那么

$$\textbf{这种字个数}\times l_1!l_2!\cdots l_n!=k!.$$

所以 $a_1^{l_1}a_2^{l_2}\cdots a_n^{l_n}$ 型的字个数为 $\dfrac{k!}{l_1!\cdots l_n!}$, 也记为 $\dbinom{k}{l_1,\cdots,l_n}$.

例 1.1.1

设 $S=\{a,b,\cdots,z\}$, 则 S 中长为 5 的字有 26^5 种.

例 1.1.2

元素为 0 或 1 的矩阵叫 $(0-1)$ 矩阵, 则 $m\times n$ 的 $(0-1)$ 矩阵有 2^{mn} 个.

例 1.1.3

在小于 10^9 的自然数中有多少个十进制表示中包含 1?

解: 考虑不含 1 的集合: $\{0\le 10^9:n\text{的十进制表示不含}1\}=\{a_8a_7\cdots a_0:a_i\in\{0,2,3,\cdots,9\}\}$. 共有 9^9 个元素, 所以欲求结果为 10^9-9^9, 这个数大约为 $61\%\times 10^9$.

例 1.1.4

52 张牌在四个牌手中分配每个人 13 张, 有多少种分配方案?

解: 设四个牌手为 A,B,C,D, 相当于问 $A^{13}B^{13}C^{13}D^{13}$ 型字有多少个, 答案为 $\dfrac{52!}{(13!)^4}\approx 5.36\times 10^{28}$.

例 1.1.5

由 a,b,c 组成 5 个字母的字, 要求 a 出现至多 2 次, b 至多 1 次, c 至多 3 次. 一共几个字?

解: 相当于求 $a^2b^0c^3, a^2b^1c^2, a^1b^1c^3$ 型字的总数, 一共为 $\dfrac{5!}{2!0!3!}+\dfrac{5!}{2!1!2!}+\dfrac{5!}{1!1!3!}=60$. □

关于组合基本定义:

- 元素取自 S 的一个无序 k 元组 $\{x_1,\cdots,x_k\}$ 叫 S 的一个 k **元可重组合**, 也叫 S 的一个 k **元可重子集**.
- n 元集的 k 元子集是 S 的 k 元 (不可重) 组合.
- n 元集的 k 元子集的个数相当于从 n 元集中选出 k 个 (无序且不允许重复), 方法数为 $\binom{n}{k}$(不要写 C_n^k). 一般地, 定义

$$\binom{x}{0}=1,\binom{x}{k}=\frac{(x)_k}{k!}=\frac{x(x-1)\cdots(x-k+1)}{k!},k\in\mathbb{Z}^+,x\in\mathbb{R}.$$

于是我们有:

$$\binom{-1}{k}=\frac{(-1)(-2)\cdots(-k)}{k!}=(-1)^k,$$
$$\binom{-x}{k}=\frac{(-x)(-x-1)\cdots(-x-k+1)}{k!}=\frac{(-1)^kx(x+1)\cdots(x+k-1)}{k!}=(-1)^k\binom{x+k-1}{k}.$$

命题 1.1.6

$$\sum_{k=0}^{n}\binom{n}{k}=2^n.$$

证明: 设 $S=\{a_1,\cdots,a_n\}$ 为 n 元集, S 的幂集 $\mathcal{P}(S)=\{A:A\subseteq S\}$. 那么 $|\mathcal{P}(S)|=2^n$. 另一方面, $|\mathcal{P}(S)|$ 也是 S 的所有 k 元子集个数之和, 因此 $|\mathcal{P}(S)|=\sum\limits_{k=0}^{n}\binom{n}{k}$.

综上, $\sum\limits_{k=0}^{n}\binom{n}{k}=|\mathcal{P}(S)|=2^n$. □

定理 1.1.7

n 元集 S 的 k 元可重子集个数为

$$\binom{n+k-1}{k}=(-1)^k\binom{-n}{k}.$$

证明: 设 $S=\{1,2,\cdots,n\}$, S 的一个 k 元可重组合可以表示成 $\{a_1,\cdots,a_k\}$, 利用无序性, 不妨设 $a_1\le a_2\le\cdots\le a_n$, 则此表示唯一. 则

$$1\le a_1+0<a_2+1<a_3+2<\cdots<a_k+(k-1)\le n+k-1,$$

对应了严格递增, 且这是一一对应的: 事实上, 若

$$1 \leq b_1 < b_2 < \cdots < b_n \leq n+k-1,$$

则让 $a_i = b_i - (i-1)$, 则 $a_i \leq a_{i+1}$. 因此相当于从 $\{1, 2, \cdots, n+k-1\}$ 中选 k 个不同的, 情况个数为

$$\binom{n+k-1}{k} = (-1)^k \binom{-n}{k}.$$

□

例 1.1.8

方程 $x_1 + x_2 + \cdots + x_n = k$ 的自然数解有几个?

解: 相当于 1 重复 x_1 次, $\cdots$, n 重复 x_n 次的 k 元可重组合数, 为 $\binom{n+k-1}{k}$. □

例 1.1.9

$S = \{1, \cdots, n\}$ 的一个 k 元子集称为 l-间隔的, 指其中任意两个之差绝对值大于 l. 问: S 的 l-间隔 k 元子集有多少个?

解: 设 k 元子集 $\{a_1, \cdots, a_k\}$ 满足

$$1 \leq a_1 < a_2 - l < \cdots < a_k - (k-1)l \leq n - (k-1)l.$$

取 $b_i = a_i - (i-1)l$, 那么

$$1 \leq b_1 < b_2 < \cdots < b_k \leq n - (k-1)l.$$

因此相当于求 $\{1, 2, \cdots, n-(k-1)l\}$ 的 k 元子集个数, 为 $\binom{n-(k-1)l}{k}$.

例 1.1.10

投掷 k 个骰子会出现多少种不同可能?

解: 相当于从 $\{1, \cdots, 6\}$ 取 k 个 k 元可重组合数, 为 $\binom{6+k-1}{k} = \binom{k+5}{5}$.

与分划有关的定义:

- 设 S 为 n 元非空集. 若 $S_1, \cdots, S_k \subseteq S$, $S_i \cap S_j = \varnothing (i \neq j)$, 且 $\bigcup_{i=1}^{k} S_i = S$, 称 $(S_1, \cdots, S_k)$ 为 S 的**有序分划 (划分, partition)**.
- 如果此分划满足 $|S_i| = n_i, i = 1, 2, \cdots, k$, 且 $n_1 + \cdots + n_k = n$, 则称 $(S_1, \cdots, S_k)$ 为 n 元集 S 的**有序 $(n_1, \cdots, n_k)$ 型分划)**.
- 问: 这种分划有几个?

定理 1.1.11

设 $n_1 + \cdots + n_k = n$, 则 n 元集的 $(n_1, \cdots, n_k)$ 型分划有 $\binom{n}{n_1, n_2, \cdots, n_k}$ 个.

证明:

$$\begin{aligned}\text{所求数} &= \binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdots\binom{n-n_1-\cdots-n_{k-1}}{n_k}\\ &= \frac{n!}{n_1!(n-n_1)!}\frac{(n-n_1)!}{n_2!(n-n_2)!}\cdots\frac{(n-n_1-\cdots-n_{k-1})!}{n_k!}\\ &= \frac{n!}{n_1!\cdots n_k!}.\end{aligned}$$

□

定理 1.1.12. 多项式定理

$$(x_1+\cdots+x_k)^n = \sum_{n_1+\cdots+n_k=n}\binom{n}{n_1,\cdots,n_k}x_1^{n_1}\cdots x_k^{n_k}.$$

注: 这相当于 $x_1^{n_1}x_2^{n_2}\cdots x_k^{n_k}$ 型字有多少个. 特别地, $k=2$ 时有二项式定理:

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

二项式系数 (binomial coefficient) 满足如下性质:

(1) 对称性: $\binom{n}{k} = \binom{n}{n-k} = \frac{n!}{k!(n-k)!}, 0\le k\le n.$

(2) 递推关系: $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$. 把 n 改成 $x\in\mathbb{R}$ 也对. 组合解释: $\{0,1,\cdots,n\}$ 取 k 个, 可以分为不含 0 的 (共 $\binom{n}{k}$ 种) 与含 0 的 (共 $\binom{n}{k-1}$ 种).

大约 1050 年, 贾宪排列了系数如下: (按照 $x^n, x^{n-1}y, \cdots, xy^{n-1}, y^n$ 的顺序排列)

$$\begin{array}{ccccccccc}
(x+y)^0 & & & & 1 & & & & \\
(x+y)^1 & & & 1 & & 1 & & & \\
(x+y)^2 & & 1 & & 2 & & 1 & & \\
(x+y)^3 & 1 & & 3 & & 3 & & 1 & \\
(x+y)^4 & 1 & & 4 & & 6 & & 4 & & 1
\end{array}$$

每个数 x 都是前一行与这个 x 相邻两个数之和, 也就是 $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$. 1261 年, 杨辉说贾宪发现了上式, 他把这个数阵叫贾宪三角. 但是在西方, 1654 年 Pascal 才发现了这一规律, 叫 Pascal 三角.

注: Newton 多项式: $x\in\mathbb{R}$,

$$(x+1)^\alpha = \sum_{n=0}^{\infty} f^{(n)}(0)\frac{x^n}{n!}.$$

其中, $f^{(n)}(x) = \alpha(\alpha-1)\cdots(\alpha-n+1)(x+1)^{\alpha-n}, f^{(n)}(0) = (\alpha)_n$.

(3) 单峰性: $\binom{n}{0} < \binom{n}{1} < \binom{n}{2} < \cdots < \binom{n}{\lfloor\frac{n}{2}\rfloor} = \binom{n}{\lfloor\frac{n+1}{2}\rfloor} > \cdots > \binom{n}{n-1} > \binom{n}{n}.$

如: $\binom{2n}{k}$ 在 $k=n$ 取最大, $\binom{2n+1}{k}$ 在 $k=n$ 与 $k=n+1$ 取最大.

§1.2 组合恒等式与生成函数

我们用 $\{a_n\}$ 表示无序的集合, (a_n) 表示有序的集合 (数列).

定义 1.2.1. 生成函数

对于序列 $(a_n) \geq 0$, 它的**生成函数 (generating function)**, 也叫**母函数**, 指

$$A(x) = \sum_{n=0}^{\infty} a_n x^n.$$

例 1.2.1

$\binom{\alpha}{n}(n = 0, 1, \cdots)$ 的生成函数是 $\sum_{n=0}^{\infty} \binom{\alpha}{n} x^n = (1+x)^{\alpha}$.

13 世纪, 元末明初的朱世杰发现了下面的恒等式:

定理 1.2.2. 朱世杰-Vandermonde 恒等式

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

证明: 证明方法就是用生成函数来证明. $(1+t)^x = \sum_{k=0}^{\infty} \binom{x}{k} t^k, (1+t)^y = \sum_{l=0}^{\infty} \binom{y}{l} t^l$, 那么

$$\sum_{n=0}^{\infty} \binom{x+y}{n} t^n = (1+t)^{x+y} = \sum_{n=0}^{\infty}\sum_{k=0}^{n} \binom{x}{k}\binom{y}{n-k} t^n.$$

比较 t^n 系数可得 $\sum_{k=0}^{n} \binom{x}{k}\binom{y}{n-k} = \binom{x+y}{n}$. □

推论 1.2.3

我们有:

$$(1) \sum_{k=0}^{n} (-1)^k \binom{x}{k} = (-1)^n \binom{x-1}{n}$$

$$(2) \sum_{k=0}^{n} \binom{x+k-1}{k} = \binom{x+n}{n}$$

$$(3) \sum_{k=0}^{n} \binom{m+k}{m} = \binom{m+n+1}{m+1}$$

证明: (1) 对前一定理取 $y = -1$, 利用 $\binom{-1}{n-k} = (-1)^{n-k}$;

(2) 对 (1) 取 x 为 $-x$, 用 $(-1)^k \binom{-x}{k} = \binom{x+k-1}{k}$;

(3) 对 (2) 取 x 为 $m+1$. □

注: (3) 的记法: 下面不动, 上面求和, 就等于下面加一个, 上面也加一个. 也可以用组合解释或者归纳法来证明.

推论 1.2.4

中心组合数可以写成平方和：$\sum_{k=0}^{n}\binom{n}{k}^2=\binom{2n}{n}$.

证明: $\sum_{k=0}^{n}\binom{n}{k}^2=\sum_{k=0}^{n}\binom{n}{k}\binom{n}{n-k}=\binom{2n}{n}$. □

定理 1.2.5. 二项式变换反演公式

$$f(n)=\sum_{k=0}^{n}\binom{n}{k}(-1)^k g(k),\forall n=0,1,\cdots,N$$
$$\iff \quad g(n)=\sum_{k=0}^{n}\binom{n}{k}(-1)^k f(k),\forall n=0,1,\cdots,N.$$

证明: 由对称性, 只需要证明一个方向. 如果左边成立, 那么

$$\begin{aligned}\sum_{k=0}^{n}\binom{n}{k}(-1)^k f(k)&=\sum_{k=0}^{n}\binom{n}{k}(-1)^k\sum_{l=0}^{k}\binom{k}{l}(-1)^l g(l)\\&=\sum_{l=0}^{n}g(l)\sum_{k=l}^{n}\binom{n}{k}\binom{k}{l}(-1)^{k-l}\\&=\sum_{l=0}^{n}g(l)\binom{n}{l}\sum_{k=l}^{n}\binom{n-l}{k-l}(-1)^{k-l}\\&=\sum_{l=0}^{n}g(l)\binom{n}{l}\delta_{ln}=g(n),\qquad(\text{二项式展开}).\end{aligned}$$

其中我们用到了 □

$$\boxed{\binom{n}{k}\binom{k}{l}=\binom{n}{l}\binom{n-l}{k-l}.}\tag{1.1}$$

此式不难证明, 在后面也会经常用到.

例 1.2.6

$\sum_{k=0}^{n}\binom{n}{k}\binom{k}{m}t^{k-m}=\binom{n}{m}(1+t)^{n-m}$.

证明: 【证法一】$m\le k\le n$ 时, 利用 (1.1) 式, 可得

$$\text{LHS}=\binom{n}{m}\sum_{k=m}^{n}\binom{n-m}{k-m}t^{k-m}=\binom{n}{m}(1+t)^{n-m}.$$

【证法二】(求导) 注意到

$$\begin{aligned}\text{LHS}&=\sum_{k=0}^{n}\binom{n}{k}\frac{(k)_m}{m!}t^{k-m}=\sum_{k=0}^{n}\binom{n}{k}\frac{1}{m!}\frac{\mathrm{d}^m}{\mathrm{d}t^m}t^k\\&=\frac{1}{m!}\frac{\mathrm{d}^m}{\mathrm{d}t^m}(1+t)^m=\frac{(n)_m}{m!}(1+t)^{n-m}=\binom{n}{m}(1+t)^{n-m}.\end{aligned}$$

定理 1.2.7

定义 $H_n = \sum_{k=1}^{n} \frac{1}{k}$ 为**调和数**, 那么

$$\sum_{k=1}^{n} \binom{n}{k} \frac{(-1)^{k-1}}{k} = H_n.$$

证明: 注意到

$$\frac{1}{k} = \int_0^1 t^{k-1} \mathrm{d}t,$$

于是

$$\begin{aligned}
\sum_{k=1}^{n} \binom{n}{k} \frac{(-1)^{k-1}}{k} &= \int_0^1 \sum_{k=1}^{n} \binom{n}{k} (-1)^{k-1} t^{k-1} \mathrm{d}t \\
&= \int_0^1 \frac{\sum_{k=0}^{n} \binom{n}{k} (-t)^k - 1}{-t} \mathrm{d}t \\
&= \int_0^1 \frac{(1-t)^n - 1}{(1-t) - 1} \mathrm{d}t \\
&= \int_0^1 \frac{x^n - 1}{x - 1} \mathrm{d}x = \int_0^1 \sum_{k=0}^{n-1} x^k \mathrm{d}x = H_n.
\end{aligned}$$

例 1.2.8

$$\sum_{k=0}^{n} \binom{n}{k} \frac{(-1)^k}{m+k+1} = \frac{m!n!}{(m+n+1)!}.$$

证明: 左边 $= \sum_{k=0}^{n} \binom{n}{k} (-1)^k \int_0^1 t^{k+m} \mathrm{d}t = \int_0^1 t^m (1-t)^n \mathrm{d}t = \frac{m!n!}{(m+n+1)!}.$ □

注: 回顾 Beta 函数:

$$B(a,b) = \int_0^1 x^{a-1} (1-x)^{b-1} \mathrm{d}x,$$

满足:

$$B(a,b) = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}, \Gamma(n+1) = n!.$$

定理 1.2.9. 李善兰恒等式

$$\sum_{j=0}^{n} \binom{x}{j} \binom{y}{j} \binom{x+y+n-j}{n-j} = \binom{x+n}{n} \binom{y+n}{n}.$$

证明: 方法是把复杂的式子变成和式, 好处就是可以交换求和号.

$$\begin{aligned}
\text{LHS} &= \sum_{j=0}^{n} \binom{x}{j}\binom{y}{j} \sum_{k=j}^{n} \binom{x+n}{n-k}\binom{y-j}{k-j} && \text{(朱世杰-Vandermonde 恒等式)} \\
&= \sum_{k=0}^{n} \binom{x+n}{n-k} \sum_{j=0}^{k} \binom{x}{j}\binom{y}{j}\binom{y-j}{k-j} \\
&= \sum_{k=0}^{n} \binom{x+n}{n-k} \sum_{j=0}^{k} \binom{x}{j}\binom{y}{k}\binom{k}{j} && \text{(用 (1.1) 式)} \\
&= \sum_{k=0}^{n} \binom{x+n}{n-k}\binom{y}{k}\binom{x+k}{k} && \text{(朱世杰-Vandermonde 恒等式, } \tbinom{k}{j} = \tbinom{k}{k-j}\text{)} \\
&= \sum_{k=0}^{n} \frac{(x+n)\cdots(x+n-(n-k)+1)}{(n-k)!} \cdot \frac{(x+k)\cdots(x+1)}{k!}\binom{y}{k} \\
&= \sum_{k=0}^{n} \binom{x+n}{n}\binom{n}{k}\binom{y}{k} \\
&= \binom{x+n}{n}\binom{y+n}{n} && \text{(朱世杰-Vandermonde 恒等式)} \qquad \square
\end{aligned}$$

注: 李善兰恒等式由清代数学家李善兰于 1859 年在《垛积比类》一书中首次提出.

定理 1.2.10. Dyson 猜想

设 $a_1, \cdots, a_n \in \mathbb{N}$, 把

$$\prod_{i\neq j}\left(1-\frac{x_i}{x_j}\right)^{a_i} = \prod_{1\le i<j\le n}\left(1-\frac{x_i}{x_j}\right)^{a_i}\left(1-\frac{x_i}{x_j}\right)^{a_j}$$

展开为 $x_1, \cdots, x_n$ 的 Laurent 多项式 (指数允许为负数的多项式) 以后, 其常数项是多重组合数 $\dfrac{(a_1+\cdots+a_n)!}{a_1!\cdots a_n!}$.

证明: 我们需要利用 **Lagrange 插值多项式:**

引理 1.2.11. Lagrange 插值多项式

设 $P(x)$ 是域 F 上次数小于 n 的多项式, $x_1, \cdots, x_n$ 两两不同 (或为未定元), 则

$$P(x) = \sum_{i=1}^{n} P(x_i) \prod_{i\neq j} \frac{x-x_j}{x_i-x_j}.$$

证明: 设右边多项式是 $Q(x)$, 则 $\deg P(x), \deg Q(x) < n$. 当 $1 \le k \le n$ 时, 容易证明

$$P(x_k) = Q(x_k),$$

即 $P(x) - Q(x)$ 有 n 个不同的根, 所以 $P(x) - Q(x) \equiv 0$. $\square$

注: 朱富海的《高等代数与解析几何》一书有更多证明, 可以看此书复习线性代数有关知识.

推论 1.2.12

设 $x_1,\cdots,x_n$ 是域 F 中不同的元素, 则

$$\sum_{k=1}^{n} x_j^m \prod_{j\neq i}\left(1-\frac{x_i}{x_j}\right)^{-1}=\begin{cases}1, & m=0,\\ 0, & 1\leq m\leq n-1.\end{cases}$$

证明: 根据推论, $\sum\limits_{j=1}^{n}\sum\limits_{j\neq i}\left(1-\dfrac{x_i}{x_j}\right)^{-1}=1$. 两边同乘 $\prod\limits_{1\leq i\neq j\leq n}\left(1-\dfrac{x_i}{x_j}\right)^{a_i}$, 得到

$$\begin{aligned}\prod_{1\leq i\neq j\leq n}\left(1-\frac{x_i}{x_j}\right)^{a_i}&=\sum_{i=1}^{n}\prod_{j\neq i}\left(1-\frac{x_i}{x_j}\right)^{-1}\prod_{1\leq j\neq k\leq n}\left(1-\frac{x_k}{x_j}\right)^{a_k}\\&=\sum_{i=1}^{n}\prod_{j\neq i}\left(1-\frac{x_i}{x_j}\right)^{a_i-1}\prod_{\substack{1\leq j\neq k\leq n\\ k\neq i}}\left(1-\frac{x_k}{x_j}\right)^{a_k}.\end{aligned}$$

记 $C(a_1,a_2,\cdots,a_n)$ 表示 $\prod\limits_{1\leq i\neq j\leq n}\left(1-\dfrac{x_i}{x_j}\right)^{a_i}$ 的常数项, 则当 $a_1,\cdots,a_n$ 都大于 0 时,

$$C(a_1,\cdots,a_n)=\sum_{i=1}^{n}C(a_1,\cdots,a_{i-1},a_i-1,a_{i+1},\cdots,a_n).$$

若某个 $a_k=0$, 则

$$\prod_{1\leq i\neq j\leq n}\left(1-\frac{x_i}{x_j}\right)^{a_i}=\prod_{i\neq k}\underbrace{\left(1-\frac{x_i}{x_k}\right)^{a_i}}_{①}\prod_{i\neq j,j\neq k}\Big[\underbrace{\left(1-\frac{x_i}{x_k}\right)^{a_i}}_{②}\underbrace{\left(1-\frac{x_k}{x_i}\right)^{a_k}}_{\text{恒为 }1}\Big]$$

注意②中包含 x_k 的项不可能被①中项消掉, 如果要得到常数项, 必须取①②中的常数项相乘. 而②的常数项是 1. 因此

$$C(a_1,\cdots,a_n)=C(a_1,\cdots,a_{k-1},a_{k+1},\cdots,a_n),\text{其中}a_k=0.$$

对 $n+a_1+\cdots+a_n$ 归纳证明 $C(a_1,\cdots,a_n)=\dfrac{(a_1+\cdots+a_n)!}{a_1!\cdots a_n!}$ 如下:

(i) 当 $n+a_1+\cdots+a_n=1$ 时, $n=1,a_1=\cdots=a_n=0$, 此时常数项是 1.

(ii) 对于 $n+a_1+\cdots+a_n>1$, 且此和更小时结论正确, 如果有 $1\leq k\leq n$ 使得 $a_k=0$, 则

$$\begin{aligned}C(a_1,\cdots,a_n)&=C(a_1,\cdots,a_{k-1},a_{k+1},\cdots,a_n)\\&=\frac{(a_1+\cdots+a_{k-1}+a_{k+1}+\cdots+a_n)}{a_1!\cdots a_{k-1}!a_{k+1}!\cdots a_n!}=\frac{(a_1+\cdots+a_n)!}{a_1!\cdots a_n!},\end{aligned}$$

如果都有 $a_k>0$, 则 (最后分子分母都乘 a_i)

$$\begin{aligned}C(a_1,\cdots,a_n)&=\sum_{i=1}^{n}C(a_1,\cdots,a_{i-1},a_i-1,a_{i+1},\cdots,a_n)\\&=\sum_{i=1}^{n}\frac{(a_1+\cdots+a_n-1)!}{a_1!\cdots a_{i-1}!(a_i-1)!a_{i+1}!\cdots a_n!}=\frac{(a_1+\cdots+a_n)!}{a_1!\cdots a_n!}.\end{aligned}$$

结论证明完成. □

定理 1.2.13. Newton-Gregory 插值公式

已知 $f(0),\cdots,f(n)$ 给定, 则

$$f(x)=\sum_{k=0}^{n}a_k\binom{x}{k}+R_n(x).$$

其中, $a_k=\sum_{l=0}^{k}\binom{k}{l}(-1)^{k-l}f(l)$, 多项式逼近的余项

$$R_n(x)=\begin{vmatrix}0^0 & 1^0 & \cdots & n^0 & x^0\\ 0^1 & 1^1 & \cdots & n^1 & x^1\\ 0^2 & 1^2 & \cdots & n^2 & x^2\\ \vdots & \vdots & & & \\ 0^n & 1^n & \cdots & n^n & x^n\\ f(0) & f(1) & \cdots & f(n) & f(x)\end{vmatrix}\Bigg/\begin{vmatrix}1^1 & 2^1 & \cdots & n^1\\ 1^2 & 2^2 & \cdots & n^2\\ \vdots & \vdots & & \\ 1^n & 2^n & \cdots & n^n\end{vmatrix}.$$

特别地, 若 $f(x)$ 是不超过 n 次的多项式, 则 $R_n(x)=0$.

证明: 由于 $(-1)^k a_k=\sum_{l=0}^{k}\binom{k}{l}(-1)^l f(l)$, 当 $0\le k\le n$ 时, 根据二项式反演公式, 可得

$$(-1)^l f(l)=\sum_{k=0}^{m}\binom{m}{k}[(-1)^k a_k](-1)^k.$$

令 $q_n(x)=\sum_{k=0}^{n}a_k\binom{x}{k}$, 则当 $0\le m\le n$ 时,

$$f(m)=\sum_{k=0}^{m}\binom{m}{k}a_k=\sum_{k=0}^{n}\binom{m}{k}a_k=q_n(m).$$

这里当 $k>m$ 时, $\binom{m}{k}=0$. 把 $R_n(x)$ 按最后一行展开, 可得它形如 $R_n(x)=f(x)-P_n(x)$, 其中 $P_n(x)$ 是次数小于 n 的多项式, 下证 $R_n(x)=q_n(x)$. 当 $0\le m\le n$ 时, $f(m)-P_n(m)=R_n(m)=0$, 而当 $0\le m\le n$ 时, $f(m)=q_n(m)$, 所以 $P_n(x)-q_n(x)=0$ 有 $n+1$ 个不同根 $x_0,\cdots,x_n$, 于是 $P_n(x)\equiv q_n(x)$. □

推论 1.2.14

设多项式 $f(x)$ 次数不超过 n, 则 $f(x)$ 为整系数多项式的充分必要条件是: 有正整数 $a_1,\cdots,a_n$ 使得 $f(x)=\sum_{j=0}^{n}a_j\binom{x}{j}$.

证明: "⇐": 当 $x\in\mathbb{N}$ 时, $\binom{x}{k}\in\mathbb{Z}$, 而 $\binom{-m}{k}=\binom{m+k-1}{k}(-1)^k\in\mathbb{Z}$, 所以 $f(x)$ 是整系数多项式.

"⇒": 设 $f(x)$ 是次数不超过 n 的整系数多项式, 令 $a_k=\sum_{l=0}^{k}\binom{k}{l}(-1)^{k-l}f(l)\in\mathbb{Z}(k=$

$0,1,\cdots,n)$, 则 $f(x)=\sum_{k=0}^{n}a_k\binom{x}{k}+\underbrace{R_n(x)}_{=0}$. □

其他恒等式:

(1)**Dixon 恒等式**:

$$\sum_{k=-n}^{n}(-1)^k\binom{2n}{n+k}=\binom{3n}{n,n,n}=\frac{(3n)!}{(n!)^3}.$$

(2) **孙智伟在大三就证明的恒等式:** 如果你不用上网找也能证出来就很厉害了.

$$(x+m+1)\sum_{k=0}^{m}(-1)^k\binom{x+y+k}{m-k}\binom{y+2k}{k}-\sum_{k=0}^{m}\binom{x+k}{m-k}(-4)^k=(x-m)\binom{x}{m}.$$

上个世纪 90 年代, 组合恒等式被发现可以用计算机证明. H.Wilf, D.Zeilberger 设计了方法可以用于机器证明恒等式, 要证 $\sum_k a_{n,k}=b_n$, 先化成 $\sum_k F(n,k)=1$(把 b_n 除过去), 用机器找有理函数 $R(n,k)$, 使得 $G(n,k)=R(n,k)F(n,k)$ 满足

$$F(n+1,k)-F(n,k)=G(n,k+1)-G(n,k).$$

此时称 $\langle F,G\rangle$ 为 **WZ pair(WZ 对)**. 当 k 很大或者 k 为负时, $G(n,k)=0$. 于是

$$\sum_k F(n+1,k)-\sum_k F(n,k)=0.$$

所以 $\sum_k F(n,k)$ 与 n 无关, 代入 $n=0$ 来算即可.

例 1.2.15

用 WZ 方法证明 $\sum_{k=0}^{n}\binom{n}{k}=2^n$.

证明: 取 $F(n,k)=\frac{1}{2^n}\binom{n}{k}$, 要证明 $\sum_k F(n,k)=1$, 用机器找出 $R(n,k)=\frac{k}{2(k-n-1)}$, 令

$$G(n,k)=R(n,k)F(n,k)=-\binom{n}{k-1}2^{-n-1},$$

于是 $\langle F,G\rangle$ 是 WZ 对, 从而 $\sum_k F(n,k)=\sum_k F(0,k)=1$. □

注: 称 $f(n,k)$ 是**超几何 (hypergeometric) 的**, 指 $\frac{f(n+1,k)}{f(n,k)}$ 与 $\frac{f(n,k+1)}{f(n,k)}$ 都是有理函数. 用 Zeilberger 算法可以产生组合和式递推关系: $\sum_{k=0}^{n}f(n,k)=\sum_{k=0}^{n}g(n,k)$. 其中“$f,g$”都是超几何函数.

有兴趣的读者可以翻阅 D.Zeilberger 的《$A=B$》这本书. 除此之外还有 Sigma 软件包, 先产生递推关系, 再解递推关系, 找尽可能简单的解.

§1.3 正整数的分拆

对于正整数 n, 让 $p(n)$ 表示把 n 写成若干个正整数之和的方法数（不计顺序）, 把 $p(n)$ 叫**分拆函数 (partition function)**, 例如:

$$5=4+1=3+2=3+1+1=2+2+1=2+1+1+1=1+1+1+1+1,$$

所以 $p(5)=7$, 约定 $p(0)=1$. Euler 发现

$$\boxed{\sum_{n=1}^{\infty}p(n)x^n=\prod_{k=1}^{\infty}\sum_{m_k=0}^{\infty}x^{km_k}}=\prod_{k=1}^{\infty}\frac{1}{1-x^k}=\frac{1}{\prod\limits_{n=1}^{\infty}(1-x^n)}.$$

设

$$\prod_{n=1}^{\infty}(1-x^n)=\sum_{l=0}^{\infty}a_lx^l, \tag{1.2}$$

则

$$\sum_k p(k)x^k\sum_l a_lx^l=1.$$

当 $n>0$ 时, 比较 x^n 项的系数可得 $p(n)$ 的递推式

$$\sum_{l=0}^{n}a_lp(n-l)=0.$$

Euler 展开 (1.2) 式发现了下式的规律 (观察一下每项幂次之差):

$$\prod_{n=1}^{\infty}(1-x^n)=1-x-x^2+x^5+x^7-x^{12}-x^{15}+x^{22}+x^{26}-x^{35}-x^{40}+\cdots,$$

所以

$$\prod_{n=1}^{\infty}(1-x^n)=1+\sum_{k=1}^{\infty}(-1)^k\left(x^{\frac{k(3k-1)}{2}}+x^{\frac{k(3k+1)}{2}}\right)=\sum_{k=-\infty}^{\infty}(-1)^kx^{\frac{k(3k-1)}{2}}.$$

不过 Euler 没有严格证明上式, 事实上是可以严格证明的. 后面我们会给出证明.

定理 1.3.1. Euler

正整数 n 写成**不同**正整数之和的方法数 $f(n)$ 等于把 n 写成**正奇数**之和的方法数 $g(n)$.

证明: 让 $f(0)=g(0)=1$. 于是

$$\begin{aligned}\sum_{n=0}^{\infty}f(n)x^n&=\prod_{k=1}^{\infty}(1+x^k)=(1+x)(1+x^2)(1+x^3)\cdots\\&=\frac{1-x^2}{1-x}\cdot\frac{1-x^4}{1-x^2}\cdot\frac{1-x^6}{1-x^3}\cdots\\&=\frac{1}{(1-x)(1-x^3)(1-x^5)\cdots}\qquad\text{(约去偶数)}\\&=\prod_{k=1}^{\infty}\frac{1}{1-x^{2k-1}}=\prod_{k=1}^{\infty}\sum_{m_k=0}^{\infty}x^{(2k-1)m_k}=\sum_{n=1}^{\infty}g(n)x^n.\end{aligned}$$

□

对 (1.2) 两边取对数再求导可得

$$\sum_{n=1}^{\infty}\frac{-nx^{n-1}}{1-x^n}=\frac{f'(x)}{f(x)}$$

所以

$$\begin{aligned}\frac{xf'(x)}{f(x)}&=-\sum_{d=1}^{\infty}\frac{dx^d}{1-x^d}=-\sum_{d=1}^{\infty}dx^d(1+x^d+x^{2d}+\cdots)\\&=-\sum_{d=1}^{\infty}d(x^d+x^{2d}+\cdots)=-\sum_{n=1}^{\infty}\underbrace{\left(\sum_{d|n}d\right)}_{\triangleq\sigma(n)}x^n.\end{aligned}$$

因此上式代入幂级数可得

$$\sum_{k=1}^{\infty}a_kx^k\sum_{l=1}^{\infty}\sigma(l)x^l+x\sum_{n=1}^{\infty}na_nx^{n-1}=0.$$

比较 x^n 系数可得

$$\sum_{k=0}^{n-1}a_k\sigma(n-k)+na_n=0.$$

得到了 $\sigma(n)$ 的递推式. 注意 n 是素数等价于 $\sigma(n)=n+1$, Euler 看着可以用它来判断一个数是否为素数, 感到很神奇, 但实际上 $\sigma(n)$ 表达式很复杂, 计算起来也不方便.

当 $n\to+\infty$ 时, $p(n)\to+\infty$. 例如 $p(200)=3972999029388$. 事实上有如下的公式:

定理 1.3.2. Hardy-Ramanujan

$$p(n)\sim\frac{e^{\pi\sqrt{\frac{2n}{3}}}}{4\sqrt{3}n}.$$

这个定理的证明用到了“圆法”, 是目前解析数论用到的基本工具.

Ramanujan 还发现了 $p(5n+4)\equiv0(\mathrm{mod}\ 5)$, 他用了生成函数来证明:

$$\sum_{n=0}^{\infty}p(5n+4)x^n=5\prod_{n=1}^{\infty}\frac{(1-x^{5n})^5}{(1-x^n)^6}.$$

Ramanujan 的公式让 Hardy 很惊讶, 一些公式见习题部分. 这里介绍 **Rogers-Ramanujan 公式**, Rogers 找到了第二个证明的时候 Ramanujan 才发现了它:

$$\prod_{n=0}^{\infty}\frac{1}{(1-x^{5n+1})(1-x^{5n+4})}=1+\sum_{n=1}^{\infty}\frac{x^{n^2}}{(1-x)(1-x^2)\cdots(1-x^n)}$$

$$\prod_{n=0}^{\infty}\frac{1}{(1-x^{5n+2})(1-x^{5n+3})}=1+\sum_{n=1}^{\infty}\frac{x^{n(n+1)}}{(1-x)(1-x^2)\cdots(1-x^n)}$$

此式的组合意义如下. 有兴趣可以寻找它的组合意义证明.

$$\begin{aligned}&\left|\{n\text{的分划}n=n_1+\cdots+n_k|n_1\geq n_2\geq\cdots\geq n_k,n_i-n_{i+1}\geq2\}\right|\\&\quad=\left|\{n\text{的分划}n=n_1+\cdots+n_k|n_1\geq n_2\geq\cdots\geq n_k,n_i\equiv1\text{或}4(\mathrm{mod}\ 5)\}\right|\end{aligned}$$

$$\begin{aligned}&\left|\{n\text{的分划}n=n_1+\cdots+n_k|n_1\geq n_2\geq\cdots\geq n_k\geq 2,n_i-n_{i+1}\geq 2\}\right|\\=&\left|\{n\text{的分划}n=n_1+\cdots+n_k|n_1\geq n_2\geq\cdots\geq n_k,n_i\equiv 2\text{或}3(\mathrm{mod}\ 5)\}\right|\end{aligned}$$

定理 1.3.3. Jacobi 三积恒等式

设 $q,z\in\mathbb{C},|q|<1,z\neq 0$. 则

$$\prod_{n=1}^{\infty}(1+q^{2n-1}z)(1+q^{2n-1}z^{-1})(1-q^{2n})=\sum_{n=-\infty}^{+\infty}q^{n^2}z^n.$$

证明: 可以参考徐利治《数学分析中的问题与方法》第二章的第 124 题. □

推论 1.3.4

设 $k\in\mathbb{N},l\in\mathbb{Z},0<|x|<1$, 则

$$\prod_{n=1}^{\infty}(1+x^{2kn-k-l})(1+x^{2kn-k+l})(1-x^{2kn})=\sum_{n=-\infty}^{\infty}x^{kn^2+ln}.$$
$$\prod_{n=1}^{\infty}(1-x^{2kn-k-l})(1-x^{2kn-k+l})(1-x^{2kn})=\sum_{n=-\infty}^{\infty}(-1)^nx^{kn^2+ln}.$$

证明: 在 Jacobi 恒等式中取 $q=x^k,z=\pm x^l$. □

推论 1.3.5

设 $k\in\mathbb{N},l\in\mathbb{Z},0<|x|<1$, 则

$$\prod_{n=1}^{\infty}(1+x^{kn})(1+x^{kn-l})(1+x^{k(n-1)+l})=\sum_{n=-\infty}^{\infty}x^{k\binom{n}{2}+ln}.$$
$$\prod_{n=1}^{\infty}(1+x^{kn})(1-x^{kn-l})(1-x^{k(n-1)+l})=\sum_{n=-\infty}^{\infty}(-1)^nx^{k\binom{n}{2}+ln}.$$

证明: 写 $x^k=re^{i\theta}(r>0,\theta\in\mathbb{R})$, 取 $q=\sqrt{r}e^{\frac{i\theta}{2}},z=\pm\dfrac{x^l}{q}$.

命题 1.3.6. Euler

$$\prod_{n=1}^{\infty}(1-x^n)=\sum_{k=-\infty}^{\infty}(-1)^kx^{\frac{k(3k-1)}{2}}.$$

证明: 在前一推论取 $k=3,l=1$. □

命题 1.3.7. Gauss

$$\prod_{n=1}^{\infty}\frac{1-x^{2n}}{1-x^{2n-1}}=2\sum_{n=0}^{\infty}x^{\frac{n(n+1)}{2}}.$$

证明: 在前一推论取 $k=l=1$, 于是

$$\prod_{n=1}^{\infty}(1-x^n)(1+x^{n-1})(1+x^n)=\sum_{n=-\infty}^{\infty}x^{\frac{n(n+1)}{2}}=2\sum_{n=0}^{\infty}x^{\frac{n(n+1)}{2}}.$$

而根据

$$\text{LHS}=\prod_{n=1}^{\infty}(1+x^{n-1})=\prod_{n=1}^{\infty}\frac{1-x^{2(n-1)}}{1-x^{n-1}}=\prod_{n=1}^{\infty}\frac{1}{1-x^{2n-1}}. \qquad \text{(约掉偶指数)}$$

整理即可得欲证式子. □

§1.4 两类 Stirling 数

1.4.1 (*) 置换回顾

首先复习一下近世代数里面的置换. 令 Ω 是 n 元有限集, 不妨设 $\Omega=\{1,2,\cdots,n\}$, 由 $\Omega\to\Omega$ 的全体一一变换组成的集合记作 $S_n(\Omega)$, 或简记为 S_n, 其元素通常用小写希腊字母表示, 叫做**置换**. 于是

$$S_n=\{\{1,2,\cdots,n\}\text{上的置换}\}.$$

置换直观的方式来表示任意置换 $\sigma: i\mapsto\sigma(i), i=1,2,\cdots,n$ 如下:

$$\sigma=\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix}.$$

它完全指明了所有的像.

置换上的乘法运算对应于映射合成的一般法则: $(\sigma\tau)(i)=\sigma(\tau(i))$.

例 1.4.1

设 $\sigma=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 4 & 1\end{pmatrix}, \tau=\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 3 & 2 & 1\end{pmatrix}$, 则 $\sigma\tau\neq\tau\sigma$.

证明: 注意映射的运算顺序.

$$\sigma\tau=\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 4 & 3 & 2\end{pmatrix}$$

类似有

$$\tau\sigma=\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 2 & 1 & 4\end{pmatrix}.$$

所以 $\sigma\tau\neq\tau\sigma$. □

命题 1.4.2

置换的乘法满足下述规律:

(1) 结合律: $\forall\alpha,\beta,\gamma\in S_n, (\alpha\beta)\gamma=\alpha(\beta\gamma)$.

(2) 单位元 e 是恒同映射: $\forall\sigma\in S_n, \sigma e=\sigma=e\sigma$.

(3) 逆元存在: $\forall\sigma\in S_n, \exists\tau$ 使得 $\sigma\tau=e=\tau\sigma$, 记为 $\tau=\sigma^{-1}$.

根据此命题, S_n 依据映射复合构成群, 叫做$\boldsymbol{n}$ **元对称群**或$\boldsymbol{n}$ **个文字上的对称群**.

设置换 $\sigma\in S^k$ 满足

$$\sigma=\begin{pmatrix}a_1 & a_2 & \cdots & a_{k-1} & a_k\\ a_2 & a_3 & \cdots & a_k & a_1\end{pmatrix}$$

那么这个置换叫长为 k 的**循环置换**或k-**轮换**, 简记为 $(a_1,a_2,\cdots,a_k)$ 或 $(a_1\ a_2\ \cdots\ a_k)$.

引理 1.4.3

设 X 是非空集, $a_1,\cdots,a_k,b_1,\cdots,b_l$ 是 X 中不同元, 则

$$(a_1,a_2,\cdots,a_k)(b_1,b_2,\cdots,b_l)=(b_1,b_2,\cdots,b_l)(a_1,a_2,\cdots,a_k).$$

注: 此时称这两个轮换是不相交的, 因为 $\{a_1,\cdots,a_l\}\cap\{b_1,\cdots,b_l\}=\varnothing$.

定理 1.4.4

设 X 是 n 元集, 对每个 $\sigma\in S_n(X)$, 存在唯一的 X 的分划

$$\pi=\Big\{\{a_{11},\cdots,a_{1l_1}\},\{a_{21},\cdots,a_{2l_2}\},\cdots,\{a_{k1},\cdots,a_{kl_k}\}\Big\},$$

使得

$$\sigma=(a_{11}\cdots a_{1l_1})(a_{21}\cdots a_{2l_2})\cdots(a_{k1}\cdots a_{kl_k}).$$

即可以把 σ 分成不相交轮换的乘积, 而且不计因子顺序与各个轮换乘法顺序情况下表示方法唯一.

例 1.4.5

S_7 中, $\sigma=\begin{pmatrix}1&2&3&4&5&6&7\\4&2&7&1&3&6&5\end{pmatrix}=(1\,4)(2)(3\,7\,5)(6)$.

把 $\sigma\in S_n$ 分成不相交轮换乘积以后, 设其中长为 l 的轮换有 λ_l 个. 则说 σ 是 $\mathbf{1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}}$ **型的**. 上例中, σ 是 $1^22^13^14^05^06^07^0$ 型的.

1.4.2 第一类 Stirling 数

第一类 Stirling 数与置换有关. 我们要考虑 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$ 型置换的个数, 其中 $\sum\limits_{k=1}^{\infty}k\lambda_k=n$.

定理 1.4.6. Cauchy

设 $n\in\mathbb{Z}^+,\lambda_1,\cdots,\lambda_n\in\mathbb{N}$, $\sum\limits_{l=1}^{n}l\lambda_l=n$. 则 S_n 中 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$ 型置换的个数是

$$\frac{n!}{\prod\limits_{l=1}^{n}(\lambda_l!l^{\lambda_l})}.$$

证明: 把 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$ 型置换写成不相交轮换乘积, 短的轮换写在前面, 长的写在后面, 去掉括号之后可得 $1,2,\cdots,n$ 的一个全排列. 而每个全排列都可以对应一个 $\tau\in S_n$(按照 λ_l 的取值来加括号即可).

反之, 给定 $\tau\in S_n$, 我们来说明它可以对应多个 $1,2,\cdots,n$ 的全排列. 把 τ 记为

$$(\tau(1))(\tau(2))\cdots(\tau(\lambda_1))(\tau(\lambda_1+1)\ \tau(\lambda_1+2))\cdots$$

但是, 在轮换 $(a_1,\cdots,a_l)$ 中可以让 a_i 放在第一位, 因此轮换 $(a_1,\cdots,a_l)$ 可以得到 l 个 $a_1,\cdots,a_l$ 的全排列. 而 λ_l 个长为 l 的轮换的排列有 $\lambda_l!$ 种.

因此每个 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$ 型置换 σ 对应着 $\prod_{l=1}^{n}(\lambda_l!l^{\lambda_l})$ 个 $1,\cdots,n$ 的全排列, 而每个 $1,\cdots,n$ 的全排列可以确定唯一的 σ. 所以

$$\left|\{1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}\text{型置换}\}\right|\cdot\prod_{l=1}^{n}(\lambda_l!l^{\lambda_l})=n!.$$

整理可得欲证结论. □

定义 1.4.1. 第一类 Stirling 数

定义为 $\left|\{\sigma\in S_n:\sigma\text{轮换分解式中恰有 }k\text{ 个轮换}\}\right|\triangleq s(n,k)$或$\begin{bmatrix}n\\k\end{bmatrix}$.

约定: $s(0,0)=\begin{bmatrix}0\\0\end{bmatrix}=1$. 当 $n>0$ 时, $s(n,0)=\begin{bmatrix}n\\0\end{bmatrix}=0$; 当 $k>n$ 时, $s(n,k)=\begin{bmatrix}n\\k\end{bmatrix}=0$.

回顾: $\binom{n}{k}=\binom{n-1}{k}+\binom{n-1}{k-1}$, 那么 Stirling 数也有类似的递推式, 这就是为什么要简记为 $\begin{bmatrix}n\\k\end{bmatrix}$.

定理 1.4.7

对任意 $n,k\in\mathbb{Z}^+$, 有

$$\begin{bmatrix}n\\k\end{bmatrix}=(n-1)\begin{bmatrix}n-1\\k\end{bmatrix}+\begin{bmatrix}n-1\\k-1\end{bmatrix}.$$

证明: 当 $n<k$ 时两边为 0. 下设 $n\geq k$. 轮换分解式中恰有 k 个轮换的 $\sigma\in S_n$ 分两种:

$(1)\sigma(n)=n$, 这样的 σ 有 $\begin{bmatrix}n-1\\k-1\end{bmatrix}$ 个.

$(2)\sigma(n)=\{1,\cdots,n-1\}$, 记 $\sigma(n)=m$, 于是可以写

$$\sigma=(\cdots)(\cdots)(n\ m\cdots)(\cdots)\cdots.$$

这就相当于 $1,\cdots,n-1$ 中有 k 个轮换乘积的情况下, 在其中一个轮换插入 n, 而且 n 可以放在任何数后面. 因此一共有 $(n-1)\begin{bmatrix}n-1\\k\end{bmatrix}$ 种.

结合 (1)(2) 即可证明递推式. □

定理 1.4.8

我们有

$$x(x+1)\cdots(x+n-1)=\sum_{k=0}^{n}\begin{bmatrix}n\\k\end{bmatrix}x^k$$

$$(x)_n=x(x-1)\cdots(x-n+1)=\sum_{k=0}^{n}(-1)^{n-k}\begin{bmatrix}n\\k\end{bmatrix}x^k.$$

证明: (1) 记 $\prod_{0\leq j<n}(x+j)=\sum_{k=0}^{n}c(n,k)x^k$, 下证 $c(n,k)=\begin{bmatrix}n\\k\end{bmatrix}$.

显然 $c(0,0)=s(0,0)=1$, 而 $k>n$ 时 $c(n,k)=0=s(n,k)$, 下设 $n>0$. 注意到

$$\begin{aligned} x(x+1)\cdots(x+n-1) &= x(x+1)\cdots(x+n-2)(x+n-1) \\ &= \sum_{k=0}^{n-1} c(n-1,k)x^k(x+n-1) \\ &= \sum_{k=1}^{n} c(n-1,k-1)x^k + \sum_{k=0}^{n-1}(n-1)c(n-1,k)x^k. \end{aligned}$$

比较 x^k 的系数可得

$$c(n,k)=c(n-1,k-1)+(n-1)c(n-1,k).$$

这与第一类 Stirling 数的递推关系一样, 于是 $c(n,k)=s(n,k)$.

(2) 代入 x 为 $-x$ 得第二条式子. □

注: 通过对 $\prod_{0\le j<n+k}(x+j)$ 的 x^k 项系数展开即可得到

$$\begin{bmatrix} n+k \\ k \end{bmatrix} = \sum_{1\le j_1<\cdots<j_n\le n+k} j_1\cdots j_n,$$

有 0 的项对乘积没有贡献.

1.4.3 第二类 Stirling 数

把 n 元集分成 k 块非空子集 (不计顺序) 称为***k* 部分拆**. n 元集的 k 部分拆个数叫第二类 Stirling 数, 记为 $S(n,k)=\begin{Bmatrix} n \\ k \end{Bmatrix}$. 当 $k>n$ 时 $S(n,k)=0$. 约定 $S(0,0)=1$.

例 1.4.9

$\{1,2,3,4\}$ 有 7 个 2 部分拆:

$$\{1\}\{2,3,4\};\{2\}\{1,3,4\};\{3\}\{1,2,4\};\{4\}\{1,2,3\};\{1,2\}\{3,4\};\{1,3\}\{2,4\};\{1,4\}\{2,3\}.$$

因此 $S(4,2)=7$.

下面求 $S(n,k)$ 的递推关系.

定理 1.4.10

对 $n,k\in\mathbb{Z}^+$, 有 $\begin{Bmatrix} n \\ k \end{Bmatrix} = k\begin{Bmatrix} n-1 \\ k \end{Bmatrix} + \begin{Bmatrix} n-1 \\ k-1 \end{Bmatrix}$.

证明: 考虑 $S=\{0,1,\cdots,n-1\}$ 的 k 部分拆, 分为两种:

(1)0 单独构成一块, 共有 $\begin{Bmatrix} n-1 \\ k-1 \end{Bmatrix}$ 种.

(2)$\{1,\cdots,n-1\}$ 作 k 步分拆后, 把 0 插入其中一个, 一共 $k\begin{Bmatrix} n-1 \\ k \end{Bmatrix}$ 种.

结合 (1)(2) 即可得欲证等式. □

下面给出第二类 Stirling 数的解析形式的表达式.

定理 1.4.11

$$S(n,k)=\frac{1}{k!}\sum_{l=0}^{k}\binom{k}{l}(-1)^{k-l}l^n.$$

证明: 从 n 元集 S 到 m 元集 T 的映射个数有 m^n. 另外, $\left|\{f:S\to T|\mathrm{Ran}(f)恰有k个元素\}\right|=k!\begin{Bmatrix}n\\k\end{Bmatrix}$, (把原来的集合分成 k 块, 但是这 k 块是有排列顺序的.) 对所有 k 求和可得

$$\sum_{k=0}^{m}\binom{m}{k}k!\begin{Bmatrix}n\\k\end{Bmatrix}=m^n,\forall m. \tag{1.3}$$

根据二项式变换反演公式 (令 $f(k)=(-1)^k k!\begin{Bmatrix}n\\k\end{Bmatrix}, g(m)=m^n$), 得到

$$\begin{Bmatrix}n\\m\end{Bmatrix}m!(-1)^m=\sum_{k=0}^{m}\binom{m}{k}(-1)^k k^n.$$

整理一下即可得欲证式子. □

定理 1.4.12

$$x^n=\sum_{k=0}^{n}\begin{Bmatrix}n\\k\end{Bmatrix}(x)_k.$$

证明: 把 (1.3) 式改写为

$$\sum_{k=0}^{m}(m)_k\begin{Bmatrix}n\\k\end{Bmatrix}=m^n,\forall m=1,2,\cdots,n.$$

令 $P(x)=x^n-\sum_{k=0}^{n}\begin{Bmatrix}n\\k\end{Bmatrix}(x)_k$, 则 $P(x)$ 有 n 个零点 $1,2,\cdots,n$, 但是 $\deg P<n$, 于是 $P(x)\equiv 0$. □

下面让 $V_n=\{P(x)\in\mathbb{C}[x]|\deg P(x)\le n\}$, 它是 $\mathbb{C}$ 上的线性空间, 而 $x^0,x^1,\cdots,x^n$ 是一组基, 所以 $\dim V_n=n+1$.

引理 1.4.13

设 $P_k(x)\in\mathbb{C}[x]$, $\deg P_k=k$, 则 $P_0,P_1,\cdots,P_n$ 也是 V_n 的一组基.

证明: 只需证明 $P_0,\cdots,P_n$ 在 $\mathbb{C}$ 上线性无关. 设 $\sum_{k=0}^{n}c_kP_k(x)=0$, 其中 $c_k\in\mathbb{C}$, 比较 x^n 项系数可得 $c_n=0$, 于是 $\sum_{k=0}^{n-1}c_kP_k(x)=0$, 再比较 x^{n-1} 项系数可得 $c_{n-1}=0$. 以此类推, $c_0=0$. □

注: $\{(x)_n\}_{n=0}^m$ 与 $\{x^k\}_{k=0}^m$ 都构成 V_m 的一组基, 根据定理1.4.8与定理1.4.12, 这两组基可以相互表示.

定理 1.4.14. Stirling 数的正交关系

我们有

$$\sum_{k=l}^{n} \begin{Bmatrix} n \\ k \end{Bmatrix} \begin{bmatrix} k \\ l \end{bmatrix} (-1)^{k-l} = \delta_{ln},$$
$$\sum_{k=l}^{n} \begin{bmatrix} n \\ k \end{bmatrix} \begin{Bmatrix} k \\ l \end{Bmatrix} (-1)^{k-l} = \delta_{ln}.$$

证明: 只证第一条. 利用定理1.4.8与定理1.4.12, 我们可以得到

$$x^n = \sum_{k=0}^{n} \begin{Bmatrix} n \\ k \end{Bmatrix} \sum_{l=0}^{k} (-1)^{k-l} \begin{bmatrix} k \\ l \end{bmatrix} x^l = \sum_{0 \le l \le k \le n} \begin{Bmatrix} n \\ k \end{Bmatrix} \begin{bmatrix} k \\ l \end{bmatrix} (-1)^{k-l} x^l.$$

比较两边多项式的系数即可. □

注: 回顾定理1.2.5的证明过程. 把这里的方括号改为圆括号我们有

$$\sum_{k=l}^{n} \binom{n}{k} \binom{k}{l} (-1)^{k-l} = \delta_{ln}.$$

定理 1.4.15. Stirling 数反演公式

$$f(n) = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} (-1)^k g(k) \qquad (n = 0, \cdots, N)$$
$$\Leftrightarrow \qquad g(n) = \sum_{k=0}^{n} \begin{Bmatrix} n \\ k \end{Bmatrix} (-1)^k f(k) \qquad (n = 0, \cdots, N).$$

证明: 利用正交关系即可. “⇒”:

$$\begin{aligned} \sum_{k=0}^{n} \begin{Bmatrix} n \\ k \end{Bmatrix} (-1)^k f(k) &= \sum_{k=0}^{n} \begin{Bmatrix} n \\ k \end{Bmatrix} (-1)^k \sum_{l=0}^{k} \begin{bmatrix} k \\ l \end{bmatrix} (-1)^l g(l) \\ &= \sum_{l=0}^{n} \sum_{k=l}^{n} (-1)^{k-l} \begin{Bmatrix} n \\ k \end{Bmatrix} \begin{bmatrix} k \\ l \end{bmatrix} g(l) \\ &= \sum_{l=0}^{n} \delta_{nl} g(l) = g(n). \qquad \square \end{aligned}$$

序列 $(a_n)_{n \ge 0}$ 的**指数型母函数 (生成函数)** 指 $\sum_{n=0}^{\infty} a_n \frac{x^n}{n!}$.

定理 1.4.16

$$\sum_{n=0}^{\infty} S(n,k) \frac{x^n}{n!} = \frac{(e^x - 1)^k}{k!}, \sum_{m=0}^{\infty} s(m,k) \frac{x^m}{m!} = \frac{(-1)^k \ln^k (1-x)}{k!}.$$

证明: (1) 由于

$$(e^x - 1)^k = \left(\sum_{m=1}^{\infty} \frac{x^m}{m!} \right)^k = \sum_{n=1}^{\infty} \sum_{\substack{m_1 + \cdots + m_k = n \\ m_i \ge 1}} \binom{n}{m_1, \cdots, m_k} \frac{x^n}{n!}.$$

注意 n 元集到 k 元集的满射个数为

$$S(n,k)=\sum_{\substack{m_1+\cdots+m_k=n\\ m_i\geq 1}}\binom{n}{m_1,\cdots,m_k},$$

(n 元集分成 k 块的分划数就是 $\binom{n}{m_1,\cdots,m_k}$, 再把所有情况加起来.)

(2) 利用正交关系,

$$\begin{aligned}
&\sum_{m=0}^{\infty}\frac{(e^x-1)^m}{m!}(-1)^{m-k}s(m,k)\\
=&\sum_{m=0}^{\infty}\left(\sum_{n=0}^{\infty}S(n,m)\frac{x^n}{n!}\right)(-1)^{m-k}s(m,k)\\
=&\sum_{n=0}^{\infty}\frac{x^n}{n!}\sum_{m=k}^{n}S(n,m)s(m,k)(-1)^{m-k}\qquad (\text{当 } m<k \text{ 或 } m>n \text{ 时右边项为 } 0)\\
=&\sum_{n=0}^{\infty}\frac{x^n}{n!}\delta_{kn}=\frac{x^k}{k!}.
\end{aligned}$$

再令 $z=1-e^x$ 即可. □

§1.5 Catalan 数, Bell 数, 更列数

1.5.1 Catalan 数

我们要计算 $a_0a_1\cdots a_n$, 在它们之间作乘法, 有多少种加括号的方式?

对 $a_0,a_1,\cdots,a_n$ 加括号进行二元乘积的方法数叫 **Catalan 数**, 记为 C_n.

显然, $C_0=1,C_1=1,C_2=2,C_3=5$.

定理 1.5.1

$$C_n=\frac{1}{n+1}\binom{2n}{n}.$$

证明: 首先得到递推关系:

$$C_{n+1}=\sum_{k=0}^{n}C_kC_{n-k},$$

这是因为, 对任意 $k\in\{0,1,\cdots,n+1\}$, $(a_0,\cdots,a_k)(a_{k+1},\cdots,a_{n+1})$ 加括号后, 两个括号里面分别有 C_k 与 C_{n-k} 种加括号方式. 接下来只需解这个递推关系.

令 $f(x)=\sum_{k=0}^{\infty}C_kx^k$, 则

$$f^2(x)=\left(\sum_{k=0}^{\infty}C_kx^k\right)\left(\sum_{l=0}^{\infty}C_lx^l\right)=\sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}C_kC_{n-k}\right)x^n=\sum_{n=0}^{\infty}C_{n+1}x^n.$$

所以

$$xf^2(x)=\sum_{n=0}^{\infty}C_{n+1}x^{n+1}=f(x)-1,$$

这是关于 $f(x)$ 的函数方程, 解得 $f(x)=\dfrac{1\pm\sqrt{1-4x}}{2x}$.

由于 $f(0)=C_0=1$, 所以必定有 $f(x)=\dfrac{1-\sqrt{1-4x}}{2x}$. 由 Taylor 公式,

$$\sqrt{1-4x}=\sum_{k=0}^{n}\binom{\frac{1}{2}}{k}(-4x)^k.$$

代入 $\binom{\frac{1}{2}}{k}=\dfrac{1}{2k}\binom{-\frac{1}{2}}{k-1}$ 与 $\binom{-\frac{1}{2}}{n}=\dfrac{1}{(-4)^n}\binom{2n}{n}$ 得到

$$\sqrt{1-4x}=1+\sum_{k=1}^{\infty}\frac{1}{2k}\frac{\binom{2(k-1)}{k-1}}{(-4)^{k-1}}(-4)^kx^k=1-2\sum_{n=0}^{\infty}\frac{1}{n+1}\binom{2n}{n}x^{n+1},$$

所以

$$f(x)=\sum_{n=0}^{\infty}\frac{1}{n+1}\binom{2n}{n}x^n,$$

比较 x^n 的系数得到 $C_n=\dfrac{1}{n+1}\binom{2n}{n}$. □

Catalan 数是很基本的一类数, 它有很多种组合解释, 这里列举两种组合解释:

(1) 长为 $2n$ 的 **Dyck 字**由 n 个 X 与 n 个 Y 组成, 但从前面开始数, Y 的个数总不多于 X 的个数, 例如

$$XXXYYY, XYXXYY, XYXYXY, XXYYXY, XXYXYY.$$

或者说, 在平面中, 从 $(0,0)$ 出发到 (n,n), 只能向右或者向上走, 且不能超过直线 $y=x$, 这样的路叫 **Dyck 路**. 长为 $2n$ 的 Dyck 字一共有 C_n 条.

(2) 把凸 $n\geq 3$ 边形用仅可能在顶点相交的对角线完全剖分成三角形的方法数 C_{n-2} 种. 证明如下: 设 A_n 表示剖分方法数, 约定 $A_2=1$. 对某个 $i\in\{2,3,\cdots,n-1\}$, 连接 P_1P_i 与 P_nP_i, 那么 $P_1P_nP_i$ 构成三角形, 而且得到一个 i 边形与一个 $n-i+1$ 边形, 于是

$$A_n=\sum_{i=2}^{n-1}A_iA_{n-i+1}.$$

另一方面,

$$C_0=1, C_{n-2}=\sum_{k=0}^{n-3}C_kC_{n-3-k}=\sum_{i=2}^{n-1}C_{i-2}C_{n-1-i}.$$

递推关系相同, 利用归纳法可以证明 $A_n=C_{n-2}$. □

1.5.2 Bell 数

用 B_n 表示 n 元集分类 (划分为若干个非空集) 个数, 即 n 元集上等价关系的个数. 约定 $B_0=1$. 显然,

$$B_n=\sum_{k=0}^{n}\left\{{n\atop k}\right\} \tag{1.4}$$

定理 1.5.2. Dobinski 公式

$$B_n = e^{-1}\sum_{m=0}^{\infty}\frac{m^n}{m!}.$$

证明: 由定理1.4.12, 可知 $\dfrac{m^n}{m!} = \sum\limits_{k=0}^{n}\left\{{n \atop k}\right\}\dfrac{(m)_k}{m!} = \sum\limits_{k=0}^{\min\{m,n\}}\left\{{n \atop k}\right\}\dfrac{1}{(m-k)!}$. 因此

$$\begin{aligned}\sum_{m=0}^{\infty}\frac{m^n}{m!}x^m &= \sum_{k=0}^{n}\left\{{n \atop k}\right\}x^k\sum_{l=0}^{\infty}\frac{x^l}{l!} \qquad (\text{换元 } l=m-k)\\ &= e^x\sum_{k=0}^{n}\left\{{n \atop k}\right\}x^k.\end{aligned}$$

再取 $x=1$ 并结合 (1.4) 式即可. □

定理 1.5.3

$$\sum_{n=0}^{\infty}B_n\frac{x^n}{n!} = e^{e^x-1}.$$

证明: $e^{e^x-1} = \sum\limits_{k=0}^{\infty}\dfrac{(e^x-1)^k}{k!} = \sum\limits_{k=0}^{\infty}\sum\limits_{n=0}^{\infty}s(n,k)\dfrac{x^n}{n!} = \sum\limits_{n=0}^{\infty}\dfrac{x^n}{n!}\left(\sum\limits_{k=0}^{\infty}s(n,k)\right) = \sum\limits_{n=0}^{\infty}B_n\dfrac{x^n}{n!}.$

注意当 $k>n$ 时, $s(n,k)=0$, 于是 $\sum\limits_{k=0}^{\infty}s(n,k) = \sum\limits_{k=0}^{n}s(n,k)$. □

定理 1.5.4

$$B_{n+1} = \sum_{k=0}^{n}\binom{n}{k}B_k.$$

证明: $\{0,1,\cdots,n\}$ 的分类中, 含 0 的那块恰有 $k+1$ 个元素的分类有 $\dbinom{n}{k}B_{n-k}$ 种,

因此 $B_{n+1} = \sum\limits_{k=0}^{n}\dbinom{n}{k}B_{n-k} = \sum\limits_{k=0}^{n}\dbinom{n}{k}B_k$. □

1.5.3 更列数

设 $X=\{x_1,\cdots,x_n\}$ 为 n 元集, X 的一个置换 $x_{i_1},x_{i_2},\cdots,x_{i_n}$ 叫**错位排列 (更列, derangement)**, 指 $i_j\neq j(j=1,2,\cdots,n)$. 这样的排列的个数记为

$$D_n = \Big|\{\sigma\in S_n:\sigma(i)\neq i, i=1,2,\cdots,n\}\Big|,$$

约定 $D_0=1$. 容易知道 $D_1=0, D_2=1$.

定理 1.5.5. Euler

$$D_n = (n-1)(D_{n-1}+D_{n-2})(n\geq 2).$$

证明: 把 $1,\cdots,n$ 的更列 $a_1,\cdots,a_n$ 分为两类, 固定 $k\in\{2,\cdots,n\}$, 并让 $a_1=k$.

第一类: $a_k=1$, 其他 $n-2$ 个元素错位排列, 这种排列一共有 D_{n-2} 种.

第二类: $a_k\neq 1$, 此时 $a_2\cdots a_{k-1}a_ka_{k+1}\cdots a_n$ 是 $2,\cdots,k-1,1,k+1,\cdots,n$ 的更列, 这种排列一共有 D_{n-1} 种. □

定理 1.5.6

$D_n = n!\sum_{k=0}^{n}\frac{(-1)^k}{k!} = \left\langle \frac{n!}{e} \right\rangle$. 其中, 我们把最靠近 x 的整数记为 $\langle x \rangle$.

证明: (1) 由前一定理,

$$\begin{aligned} D_n - nD_{n-1} &= -[D_{n-1} - (n-1)D_{n-2}] \\ &= (-1)^2[D_{n-2} - (n-2)D_{n-3}] \\ &= \cdots = (-1)^{n-1}(D_1 - 1D_0) = (-1)^n. \end{aligned}$$

于是

$$\frac{D_n}{n!} - \frac{D_{n-1}}{(n-1)!} = \frac{(-1)^n}{n!} \Rightarrow \frac{D_n}{n!} - \frac{D_0}{0!} = \sum_{k=1}^{n}\frac{(-1)^k}{k!}, \Rightarrow \frac{D_n}{n!} = \sum_{k=0}^{n}\frac{(-1)^k}{k!}.$$

(或者设 $d_n = n!\sum_{k=0}^{n}\frac{(-1)^k}{k!}$, 验证 $d_n - nd_{n-1} = (-1)^n$ 与 $d_0 = 1$, 归纳可得 $d_n = D_n$.)

(或者考虑 $\{1, \cdots, n\}$ 的置换总个数是 $n! = \sum_{k=0}^{n}\binom{n}{k}D_{n-k}$, 这里 k 个不动, 其他 $n-k$ 个动, 再用反演公式得到 $(-1)^n D_n = \sum_{k=0}^{n}\frac{n!}{k!}(-1)^{n-k}$.)

注: 当 $n \to \infty$ 时, 错位排列占总排列个数的 $\frac{1}{e}$.

(2) 注意 $\left|\frac{n!}{e} - D_n\right| = \left|n!\sum_{k=n+1}^{\infty}\frac{(-1)^k}{k!}\right| < \frac{n!}{(n+1)!} = \frac{1}{n+1} \le \frac{1}{2}$, 则 $D_n = \left\langle \frac{n!}{e} \right\rangle$. □

例 1.5.7

在一次晚会上, 7 个人去取回被搅乱的帽子, 各拿取一个, 至少有 2 人取到自己帽子的方法数有

$$\sum_{k=2}^{7}\binom{7}{k}D_{7-k} = \sum_{j=0}^{5}\binom{7}{j}D_j = \sum_{j=0}^{5}\binom{7}{j}j!\sum_{k=0}^{j}\frac{(-1)^k}{k!}.$$

第一章习题

1. k 个相同的球放入 n 个不同的盒子中, 一共有_____ 种放法.
2. 计算 $\sum_{k=1}^{n}k\binom{n}{k}\binom{n+1}{k}$ =_____.
3. 计算 $\sum_{k=1}^{n}k\binom{n}{k}^2$ =_____.
4. 设 m, n 是正整数, 计算 $\sum_{k=0}^{n}(m+k)!k!$ =_____.
5. 计算 $\sum_{k=1}^{n}k(k+1)(k+2)$ =_____.
6. 设 m, n 是正整数, $m < n$, 计算 $\sum_{k=m}^{n}\binom{k}{m}\binom{n}{k}$ =_____.

7. 当 $n=4m$ 时, 计算 $\binom{n}{0}-\binom{n}{2}+\binom{n}{4}-\cdots+\binom{n}{n}=$_____.
8. 用归纳法证明 $\sum_{k=0}^{n}\binom{m+k}{m}=\binom{m+n+1}{n+1}$, 并尝试给出组合解释. (提示: 在编号为 $1,\cdots,m+n+1$ 的 $m+n+1$ 个球中选 $n+1$ 个球, 考虑被选中的球的最大编号)
9. 用组合解释来证明
   (1) $\left\{\begin{matrix} n \\ n-1 \end{matrix}\right\}=\binom{n}{2}$;
   (2) $\left\{\begin{matrix} n \\ n-2 \end{matrix}\right\}=\binom{n}{3}+3\binom{n}{4}$;
   (3) $\left\{\begin{matrix} n \\ n-3 \end{matrix}\right\}=\binom{n}{4}+10\binom{n}{5}+15\binom{n}{6}$.
10. 证明: 对正整数 n, 有 $\sum_{k=1}^{n}\binom{n}{k}(-1)^k H_k^{(2)}=-\frac{H_n}{n}$.

    其中, $H_n^{(2)}=\sum_{k=1}^{n}\frac{1}{k^2}$ 是二阶调和数, $H_n=\sum_{k=1}^{n}\frac{1}{k}$ 是调和数.
11. 证明: $\sum_{k=1}^{n}\binom{n}{k}\frac{(-1)^{k-1}}{k}H_k=H_n^{(2)}$.
12. $\sigma,\tau\in S_n$ 是同型的 $\Leftrightarrow$ σ 与 τ 共轭, 即存在 $\rho\in S_n$ 使得 $\rho\sigma\rho^{-1}=\tau$.
13. 证明:
$$S(n+1,k+1)=\sum_{m=k}^{n}\binom{n}{m}S(m,k),$$
$$s(n+1,k+1)=\sum_{m=k}^{n}(n)_{n-m}s(m,k),$$
    方法一: 找组合解释; 方法二: 对 $S(n,k)$ 与 $s(n,k)$ 的生成函数求导.
14. 1,2,3,4,5,6 中有多少更列使得第 $2\sim4$ 个位置上的数字是 2,3,4 的排列?
15. 设 n 是正整数, $C_k=\frac{1}{k+1}\binom{2k}{k}$ 是 Catalan 数, 证明: $\sum_{k=0}^{n-1}(-1)^k\binom{n+k}{2k+1}C_k=1$.
16. 设 n 是正整数, 证明: $\sum_{k=0}^{n}\frac{(-1)^k}{k+1}\binom{n}{k}\binom{n+k}{k}=0$.

选做题

1. 证明 Ramanujan 发现的公式:
   (1) $\displaystyle\int_0^\infty \prod_{n=1}^{\infty} \frac{1+(\frac{x}{b+n})^2}{1+(\frac{x}{a+n-1})^2}\mathrm{d}x = \frac{\sqrt{\pi}}{2}\cdot\frac{\Gamma(a+\frac{1}{2})\Gamma(b+1)\Gamma(b-a+\frac{1}{2})}{\Gamma(a)\Gamma(b+\frac{1}{2})\Gamma(b-a+1)}.$
   (2) $\displaystyle 1+9\left(\frac{1}{4}\right)^4+17\left(\frac{1\times5}{4\times8}\right)^4+25\left(\frac{1\times5\times9}{4\times8\times12}\right)^2+\cdots=\frac{2\sqrt{2}}{\sqrt{\pi}\Gamma(\frac{3}{4})^2}.$
   (3) 让 $\displaystyle u=\cfrac{x}{1+\cfrac{x^5}{1+\cfrac{x^{10}}{1+\ddots}}}, v=\cfrac{\sqrt[5]{x}}{1+\cfrac{x}{1+\cfrac{x^2}{1+\ddots}}}$, 则 $\displaystyle v^5=u\frac{1-2u+4u^2-3u^3+u^4}{1+3u+4u^2+2u^3+u^4}.$
   (4) $\displaystyle\sum_{k=0}^{\infty}\frac{26390k+1103}{396^{4k}}\binom{4k}{k,k,k,k}=\frac{99^2}{2\pi\sqrt{2}}.$
2. 证明 **Touchard 同余式**: 设 p 是素数, 则 $B_{n+p}\equiv B_n+B_{n+1}(\mathrm{mod}\ p)$.
3. 证明下面的猜想:
   (1) 设 p 是素数, B_n 是 Bell 数, 则 $B_{n+t}\equiv B_n(\mathrm{mod}\ p)$ 的最小正周期是 $\dfrac{p^p-1}{p-1}$.
   (2) (2013, 孙智伟)Bell 数 $B_n(n>1)$ 的分拆数 $p(n)(n>1)$ 不可能是完全方幂.
   (3) (1982, F.Firoozbakht(伊朗)) 设 $(p_n)_{n\geq1}$ 是素数列. 则数列 $(\sqrt[n]{p_n})_{n\geq1}$ 单调递减.
4. 证明下面孙智伟的猜想:
   (1) $(\sqrt[n]{B_n})_{n\geq1}$ 单调递增趋于 1, $\left(\dfrac{\sqrt[n+1]{B_{n+1}}}{\sqrt[n]{B_n}}\right)_{n\geq1}$ 单调递减趋于 1. (小百合上的 G. Zhang 用二重积分证明了当 n 充分大时成立; G. Zhang 不是张高飞, 而是 IP 位于加拿大的某人.)
   (2) $(\sqrt[n]{D_n})_{n\geq1}$ 单调递增, $\left(\dfrac{\sqrt[n+1]{D_{n+1}}}{\sqrt[n]{D_n}}\right)_{n\geq1}$ 单调递减.
   (3) 设 F_n 是 Fibonacci 数, 则 $(\sqrt[n]{F_n})_{n\geq1}$ 单调递增, $\left(\dfrac{\sqrt[n+1]{F_{n+1}}}{\sqrt[n]{F_n}}\right)_{n\geq1}$ 单调递减.
   (类似的猜想有很多, 比如 Bernoulli 数的版本. 很多人一起做)
5. 设 p 是素数, 把有理数 $\dfrac{a}{b}$ 称为***p*-整数** (有理的 p 进数), 若 $a,b\in\mathbb{Z}$ 且 $(b,p)=1$. 所有 p-整数构成一个环 R_p, 它是 p 进整数环 $\mathbb{Z}_p$ 的子环. 对于一个 p-整数 $\dfrac{a}{b}$, 如果整数 c 与一个非负整数 n 满足 $\dfrac{a}{b}=c+p^nq$, 其中 $q\in R_p$(这等价于 $a\equiv bc(\mathrm{mod}\ p^n)$), 那么我们记

$$\boxed{\frac{a}{b}\equiv c(\mathrm{mod}\ p^n).}$$

   例如, $\displaystyle 1+\frac{1}{2}\equiv1-4=-3(\mathrm{mod}\ 3^2)$. 孙智伟于 2010 年 7 月 17 日猜想: 对任意正整数 n, 存在唯一的整数 a_n 使得

$$\sum_{k=0}^{p-1}\frac{B_k}{(-n)^k}\equiv a_n(\mathrm{mod}\ p), 对任意素数p\nmid n.$$

   例如, $a_8=-1853$. 后来孙智伟受 D.Zagier 启发, 改写上式为 $\displaystyle\sum_{k=1}^{p-1}\frac{B_k}{(-n)^k}\equiv a_n-1(\mathrm{mod}\ p)$, 进一步发现了 Bell 数 B_n 与更列数 D_n 之间的关系:

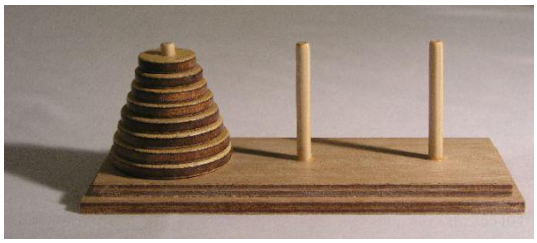
$$a_n-1\equiv(-1)^{n-1}D_{n-1}(\mathrm{mod}\ p).$$

   文章可以见 Bull. Austral. Math. Soc., 84(2011). 关于此式也有许多推广.

第 2 章　递归序列

§ 2.1　一阶线性递归序列

1883 年, E.Lucas 提出如下的河内塔问题: 相传它源于印度神话中的大梵天创造的三个金刚柱, 一根柱子上叠着上下从小到大 64 个黄金圆盘. 大梵天命令婆罗门将这些圆盘按从小到大的顺序移动到另一根柱子上, 其中大圆盘不能放在小圆盘上面. 当这 64 个圆盘移动完的时候，世界就将毁灭.



问题: 如果一共有 n 个盘子, 至少要多少次才能把一个柱子上的所有圆盘转移到另一个柱子上?

假设至少要搬 $f(n)$ 次, 则 $f(1)=1, f(2)=3$. 一般地, $f(n)=2f(n-1)+1$, 从而

$$f(n)=2^2f(n-2)+2+1=2^3f(n-3)+2^2+2+1=\cdots=2^{n-1}f(1)+\sum_{k=0}^{n-2}2^k=2^n-1.$$

对于一阶常系数线性递归序列 $a_{n+1}=ba_n+c(n=0,1,2,\cdots)(b\neq 0)$, 两边同除以 b^{n+1} 得到

$$\frac{a_{n+1}}{b^{n+1}}=\frac{a_n}{b^n}+\frac{c}{b^{n+1}},$$

再求和可得

$$\frac{a_n}{b^k}-\frac{a_0}{b^0}=\sum_{k=0}^{n-1}\left(\frac{a_{k+1}}{b^{k+1}}-\frac{a_k}{b^k}\right)=\sum_{k=0}^{n-1}\frac{c}{b^{k+1}}=\begin{cases}\dfrac{c}{b^n}\dfrac{b^n-1}{b-1}, & b\neq 1,\\ cn, & b=1.\end{cases}$$

§ 2.2　二阶递推关系与 Lucas 序列

2.2.1　Fibonacci 数列

L.Fibonacci(1170-1250) 在 1202 年研究了兔子繁殖问题: 假设一对幼年兔子需要一个月长成成年兔子, 一对成年兔子一个月后每个月都可以繁衍出一对新的幼年兔子. 不考虑死亡的情况，如果第一个月有一对兔子, 问第 n 个月时共有多少对兔子?

假设第 n 个月底兔子有 F_n 对, 那么 $F_1=1, F_2=1, F_3=2, F_4=3, F_5=5,\cdots$, 满足递推式:

$$F_{n+1}=F_n+F_{n-1}.$$

这里 F_n 表示原来的兔子, 而 F_{n-1} 表示前 $n-1$ 个月的成熟兔子都生下来的新兔子. 约定 $F_0=0$, Lucas(1842-1891) 把此数列 (F_n) 称作 **Fibonacci 数列**.

定理 2.2.1

Fibonnaci 数列中一个数的方幂只有 $1, 8$ 与 144.

证明要用到费马大定理的思想, 参见https://arxiv.org/pdf/math/0403046v1.pdf

例 2.2.2. Fibonacci 数列的组合解释

由 $0,1$ 组成的有穷串叫 $(0,1)$-串. 长为 n 的不含连续两个 0 的 $(0,1)$-串有多少个?

答: 记其个数为 W_n, 那么 $W_1=2, W_2=3, W_3=5$, 而且 $W_{n+1}=W_n+W_{n-1}$. (若尾巴是 1, 那前 n 个共 W_n 种; 若尾巴是 0, 那么倒数第二个必为 1, 前 $n-1$ 个共 W_{n-1} 种.) 所以 $W_n=F_{n+2}$. □

Fibonacci 数列的对偶序列 $(L_n)_{n\geq 0}$ 定义为: $L_0=2, L_1=1, L_{n+1}=L_n+L_{n-1}(n=1,2,\cdots)$, 把 (L_n) 叫 **Lucas 数**.

2.2.2 Lucas 型序列

19 世纪 Lucas 才开始研究递归序列. Lucas 型递推数列 $u_n=u_n(A,B)(n\geq 0)$ 定义为:

$$u_0=1, u_1=1, u_{n+1}=Au_n-Bu_{n-1}, n=1,2,\cdots .$$

(u_n) 的**对偶序列** $v_n=v_n(A,B)(n\geq 0)$ 为:

$$v_0=2, v_1=A, v_{n+1}=Av_n-Bv_{n-1}, n=1,2,\cdots .$$

若 $A=1, B=-1$, 此时 $u_n(1,-1)=(F_n)$ 为 Fibonacci 数列, 它的对偶序列是 $v_n(1,-1)=L_n$.

若 $A=2, B=-1$, 定义 **Pell 序列** (P_n) 为 $P_n=u_n(2,-1)$, 它的对偶序列 (Q_n) 定义为 $Q_n=v_n(2,-1)$.

此外我们定义 $S_n=u_n(4,1), T_n=v_n(4,1)$.

定理 2.2.3. Lucas 同余式

设 p 是素数, $a_i,b_i\in\{0,\cdots,p-1\}$, $a=\sum_{i=0}^{k}a_ip^i, b=\sum_{i=0}^{k}b_ip^i$, 则

$$\binom{a}{b}\equiv\prod_{i=0}^{k}\binom{a_i}{b_i}(\mathrm{mod}\ p).$$

Lucas 用了他的一个 Mersene 素数判别法算出了 $2^{127}-1$ 是素数.

Lucas 死于非命. 在一次年度报告的宴会上, 一个服务员把一个餐具掉在了地上, 一个碎盘子切了 Lucas 的脸, 几天后 Lucas 因为皮肤严重发炎死亡, 可能是由败血病导致的, 当时 Lucas 年仅 49 岁.

我们主要研究 u 序列 (u_n) 与 v 序列 (v_n). 设 $A,B\in\mathbb{Z}$, $\Delta=A^2-4B$. 那么方程 $x^2-Ax+B=0$ 有两根

$$\alpha=\frac{A+\sqrt{\Delta}}{2}, \beta=\frac{A-\sqrt{\Delta}}{2}.$$

命题 2.2.4. Binet,1843

对任意 $n=0,1,2,\cdots$, 我有

$$u_n=\sum_{0\le k<n}\alpha^k\beta^{n-1-k}=\begin{cases}\dfrac{\alpha^n-\beta^n}{\alpha-\beta}, & \Delta\neq 0,\\ n\left(\dfrac{A}{2}\right)^{n-1}, & \Delta=0.\end{cases},\qquad v_n=\alpha^n+\beta^n.$$

证明: 利用 $A=\alpha+\beta, B=\alpha\beta$, 对 n 归纳. □

注: 如果 $\Delta=0$, 则 $\alpha=\beta=A/2$, 此时

$$u_n=\sum_{0\le k<n}\alpha^{n-1}=n\left(\frac{A}{2}\right)^{n-1}, v_n=2\alpha^n=2\left(\frac{A}{2}\right)^n.$$

我们可以用 n,A,Δ 来表示 u_n,v_n:

$$\sqrt{\Delta}u_n=(\alpha-\beta)u_n=\alpha^n-\beta^n=\left(\frac{A+\sqrt{\Delta}}{2}\right)^n-\left(\frac{A-\sqrt{\Delta}}{2}\right)^n=\frac{\sqrt{\Delta}}{2^{n-1}}\sum_{\substack{k=0\\2\nmid k}}^{n}\binom{n}{k}A^{n-k}\Delta^{(k-1)/2}.$$

所以

$$2^{n-1}u_n=\sum_{k=0}^{\lfloor(n-1)/2\rfloor}\binom{n}{2k+1}A^{n-1-2k}\Delta^k.$$

(当 $\Delta=0$ 时也满足.) 类似地,

$$v_n=\alpha^n+\beta^n=\left(\frac{A+\sqrt{\Delta}}{2}\right)^n+\left(\frac{A-\sqrt{\Delta}}{2}\right)^n=\frac{1}{2^{n-1}}\sum_{k=0}^{\lfloor n/2\rfloor}\binom{n}{2k}A^{n-2k}\Delta^k.$$

对于 Fibonacci 数列 (F_n) 与它的对偶序列 (L_n), $\Delta=5$, 所以

$$\sqrt{5}F_n=\left(\frac{1+\sqrt{5}}{2}\right)^n-\left(\frac{1-\sqrt{5}}{2}\right)^n,\qquad L_n=\left(\frac{1+\sqrt{5}}{2}\right)^n+\left(\frac{1-\sqrt{5}}{2}\right)^n.$$

对于 Pell 序列 (P_n) 与它的对偶 (Q_n), $\Delta=8$, 我们有

$$2\sqrt{2}P_n=(1+\sqrt{2})^n-(1-\sqrt{2})^n,\qquad Q_n=(1+\sqrt{2})^n+(1-\sqrt{2})^n.$$

对于序列 (S_n) 与它的对偶 (T_n), $\Delta=12$, 我们有

$$S_n=\frac{1}{2\sqrt{3}}\Big((2+\sqrt{3})^n-(2-\sqrt{3})^n\Big),\qquad T_n=(2+\sqrt{3})^n+(2-\sqrt{3})^n.$$

我们可以得到下面性质:

命题 2.2.5

对 $n\in\mathbb{N}$, 我们有

$$v_n=2u_{n+1}-Au_n, \Delta u_n=2v_{n+1}-Av_n, v_n^2-\Delta u_n^2=4B^n.$$

证明: 注意 $A=\alpha+\beta, \sqrt{\Delta}u_n=\alpha^n-\beta^n, v_n=\alpha^n+\beta^n$ 即可. □

注: 特别地,

$$L_n = 2F_{n+1} - F_n, 5F_n = 2L_{n+1} - L_n, L_n^2 - 5F_n^2 = 4(-1)^n.$$

命题 2.2.6. 邻项公式

对任意 $n \in \mathbb{N}$, 我们有

$$u_{n+1}^2 - Au_{n+1}u_n + Bu_n^2 = B^n, v_{n+1}^2 - Av_{n+1}v_n + Bv_n^2 = -\Delta B^n.$$

换言之, 若 $n \in \mathbb{Z}^+ = \{1, 2, 3, \cdots\}$, 则

$$u_n^2 - u_{n-1}u_{n+1} = B^{n-1}, v_n^2 - v_{n-1}v_{n+1} = -\Delta B^{n-1}.$$

证明: 由命题2.2.5,

$$4B^n = v_n^2 - \Delta u_n^2 = (2u_{n+1} - Au_n)^2 - \Delta u_n^2$$

且

$$4\Delta B^n = \Delta v_n^2 - (\Delta u_n)^2 = \Delta v_n^2 - (2v_{n+1} - 4Av_n)^2.$$

□

注: 例如,$F_{n+1}^2 - F_{n+1}F_n - F_n^2 = (-1)^n$, $L_{n+1}^2 - L_{n+1}L_n - L_n^2 = 5(-1)^{n-1}$.

命题 2.2.7. 加法公式

对任意 $m, n \in \mathbb{N}$, 我们有

$$u_{m+n} = \frac{u_m v_n + u_n v_m}{2}, v_{m+n} = \frac{v_m u_n + \Delta u_m v_n}{2}.$$

命题 2.2.8. 二倍公式

对任意 $n \in \mathbb{N}$, 我们有

$$u_{2n} = u_n v_n, v_{2n} = v_n^2 - 2B^n = \frac{v_n^2 + \Delta u_n^2}{2} = \Delta u_n^2 + 2B^n,$$

$$u_{2n+1} = u_{n+1}^2 - Bu_n^2, v_{2n+1} = v_n v_{n+1} - AB^n.$$

命题 2.2.9. 乘法公式

对任意 $k, n \in \mathbb{N}$, 我们有

$$u_{kn} = u_k \cdot u_n(v_k, B^k), v_{kn} = v_n(v_k, B^k).$$

证明: 设 $A' = v_k, B' = B^k$, 则 $\Delta' = v_k^2 - 4B^k = \Delta u_k^2$,

$$\alpha' = \frac{v_k + \sqrt{\Delta}u_k}{2}, \beta' = \frac{v_k - \sqrt{\Delta}u_k}{2}.$$

所以

$$\begin{aligned}(\alpha')^n + (\beta')^n &= \left(\frac{v_k + \sqrt{\Delta}u_k}{2}\right)^n + \left(\frac{v_k - \sqrt{\Delta}u_k}{2}\right)^n \\ &= \left(\frac{A + \sqrt{\Delta}}{2}\right)^{kn} + \left(\frac{A - \sqrt{\Delta}}{2}\right)^{kn} = v_{kn}.\end{aligned}$$

类似可以证明 $u_{kn} = u_k \cdot u_n(v_k, B^k)$. □

命题 2.2.10. 按 A, B 展开

对任意 $n \in \mathbb{Z}^+$ 我们有

$$u_n = \sum_{k=0}^{\lfloor (n-1)/2 \rfloor} \binom{n-1-k}{k} A^{n-1-2k}(-B)^k,$$

$$v_n = \sum_{k=0}^{\lfloor n/2 \rfloor} \frac{n}{n-k}\binom{n-k}{k} A^{n-2k}(-B)^k.$$

证明: 注意到

$$\begin{aligned}
\sum_{m=1}^{\infty} u_m x^{m-1} &= \sum_{m=1}^{\infty}\sum_{k=0}^{m-1} \alpha^k \beta^{m-1-k} x^{m-1} \\
&= \sum_{m=1}^{\infty}\sum_{k=0}^{m-1} (\alpha x)^k (\beta x)^{m-1-k} \\
&= \sum_{k=0}^{\infty} (\alpha x)^k \sum_{j=0}^{\infty} (\beta x)^j \\
&= \frac{1}{1-\alpha x} \cdot \frac{1}{1-\beta x} = \frac{1}{1-Ax+Bx^2}.
\end{aligned}$$

记 $[x^m]f(x)$ 代表 $f(x)$ 幂级数中 x^m 的系数, 则

$$\begin{aligned}
u_{n-1} &= [x^{n-1}] \sum_{m=1}^{\infty} u_m x^{m-1} = [x^{n-1}] \frac{1}{1-Ax+Bx^2} \\
&= [x^{n-1}] \frac{1-(x(A-Bx))^n}{1-x(A-Bx)} \\
&= [x^{n-1}] \sum_{k=0}^{n-1} x^k (A-Bx)^k \\
&= [x^{n-1}] \sum_{k=0}^{n-1} x^{n-1-k} (A-Bx)^{n-1-k} \\
&= \sum_{k=0}^{\lfloor (n-1)/2 \rfloor} \binom{n-1-k}{k} (-B)^k A^{n-1-2k}.
\end{aligned}$$

而且

$$\begin{aligned}
v_n &= 2u_{n+1} - Au_n \\
&= 2\sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n-k}{k} A^{n-2k}(-B)^k - A\sum_{k=0}^{\lfloor (n-1)/2 \rfloor} \binom{n-1-k}{k} A^{n-1-2k}(-B)^k \\
&= \sum_{k=0}^{\lfloor n/2 \rfloor} \left(2\binom{n-k}{k} - \binom{n-1-k}{k} \right) A^{n-2k}(-B)^k \\
&= \sum_{k=0}^{\lfloor n/2 \rfloor} \frac{n}{n-k}\binom{n-k}{k} A^{n-2k}(-B)^k.
\end{aligned}$$

注: 特别地, 对任意 $n \in \mathbb{Z}^+$, 我们有

$$F_n = \sum_{k\in\mathbb{N}} \binom{n-1-k}{k}, L_n = \sum_{0\le k\le n/2} \frac{n}{n-k}\binom{n-k}{k}.$$

命题 2.2.11. 线性下标

设 $w_{n+1} = Aw_n - Bw_{n-1}, n = 1, 2, 3, \cdots$. 则, 对任意 $k \in \mathbb{Z}^+$, 且 $l, n \in \mathbb{N}$, 我们有

$$w_{kn+l} = \sum_{j=0}^{n} \binom{n}{j} (-Bu_{k-1})^{n-j} u_k^j w_{l+j}.$$

证明: 对 n 归纳. 当 $n = 0$ 时结论平凡. 假设结论对 n 正确, 则

$$\begin{aligned}
w_{k(n+1)+l} = w_{kn+(k+l)} &= \sum_{j=0}^{n} \binom{n}{j} (-Bu_{k-1})^{n-j} u_k^j w_{k+l+j} \\
&= \sum_{j=0}^{n} \binom{n}{j} (-Bu_{k-1})^{n-j} u_k^j (u_k w_{l+j+1} - Bu_{k-1} w_{l+j}) \\
&= u_k^{n+1} + \sum_{j=1}^{n} \binom{n}{j-1} (-Bu_{k-1})^{n+1-j} u_k^j w_{l+j} \\
&\quad + \sum_{j=1}^{n} \binom{n}{j} (-Bu_{k-1})^{n+1-j} u_k^j w_{l+j} + (-Bu_{k-1})^{n+1} w_l \\
&= \sum_{j=0}^{n+1} \binom{n+1}{j} (-Bu_{k-1})^{n+1-j} u_k^j w_{l+j}.
\end{aligned}$$

注: 特别地, 对任意 $n \in \mathbb{N}$, 我们有

$$F_{2n} = \sum_{j=0}^{n} \binom{n}{j} F_j, F_{2n+1} = \sum_{j=0}^{n} \binom{n}{j} F_{j+1}.$$

定理 2.2.12. E.Lucas

设 $A, B \in \mathbb{Z}, (A, B) = 1$, 则

$$(u_m, u_n) = |u_{(m,n)}|, \forall m, n \in \mathbb{N}.$$

证明: 由归纳法可以证明

$$u_{n+1} \equiv A^n (\mathrm{mod}\ B).$$

由于 $(A, B) = 1$, 则 $(u_{n+1}, B) = 1$. 由前面的命题2.2.6, $u_{n+1}^2 - Au_{n+1}u_n + Bu_n^2 = B^n$, 所以 $(u_n, u_{n+1})|B^n \Rightarrow (u_n, u_{n+1})|(u_{n+1}, B^n) = 1$. 由命题2.2.11, 对任意 $n \in \mathbb{Z}^+, q, r \in \mathbb{N}$, 我们有

$$\begin{aligned}
u_{nq+r} &= \sum_{j=0}^{q} \binom{q}{j} (-Bu_{n-1})^{q-j} u_n^j u_{r+j} \\
&\equiv (-Bu_{n-1})^q u_r = (u_{n+1} - Au_n)^q u_r \equiv u_{n+1}^q u_r (\mathrm{mod}\ u_n).
\end{aligned}$$

所以 $(u_{nq+r}, u_n) = (u_n, u_r)$.

显然, $(u_m, u_0) = (u_m, 0) = |u_m| = |u_{(m,0)}|$, 下面设 $r_0 = m, r_1 = n \in \mathbb{Z}^+$, 对 $i = 1, \cdots, k$, 记 $r_{i-1} = r_i q_i + r_{i+1}$, 其中 $r_1 > r_2 > \cdots > r_k > r_{k+1} = 0$, 对任意 $i = 1, 2, \cdots, k$, 我们有

$$(u_{r_{i-1}}, u_{r_i}) = (u_{q_i r_i + r_{i+1}}, u_{r_i}) = (u_{r_i}, u_{r_{i+1}}).$$

因此,

$$(u_m, u_n) = (u_{r_0}, u_{r_1}) = (u_{r_1}, u_{r_2}) = \cdots = (u_{r_k}, u_{r_{k+1}}) = (u_{(m,n)}, u_0) = |u_{(m,n)}|. \quad \square$$

注: 对 $m, n \in \mathbb{Z}^+$, 我们可以证明

$$(v_m, v_n) = \begin{cases} |v_{(m,n)}|, & \text{如果} \mathrm{ord}_2(m) = \mathrm{ord}_2(n), \\ (2, v_{(m,n)}), & \text{否则}. \end{cases}$$

命题 2.2.13. u_n, v_n **的符号刻画**

下面命题等价:

$(1) u_n \geq 0, \forall n \in \mathbb{N}$;

$(2) v_n \geq 0, \forall n \in \mathbb{N}$;

$(3) A \geq 0, \Delta = A^2 - 4B \geq 0$.

证明: "(3)⇒(1)(2)": 若 $A \geq 0$ 且 $\Delta \geq 0$, 则根据命题2.2.4, $u_n \geq 0$ 且 $v_n \geq 0$.

"(1) ⇒ (3)": 设 $u_n \geq 0 (\forall n \in \mathbb{N})$, 则 $A = u_2 \geq 0$. 若 $\Delta < 0$, 则 $u_{n+1}^2 - u_n u_{n+2} = B^n > 0$, 从而递减序列 $\left(\frac{u_{n+1}}{u_n}\right)_{n \geq 1}$ 有极限 θ. 由于

$$\frac{u_{n+2}}{u_{n+1}} = \frac{A u_{n+1} - B u_n}{u_{n+1}} = A - \frac{B}{u_{n+1}/u_n}, n = 1, 2, 3, \cdots,$$

则 $\theta^2 - A\theta + B = 0$, 所以 $\Delta \geq 0$, 矛盾. "(2) ⇒ (3)": 证明类似. $\square$

命题 2.2.14. **模 m 周期性**

设 $m \in \mathbb{Z}^+, (B, m) = 1$. 则存在正整数 λ 使得

$$u_{n+\lambda} \equiv u_n (\mathrm{mod}\ m), \forall n \in \mathbb{N},$$
$$v_{n+\lambda} \equiv v_n (\mathrm{mod}\ m), \forall n \in \mathbb{N}.$$

证明: 考虑 $m^2 + 1$ 个有序对

$$\langle u_i, u_{i+1} \rangle (i = 0, \cdots, m^2),$$

由鸽笼原理, 上面必有其中两个模 m 同余. 取最小的 $\lambda \in \{0, 1, \cdots, m^2\}$, 使得

$$\langle u_\lambda \rangle \equiv \langle u_j, u_{j+1} \rangle (\mathrm{mod}\ m), \text{对某个} j < \lambda,$$

由于

$$-B u_{j-1} = u_{j+1} - A u_j \equiv u_{\lambda+1} - A u_\lambda = -B u_{\lambda-1} (\mathrm{mod}\ m)$$

且 $(B, m) = 1$, 则 $u_{j-1} \equiv u_{\lambda-1} (\mathrm{mod}\ m)$. 对这个步骤进行下去可以得到

$$\langle u_{\lambda-j}, u_{\lambda-j+1} \rangle \equiv \langle u_0, u_1 \rangle (\mathrm{mod}\ m).$$

由 λ 的选取, 必有 $j=0$, 从而

$$\langle u_\lambda, u_{\lambda+1}\rangle \equiv \langle u_0, u_1\rangle (\mathrm{mod}\ m).$$

所以 $u_{n+\lambda} \equiv u_n (\mathrm{mod}\ m), \forall n = 0,1,2,\cdots$.

对任意 $n \in \mathbb{N}$, 有

$$v_{n+\lambda} = 2u_{n+\lambda+1} - Au_{n+\lambda} \equiv 2u_{n+1} - Au_n = v_n (\mathrm{mod}\ m).$$

证明完成. □

2.2.3 与 Chebyshev 多项式的关系

第一类 Chebyshev 多项式 $T_n(x)(n \in \mathbb{N})$ 与第二类 Chebyshev 多项式 $U_n(x)(n \in \mathbb{N})$ 定义为

$$\cos n\theta = T_n(\cos\theta), \sin((n+1)\theta) = \sin\theta \cdot U_n(\cos\theta).$$

显然,

$$T_0(x) = 1, T_1(x) = x, T_2(x) = 2x^2 - 1$$
$$U_0(x) = 1, U_1(x) = 2x, U_2(x) = 4x^2 - 1.$$

由三角恒等变换可知

$$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x), U_{n+1}(x) = 2xU_n(x) - U_{n-1}(x).$$

由于 $2T_0(x) = 2, 2T_1(x) = 2x, U_0(x) = 1, U_1(x) = 2x$, 所以

$$2T_n(x) = v_n(2x,1), U_n(x) = u_{n+1}(2x,1).$$

因此对任意 $n \in \mathbb{Z}^+$, 由命题2.2.10, 可得

$$T_n(x) = \frac{1}{2}\sum_{k=0}^{\lfloor n/2\rfloor} \frac{n}{n-k}\binom{n-k}{k}(2x)^{n-2k}(-1)^k,$$

且

$$U_n(x) = \sum_{k=0}^{\lfloor n/2\rfloor} \binom{n-k}{k}(2x)^{n-2k}(-1)^k.$$

§ 2.3 m 阶常系数齐次线性递归序列

设 $(w_n)_{n\geq 0}$ 满足

$$w_{n+m} = a_1 w_{n+m-1} + \cdots + a_m w_m (n = 0,1,2,\cdots). \tag{2.1}$$

其中, (a_i) 是常数. 如何求 (w_n) 的通项公式?

定理 2.3.1

设

$$p(x)=x^m-a_1x^{m-1}-\cdots-a_{m-1}x-a_m=(x-\alpha_1)^{e_1}(x-\alpha_2)^{e_2}\cdots(x-\alpha_r)^{e_r},$$

其中 $\alpha_1,\cdots,\alpha_r$ 两两不同, $e_1+\cdots+e_r=n$. 则 (w_n) 满足递推关系 (2.1) $\Leftrightarrow$ 存在次数小于 e_s 的多项式 $P_s(x)$ 使得

$$w_n=\sum_{s=1}^{r}P_s(n)\alpha_s^n.$$

证明: 令 $q(x)=x^mp\left(\dfrac{1}{x}\right)=1-a_1x-\cdots-a_mx^m=(1-\alpha_1x)^{e_1}\cdots(1-\alpha_rx)^{e_r}$. 让 $W(x)=\sum\limits_{n=0}^{\infty}w_nx^n$, 则

$$[x^{n+m}]q(x)W(x)=w_{n+m}-a_1w_{n+m-1}-\cdots-a_mw_n,$$

序列 (w_n) 满足递推关系 (2.1)$\Leftrightarrow$ $q(x)W(x)$ 中 x^{n+m} 的系数为 $0(n=0,1,2,\cdots)$ $\Leftrightarrow$ $q(x)W(x)$ 是次数不超过 m 的多项式 $C(x)\triangleq\sum\limits_{n=0}^{m-1}c_nx^n$.

于是, 真分式 $\dfrac{C(x)}{q(x)}=\dfrac{C(x)}{(1-\alpha_1x)^{e_1}\cdots(1-\alpha_rx)^{e_r}}$ 可以唯一表示成部分分式之和: $\sum\limits_{s=1}^{r}\sum\limits_{t=1}^{e_s}\dfrac{\beta_{st}}{(1-\alpha_sx)^t}$. 由于

$$\frac{1}{(1-\alpha x)^t}=\sum_n\binom{-t}{n}(-\alpha x)^n=\sum_n\binom{t+n-1}{n}(\alpha x)^n.$$

所以

$$\begin{aligned}\frac{C(x)}{q(x)}&=\sum_{s=1}^{r}\sum_{t=1}^{e_s}\beta_{st}\sum_{n=0}^{\infty}\binom{t+n-1}{n}\alpha_s^nx^n\\&=\sum_{n=0}^{\infty}x^n\sum_{s=1}^{r}\underbrace{\sum_{t=1}^{e_s}\beta_{st}\binom{t+n-1}{n}}_{\text{关于 }n\text{ 次数}<e_s\text{ 的多项式}}\alpha_s^n\\&=\sum_n x^n\sum_{s=1}^{r}P_s(n)\alpha_s^n,\text{其中}\deg P_s<e_s.\end{aligned}$$

因此, (w_n) 满足递推关系 (2.1) 等价于

$$w_n=\sum_{s=1}^{r}P_s(n)\alpha_s^n,\text{其中}\deg P_s<e_s.$$

我们得到了

注: $(1-a_1x-\cdots-a_mx^m)\sum\limits_{k=0}^{\infty}w_kx^k=\sum\limits_{n=0}^{m-1}c_nx^n$, 而 $c_n=w_n-a_1w_{n-1}-\cdots-a_nw_0(n=0,1,\cdots,m-1)$. 所以利用初值与递推关系可以得到 c_n, 从而得到 $C(x)$, 从而得到 β_{st}, 进而找到了 $P_s(x)$. 反过来, 用 $c_n,w_{n-1},\cdots,w_0$ 也可以算 w_n.

例 2.3.2

设 $u_0=0,u_1=1,u_{n+1}=Au_n-Bu_{n-1}(n\geq1)$. 求 u_n 通项公式.

解: $x^2-Ax+B=(x-\alpha)(x-\beta)$. 若 $\Delta=A^2-4B\neq0,\alpha\neq\beta$, 则 u_n 形如 $c_1\alpha^n+c_2\beta^n$(此时

$\deg P_s(n) < 1$, 所以 $P_s(n)$ 是常数.) 代入 $n = 0, n = 1$ 得到

$$\begin{cases} c_1 + c_2 = u_0 = 0, \\ c_1\alpha + c_2\beta = u_1 = 1, \end{cases} \Rightarrow \begin{cases} c_1 = \dfrac{1}{\alpha - \beta}, \\ c_2 = -\dfrac{1}{\alpha - \beta} \end{cases}$$

因此 $u_n = \dfrac{1}{\alpha - \beta}(\alpha^n - \beta^n)$.

若 $\Delta = 0$, 则 $x^2 - Ax + B = (x-\alpha)^2$, 此时 u_n 形如 $(an+b)\alpha^n = (an+b)\left(\dfrac{A}{2}\right)^n$. 代入 $n = 0, n = 1$ 得到

$$\begin{cases} b = u_0 = 0, \\ (a+b)\dfrac{A}{2} = u_1 = 1, \end{cases} \Rightarrow \begin{cases} a = \dfrac{2}{A} \\ b = 0. \end{cases}$$

则 $u_n = n\left(\dfrac{A}{2}\right)^{n-1}$. □

2.3.1 (*)Bernoulli 数

J.Bernoulli 于 1713 年研究了等幂和: $S_k(n) = \sum_{r=0}^{n-1} r^k = ?$

我们知道, $S_1(n) = \dfrac{n(n-1)}{2}, S_2(n) = \dfrac{n(n+1)(2n+1)}{6}, S_3(n) = \left(\dfrac{n(n-1)}{2}\right)^2$.

$$\sum_{k=0}^{\infty} S_k(n)\frac{x^k}{k!} = \sum_{k=0}^{\infty}\sum_{r=0}^{n-1}\frac{(rx)^k}{k!} = \sum_{r=0}^{n-1}\sum_{k=0}^{\infty}\frac{(rx)^k}{k!} = \sum_{r=0}^{n-1}(e^x)^r = \frac{e^{nx}-1}{e^x-1} = \frac{x}{e^x-1}\cdot\frac{e^{nx}-1}{x}.$$

因此只需要把上式写成幂级数即可得到 $S_k(n)$.

Bernoulli 数如下给出: $\dfrac{x}{e^x-1} = \sum_{n=0}^{\infty} B_n\dfrac{x^n}{n!}$, 由此可得

$$(k+1)S_k(n) = \sum_{l=0}^{k}\binom{k+1}{l}B_l n^{k+1-l}.$$

Bernoulli 数的求法如下: 利用

$$\sum_{k=0}^{\infty} B_k\frac{x^k}{k}\cdot\frac{e^x-1}{x} = 1,$$

可以得到递推关系

$$B_0 = 1, \sum_{k=0}^{n}\binom{n+1}{k}B_k = 0, (n = 1, 2, \cdots.)$$

设 **Zeta 函数**为

$$\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s},$$

Euler 发现了 Bernoulli 数与 Zeta 函数有如下关系:

$$\zeta(2m) = (-1)^{m-1}\frac{(2\pi)^{2m}}{(2m)!}\cdot\frac{B_{2m}}{2}.$$

例如, $\zeta(2)=\dfrac{\pi^2}{6},\zeta(4)=\dfrac{\pi^4}{90},\cdots$.

第二章习题

1. 设 $\{a_n\}_{n\geq 1}$ 满足 $a_1=1,a_2=7$, 当 $n\geq 3$ 时, $a_n=7a_{n-1}-12a_{n-2}$, 求 $\{a_n\}$ 的通项公式.
2. 设 $\{u_n\}_{n\geq 0}$ 满足 $u_0=1,u_1=2,u_2=8$, 当 $n\geq 0$ 时, $u_{n+3}+6u_{n+2}+12u_{n+1}+8u_n=0$, 求 $\{u_n\}$ 的通项公式.
3. 设 $\{w_n\}_{n\geq 0}$ 满足 $w_0=1,w_1=0,w_2=2$, 当 $n\geq 3$ 时, $w_n=4w_{n-2}+3w_{n-3}$. 求 $\{w_n\}_{n\geq 0}$ 的通项公式.

第 3 章　容斥原理与反演公式

§ 3.1　容斥原理及其应用

在高中时我们学过: 若 S_1, S_2 是有穷集, 则 $|S_1 \cup S_2| = |S_1| + |S_2| - |S_1 \cap S_2|$.

3.1.1　容斥原理

定理 3.1.1. 容斥原理 (Inclusion-Exclusion Theorem)

设 $S_1, \cdots, S_n$ 是有穷集, 则

$$\begin{aligned}\left|\bigcup_{i=1}^{n} S_i\right| &= \sum_{i=1}^{n} |S_i| - \sum_{1\le i<j\le n} |S_i \cap S_j| - \cdots + (-1)^{n-1} |S_1 \cap S_2 \cap \cdots \cap S_n| \\ &= \sum_{\varnothing \ne I \subseteq \{1,\cdots,n\}} (-1)^{|I|-1} \left|\bigcap_{i\in I} S_i\right|.\end{aligned} \tag{3.1}$$

证明: (直接证明) 设 $S = \bigcup_{i=1}^{n} S_i$, 对 $a \in S$, 假设 a 属于 $S_1, \cdots, S_n$ 中恰好 m 个, 则 $\sum_{i=1}^{n} |S_i|$ 把 a 统计了 m 次, $\sum_{1\le i_1<i_2\le n} |S_{i_1} \cap S_{i_2}|$ 把 n 统计了 $\binom{m}{2}$ 次. 类似地, $\sum_{1\le i_1<\cdots<i_k\le n} |S_{i_1} \cap \cdots \cap S_{i_k}|$ 统计了 $\binom{m}{k}$ 次. 因此, (3.1) 式等号右边把 a 统计的次数是

$$\binom{m}{1} - \binom{m}{2} + \binom{m}{3} - \cdots + (-1)^{m-1}\binom{m}{m} = 1 - \sum_{k=0}^{m} \binom{m}{k} (-1)^k = 1 - (1-1)^m = 1.$$

而等号左边把 a 统计了 1 次. 另外当 $a \notin S$ 时左、右都统计了 0 次. □

下面用 $\overline{A}$ 表示 A 的补集. 设 $S_1, \cdots, S_n$ 是 S 的子集, 则

$$\left|\bigcap_{i=1}^{n} \overline{S_i}\right| = \left|\overline{\left(\bigcup_{i=1}^{n} S_i\right)}\right| = |S| - \left|\bigcup_{i=1}^{n} S_i\right|.$$

实际应用方法如下: 设 S 是 N 元集, 记

$$\begin{aligned} S_i &= \{a \in S | a\text{具有性质} P_i\}, \\ N(P_{i_1} P_{i_2} \cdots P_{i_k}) &= \{a \in S | a\text{具有性质} P_{i_1}, \cdots, P_{i_k}\}, \\ N(P'_{i_1} P'_{i_2} \cdots P'_{i_k}) &= \{a \in S | a\text{不具有} P_{i_1}, \cdots, P_{i_k}\text{中任何一个性质}\}, \end{aligned}$$

则

$$\begin{aligned}|N(P'_1 P'_2 \cdots P'_n)| &= \left|\bigcap_{i=1}^{n} \overline{S_i}\right| = |S| - \left|\bigcup_{i=1}^{n} S_i\right| \\ &= N - \sum_{i=1}^{n} N(P_i) + \sum_{1\le i<j\le n} N(P_i P_j) - \cdots + (-1)^n N(P_1 P_2 \cdots P_n).\end{aligned} \tag{3.2}$$

3.1.2 容斥原理的应用

解析数论有两大研究方法: 筛法 (依赖容斥原理)、圆法 (生成函数).

例 3.1.2

设 $p_1,\cdots,p_k$ 为不同素数, 则 $1,\cdots,N$ 中不被 $p_1,\cdots,p_k$ 中任何一个整除的个数是

$$N-\sum_{i=1}^{k}\left\lfloor\frac{N}{p_i}\right\rfloor+\sum_{1\le i<j\le k}\left\lfloor\frac{N}{p_ip_j}\right\rfloor-\cdots+(-1)^k\left\lfloor\frac{N}{p_1p_2\cdots p_k}\right\rfloor.$$

证明: 让 $S=\{1,\cdots,N\}$, $a\in S$ 具有性质 P_i 指 $p_i|a$. 当 $1\le i_1<\cdots<i_r\le k$ 时,

$$N(p_{i_1},\cdots,p_{i_r})=\left|\{1\le n\le N:p_{i_j}|n,\forall j=1,2,\cdots,r\}\right|=\left\lfloor\frac{N}{p_{i_1}p_{i_2}\cdots p_{i_r}}\right\rfloor.$$

利用 (3.2) 式立即得到欲证结论. □

在数论中, 记 $\pi(x)$ 是不超过 x 的素数个数. 不超过 $\sqrt{N}$ 的素数有 $p_1,p_2,\cdots,p_{\pi(\sqrt{N})}$. 那么

“$n\in\{1,\cdots,N\}$ 不被 $p_1,\cdots,p_{\pi(\sqrt{N})}$ 中任一个整除”等价于“$n=1$ 或 n 是 $(\sqrt{N},N]$ 中素数”.

利用 (3.2) 式, 可得

$$\pi(N)-\pi(\sqrt{N})+1=N-\sum_{i=1}^{k}\left\lfloor\frac{N}{p_i}\right\rfloor+\sum_{1\le i<j\le k}\left\lfloor\frac{N}{p_ip_j}\right\rfloor-\cdots+(-1)^k\left\lfloor\frac{N}{p_1p_2\cdots p_{\pi(\sqrt{N})}}\right\rfloor.$$

这就是 **Eratosthenes 筛法**, 但很麻烦, 不实用.

在数论中, 定义 **Euler 函数**为 $\varphi(N)=|\{1\le n\le N:(n,N)=1\}|$.

例 3.1.3

设 $N=p_1^{a_1}\cdots p_k^{a_k}(a_i>0,p_1,\cdots,p_k$是不同素数). 则对于 $n\in\{1,2,\cdots,N\}$,

“$(n,N)=1$”等价于“n 不被 $p_1,\cdots,p_k$ 中任一个整除”.

由 (3.2) 式,

$$\begin{aligned}\varphi(N)&=N-\sum_{i=1}^{k}\left\lfloor\frac{N}{p_i}\right\rfloor+\sum_{1\le i<j\le k}\left\lfloor\frac{N}{p_ip_j}\right\rfloor-\cdots+(-1)^k\left\lfloor\frac{N}{p_1p_2\cdots p_k}\right\rfloor\\&=N\left(1-\sum_{i=1}^{k}\frac{1}{p_i}+\sum_{1\le i<j\le k}\frac{1}{p_ip_j}-\cdots+(-1)^k\frac{1}{p_1\cdots p_k}\right)\\&=N\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)=\prod_{i=1}^{k}p_i^{a_i-1}(p_i-1).\end{aligned}$$

例 3.1.4

用容斥原理给出 $S(m,n)$ 的计算公式.

解: $n!S(m,n)$ 是 m 元集 A 到 n 元集 B 的满射个数, $B=\{b_1,\cdots,b_n\}$. $f:A\to B$ 具有性质 P_i 指 $b_i\notin\mathrm{Ran}(f)$. 于是映射总数 $N=|\{f:A\to B\}|=n^m$, 而

$$N(P_{i_1},\cdots,P_{i_k})=|\{f:A\to B\setminus\{b_{i_1},\cdots,b_{i_k}\}|=(n-k)^m.$$

由 (3.2) 式, 可得

$$\begin{aligned} n!S(m,n) &= n^m - n(n-1)^m + \binom{n}{2}(n-2)^m - \cdots \\ &= \sum_{k=0}^{n}\binom{n}{k}(-1)^k(n-k)^m = \sum_{k=0}^{n}\binom{n}{k}(-1)^{n-k}k^m. \end{aligned}$$

Brun 观察到: 如果 $m \in \{1,\cdots,n\}$ 是偶数, 则

$$\begin{aligned} \left|S \setminus \bigcup_{k=1}^{n} S_k\right| \le |S| - \sum_{i=1}^{n}|S_i| + \sum_{1\le i<j\le n}|S_i \cap S_j| - \cdots \\ + \sum_{1\le i_1<\cdots<i_m\le n}(-1)^m|S_{i_1}\cap\cdots\cap S_{i_m}|. \end{aligned}$$

这个不等式与

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots \le 1 - \frac{1}{3} + \frac{1}{5}$$

类似. 这就是 Brun 筛法, 根据需要算到具体某一项. 它曾经被用来证明 Goldbach 猜想的弱化版本的命题 (Brun 证明了“9+9”).

通过非常复杂的带权的线性筛法, 我国数学家陈景润建立了如下的“1+2”结论:

定理 3.1.5. 陈景润, 1973

(1) 大的偶数可以写成 $p+q$, 其中 p 是素数, q 要么是素数要么是两个素数的乘积.
(2) 存在无穷多个素数 p 使得 $p+2$ 要么是素数要么是两个素数的乘积.

注: (1) 离 Goldbach 猜想很接近; (2) 离孪生素数猜想很接近.

我们知道素数定理

$$\pi(x) \sim \frac{x}{\log x}(x \to \infty).$$

当 $x > 0$ 时, 令

$$\pi_2(x) := |\{p \le x : p+2\text{是素数}\}|$$

Hardy-Littlewood 猜想: *我们有*

$$\pi_2(x) \sim 2C_2\frac{x}{\log^2 x}, x \to \infty.$$

其中, $C_2 = \prod_{p>2}\left(1 - \frac{1}{(p-1)^2}\right) \approx 0.66.$

利用 Brun 筛法, Brun 证明了如下定理:

定理 3.1.6. Brun, 1920

存在常数 $C > 0$ 使得对任意 $x \ge 2$ 有

$$\pi_2(x) := |\{p \le x : p+2\text{是素数}\}| \le C\frac{x(\log\log x)^2}{(\log x)^2}.$$

2014 年 1 月 29 日, 孙智伟把哥德巴赫猜想与孪生素数猜想结合了起来, 提出如下猜想:

猜想 (孙智伟, 2014-1-29): *对任意正整数 $n > 2$, 存在素数 q 使得 $2n - q$ 与 $p_{q+2} + 2$ 都是素数.*

显然这个猜想比 Goldbach 猜想强, 而也可以证明它可以推出孪生素数猜想. 事实上, 如果所有满足 $p_{q+2}+2$ 是素数的素数 q 都比某个偶数 $N>2$ 小, 则对任意这类素数 q, $N!-q$ 都是合数, 这是因为

$$N!-q\equiv 0(\mathrm{mod}\ q)且N!-q\geq q(q+1)-q>q.$$

3.1.3 带权的容斥原理

定理 3.1.7

设 S 是有限集, 对每个 $a\in S$, 赋以权 $w(a)\in\mathbb{R}$. 对 $T\subseteq S$, 记 $W(T)=\sum_{a\in T}w(a)$. 设 $S_1,\cdots,S_k$ 是 S 的子集, $m\in\mathbb{N}$, 则 $W(\{a\in S:a属于S_1,\cdots,S_k中恰好\ m\ 个\})=\sum_{l=0}^{k}\binom{l}{m}(-1)^{l-m}w_l$. 这儿 $w_0=W(S)$, 当 $l>0$ 时, $w_l=\sum_{1\leq i_1<\cdots<i_l\leq k}W(S_{i_1}\cap\cdots\cap S_{i_l})$.

证明: 记 $N_a=\sum_{l=0}^{k}\binom{l}{m}(-1)^{l-m}\sum_{\substack{1\leq i_1<\cdots<i_l\leq k\\ a\in S_{i_1}\cap\cdots\cap S_{i_l}}}1$, 则 RHS$=\sum_{a\in S}N_aw(a)$. 假定 a 属于 $S_1,\cdots,S_k$ 中恰好 n 个.

第一种情况: $n<m$, 此时如果 $m\leq l\leq k$, 由 $l>n$, 则 $a\notin S_{i_1}\cap\cdots\cap S_{i_l}\Rightarrow N_a=0$.

第二种情况: $n\geq m$, 此时 $m\leq n\leq k$, 则

$$N_a=\sum_{l=m}^{k}\binom{l}{m}(-1)^{l-m}\sum_{\substack{1\leq i_1<\cdots<i_l\leq k\\ a\in S_{i_1}\cap\cdots\cap S_{i_l}}}1=\sum_{l=m}^{k}\binom{l}{m}(-1)^{l-m}\binom{n}{l}$$

$$=\sum_{l=m}^{k}\binom{n}{m}\binom{n-m}{l-m}(-1)^{l-m}=\binom{n}{m}\delta_{mn}=\delta_{mn}.$$

因此右边就是属于恰好 m 个集合的 a 的带权和. □

例 3.1.8

计算 $\sum_{\substack{m=1\\(m,n)=1}}^{n}m^2$.

解: 设 $n=p_1^{a_1}\cdots p_k^{a_k}$, 其中 $a_1,\cdots,a_k>0$. $S=\{1,\cdots,n\},S_i=\{m:p_i|m,1\leq m\leq n\}$. 对 $m\in S$, 让 $w(m)=m^2$, 则

$$\sum_{\substack{m=1\\(m,n)=1}}^{n}m^2=W(\overline{S_1}\cap\cdots\cap\overline{S_k})=W(\{a\in S:a属于S_1,\cdots,S_k中0个\})=W_0-W_1+W_2-\cdots+(-1)^kW_k.$$

其中,

$$\begin{aligned} W_0 = W(S) &= \sum_{m=1}^{n} m^2 = \frac{n(n+1)(2n+1)}{6} = \frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6} \\ W_l &= \sum_{1\le i_1<\cdots<i_l\le k} W(S_{i_1}\cap\cdots\cap S_{i_l}) \\ &= \sum_{1\le i_1<\cdots<i_l\le k} \sum_{q=1}^{\frac{n}{p_{i_1}\cdots p_{i_l}}} (p_{i_1}\cdots p_{i_l}q)^2 = \sum_{1\le i_1<\cdots<i_l\le k} (p_{i_1}\cdots p_{i_l})^2 \left(\sum_{q=1}^{\frac{n}{p_{i_1}\cdots p_{i_l}}} q^2\right) \\ &= \sum_{1\le i_1<\cdots<i_l\le k} (p_{i_1}\cdots p_{i_l})^2 \left(\frac{n^3}{3(p_{i_1}\cdots p_{i_l})^3} + \frac{n^2}{2(p_{i_1}\cdots p_{i_l})^2} + \frac{n}{6p_{i_1}\cdots p_{i_l}}\right). \end{aligned}$$

因此约掉分子分母可得

$$\sum_{\substack{m=1\\(m,n)=1}}^{n} m^2 = \cdots = \frac{n^3}{3}\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right) + 0 + \frac{n}{6}\prod_{i=1}^{k}(1-p_i) = \frac{n^3}{3}\varphi(n) + \frac{(-1)^n}{6}p_1\cdots p_k\varphi(n). \quad \square$$

§ 3.2 半序集上的 Möbius 反演

3.2.1 数论上的 Möbius 反演

Möbius 函数定义为

$$\mu(n) = \begin{cases} 1, & n = 1, \\ (-1)^r, & n\text{是 } r \text{ 个不同素数成绩}, n \in \mathbb{Z}^+. \\ 0, & n\text{有平方因子} \end{cases}$$

引理 3.2.1

$$\sum_{d|n}\mu(d) = \begin{cases} 1, & n = 1, \\ 0, & n > 1, \end{cases} = \left\lfloor \frac{1}{n} \right\rfloor.$$

证明: $\mu(1) = 1$ 显然. 设 $n > 1$ 有素数分解式 $p_1^{\alpha_1}\cdots p_k^{\alpha_k}(\alpha_1,\cdots,\alpha_k > 0)$, 则

$$\sum_{d|n}\mu(d) = \sum_{0\le\beta_i\le\alpha_i}\mu(p_1^{\beta_1}\cdots p_k^{\beta_k}) = \sum_{I\subseteq\{1,\cdots,k\}}\mu\left(\prod_{i\in I}p_i\right) = \sum_{I\subseteq\{1,\cdots,k\}}(-1)^{|I|} = 0.$$

(最后一个等号根据容斥原理.) $\square$

定义映射集 $\mathscr{D} = \{f : \mathbb{Z}^+ \to \mathbb{C}\}$, 定义 $\mathscr{D}$ 上的加法为函数加法, 而乘法定义为**卷积**:

$$(f * g)(n) = \sum_{d_1d_2=n} f(d_1)g(d_2) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right).$$

容易验证卷积具有交换律与结合律, 且加法关于卷积有分配律.

定理 3.2.2

$\mathscr{D}$ 依函数加法与卷积构成一个交换幺环, 单位元是 $e(n)=\left\lfloor\frac{1}{n}\right\rfloor=\begin{cases}1, & n=1,\\ 0, & n>1.\end{cases}$

证明: 只需要注意 $e*f(n)=\sum\limits_{d|n}e(d)f\left(\frac{n}{d}\right)=e(1)f(n)=f(n)$. □

下面定义 $I(n)=1$ 为处处取 1 的函数, 则

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

即 $\mu*I=e$, 从而 I 与 μ 互为卷积逆元.

定理 3.2.3. 数论中的 Möbius 反演公式

设 f,g 是数论函数, 则

$$f(n)=\sum_{d|n}g(d)(n=1,2,\cdots)\Leftrightarrow g(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)f(d)(n=1,2,\cdots).$$

证明: LHS$\Leftrightarrow f=I*g\Leftrightarrow\mu*f=g\Leftrightarrow$RHS. □

注: $f=I*g\Rightarrow\mu*f=\mu*(I*g)=(\mu*I)*g=g$, 反之类似.

3.2.2 半序集上的 Möbius 反演

定义 3.2.1

设 $\leq$ 是集合 A 上二元关系, 若它满足

(1) 自反性: $\forall x\in A(x\leq x)$;

(2) 反对称: $\forall x\in A\forall y\in A((x\leq y\wedge y\leq x)\to x=y)$;

(3) 传递性: $\forall x\in A\forall y\in A\forall z\in A(x\leq y\leq z\to x\leq z)$.

则称 $\leq$ 为 A 上**半序 (semi order)** 或**偏序 (partial order)**. A 依 $\leq$ 构成**半序集**, $\langle A,\leq\rangle$ 构成**半序结构**.

当 A 是半序集时, 对 $x,y\in A$, $x<y$ 指 $x\leq y$ 但 $x\neq y$.

定义闭区间 $[x,y]=\{z\in A:x\leq z\leq y\}$. 若 $x\not\leq y$, 则 $[x,y]=\varnothing$. 如果半序集中任意闭区间有限, 称 $\langle A,\leq\rangle$ 是**局部有限的**.

对半序集定义直积如下: 设 $\langle X_1,\leq_1\rangle,\cdots,\langle X_n,\leq_n\rangle$ 是半序结构, 在 $X=X_1\times\cdots\times X_n$ 中定义 $\leq$ 如下: $x=\langle x_1,\cdots,x_n\rangle\leq\langle y_1,\cdots,y_n\rangle=y$ 指 $x_1\leq_1y_1,\cdots,x_n\leq_n y_n$. 于是

$$[x,y]=\{z\in X:x\leq z\leq y\}=\{\langle z_1,\cdots,z_n\rangle\in X:z_i\in[x_i,y_i]\}=[x_1,y_1]\times\cdots\times[x_n,y_n].$$

下面设 $\langle X,\leq\rangle$ 是局部有限的半序结构, 令

$$\mathscr{D}(X)=\{\alpha:X\times X\to\mathbb{R}:x\not\leq y\text{时}\alpha(x,y)=0\}.$$

对 $\alpha,\beta\in\mathscr{D}(X)$, 定义加法为函数加法, $\alpha\beta:X\times X\to\mathbb{R}$ 如下:

$$\alpha\beta(x,y)=\sum_{x\leq z\leq y}\alpha(x,z)\beta(z,y).$$

(这里要保证是有限和，所以我们定义中是局部有限的.) 则 $\alpha\beta\in\mathscr{D}(X)$. (对乘法封闭)

定理 3.2.4

设 $\langle X,\leq\rangle$ 是局部有限的半序结构, 则 $\mathscr{D}(X)$ 按加法、乘法构成幺环.

证明: 当 $\alpha,\beta,\gamma\in\mathscr{D}(X)$ 时,

$$\begin{aligned}(\alpha\beta)\gamma(x,y)&=\sum_{x\leq w\leq y}\alpha\beta(x,w)\gamma(w,y)\\&=\sum_{x\leq w\leq y}\sum_{x\leq z\leq w}\alpha(x,z)\beta(z,w)\gamma(w,y)\\&=\sum_{x\leq z\leq w\leq y}\alpha(x,z)\beta(z,w)\gamma(w,y).\end{aligned}$$

类似可得

$$\alpha(\beta\gamma)(x,y)=\sum_{x\leq z\leq w\leq y}\alpha(x,z)\beta(z,w)\gamma(w,y).$$

所以乘法有结合律. 容易证明加法对乘法的分配律. 定义

$$\delta(x,y)=\delta_{xy}=\begin{cases}1, & x=y,\\ 0, & x\neq y\end{cases}$$

容易验证它是乘法单位元. □

现在的问题关键在于数论版本中的“$I(n)$”与“$\mu(n)$”分别对应半序版本的哪个.

考虑数论函数 f,g 的 Dirichlet 级数

$$F(s)=\sum_{n=1}^{\infty}\frac{f(n)}{n^s},G(s)=\sum_{n=1}^{\infty}\frac{g(n)}{n^s}.$$

则

$$F(s)G(s)=\sum_{n=1}^{\infty}\frac{f*g(n)}{n^s}.$$

而 $I(n)$ 的 Dirichlet 级数恰好就是 Riemann-Zeta 函数, 于是可以定义

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

它就对应数论版本中的“I_n”. 可以证明 $\zeta(x,y)$ 在 $\mathscr{D}$ 中可逆, 把 $\zeta(x,y)$ 的逆元 $\mu(x,y)\triangleq\zeta^{-1}(x,y)$ 叫半序集 X 上的 Möbius 函数. (参考: 李乔的《组合数学基础》)

定理 3.2.5

设 $\langle X,\leq\rangle$ 是局部有限的半序结构, $\alpha\in\mathscr{D}(X)$. 则下面四条等价:

(1)α 有左逆元. (2)α 有右逆元. (3)α 可逆. (4)$\forall x\in X(\alpha(x,x)\neq 0)$.

证明: “(1) ⇒ (4)”: 设 α 有左逆元 β, 即 $\sum_{x\leq z\leq y}\beta(x,z)\alpha(z,y)=\delta(x,y)$. 由 $\beta(x,x)\alpha(x,x)=\delta(x,x)=1$, 则 $\alpha(x,x)\neq 0$.

“(4) ⇒ (1)”: 假如 $\forall x\in X(\alpha(x,x)\neq 0)$, 找 α 的左逆元 β: 定义 $\beta(x,x)=\dfrac{1}{\alpha(x,x)}$, 递归定义

$\beta(x,y)$ 如下:

$$\sum_{x\le z<y}\beta(x,z)\alpha(z,y)\triangleq -\beta(x,y)\alpha(y,y).$$

(短区间定义好之后就定义长区间的.) 于是当 $x<y$ 时, $\sum_{x\le z\le y}\beta(x,z)\alpha(z,y)=0$. 则 β 是 α 的左逆元.

类似有“(2) $\Leftrightarrow$ (4)”, 而“(1)(2) $\Leftrightarrow$ (3)”, 所以 (1)-(4) 相互等价. □

设 $\langle X,\le\rangle$ 是局部有限半序结构, $\zeta(x,y)$ 在 $\mathscr{D}(X)$ 上的逆元记为 $\mu(x,y)$, 称为 X 上的 **Möbius 函数**.

注: 经典 Möbius 函数也是递归定义得到的:$\mu(n)=-\sum_{\substack{d\mid n\\ d\neq n}}\mu(d)$.

例 3.2.6

$\mathbb{N}=\{0,1,\cdots\}$ 按 $\le$ 构成局部有限的半序集, $\mu\zeta=\delta$, 所以

$$\delta(k,n)=\sum_{k\le m\le n}\mu(k,m)\underbrace{\zeta(m,n)}_{=1}=\sum_{k\le m\le n}\mu(k,m).$$

如果 $n=k$, 则 $\mu(k,k)=\delta(k,k)=1$;
如果 $n=k+1$, 则 $\mu(k,k+1)=-\mu(k,k)=-1$;
如果 $n=k+2$, 则 $\mu(k,k+2)=-\mu(k,k)-\mu(k,k+1)=-1+1=0$;
如果 $n=k+3$, 则 $\mu(k,k+3)=-\mu(k,k)-\mu(k,k+1)-\mu(k,k+2)=0,\cdots,$
于是当 $j\ge 2$ 时, $\mu(k,k+j)=0$, 这样, $\mathbb{N}$ 的 Möbius 函数是

$$\mu(k,m)=\begin{cases}(-1)^{m-k}, & m=k,k+1,\\ 0, & \text{此外}.\end{cases}. \tag{3.3}$$

已知半序结构 $\langle X,\le\rangle$, 称 X 是**下有限的**, 如果各个元素的下面只有有限个元素, 即对任意的 $a\in X$, 集合$\{x\in X:x\le a\}$有限.

定理 3.2.7. 半序集上的 Möbius 反演

设 X 是下有限的半序集, 函数 $f,g:X\to\mathbb{R}$, 则

$$f(y)=\sum_{x\le y}g(x),\forall y\in X \quad\Leftrightarrow\quad g(y)=\sum_{x\le y}f(x)\mu(x,y),\forall y\in X.$$

证明: 记 $M(X)=\{\text{所有函数}f:X\to\mathbb{R}\}, R\triangleq\mathscr{D}(X)=\{\alpha:X\times X\to\mathbb{R}|\text{当}x\not\le y\text{时},\alpha(x,y)=0\}$.

下面证明 $M(X)$ 是右 R-模: 显然 $M(X)$ 是个 Abel 群; 对 $f\in M(x),\varphi\in\mathscr{D}(X)$, 定义

$$f\varphi(y)=\sum_{x\le y}f(x)\varphi(x,y).$$

若 $\varphi,\psi\in\mathscr{D}(X)$, 下证 $f(\varphi\psi)=(f\varphi)\psi$, 事实上,

$$\begin{aligned}f\circ\varphi\psi(y)&=\sum_{x\leq y}f(x)\varphi\psi(x,y)\\&=\sum_{x\leq y}f(x)\sum_{x\leq z\leq y}\varphi(x,z)\psi(z,y)\\&=\sum_{z\leq y}\left(\sum_{x\leq z}f(x)\varphi(x,z)\right)\psi(z,y)\\&=\sum_{z\leq y}f\circ\varphi(z)\psi(z,y)=(f\circ\varphi)\circ\psi(y).\end{aligned}$$

而分配律容易验证. 单位元:

$$f\circ\delta(y)=\sum_{x\leq y}f(x)\delta(x,y)=f(y),$$

所以 $M(X)$ 构成右 R-模.

注意

$$f(y)=\sum_{x\leq y}g(x)\Leftrightarrow f(y)=\sum_{x\leq y}g(x)\zeta(x,y)\Leftrightarrow f=g\circ\zeta,$$

同理, $g(y)=\sum_{x\leq y}f(x)\mu(x,y)\Leftrightarrow g=f\circ\mu$, 所以只需证 $f=g\circ\zeta\Leftrightarrow g=f\circ\mu$.

“$\Rightarrow$”: $f\circ\mu=(g\circ\zeta)\circ\mu=g\circ(\zeta\mu)=g\circ\delta=g$,

“$\Leftarrow$”: $g\circ\zeta=(f\circ\mu)\circ\zeta=f\circ(\mu\zeta)=f\circ\delta=f$. □

例 3.2.8

$\mathbb{N}=\{0,1,2,\cdots\}$ 按 $\leq$ 构成下有限的半序集, 其上的 Möbius 函数为 (3.3) 式. 因此,

$$f(y)=\sum_{x\leq y}g(x),\forall y\in\mathbb{N}\quad\Leftrightarrow\quad g(y)=\sum_{x\leq y}f(x)\mu(x,y)=f(y)-f(y-1),\forall y\in\mathbb{N}.$$

这是平凡的结果. 求和的逆元就是差分.

称半序结构 $\langle X,\leq\rangle$ 与 $\langle X',\leq'\rangle$ **同构**, 指有双射 $f:X\to X'$ 使得 “$x\leq y\Leftrightarrow f(x)\leq f(y),\forall x,y\in X$.” 利用 Möbius 函数递归定义, 容易证明, 如果半序集 $\langle X,\leq\rangle$ 与 $\langle X',\leq'\rangle$ 通过 f 同构, 且为局部有限的, 则 $\mu(x,y)=\mu'(f(x),f(y))$.

设 $\langle X_1,\leq_1\rangle,\cdots,\langle X_k,\leq_k\rangle$ 是局部有限的半序结构, $x=\langle x_1,\cdots,x_k\rangle\leq y=\langle y_1,\cdots,y_k\rangle$ 指 $x_1\leq_1 y_1,\cdots,x_k\leq_k y_k$ 同时成立, 则 X 依 $\leq$ 也构成局部有限半序集, 叫半序集 $X_1,\cdots,X_n$ 的**直积**. 那么我们有

$$\delta(x,y)=\prod_{i=1}^{k}\delta_i(x_i,y_i)\tag{3.4}$$

$$\zeta(x,y)=\prod_{i=1}^{k}\zeta_i(x_i,y_i)\tag{3.5}$$

$$\mu(x,y)=\prod_{i=1}^{k}\mu_i(x_i,y_i)\tag{3.6}$$

这里 (3.4)(3.5) 式都是显然的, 下看 (3.6) 式. 事实上,

$$\sum_{x\le z\le y}\zeta(x,z)\prod_{i=1}^{k}\mu_i(z_i,y_i)=\sum_{\substack{x_i\le z_i\le y_i\\ i=1,2,\cdots,k}}\prod_{i=1}^{k}\zeta_i(x_i,z_i)\mu_i(z_i,y_i)$$

$$=\prod_{i=1}^{k}\sum_{x_i\le z_i\le y_i}\zeta_i(x_i,z_i)\mu_i(z_i,y_i)=\prod_{i=1}^{k}\delta_i(x_i,y_i)\delta(x,y).$$

让 $\tilde{\mu}(x,y)=\prod_{i=1}^{k}\mu_i(x_i,y_i)$, 则 $\zeta\tilde{\mu}=\delta$, 从而 $\tilde{\mu}=\zeta^{-1}=\mu$. □

例 3.2.9

设 $p_1,\cdots,p_k$ 为不同素数, $\mathscr{D}(p_1,\cdots,p_k)=\left\{\prod_{i=1}^{k}p_i^{\alpha_i}:\alpha_i\ge 0\right\}$, 它依整除关系构成下有限的半序集, 注意到

$$\prod_{i=1}^{k}p_i^{\beta_i}\Big|\prod_{i=1}^{k}p_i^{\alpha_i}\Leftrightarrow\beta_i\le\alpha_i,i=1,2,\cdots,k\Leftrightarrow(\beta_1,\cdots,\beta_k)\le(\alpha_1,\cdots,\alpha_k),$$

故半序集 $\mathscr{D}(p_1,\cdots,p_k)\cong\mathbb{N}^k$. 记 $d=\prod_{i=1}^{k}p_i^{\beta_i},n=\prod_{i=1}^{k}p_i^{\alpha_i}$, 则

$$\mu_{\mathscr{D}(p_1,\cdots,p_k)}(d,n)=\mu_{\mathbb{N}^k}((\beta_1,\cdots,\beta_k),(\alpha_1,\cdots,\alpha_k))=\prod_{i=1}^{k}\mu_{\mathbb{N}}(\beta_i,\alpha_i)$$

$$=\begin{cases}\prod_{i=1}^{k}(-1)^{\alpha_i-\beta_i}, & \alpha_i-\beta_i\in\{0,1\},i=1,2,\cdots,k\\ 0, & \text{此外,}\end{cases}$$

$$=\begin{cases}(-1)^{\sum_{i=1}^{k}(\alpha_i-\beta_i)}, & \dfrac{n}{d}=\prod_{i=1}^{k}p_i^{\alpha_i-\beta_i}\text{无重因子}\\ 0, & \text{此外,}\end{cases}=\begin{cases}\mu\left(\dfrac{n}{d}\right), & d|n,\\ 0, & \text{此外,}\end{cases}$$

在 $\mathscr{D}(p_1,\cdots,p_n)$ 上,

$$f(n)=\sum_{d|n}g(d),(n\in\mathscr{D}(p_1,\cdots,p_n))\Leftrightarrow g(n)=\sum_{d|n}f(d)\mu\left(\frac{n}{d}\right),(n\in\mathscr{D}(p_1,\cdots,p_n)).$$

例 3.2.10

设 $X=\{x_1,\cdots,x_n\}$ 为 n 元集, $\mathcal{P}(X)$ 依被包含关系 "$\subseteq$" 构成下有限的半序集. 对 $S\subseteq X$, 定义特征函数 $\chi_S:X\to\{0,1\}$ 为 $\chi_S(x_i)=\begin{cases}1, & x_i\in S,\\ 0, & x_i\notin S.\end{cases}$, 则当 $S,T\subseteq X$ 时,

$$S\subseteq T\Leftrightarrow\chi_S(x_i)\leq\chi_T(x_i),\forall i=1:n,\Leftrightarrow(\chi_S(x_1),\cdots,\chi_S(x_n))\leq(\chi_T(x_1),\cdots,\chi_T(x_n)).$$

所以

$$\begin{aligned}\mu(S,T)&=\mu_{\{0,1\}^n}((\chi_S(x_1),\cdots,\chi_S(x_n)),(\chi_T(x_1),\cdots,\chi_T(x_n)))\\&=\prod_{k=1}^{n}\mu_{\{0,1\}}(\chi_S(x_k),\chi_T(x_k)).\end{aligned}\tag{3.7}$$

而在 $\langle\{0,1\},\leq\rangle$ 上的 Möbius 函数满足 $\mu(0,0)=\mu(1,1)=1,\mu(1,0)=0,\mu(0,1)=-1$, 所以化简 (3.7) 式得

$$\mu(S,T)=\begin{cases}\prod_{i=1}^{n}(-1)^{\chi_T(x_k)-\chi_S(x_k)}, & \text{当}S\subseteq T,\\ 0, & \text{当}S\nsubseteq T,\end{cases}=\begin{cases}(-1)^{|T|-|S|}, & \text{当}S\subseteq T,\\ 0, & \text{当}S\nsubseteq T,\end{cases}$$

反演公式为

$$f(T)=\sum_{S\subseteq T}g(S),\forall T\subseteq X\Leftrightarrow g(T)=\sum_{S\subseteq T}f(S)(-1)^{|T|-|S|},\forall T\subseteq X.$$

令 $F(S)=f(S)$, $G(T)=(-1)^{|T|}g(T)$, 那么可以把上式改写为更加对称的版本:

$$F(T)=\sum_{S\subseteq T}(-1)^{|S|}G(S),\forall T\subseteq X\Leftrightarrow G(T)=\sum_{S\subseteq T}(-1)^{|S|}F(S),\forall T\subseteq X.\tag{3.8}$$

如果 $G(S)$ 只依赖于 S 的基数, 即 $G(S)=\varphi(|S|)$, 那么 (3.8) 式就是

$$f(n)=\sum_{k=0}^{n}\binom{n}{k}(-1)^kg(k),\forall n\in\mathbb{N}\Leftrightarrow g(n)=\sum_{k=0}^{n}\binom{n}{k}(-1)^kf(k),\forall n\in\mathbb{N}.$$

§ 3.3 用多项式空间构造反演公式

回顾: 设 $V_n=\{p(x)\in\mathbb{C}[x],\deg p\leq n\}$ 是 $\mathbb{C}$ 上的 $n+1$ 维向量空间, 如果 $p_k(x)\in\mathbb{C}[x],\deg p_k=k(k=0:n)$, 则 $\{p_k\}_{k=0}^n$ 为 V_n 的一组基底.

下设 $p_k(x),q_k(x)\in\mathbb{C}[x],\deg p_k=\deg q_k=k(k=0:n)$, 写

$$p_m(x)=\sum_{k=0}^{m}a_{m,k}q_k(x),q_m(x)=\sum_{k=0}^{m}b_{m,k}q_k(x),m=0:n.$$

我们用 $a_{m,k},b_{m,k}$ 来构造反演公式, 比如以前的与 Stirling 数有关的反演公式.

命题 3.3.1

在上述条件下,

$$f(m)=\sum_{k=0}^{m}a_{m,k}g(k),m=0:n\Leftrightarrow g(m)=\sum_{k=0}^{m}b_{m,k}f(k),m=0:n.$$

证明: 仅证“⇒”. $\sum_{k=0}^{m}b_{m,k}f(k)=\sum_{k=0}^{m}b_{m,k}\sum_{l=0}^{k}a_{k,l}g(l)=\sum_{l=0}^{m}g(l)=\sum_{l\le k\le m}b_{m,k}a_{k,l}\overset{\text{下证}}{=\!=}g(m).$

由 p_m,q_m 的定义, $q_m(x)=\sum_{k=0}^{m}b_{m,k}p_k(x)=\sum_{k=0}^{m}b_{m,k}\sum_{l=0}^{k}a_{k,l}q_l(x)=\sum_{l=0}^{m}q_l(x)\sum_{l\le k\le m}b_{m,k}a_{k,l}$, 注意 $q_l(x)$ 是基底! 所以 $\sum_{l\le k\le m}b_{m,k}a_{k,l}=\delta_{lm}$. □

例 3.3.2

取 $p_n(x)=x^n,q_n(x)=(1-x)^n,n=0,1,2,\cdots$, 则

$$p_n(x)=[1-(1-x)]^n=\sum_{k=0}^{n}\binom{n}{k}(-1)^kq_k(x),q_n(x)=[1-x]^n=\sum_{k=0}^{n}\binom{n}{k}(-1)^kp_k(x),$$

由命题 3.3.1, 可得**二项式系数反演公式**

$$f(n)=\sum_{k=0}^{n}\binom{n}{k}(-1)^kg(k),\forall n\in\mathbb{N}\Leftrightarrow g(n)=\sum_{k=0}^{n}\binom{n}{k}(-1)^kf(k),\forall n\in\mathbb{N}.$$

例 3.3.3

设 $p_n(x)=x^n,q_n(x)=(x)_n$, 则 $x^n=\sum_{k=0}^{n}\left\{{n\atop k}\right\}(x)_k,(x)_n=\sum_{k=0}^{n}\left[{n\atop k}\right](-1)^{n-k}x^k$, 由命题 3.3.1, 可得

Stirling 反演公式

$$f(n)=\sum_{k=0}^{n}\left\{{n\atop k}\right\}(-1)^kg(k),\forall n\in\mathbb{N},\Leftrightarrow(-1)^ng(n)=\sum_{k=0}^{n}\left[{n\atop k}\right]f(n)(-1)^{n-k},\forall n\in\mathbb{N}.$$

例 3.3.4

设 $p_n(x)=(-x)_n=(-x)(-x-1)\cdots(-x-n+1), q_n(x)=(x)_n=x(x-1)\cdots(x-n+1)$, 则

$$\frac{p_n(x)(-1)^n}{n!}=\frac{x(x+1)\cdot(x+n-1)}{n!}=\binom{x+n-1}{n}\overset{\text{朱-Vandermonde}}{=\!=\!=}\sum_{k=1}^{n}\binom{n-1}{n-k}\binom{x}{k},$$

所以

$$(-x)_n=(-1)^n n!\sum_{k=1}^{n}\binom{n-1}{k-1}\frac{(x)_k}{k!}=\sum_{k=1}^{n}\binom{n-1}{k-1}\frac{n!}{k!}(-1)^n(x)_k\triangleq\sum_{k=1}^{n}l_{n,k}(x)_k, \tag{3.9}$$

这里 $l_{n,k}=\binom{n-1}{k-1}\frac{n!}{k!}(-1)^n$ 叫 **Lah 数**, 规定 $l_{0,0}=1, l_{n,0}=0(n>0)$, 把 x 换成 $-x$ 可得

$$(x)_n=\sum_{k=0}^{n}l_{n,k}(-x)_k, \tag{3.10}$$

由 (3.9)(3.10) 式, 有 **Lah 反演公式**: $f(n)=\sum_{k=0}^{n}l_{n,k}g(k)\Leftrightarrow g(n)=\sum_{k=0}^{n}l_{n,k}f(k)$.

注: 事实上 Lah 反演公式是“假”的, 与二项式反演是一回事. 可以把 Lah 反演公式改写为

$$(-1)^n\frac{f(n)}{(n-1)!}=\sum_{k=1}^{n}\binom{n}{k}(-1)^k\frac{g(k)(-1)^k}{(k-1)!}.$$

推广需要看与之前的命题是否等价, 不要做“假的推广”、“无聊的推广”.

H.W.Gould 与徐利治在 1973 年提出反演公式:

定理 3.3.5. Gould-Hsu 反演公式

设 $(a_i)_{i=1}^n,(b_i)_{i=1}^n$ 是数列, 满足

$$\psi(x,n)=\prod_{i=1}^{n}(a_i+b_ix)\neq 0,\forall x,n\in\mathbb{Z}^+,$$

其中 $\psi(x,0)=1$. 则有如下的反演公式:

$$\begin{aligned}f(n)&=\sum_{k=0}^{n}(-1)^k\binom{n}{k}\psi(k,n)g(k),n\in\mathbb{N},\\ g(n)&=\sum_{k=0}^{n}(-1)^k\binom{n}{k}(a_{k+1}+kb_{k+1})\psi(n,k+1)^{-1}f(k),n\in\mathbb{N}.\end{aligned} \tag{3.11}$$

Gould-Hsu 有如下的矩阵反演公式:

定理 3.3.6

设 (a_i) 是复数序列, $\boldsymbol{F}=(f_{n,k})$ 与 $\boldsymbol{G}=(g_{n,k})$ 是下三角矩阵, 且

$$f_{n,k}=\frac{\prod_{j=k}^{n-1}(a_j+k)}{(n-k)!}$$
$$g_{n,k}=(-1)^{n-k}\frac{a_k+k}{a_n+n}\frac{\prod_{j=k+1}^{n}(a_j+n)}{(n-k)!},$$

则 $\boldsymbol{F},\boldsymbol{G}$ 互为逆矩阵.

马欣荣做 (f,g)-反演进一步推广了 Gould-Hsu 矩阵反演, 得到更加一般化的反演公式.

第三章习题

1. 直接证明 (3.8) 式.
2. 设定义在 $\mathbb{N}$ 上的函数 f 满足
$$\sum_{d|n}f(d)=\log n, n\in\mathbb{N}.$$
证明当 n 是素数幂次 p^l 时, $f(n)=\log p$, 其余情形 $f(n)=0$.
3. 证明: $\displaystyle\sum_{\substack{m=1\\(m,n)=1}}^{n}e^{2\pi i\frac{m}{n}}=\mu(n)$.
4. 设 $d,n\in\mathbb{Z}^+, d|n$, 整数 c,d 互素, 证明: $\{1\le m\le n: m\equiv c(\mathrm{mod}\ d)\}$ 恰好有 $\dfrac{\varphi(n)}{\varphi(d)}$ 个与 n 互素.
5. 对任意 m 与 $\{0,1,\cdots,m-1\}$ 到 $\mathbb{C}$ 的映射 f,g, 证明离散 Fourier 反演公式
$$g(n)=\sum_{k=0}^{m-1}f(k)e^{2\pi ikn/m}, n=0,1,\cdots,m-1$$
$$\Leftrightarrow f(n)=\frac{1}{m}\sum_{k=0}^{m-1}g(k)e^{-2\pi ikn/m}, n=0,1,\cdots,m-1.$$

第 4 章　Ramsey 理论

名人名言: 如果要求在组合数学中举出一个但仅一个优美的定理, 大多数组合学家会提名 Ramsey 定理.　　——G.Rotta

F.P.Ramsey(1903-1930) 是美国逻辑学家、哲学家、经济学家, 1928 年他研究命题演算的一个问题, 证明一个东西可判定, 但他不知道哥德尔的不完备定理, 相当于在证一个不存在的东西, 于是得到了副产品——Ramsey 定理. 在伦敦数学会宣读“On a problem of formed logic”, proc. London Math. Soc. 30(130),264-286.

Ramsey 定理在哲学上的意义: 任何一个足够大的结构里, 一定包含给定大小的规则的子结构.

§ 4.1　抽屉原理及其应用

抽屉原理 (Pigeon-Hole Principle, 鸽笼原理): 如果将至少 $n+1$ 个物体放入 n 个抽屉中, 一定有至少一个抽屉包含至少两个物体.

抽屉原理也叫 Dirichlet 原理. Dirichlet 第一次使用它证明用有理数逼近无理数的结论.

例 4.1.1. Dirichlet

有无穷多个既约有理数 $\frac{p}{q}(p\in\mathbb{Z}^+,q\in\mathbb{Z}^+,(p,q)=1)$, 使得 $\left|\theta-\frac{p}{q}\right|<\frac{1}{q^2}$.

证明: $[0,1)$ 是 n 个不相交小区间 $\left[0,\frac{1}{n}\right),\left[\frac{1}{n},\frac{2}{n}\right),\cdots,\left[\frac{n-1}{n},1\right)$ 之并, 而有 $n+1$ 个数 $\{0\theta\},\{1\theta\},\cdots,\{n\theta\}$. ($\{\cdot\}$ 代表一个数的小数部分) 由抽屉原理, 一定存在两个数 $\{k\theta\},\{l\theta\}(0\le k<l\le n)$ 落在同一个小区间中, 于是

$$\frac{1}{n}>|\{l\theta\}-\{k\theta\}|=|l\theta-\lfloor l\theta\rfloor-(k\theta-\lfloor k\theta\rfloor)|=|(l-k)\theta+\lfloor k\theta\rfloor-\lfloor l\theta\rfloor|.$$

令

$$p_0=\frac{\lfloor l\theta\rfloor-\lfloor k\theta\rfloor}{(l-k,\lfloor l\theta\rfloor-\lfloor k\theta\rfloor)},q_0=\frac{l-k}{(l-k,\lfloor l\theta\rfloor-\lfloor k\theta\rfloor)}(\le l-k\le n),$$

则

$$|q_0\theta-p_0|<\frac{1}{n}\Rightarrow\left|\theta-\frac{p_0}{q_0}\right|<\frac{1}{q_0n}\le\frac{1}{q_0^2}.$$

下面证明可以找无穷多个这样的 $\frac{p}{q}$. 取 $n'\in\mathbb{N}^+$ 使得 $n'>\frac{1}{\left|\frac{p_0}{q_0}-\theta\right|}$, 把 $[0,1)$ 划分为 n' 个小区间, 依据上法可以找到既约有理数 $\frac{p_1}{q_1}$, 使得

$$\left|\theta-\frac{p_1}{q_1}\right|<\frac{1}{n'q_1}\le\frac{1}{q_1^2}.$$

注意

$$\left|\theta-\frac{p_0}{q_0}\right|>\frac{1}{n'}>\frac{1}{n'q_1}>\left|\theta-\frac{p_1}{q_1}\right|,$$

则 $\frac{p_1}{q_1}$ 逼近效果更好, 继续下去就可以找到无穷多个既约有理数 $\frac{p_i}{q_i}$, 使得

$$\left|\theta-\frac{p_i}{q_i}\right|<\frac{1}{q_i^2}\text{且}\left|\theta-\frac{p_i}{q_i}\right|>\left|\theta-\frac{p_{i+1}}{q_{i+1}}\right|.$$

例 4.1.2. Kronecker

设 ξ 为无理数, 则 $\{1\xi\},\{2\xi\},\cdots,\{n\xi\},\cdots$ 在 $[0,1]$ 中稠密. 更一般地, $k\xi+l(k\in\mathbb{Z}^+,l\in\mathbb{Z})$ 在实数轴上稠密. (丢番图逼近)

证明: (1) 如果 $(\{k\xi\})_{k=1}^{\infty}$ 在 $[0,1]$ 中稠密, 则对任意实数 $\alpha>0$ 与 $\varepsilon>0$, 存在 $k\in\mathbb{Z}^+$ 使得 $|\{k\xi\}-\{\alpha\}|<\varepsilon$. 记 $l=-\lfloor k\xi\rfloor+\lfloor\alpha\rfloor$, 则 $|k\xi+l-\alpha|<\varepsilon$. 所以只需证 $k=1,l=0$ 的情况.

(2) 依据 Dirichlet 结果的证明, 有 $k\in\mathbb{Z}^+$ 与 $h\in\mathbb{Z}$ 使得 $|k\xi-h|<\frac{1}{N}$.

令 $\theta=\begin{cases}\{\xi\}, & k\xi>h,\\ 1-\{\xi\}, & k\xi<h,\end{cases}$, 则 $\theta\in(0,1)$ 且 $\{k\theta\}=\{|k\xi-h|\}<\frac{1}{N}$.

令 $M=\left\lfloor\frac{1}{\{k\theta\}}\right\rfloor$, 则 $N\le M<\frac{1}{\{k\theta\}}<M+1$, 所以 $\frac{1}{M+1}<\{k\theta\}<\frac{1}{M}$. 当 $1\le m\le M$ 时, $0<m\{k\theta\}<\frac{m}{M}\le 1$, 故 $m\{k\theta\}=\{mk\theta\}$.

在 $[0,1)$ 的子区间 $[0,\{k\theta\}),[\{k\theta\},2\{k\theta\}),\cdots,[(M-1)\{k\theta\},M\{k\theta\}),[M\{k\theta\},1)$ 中, 前 M 个的长度是 $\{k\theta\}<\frac{1}{N}$, 最后一个的长度是 $1-M\{k\theta\}<\{k\theta\}<\frac{1}{N}$. 任给 $\alpha\in[0,1]$, α 与 $1-\alpha$ 都落在这 $M+1$ 个小区间中.

当 $k\xi>h$ 时, 有 $1\le m\le M$ 使得 $|\alpha-m\{k\theta\}|<\frac{1}{M}$. 注意 $M<\frac{1}{\{k\theta\}}<M+1$ 即 $|\alpha-\{km\theta\}|<\frac{1}{M}$, 所以 $|\alpha-\{km\xi\}|=|\alpha-\{km\theta\}|<\frac{1}{M}\le\frac{1}{N}$;

当 $k\xi<h$ 时, 有 $1\le m\le M$ 使得 $|\alpha-\{km\xi\}|=|1-\alpha-m\{k\theta\}|<\frac{1}{N}$.

综上, 结论成立. □

Pell 方程 $x^2-dy^2=1(d\in\mathbb{Z}^+$ 不是完全平方) 有无穷多组解.

1955 年, Roth 证明了如果 ξ 是代数数且不是有理数, 则 $\forall\varepsilon>0$, 至多有有限多个既约分数 $\frac{p}{q}$ 使得 $\left|\xi-\frac{p}{q}\right|<\frac{1}{q^{2+\varepsilon}}$, 获得了 Fields 奖.

应用: $p(x,y)$ 是齐次整系数多项式, 次数大于 2, 则方程 $p(x,y)=c(\neq 0)$ 只有有限多整数解.

例 4.1.3. Erdös, Lehman

不超过 $2n$ 的 $n+1$ 个正整数中, 必有一个整除另一个.

证明: 设这 $n+1$ 个正整数是 $1\le a_1\le a_2\le\cdots\le a_{n+1}\le 2n$,

写 $a_i=2^{\alpha_i}q_i,2\nmid q_i$, 则 $q_1,q_2,\cdots,q_{n+1}\in\{1,3,5,\cdots,2n-1\}$, $n+1$ 个元素属于其中 n 个, 由抽屉原理, 有 $1\le i<j\le n+1$ 使得 $q_i=q_j$, 由 $a_i<a_j\Rightarrow\alpha_i<\alpha_j\Rightarrow a_i|a_j$. □

例 4.1.4

任给 $a_1,\cdots,a_n\in\mathbb{Z}$, 必有若干个相邻项之和为 n 的倍数.

证明: 设 $S_0=0,S_k=a_1+\cdots+a_k(k=1,2,\cdots,n)$.

由抽屉原理, 有 $0\le i<j\le n$ 使得 $S_i\equiv S_j(\mathrm{mod}\ n)$, 所以 $n|(a_{i+1}+\cdots+a_j)$. □

注: 推广: 设 G 是 n 阶加法 Abel 群, $a_1,\cdots,a_n\in G$, 让 $S_0=0, S_k=a_1+\cdots+a_k(k=1,2,\cdots,n)$, 则 $S_0,S_1,\cdots,S_n\in G$, 而 $|G|=n$, 则必有 $0\le i<j\le n$ 使得 $S_i=S_j$, 即

$$a_{i+1}+\cdots+a_j=0. \tag{4.1}$$

如果 $a_{i+1},\cdots,a_j$ 满足 (4.1) 式, 则称 $(a_{i+1},\cdots,a_j)$ 是一个**零和子序列**.

对有限 Abel 群 G, Davenport 常数 $D(G)$ 是最小的正整数 k, 使得 G 中长为 k 的元素的序列 $(a_i)_{i=1}^k$ 都有零和子序列. 因此 $D(G)\le|G|$.

对于 n 阶循环群 C_n, $D(C_n)=n$. 注意生成元 $\underbrace{\bar{1},\cdots,\bar{1}}_{n-1个}$ 之和不为 0.

回顾: p-群即 p^n 阶群. 下面有限 Abel 群结构定理的证明见抽象代数课本.

定理 4.1.5. 有限 Abel 群结构定理

设 G 是有限 Abel 群, $|G|>1$, 则:

(1) 有唯一的正整数 $n_1,\cdots,n_k$, 使得 $1<n_1|n_2|\cdots|n_{k-1}|n_k$, 使得

$$G\cong C_{n_1}\times C_{n_2}\times\cdots\times C_{n_k}.$$

(即有限 Abel 群可以唯一分解成有限个循环群的直积.)

(2)G 可以唯一分解成循环 p-群的直积:

$$G\cong(C_{p_1^{\alpha_{11}}}\times\cdots\times C_{p_1^{\alpha_{1l_1}}})\times(C_{p_2^{\alpha_{21}}}\times\cdots\times C_{p_2^{\alpha_{2l_2}}})\times\cdots\times(C_{p_r^{\alpha_{r1}}}\times\cdots\times C_{p_r^{\alpha_{rl_r}}})$$

1969 年, J.E.Olson 证明了对 Abel p-群 $G=\mathbb{Z}/_{p^{\alpha_1}\mathbb{Z}}\oplus\cdots\oplus\mathbb{Z}/_{p^{\alpha_r}\mathbb{Z}}$, 有 $D(G)=1+\sum_{i=1}^{r}(p^{\alpha_i}-1)$.

Olson 还证明了 $D(\mathbb{Z}/n\mathbb{Z}\oplus\mathbb{Z}/n\mathbb{Z})=2n-1$.

猜想: $D(\underbrace{C_n\times\cdots\times C_n}_{k个})=1+k(n-1)$, 到现在还没人会证.

定理 4.1.6. 抽屉原理一般形式

设 $q_1,\cdots,q_t\in\mathbb{Z}^+$. 将至少 $q_1+\cdots+q_t-t+1$ 个物体放入 t 个抽屉中, 则下面 t 条中至少有一条成立:

(1) 第 1 个抽屉中至少包含 q_1 个物体;

(2) 第 2 个抽屉中至少包含 q_2 个物体;

$\vdots$

(t) 第 t 个抽屉中至少包含 q_t 个物体.

证明: 反证. 若结论不对, 则物体总数 $<q_1-1+\cdots+q_t-1=q_1+\cdots+q_t-t<q_1+\cdots+q_t-t+1$, 矛盾. □

注: 通常的抽屉原理取 $q_1=\cdots=q_t=2$.

在抽屉原理一般形式中, $q_1+\cdots+q_t-t+1$ 不能换为更小的. 如果物体数 N 满足

$$N\le q_1+\cdots+q_t-t=\sum_{i=1}^{t}(q_i-1),$$

取最小的 $s \le t$ 使得 $\sum_{i=1}^{s-1}(q_i-1) < N \le \sum_{i=1}^{s}(q_i-1)$, 则 $N - \sum_{i=1}^{s-1}(q_i-1) \le q_s - 1$. 当 $1 \le i < s$ 时, 第 i 个抽屉中放入 $q_i - 1$ 个物体, 第 s 个抽屉中放入 $N - \sum_{i=1}^{s-1}(q_i-1) \le q_s - 1$ 个物体, 当 $i > s$ 时第 j 个抽屉中不放物体, 这样就不满足 (1)-(t) 的任何一个条件. □

例 4.1.7. Erdös-Szekeres

设 $(a_k)_{k=1}^{nm+1}$ 是实数列, 则或者它包含长为 $m+1$ 的不增子序列, 或者它包含长为 $n+1$ 的不减子序列. 特别地, 当 $m=n$ 时, $a_1, \cdots, a_{n^2+1}$ 必包含长为 n 的单调子序列.

证明: 若 $(a_k)_{k=1}^{mn+1}$ 不包含长为 $n+1$ 的不减子序列, 对 $i = 1, \cdots, mn+1$, 用 l_i 表示由 a_i 开始的最长不减子序列的长度, 则 $1 \le l_i \le n$. 设有标号为 $1, \cdots, n$ 的 n 个抽屉. 若 $l_i = k \in \{1, \cdots, n\}$, 则把 a_i 放入第 k 个抽屉中.

若 $a_1, \cdots, a_{mn+1}$ 都已经放入 n 个抽屉里, 令 $q_1 = \cdots = q_n = m+1$, 则 $q_1 + \cdots + q_n - n + 1 = mn+1$. 依据定理4.1.6, 存在 $1 \le k \le n$, 使得第 k 个抽屉中至少包含 $q_k = m+1$ 个数.

设 $a_{i_1}, \cdots, a_{i_{m+1}}$ 在第 k 个抽屉中, $(1 \le i_1 < \cdots < i_{m+1} \le mn+1)$ 则 $l_{i_1} = \cdots = l_{i_{m+1}} = k$. 如果 $a_{i_j} \le \underbrace{a_{i_{j+1}} \le \cdots \le \cdots}_{k\text{个}}$, 则 $l_{i_j} = k+1$, 这是不可能的 $(l_{i_j} = k)$, 因此必有 $a_{i_j} > a_{i_{j+1}} (j = 1, \cdots, m)$, 这样就找到了长为 $m+1$ 的不增子序列. □

例 4.1.8

设 n 为正奇数, $b_1, \cdots, b_n$ 是整数 $a_1, \cdots, a_n$ 的一个排列, 证明: $\prod_{i=1}^{n}(a_i - b_i)$ 必为偶数.

证明: 设 $a_i - b_i$ 为奇数的个数为 k 个, 不妨设为 $(a_1 - b_1, \cdots, a_k - b_k)$. 则 $a_{k+1} - b_{k+1}, \cdots, a_n - b_n$ 都是偶数. 由于 $(a_1 - b_1) + \cdots + (a_n - b_n) = 0$ 是偶数, 则 k 必为偶数. 由 n 是正奇数, 则 $a_n - b_n$ 必为偶数, 从而 $\prod_{i=1}^{n}(a_i - b_i)$ 必为偶数. □

例 4.1.9

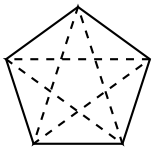
在至少有 6 个人的集会上, 必有三人为两两相互熟识或两两相互不熟识.

证明: 穷举法共 $2^{15} = 32768$ 种, 不太现实. 用 $ABCDEF$ 表示 6 人, 熟识则连实边, 不熟识则连虚边. 我们要证明: 或者有实边三角形, 或者有虚边三角形. 分两种情况:

(1) 若 A 与三个人熟识 (不妨设为 BCD), 如果 BCD 相互不熟识, 则找到了虚三角形; 如果 B, C, D 其中两个是熟识的, 比如 BC 熟识, 则 ABC 构成实三角形.

(2) 若 A 与三个人不熟识 (不妨设为 BCD), 此时与 (1) 同理. □

注: 6 不可以改为 5, 反例如图:



§4.2 Ramsey 定理

把 X 中物体放入 t 个抽屉中相当于作 X 的一个有序分划, 即 $X = X_1 \cup X_2 \cup \cdots \cup X_t$, 使得 $X_i \cap X_j = \varnothing$.

定理 4.2.1. Ramsey

设 r 为正整数, $q_1,\cdots,q_t\geq r$, 则存在一个正整数 N, 使得下列性质成立: 任给基数至少为 N 的集合 S, 设 $\mathscr{A}_1\cup\cdots\cup\mathscr{A}_t$ 为 $\mathcal{P}_r(S)=\{A\subseteq S:|A|=r\}$ 的任一个有序分划, 则下面 t 个命题之一成立:

$(1)S$ 有一个 q_1 元子集, 使得这个 q_1 元子集的所有 r 元子集都属于 $\mathscr{A}_1$;

$(2)S$ 有一个 q_2 元子集, 使得这个 q_2 元子集的所有 r 元子集都属于 $\mathscr{A}_2$;

$\vdots$

$(t)S$ 有一个 q_t 元子集, 使得这个 q_t 元子集的所有 r 元子集都属于 $\mathscr{A}_t$.

把最小的这样的 N 记为 $R_r(q_1,\cdots,q_t)$, 叫 **Ramsey 数**.

下面对 Ramsey 定理作一些说明.

(1) 当 $r=1$ 时, Ramsey 定理就是抽屉原理的一般形式. $\mathcal{P}_1(S)$ 的一个有序分划 $\mathscr{A}_1\cup\cdots\cup\mathscr{A}_t$ 对应于 S 的一个有序分划 $A_1\cup\cdots\cup A_t$, 这里 $\mathscr{A}_i=\{\{x\}:x\in A_i\},A_i=\{x\in S:\{x\}\in\mathscr{A}_i\}$. 这样 1 元子集就相当于元素了. 而且

$$R_1(q_1,\cdots,q_t)=q_1+\cdots+q_t-t+1.$$

(2) 当 $t=1$ 时, S 有一个 q_1 元子集使得其 r 元子集都属于 $\mathscr{A}_1$, 此时结论显然正确, 且 $R_r(q)=q$.

(3)$R_r(q_1,\cdots,q_t)$ *的存在性及取值与* $q_1,\cdots,q_k$ *的排列无关.*

设 $q_1,\cdots,q_k\geq r$, $i_1,\cdots,i_t$ 是 $1,\cdots,t$ 的全排列. 若 $|S|\geq R_r(q_{i_1},\cdots,q_{i_t})$, 且 $\mathscr{A}_1\cup\cdots\cup\mathscr{A}_t$ 为 $\mathcal{P}_r(S)$ 的 t 部分划, 则 $\mathscr{A}_{i_1}\cup\cdots\cup\mathscr{A}_{i_t}$ 也是 $\mathcal{P}_r(S)$ 的有序分划, 于是 S 或者有一个 q_{i_1} 元子集, 使得其 r 元子集都属于 $\mathscr{A}_{i_1}$, 或者有一个 q_{i_2} 元子集, 使得其 r 元子集都属于 $\mathscr{A}_{i_2}$, $\cdots$, 或者有一个 q_{i_t} 元子集, 使得其 r 元子集都属于 $\mathscr{A}_{i_t}$. 从而存在 $1\leq s\leq t$, 使得 S 有一个 q_s 元子集, 其 r 元子集也属于 $\mathscr{A}_s$.

由上可见, $R_r(q_{i_1},\cdots,q_{i_t})$ 存在时, $R_r(q_1,\cdots,q_t)\leq R_r(q_{i_1},\cdots,q_{i_t})$, 而不等式另一边当然也对, 因此 $R_r(q_1,\cdots,q_t)=R_r(q_{i_1},\cdots,q_{i_t})$. □

(4) *设* $q_1,\cdots,q_t\geq r$, *若* $R_r(q_1,\cdots,q_t)$ *存在, 则* $R_r(q_1,\cdots,q_t)\geq\max\{q_1,\cdots,q_t\}\geq r$.

证明: 设集合 S 的基数为 $R_r(q_1,\cdots,q_t)$, 对任意 $1\leq s\leq t$, 把 S 的 r 元子集放入第 s 个抽屉中, 其他抽屉不放, 对 $1\leq i\leq t,i\neq s$ 时, S 有 q_i 元子集, 其 r 元子集都不属于第 i 个抽屉中, 于是必定 S 有一个 q_s 元子集, 其 r 元子集都在第 s 个抽屉中. 所以 $|S|\geq q_s(\forall 1\leq s\leq t)$. □

(5) *当* $q\geq r$ *时,* $R_r(q,r)=q$.

证明: 由 (4),$R_r(q,r)\geq\max\{q,r\}=q$. 假设 $|S|=q,q_1=q,q_2=r$, $\mathscr{A}_1\cup\mathscr{A}_2$ 是 $\mathcal{P}_r(S)$ 的有序分划,

当 $\mathscr{A}_2\neq\varnothing$ 时, 有 $T\in\mathscr{A}_2$, 使得 T 是 S 的 $q_2=r$ 元子集, 从而 T 的 r 元子集只有 T 自己, 它属于 $\mathscr{A}_2$;

当 $\mathscr{A}_2=\varnothing$ 时, S 的任一个 $q_1=q$ 元子集的 r 元子集都属于 $\mathscr{A}_1$.

因此, $R_r(q,r)\leq q$(即 q 可作为 N), 所以 $R_r(q,r)=q$. □

(6) *设* $q_1,\cdots,q_t\geq r$, *如果* $q\geq\max\{q_1,\cdots,q_t\}$, *则* $R_r(\underbrace{q,\cdots,q}_{t个})$ *存在可推出* $R_r(q_1,\cdots,q_t)$ *存在, 且* $R_r(q_1,\cdots,q_t)\leq R_r(q,\cdots,q)$.

证明: 设 $|S|\geq R_r(\underbrace{q,\cdots,q}_{t个})$, $\mathscr{A}_1\cup\cdots\mathscr{A}_t$ 为 $\mathcal{P}_r(S)$ 的一个有序分划, 则有 $1\leq i\leq t$ 使得 S 有一个 q 元子集, 其 r 元子集都属于 $\mathscr{A}_i$, 则 S 有一个 q_i 元子集, 其 r 元子集都属于 $\mathscr{A}_i$. □

引理 4.2.2

设 $2\leq t\leq k$ 时 Ramsey 定理成立, 则 $t=k+1$ 时 Ramsey 定理也成立, 且 $q_1,\cdots,q_{k+1}\geq r\geq 1$ 时,

$$R_r(q_1,\cdots,q_{k+1})\leq R_r(q_1,\cdots,q_{k-1},R_r(q_k,q_{k+1})).$$

证明: 设 $|S| \geq R_r(q_1, \cdots, q_{k-1}, R_r(q_k, q_{k+1}))$, $\mathscr{A}_1 \cup \cdots \cup \mathscr{A}_{k+1}$ 为 $\mathcal{P}_r(S)$ 的一个有序分划. 于是有 $1 \leq i \leq k-1$, 使得 S 有个 q_i 元子集, 其 r 元子集都属于 $\mathscr{A}_i$, 或者 S 有个 $R_r(q_k, q_{k+1})$ 元子集, 使得其 r 元子集都属于 $\mathscr{A}_k \cup \mathscr{A}_{k+1}$. (前面的情况对的话那就不用证, 只需要看后面的情况).

如果后一种情况对, 即 S 有个 $R_r(q_k, q_{k+1})$ 元子集 T, 使得 $\mathcal{P}_r(T) \subseteq \mathscr{A}_k \cup \mathscr{A}_{k+1}$, 让

$$\mathscr{B}_1 = \{X \subseteq T : X \in \mathscr{A}_k\}, \mathscr{B}_2 = \{X \subseteq T : X \in \mathscr{A}_{k+1}\},$$

则 $\mathscr{B}_1 \cup \mathscr{B}_2$ 为 $\mathcal{P}_r(T)$ 的一个有序分划, 而 $|T| = q = R_r(q_k, q_{k+1})$, 故: 或者 T 有个 q_k 元子集, 其 r 元子集都属于 $\mathscr{B}_1 \subseteq \mathscr{A}_k$, 或者 T 有个 q_{k+1} 元子集, 其 r 元子集都属于 $\mathscr{B}_2 \subseteq \mathscr{A}_{k+1}$. □

引理 4.2.3

设 $r \geq 2, q_1, q_2 \geq r+1$, 若 $p_1 = R_r(q_1 - 1, q_2), p_2 = R_r(q_1, q_2 - 1)$ 都存在 (从而 $p_1, p_2 \geq r$), 而且 $R_{r-1}(p_1, p_2)$ 也存在, 则 $R_r(q_1, q_2)$ 存在, 且 $R_r(q_1, q_2) \leq R_r(p_1, p_2) + 1$.

证明: 设 $|S| \geq R_{r-1}(p_1, p_2) + 1$, $\mathscr{A}_1 \cup \mathscr{A}_2$ 是 $\mathcal{P}_r(S)$ 的一个二部分划. (我们要证明: S 或者有 q_1 元子集, 其 r_1 元子集都属于 $\mathscr{A}_1$, 或者有 q_2 元子集, 其 r_2 元子集都属于 $\mathscr{A}_2$.) 取 $a \in S, T = S \setminus \{a\}$, 则 $|T| \geq R_{r-1}(p_1, p_2)$, 令

$$\mathscr{B}_i = \{X \subseteq T : X \cup \{a\} \in \mathscr{A}_i\}, i = 1, 2.$$

则 $\mathscr{B}_1 \cup \mathscr{B}_2$ 是 $\mathcal{P}_{r-1}(T)$ 的二部分划.

由于 $|T| \geq R_{r-1}(p_1, p_2)$, 且 $R_{r-1}(p_1, p_2)$ 存在, 故或者 T 有个 p_1 元子集 U, 其 r_1 元子集都属于 $\mathscr{B}_1$, 或者 T 有个 p_2 元子集, 其 $r-1$ 元子集都属于 p_2. 不妨设第一种情况对 (另一种完全对称). 让

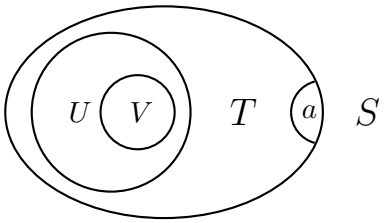
$$\mathscr{C}_i = \{X \subseteq U : X \in \mathscr{A}_i\}, i = 1, 2.$$

则 $\mathscr{C}_1 \cup \mathscr{C}_2$ 是 $\mathcal{P}_r(U)$ 的一个有序分划. 由于 $|U| = p_1 = R_r(q_1 - 1, q_2)$ 存在, 故或者 U 有个 $q_1 - 1$ 元子集 V, 其 r 元子集都属于 $\mathscr{C}_1$, 或者 U 有个 q_2 元子集, 其 r 元子集都属于 $\mathscr{C}_2$.

假如后一种情况对, 则 U 的 q_2 元子集也是 S 的 q_2 元子集, 其 r 元子集都在 $\mathscr{C}_2$ 中, 进而也在 $\mathscr{A}_2$ 中.

假如前一种情况对 (U 有个 $q_1 - 1$ 元子集 V, 使得 $\mathcal{P}_r(V) \subseteq \mathscr{C}_1$), 考虑 $W = V \cup \{a\}$, 则 $|W| = q_1$, 从而 W 是 S 的 q_1 元子集. 而 W 的 r 元子集可以分为含 a 与不含 a 的, 其中 W 的不含 a 的 r 元子集是 V 的 r 元子集, 从而属于 $\mathscr{A}_1$. 再考虑 W 的含 a 的 r 元子集, 它是 U 的 $r-1$ 元子集添加 a 可得, 而 U 的 $r-1$ 元子集都属于 $\mathscr{B}_1$, 则 W 的含 a 的 r 元子集都属于 $\mathscr{A}_1$, 故 W 的所有 r 元子集都在 $\mathscr{A}_1$ 中.

由上, S 或者有 q_1 元子集, 其 r_1 元子集都属于 $\mathscr{A}_1$, 或者有 q_2 元子集, 其 r_2 元子集都属于 $\mathscr{A}_2$. □



Ramsey 定理的证明: 由引理4.2.2, 只需要对 $t = 2$ 的情形证明. 对 r 归纳:

当 $r = 1$ 时, 由抽屉原理一般形式得到.

设 $r \geq 2$ 且当 r 更小时结论正确, 下面对 $q_1 + q_2$ 归纳证明 $q_1, q_2 \geq r$ 时 $R_r(q_1, q_2)$ 存在: 若 $r \in \{q_1, q_2\}$, 则 $R_r(q_1, q_2) = r$ 存在. 假设 $q_1, q_2 \geq r+1$, 由归纳假设, $p_1 = R_r(q_1 - 1, q_2)$ 存在,

且 $p_2 = R_r(q_1, q_2-1)$ 存在, 故 $p_1, p_2 \geq r$, 且 $R_{r-1}(p_1, p_2)$ 存在. 由引理4.2.3, $R_r(q_1, q_2)$ 存在且 $R_r(q_1, q_2) \leq R_{r-1}(p_1, p_2) + 1$. □

Ramsey 定理的无限形式: 设 r 是正常数, S 是无穷集, $\mathscr{A}_1 \cup \cdots \mathscr{A}_t$ 是 $\mathcal{P}_r(S)$ 的一个有序分划, 则 S 有个无穷子集 T, 使得其 r 元子集都在同一个 $\mathscr{A}_i$ 中.

§4.3 关于 Ramsey 数

由抽屉原理一般形式, $R_1(q_1, \cdots, q_t) = q_1 + \cdots + q_t - t + 1$. 当 $q \geq 2$ 时, $R_2(q, 2) = q$. 由前面的例4.1.9, $R_2(3,3) = 6$. 到目前为止, 已知的部分 $R_2(p,q)$ 值与上下界如下表:

p \ q	3	4	5	6	7	8	9	10
3	6	9	14	18	23	28	36	[40,43]
4		18	25	[35,41]	[49,61]	[56,84]	[73,115]	[92,149]
5			[43,49]	[58,87]	[80,143]	[101,216]	[125,316]	[143,442]

定理 4.3.1. Erdös, Szekeres

对大于 1 的整数 p, q, 有

$$R_2(p,q) \leq \binom{p+q-2}{p-1} = \binom{p+q-2}{q-1}.$$

证明: 对 $p+q$ 作归纳. 当 $p+q=4$ 时, 结论正确. 若 $p+q>4$, 且当 $p', q' \geq 2, p'+q' < p+q$ 时, $R_2(p', q') \leq \binom{p'+q'-2}{p'-1}$, 如果 $p=2$ 或 $q=2$, 则结论正确, 下设 $p, q > 2$. 由引理4.2.3,

$$\begin{aligned} R_2(p,q) &\leq R_1(R_2(p-1,q), R_2(p,q-1)) + 1 \\ &\leq \binom{(p-1)+q-2}{(p-1)-1} + \binom{p+(q-1)-2}{p-1} = \binom{p+q-2}{p-1}. \end{aligned}$$

(注意, $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.) □

注: 此定理给出了一个上界, 例如 $R_2(3,4) \leq 10$, 但实际上 $R_2(3,4) = 9$.

随着 p 的增大, 通过构造的方法得到 $R_2(p,p)$ 的下界越来越难, 而且下界难以逼近真正的值. Erdös 在 1947 年发现了新的有效方法, 不需要任何构造, 而且以后组合学的概率方法源于此.

定理 4.3.2. Erdös, 1947

当 $m \geq 3$ 时, $R_2(m,m) > \sqrt{2}^m$.

证明: 设平面上放置 n 个点, 且任意三点不共线, 任意两点相连得到完全图 K_n. 用红、蓝两种颜色对 K_n 的所有边着色, 由于 K_n 有 $\binom{n}{2}$ 条边, 所以一共有 $2^{\binom{n}{2}}$ 种不同的着色方法. 在这 n 个点中取定 m 个点后对 K_n 的边染色, 使得这 m 个点导出的子图 K_m 各边同色 (红或蓝) 的染色方法一共有 $2 \times 2^{\binom{n}{2}-\binom{m}{2}}$ 种. 所以使得 K_n 含有各边同色的 K_m 的染色方法数不超过 $N_0 = \binom{n}{m} 2 \times 2^{\binom{n}{2}-\binom{m}{2}}$ 种. (注意有的可能记重了)

如果 $n \leq \sqrt{2}^m$, 则

$$\frac{N_0}{2^{\binom{n}{2}}} = \binom{n}{m} 2^{1-\binom{m}{2}} \leq \frac{n^m}{m!} 2^{1-\binom{m}{2}} \leq \frac{(\sqrt{2}^m)^m}{m!} 2^{1-\binom{m}{2}} = \frac{2^{\frac{m}{2}+1}}{m!} < 1.$$

所以存在一种 K_n 的红-蓝着色, 使得其不含各边同色的子图 K_m.

取 $n = R_2(m,m)$, 若 $n \le \sqrt{2}^m$, 则有一种对 K_n 边的红-蓝染色使其不含各边同色的 K_m, 这与 Ramsey 数的定义矛盾 (必须有至少一个 K_m 全蓝或全红.), 因而必有 $n > \sqrt{2}^m$. □

由定理4.3.1, $R_2(m,m) \le \binom{2m-2}{m-1} \le 4^{m-1}$, 所以 $\sqrt{2} < \sqrt[m]{R_2(m,m)} \le 4$. Erdös 问题: $\lim\limits_{m\to\infty} \sqrt[m]{R_2(m,m)}$ 是否存在?

Erdös 多次用下面这个比喻来说明求 Ramsey 数的困难程度. 假设一群外星人入侵地球, 并威胁说如果地球上的人类不能在一年内求出 $R_2(5,5)$ 的值, 他们就要消灭人类. 此时我们最好的策略也许是动员地球上所有计算机和计算机科学家来解决这个问题, 以使人类免遭灭顶之灾. 然而, 如果外星人要求我们求出 $R_2(6,6)$, 那么我们除了对这批入侵者发动先发制人的打击外, 别无其它选择.

定理 4.3.3. Greenwood, Gleason

$R_2(\underbrace{3,3,\cdots,3}_{t个}) \le \lfloor t!e \rfloor + 1$.

证明: 注意

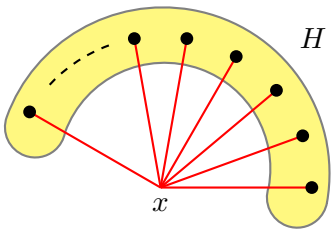
$$0 < t!e - t!\sum_{s=0}^{t}\frac{1}{s!} = t!\left(\frac{1}{(t+1)!} + \frac{1}{(t+2)!} + \cdots\right)$$
$$< \frac{1}{t+1} + \sum_{j=1}^{\infty}\frac{1}{(t+j)(t+j+1)} = \frac{2}{t+1} \le 1,$$

所以如果 $t > 1$, 则

$$\lfloor t!e \rfloor = \sum_{s=0}^{t}\frac{t!}{s!} = 1 + t\sum_{s=0}^{t-1}\frac{(t-1)!}{s!} = 1 + t\lfloor (t-1)!e \rfloor.$$

下面对 t 归纳来证明欲证命题. $R_2(3) = 3 = \lfloor 1!e \rfloor + 1$ 正确,

假设 $t > 1$ 且 $R_2(\underbrace{3,3,\cdots,3}_{t-1个}) \le \lfloor (t-1)!e \rfloor + 1$, 设 G 为 $\lfloor t!e \rfloor + 1$ 阶完全图, 用 t 种颜色对 G 的边染色, 连接顶点 x 的边的条数是 $d_G(x) = \lfloor t!e \rfloor = t\lfloor (t-1)!e \rfloor + 1$, 故由抽屉原理, 有至少 $\lfloor (t-1)!e \rfloor + 1$ 条由 x 连出的边同色, 比如叫红色.



由红边连接 x 的那些点导出的完全子图记为 H, 则 $|H| = \lfloor (t-1)!e \rfloor + 1$. 如果 H 中不含红边, 由归纳假设, H 中必有同色三角形. 如果 H 中含红边 uv, 则可以得到红色三角形 uvx. 因此 $H \cup \{x\}$ 必有同色三角形. □

§ 4.4 几个著名定理

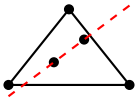
4.4.1 Erdös-Szekeres 定理

平面上 n 个点中, 如果把任两点相连, 得到的外围边界构成一个凸多边形叫做那 n 个点的**凸包**.

定理 4.4.1. Erdös-Szekeres, 1935

任给 $n \geq 3$, 如果平面上有足够多的任三点不共线的点, 则必可选出 m 个使其为凸 m 边形的顶点.

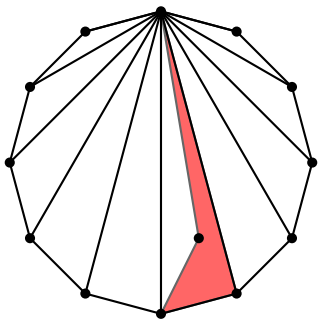
证明: (1) 设 $P_1, \cdots, P_5$ 是五个点, 任三点不共线, 下证必有 4 个点构成凸四边形的顶点. 由于 5 个点的凸包是个凸 q 多边形 ($q \in \{3,4,5\}$), 如果 $q=3$, 连接三角形内部的两点, 总有两个点在这条直线同侧, 连接这两个点与两个内点即可得到凸四边形; 如果 $q=4$ 或 5, 结论平凡.



(2) 设平面上有 $n \geq R_4(5,m)$ 个点 $P_1, \cdots, P_n$, 它们任三点不共线. 对 $S=\{P_1, \cdots, P_n\}$ 的四元子集 $\{P_i, P_j, P_k, P_l\}$, 若它是凹四边形的顶点, 则把这个四元子集放进第一个抽屉中 (叫凹抽屉), 若它是凸四边形的顶点, 则把这个四元子集放进第二个抽屉中 (叫凸抽屉).

由于 $n \geq R_4(5,m)$, 则如下两种情况至少有一种发生: (i)S 有五个点, 其任意四点都是凹四边形顶点, (ii)S 有 m 个点, 其任意四点都是凸四边形顶点. 但是由 (1), 情况 (i) 不可能发生, 所以情况 (ii) 必定成立.

设 $P_1, \cdots, P_m$ 中任四点都是凸四边形顶点, 这 m 个点的凸包是个凸 q 边形 ($q \leq m$), 若 $q=m$, 这就是欲证结论. 若 $q<m$, 把 q 个点划分为三角形, 则必有一个内点在某个三角形中, 于是可以找到一个凹四边形 (如下图), 这与 m 个点中任意四点都是凸四边形矛盾, 故必有 $q=m$. 因此, $P_1, \cdots, P_m$ 就是凸 m 边形的顶点. □



Erdös-Szekeres 数 $ES(m)$ 定义为最小的正整数 n, 使得如果平面上有 n 个任三点不共线的点, 都可以选 m 个使得其为凸 m 边形的顶点. 由刚才的证明, $ES(m) \leq R_4(5,m)$.

Erdös-Szekeres 证明了 $2^{m-2}+1 \leq ES(m) \leq \binom{2m-4}{m-2}+1$.

猜想: $ES(m)=2^{m-2}+1$(目前还没解决).

4.4.2 Schur 定理

下面的 Schur 定理提出于 1916 年, 早于 Ramsey 定理.

定理 4.4.2. Schur,1916

把 $1, \cdots, \lfloor n!e \rfloor$ 放入 n 个抽屉中, 则方程 $x+y=z$ 在某个抽屉中有解.

证明: 让 $A_k = \{$第k个抽屉中的数$\}$, $\mathscr{A}_k = \{\{i,j\} : 1 \leq i < j \leq \lfloor n!e \rfloor + 1$且$j-i \in A_k\}$, $(k=1,2,\cdots,n)$ (把二元子集分类), 则 $\mathscr{A}_1 \cup \cdots \mathscr{A}_n$ 是 $\mathcal{P}_2(S)$ 的一个有序分划, 其中, $S=\{1, \cdots, \lfloor n!e \rfloor + 1\}$. 由定理4.3.3,

$$|S| = \lfloor n!e \rfloor + 1 \geq R_2(\underbrace{3,3,\cdots,3}_{n\text{个}}),$$

则 S 有个 3 元子集 $\{a,b,c\}(a<b<c)$, 使其任意二元子集都在同一个 $\mathscr{A}_k$ 中.

所以 $x=b-a\in A_k, y=c-b\in A_k, z=c-a\in A_k$, 且 $x+y=z$. □

用 **Schur 数** $s(n)$ 表示具有下述性质的最大正整数: 可把 $\{1,2,\cdot,s(n)\}$ 划分成 n 类, 使得 $x+y=z$ 在它的每类中无解. (即 $s(n)+1$ 满足 Schur 定理)

由 Schur 定理, $s(n)=\lfloor n!e\rfloor$. 可以精确求出 $s(1)=1, s(2)=4, s(3)=13, s(4)=44$. 当 $n>5$ 时, $s(n)\geq\dfrac{3^n+1}{2}$(Schur), 且 $s(n)>C\cdot 315^{\frac{n}{5}}$(Fredricksen), 其中 C 是某个常数.

让 $t(n)$ 表示最大整数 m 使得可以把 $\{1,\cdots,m\}$ 分成 n 类, 使得 $x+y\equiv z(\mathrm{mod}\ m+1)$ 在任一类中无解, 则 $t(m)\leq s(m)$. Abbott 猜想: $t(m)=s(m)$.

4.4.3 (*)van der Waerden 定理

把**算术级数**定义为公差不为 0 的等差数列. 1927 年, B.L.van der Waerden 给出了下面定理的证明.

定理 4.4.3. van der Waerden

任给正整数 k 与 m, 若 n 足够大 $(n\geq w(k,m))$, 把 $1,\cdots,n$ 放入 k 个抽屉中, 必有某个抽屉包含长为 m 的算术级数. 把 $w(k,m)$ 叫 **van der Waerden 数**.

Schur 的学生 R.Rado 研究了方程组的整数解: 可以把 $x+y=z$ 推广到 $x_2-x_1=x_3-x_2=\cdots=x_m-x_{m-1}$, 即 $x_i+x_{i+2}=2x_{i+1}$, 其中 $i=1,2,\cdots,m-2$.

定理 4.4.4. Rado

设 $A=(a_{ij})_{1\leq i\leq n,1\leq j\leq n}, a_{ij}\in\mathbb{Z}$, 线性方程组

$$A\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}=\begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix}\tag{4.2}$$

是 partition regular(指把正整数涂成有限种颜色后，方程组 (4.2) 有同色解) 的充分必要条件是可把 A 的列向量适当重排后, 有正整数 $1\leq n_1<n_2<\cdots<n_l=n$, 使得前 $n_k(1\leq k\leq l)$ 个列向量都是前 n_{k-1} 个列向量的有理系数线性组合 (约定 $n_0=0$).

设 $a_1,\cdots,a_m\in\mathbb{Z}^+(m\geq 2)$, **二色 Rado 数** $R(a_1,\cdots,a_m)$ 是最小的正整数 N, 使得把 $1,\cdots,N$ 涂上两种颜色后, 方程 $a_1x_1+\cdots+a_mx_m=x_0$ 有同色解 $(1\leq x_i\leq N)$. 2005 年 B.Hopkins 和 D.Schaal 猜想: $R(a_1,\cdots,a_m)=av^2+v-a$. 其中, $a=\min\{a_1,\cdots,a_m\}$, $v=\sum_{i=1}^{m}a_i$. 孙智伟和他的学生郭嵩证明了此猜想, 在 2008 年发表在了 [J.Combin.Theory.Ser.Amer.2008].

对集合 S, 记 $S^n=\underbrace{S\times\cdots\times S}_{n个}=\{(x_1,\cdots,x_n)|x_i\in S\}$, 如果 $I\cup J$ 是 $\{1,\cdots,n\}$ 的一个分划, $I\cap J=\varnothing$, 映射 $f:J\to S$. 称 S^n 的子集 $L=\{(x_1,\cdots,x_n)\in S^n|i,i'\in I$时$,x_i=x_{i'};$当$j\in J$时$x_j=f(j)\}$ 为由划分 $f:I\cup J$ 与映射 $f:J\to S$ 决定的 S^n 的**组合直线**.

例如, 设 $S=\{1,2,3,4,5,6\}, f(3)=2, f(5)=1, I=\{1,2,4,6\}, J=\{3,5\}$, 则 $L=\{(x_1,\cdots,x_6)\in S^6|x_3=2,x_5=1,x_1=x_2=x_4=x_6\in S\}$.

下面的 Hales-Jewett 定理指出了 van der Waerden 定理的本质是个组合数学的定理.

定理 4.4.5. Hales-Jewett

任给正整数, n 足够大 ($n \geq h(s,t)$) 时, 下面的性质成立: 如果 $|S| = s$, 用 t 种颜色对 S^n 中的点着色后, S^n 中总有各点同色的组合直线.

下面用 Hales-Jewett 定理证明 van der Waerden 定理. (任给正整数 s 与 t, 若 n 足够大 ($n \geq w(k,m)$), 把 $0,\cdots,n-1$ 用 t 种颜色着色后, 必有一个同色类包含长为 s 的算术级数.)

证明: 让 $h = h(s,t)$. 当 $n \geq h$ 时, 把 S^n 中的点用 t 种颜色着色后, S^n 中必有同色的组合直线. 下证可取 $w = s^h$. 让 $S = \{0,1,\cdots,s-1\}, X = \{0,1,\cdots,s^h-1\}$, 作 $\varphi : S^h \to X$ 如下:

$$\varphi((x_1,\cdots,x_h)) = x = x_1 + x_2 s + \cdots + x_h s^{h-1}.$$

则 φ 是双射 (把 X 中元对应于它的 s 进制表示, 两种涂色方式一致.)

由 Hales-Jewett 定理, S^h 包含各点同色的组合直线

$$\begin{aligned} L &= \{(x_1,\cdots,x_h) \in S^h | \text{当} j \in J \text{时}, x_j = f(j) \text{固定}, \text{当} i \in I = \{1,\cdots,h\} \setminus J \text{时}, x_i \text{ 全相等.}\} \\ &= \{(x_1^{(l)},\cdots,x_h^{(l)}) | l = 1,2,\cdots,s; \text{当} j \in J \text{时}, x_j^{(l)} = f(j), \text{当} i \in I \text{时}, x_i^{(l)} = l-1.\} \end{aligned}$$

则

$$\varphi((x_1^{(l)},\cdots,x_n^{(l)})) = \sum_{k=1}^{h} x_k^{(l)} s^{k-1} = \sum_{j\in J} f(j)s^{j-1} + (l-1)\underbrace{\sum_{i\notin J} s^{i-1}}_{\text{公差}}, l = 1,2,\cdots,s. \square$$

Erdös-Graham 猜想 (后来被 Croot 证明): 把大于 1 的整数放入有限个抽屉中, 则某个抽屉中有不同的 $x_1,\cdots,x_m$, 使得 $\dfrac{1}{x_1} + \cdots + \dfrac{1}{x_m} = 1$.

下面的 Szemerédi 定理原为 Erdös-Turán 猜想 (1936). 这个定理揭示了 A 元素个数足够多, 超过了“平均数”, 则 A 包含算术级数.

定理 4.4.6. Szemerédi

设 $0 < \delta \leq 1, k \geq 3$, 则有一个正常数 $N(k,\delta)$, 使得 $n \geq N(k,\delta), A \subset \{1,\cdots,n\}, |A| \geq \delta n$, 则 A 包含长为 k 的算术级数.

$k = 3$ 的情况由 Roth 于 1952 年证明 (用了解析数论和调和分析). $k = 4$ 的情况由 Szemerédi 于 1969 年用纯组合证明. 在 1974 年, Szemerédi 证明了上述结论对任意 k 都成立, 他的证明用了很多组合技巧, 比如 Szemerédi 正则化思想. 1977 年, H.Furstenberg 给了另一个用了遍历论的证明. 2001 年, W.T.Gowers 嫌证明太长, 想简化证明, 走了 Roth 的路子, 用调和分析与关于和集的 Freeman 定理给了证明, 可以给出更好的上界, 但是事实上他的论文页数更多. 目前做到的最好结果是

$$C^{(\log\frac{1}{\delta})^{k-1}} \leq N(k,\delta) \leq 2^{2^{\delta^{-2^{2^{k+9}}}}}.$$

上界就是由 Gowers 证明出来的.

Erdös-Turán 猜想: 设 $a_1 < a_2 < \cdots$ 是正整数序列, $\displaystyle\sum_{n=1}^{\infty} \frac{1}{a_n}$ 发散, 则 $\{a_n\}_{n=1}^{\infty}$ 包含长为 k 的等差子数列.

Green-Tao 定理 (2004): 任给 $k \geq 3$, 可以找到 k 个素数成等差数列.

很明显 Green-Tao 定理是 Erdös-Turán 猜想的特殊情形. Green-Tao 定理的证明同时用了遍历论、解析数论、调和分析、伪随机测度、Szemerédi 定理. 目前用电脑找, 最多只能找到长度是

26 的素数等差数列, 而且第一项是

$$p_1 \geq 2^{2^{2^{2^{2^{2^{2^{2^{100k}}}}}}}}.$$

2019 年, 据说有人证明了 Erdös-Turán 猜想中的 $k=3$ 的情形.

第四章习题

1. 设 $n, a_1, \cdots, a_{n+1} \in \mathbb{Z}^+$, 证明: 存在 $a_i, a_j (1 \leq i < j \leq n+1)$, 使得 $n|(a_j - a_i)$.
2. 证明: $R_k(\underbrace{3,3,\cdots,3}_{k个}) \leq (k+1)!$.

   参考: https://www.zhihu.com/question/505372092/answer/2266837220
3. 设 $n \geq R_2(\underbrace{q,\cdots,q}_{k个})$, $A_1 \cup \cdots \cup A_k$ 是 $S = \{1, 2, \cdots, n\}$ 的一个分划, 证明方程 $x_1 + \cdots + x_{q-1} = x_q$ 在某个 A_j 中有解.

第 5 章　相异代表系

§5.1　Hall 定理

定义 5.1.1

设 $A_1,\cdots,A_n$ 是集合.

- 若 $a_1\in A_1,\cdots,a_n\in A_n$, 则称 $a_1,\cdots,a_n$ 为 $A_1,\cdots,A_n$ 的**代表系**.
- 若 $a_1\in A_1,\cdots,a_n\in A_n$, 且 $a_1,\cdots,a_n$ 两两不同, 称 $a_1,\cdots,a_n$ 为 $A_1,\cdots,A_n$ 的**相异代表系 (SDR, system of distinct representatives)**.

下面定理与二部图的匹配问题有关：如果有 n 个男生、n 个女生, A_k 为第 k 个男生喜欢的女生的集合. Hall 定理表明, 对于 $\varnothing\neq I\subseteq\{1,\cdots,n\}$, 有: 任取若干男生, 把他们喜欢的女生放在一起, 女生的个数都多于选取的男生个数 $\Leftrightarrow$ 每个男生可找到自己喜欢的女生做老婆.

定理 5.1.1. Hall, 1935

设 S 是集合, $S_1,\cdots,S_m$ 是其子集, 则 $M(S)=(S_1,\cdots,S_m)$ 有 SDR 的充分必要条件是对任何 $I\subseteq\{1,\cdots,n\}$, 都有 $\left|\bigcup\limits_{i\in I}A_i\right|\geq|I|$. 而且当 $M(S)$ 有 SDR 时, SDR 的个数 N 满足

$$N\geq\prod_{j=0}^{\min\{m,|S_1|,\cdots,|S_m|\}-1}(\min\{|S_1|,\cdots,|S_m|\}-j).\tag{5.1}$$

证明: "⇒" 若 $M(S)=(S_1,\cdots,S_m)$ 有 SDR$(a_1,\cdots,a_m)$, 则 $I\subseteq\{1,\cdots,n\}$ 时,

$$\bigcup_{i\in I}A_i\supseteq\{a_i:i\in I\}\Rightarrow\left|\bigcup_{i\in I}A_i\right|\geq|\{a_i:i\in I\}|=|I|.$$

"⇐" : 下面对 m 归纳证明: $\left|\bigcup\limits_{i\in I}S_i\right|\geq|I|$ 对任意 $I\subseteq\{1,\cdots,m\}$ 成立 $\Rightarrow$(5.1) 式成立.

当 $m=1$ 时, $|S_1|\geq1$, 当 $a_1\in S_1$ 时, $a_1\in S_1$ 时, a_1 是个 SDR, SDR 数目 $=|S_1|$, 故 (5.1) 式成立.

下设 $m>1$ 且 m 更小时结论正确, 又设对 $I\subseteq\{1,\cdots,m\}$ 有 $\left|\bigcup\limits_{i\in I}S_i\right|\geq|I|$.

情形 1: $\varnothing\neq I\subset\{1,\cdots,m\}$ 时, $\left|\bigcup\limits_{i\in I}S_i\right|>|I|$, 此时, 取 $a_1\in S_1$, 记 $M'(S)=(S_2\setminus\{a\},\cdots,S_n\setminus\{a\})$, $I\subseteq\{2,\cdots,m\}$ 时,

$$\left|\bigcup_{i\in I}(S_i\setminus\{a\})\right|=\left|\bigcup_{i\in I}S\setminus\{a\}\right|\geq|I|,$$

由归纳假设, $M'(S)$ 有 SDR, 且其 SDR 个数 N' 满足

$$\begin{aligned} N'(S) &\geq \prod_{j=0}^{\min\{m-1,|S_2\setminus\{a\}|,\cdots,|S_m\setminus\{a\}|\}-1} (\min\{|S_2\setminus\{a\}|,\cdots,|S_m\setminus\{a\}|\}-j) \\ &\geq \prod_{j=0}^{\min\{m,|S_2|,\cdots,|S_m|\}-2} (\min\{|S_2|,\cdots,|S_m|\}-j-1) \\ &\xlongequal{j+1=i} \prod_{i=1}^{\min\{m,|S_2|,\cdots,|S_m|\}-1} (\min\{|S_1|,\cdots,|S_m|\}-i), \end{aligned}$$

所以 $M'(S)$ 的一个 SDR$(a_2,\cdots,a_m)$ 与 $a_1\in S_1$ 可以组合成 $M(S)$ 的一个 SDR$(a_1,\cdots,a_m)$. 故 $M(S)$ 的 SDR 数目 N 满足

$$N\geq |S_1|N\geq \prod_{i=0}^{\min\{m,|S_2|,\cdots,|S_m|\}-1} (\min\{|S_1|,\cdots,|S_m|\}-i).$$

情形 2: 有 $\varnothing\neq I\subsetneq\{1,\cdots,m\}$, 使得 $\left|\bigcup_{i\in I}S_i\right|=|I|(\geq|S_i|)$. 当 $J\subseteq I$ 时, $\left|\bigcup_{i\in J}S_i\right|\geq|J|, |I|<m$, 由归纳假设 $M_I(S)=(S_i)_{i\in I}$ 有 SDR, 且其 SDR 个数 N_I 满足

$$\begin{aligned} N_I &\geq \prod_{j=0}^{\min\{|I|,\min_{i\in I}|S_i|\}-1} \left(\min_{i\in I}|S_i|-j\right) \\ &= \prod_{j=0}^{\min\limits_{i\in I}|S_i|-1} \left(\min_{i\in I}|S_i|-j\right) \qquad (\text{注意 } |I|\geq|S_i|) \\ &= \left(\min_{i\in I}|S_i|\right)! \end{aligned}$$

对于 $M_I(S)$ 的一个 SDR $D_I=(a_i|i\in I)$(先取好 $(a_i)_{i\in I}$), 让

$$M_I'(S)=(S_j\setminus\{a_i|i\in I\}|j\in I^c),$$

(S_j 的代表元与已经取的不一样, 找 SDR. 注意 $|I^c|<m$, 所以可以用归纳假设.)

当 $J\subseteq I^c$ 时, 可得

$$\begin{aligned} \left|\bigcup_{j\in J}(S_j\setminus\{a_i|i\in I\})\right|+|I| &\geq \left|\bigcup_{j\in J}(S_j\setminus\underbrace{\{a_i|i\in I\}}_{\text{都在 }S_i})\cup\bigcup_{i\in I}S_i\right| \\ &= \left|\bigcup_{i\in I\cup J}S_i\right|\geq|I\cup J|=|I|+|J|. \end{aligned}$$

所以 $\left|\bigcup_{j\in J}(S_j\setminus\{a_i|i\in I\})\right|\geq|J|$. 由归纳假设, $M_I'(S)$ 有 SDR.

则 $M_I'(S)$ 的 SDR 与 $M_I(S)$ 的 SDR 组合在一起, 有 $M(S)=(S_1,\cdots,S_m)$ 的 SDR, 故

$$M(S)\text{的 SDR 数目}N\geq N_I\geq\left(\min_{i\in I}|S_i|\right)!\geq\prod_{j=0}^{\min\{m,|S_1|,\cdots,|S_m|\}-1}\left(\min_{1\leq i\leq m}|S_i|-j\right).$$

□

推论 5.1.2

设 $M(S)=(S_1,\cdots,S_m)$ 是集合 S 的一个子集列, 若满足:
(1) 每个子集至少含有 n 个元素, 且
(2) 每个 $a\in S$ 属于 $S_1,\cdots,S_m$ 中至多 n 个子集, 则 $M(S)$ 有 SDR.

证明: $I\subseteq\{1,\cdots,m\}$ 时, 由条件 (2),

$$n\Big|\bigcup_{i\in I}S_i\Big|\geq\sum_{i\in I}|S_i|\geq n|I|,$$

所以 $\Big|\bigcup_{i\in I}S_i\Big|\geq|I|$. 由 Hall 定理, $M(S)$ 有 SDR. □

注: Hall 定理的证明太啰嗦, 下面是孙智伟对这个定理的证明.

定理 5.1.3. 孙, Proc AMS, 129(2001)p3129-3131

设 $A_1,\cdots,A_n(n\geq1)$ 为 X 的子集, 且 $\{a_i\}_{i=1}^n$ 为 $\{A_i\}_{i=1}^n$ 的一个 SDR, 则有 $n\in J\subseteq\{1,\cdots,n\}$ 使得 X 中恰有 $\Big|\bigcup_{j\in J}A_j\Big|-|J|+1$ 个元素 a, 使 a 与 $a_1,\cdots,a_{n-1}$ 适当排序后可以组成 $\{A_i\}_{i=1}^n$ 的 SDR, 而且 $i\notin J$ 时, A_i 的代表元是 a_i.

根据上面定理, 由 $n-1$ 的情况推 n 的情况 (加元素并排序) 就证出来了, 从而可以直接归纳证明 Hall 定理.

证明: (1) 考虑一个连通图 G, 顶点是 $1,\cdots,n$, 且 i,j 之间有边当且仅当 $i\neq n$ 且 $a_i\in A_j$. 记

$$J=\{1\leq j\leq n:\text{存在 }G\text{ 中 }j\text{ 到 }n\text{ 的通路}\}.$$

(路经过的顶点都不同) 并记 $A=\bigcup_{j\in J}A_j$. 对任意 $i=1,2,\cdots,n-1$, 有:

$$\begin{aligned}a_i\in A&\Leftrightarrow a_i\in A_j,\text{对某个}j\in J\\&\Leftrightarrow\text{存在 }G\text{ 中从 }i\text{ 到某个 }j\in J\text{ 的边}\\&\Leftrightarrow G\text{ 包含一个从 }i\text{ 到 }n\text{ 的路}\Leftrightarrow i\in J.\end{aligned}$$

所以 $\{1\leq i<n:a_i\in A\}=J\setminus\{n\}$.

记集合 $B=A\setminus\{a_i:i\in J\setminus\{n\}\}$, 则 $|B|=|A|-|J|+1$, 且 $B\cup\{a_1,\cdots,a_{n-1}\}=\varnothing$. ($a_i\in B\Rightarrow a_i\in A\Rightarrow i\in J\setminus\{n\}\Rightarrow a_i\notin B$, 矛盾).

(2) 接下来证明 "$a,a_1,\cdots,a_{n-1}$ 可以组合成 $\{A_i\}_{i=1}^n$ 的 SDR, 且 $i\notin J$ 时用 a_i 代表 A_i" $\Leftrightarrow$ "$a\in B$".

让 $a\in X$, 如果 a 和 $a_1,\cdots,a_{n-1}$ 可以重新排列组成 $\{A_i\}_{i=1}^n$ 的 SDR, 其中 a_i 是 A_i 的代表元 ($i\notin J$), 则由于 a 是某个 A_j 的代表元 ($j\in J$), 则 $a\in B$.

反过来, 如果 $a\in B$, 则对某个 $j\in J$ 有 $a\in A_j$.

若 $j=n$, 则 $a_n=a\in A_n$, 故 $(a_1,\cdots,a_n)$ 是 $(A_1,\cdots,A_n)$ 的 SDR, 且当 $i\notin J$ 时, A_i 的代表元是 a_i.

若 $j\neq n$, 则 G 包含从 j 到 n 的路 $j_0j_1\cdots j_l$, 其中 $j_0=j,j_l=n$. 注意 $I=\{j_0,\cdots,j_l\}\subseteq J$. 令 $b_{j_0}=a,b_{j_1}=a_{j_0},\cdots,b_{j_l}=a_{j_{l-1}}$, 则当 $i\in I$ 时, $b_i\in A_i$. 这里如果 $i\notin I$, 我们记 $b_i=a_i$, 用原来的代表元 a_i 来代表 A_i, 所以 $\{b_i\}_{i=1}^n$ 是 $\{A_i\}_{i=1}^n$ 的 SDR. (需要验证一下各个 a_i 两两不同)

由上, $a \in X$ 可以与 $a_1, \cdots, a_{n-1}$ 组合成 $\{A_i\}_{i=1}^n$ 的 SDR, 使得 $i \notin I$ 时, 仍用 a_i 代表 $A_i \Leftrightarrow a \in B$. 而且 $|B| = |A| - |J| + 1$. □

定理 5.1.4. 亏量形式的 Hall 定理

集合 S 的子集列 $M(S) = (S_1, \cdots, S_m)$ 具有 (至少)$m-d$ 个相异代表元 $\Leftrightarrow$ 对任何 $I \subseteq \{1, \cdots, m\}$, 有

$$\left|\bigcup_{i\in I} S_i\right| \geq |I| - d. \tag{5.2}$$

证明: 取 d 元集 T 使得 $S \cap T = \varnothing$. $(S_1, \cdots, S_m)$ 具有至少 $m-d$ 个相异代表元 $\Leftrightarrow S \cup T$ 的子集列 $(S_1 \cup T, \cdots, S_m \cup T)$ 有 SDR. (剩下 d 个代表元从 T 中取, 得到 m 个相异代表元.) $\Leftrightarrow$ 对任何 $I \subseteq \{1, \cdots, m\}$, 有 $\left|\bigcup_{i\in I}(S_i \cup T)\right| \geq |I| \Leftrightarrow \left|\bigcup_{i\in I} S_i\right| \geq |I| - |T| = |I| - d$. □

注: 相异代表系的情况就是 $d = 0$. 如果 $d = 0$ 取不到, 我们希望尽可能找到小的 d. 根据此定理, 满足 (5.2) 式的最大 $m-d$ 值为 $\min\left\{m - |I| + \left|\bigcup_{i\in I} S_i\right| : I \subseteq \{1, \cdots, m\}\right\}$. 所以

$$\max_{\substack{M'(S)\subseteq M(S)\\ M'(S)\text{有 SDR}}} |M'(S)| = \min\left\{m - |I| + \left|\bigcup_{i\in I} S_i\right| : I \subseteq \{1, \cdots, m\}\right\}. \tag{5.3}$$

Hall 定理的本质就是解上面的方程.

5.1.1 Hall 定理在拉丁矩形的应用

定义 5.1.2

设 $\boldsymbol{A} = (a_{ij})_{r\times s}$, $r, s \leq n$. 如果 $\boldsymbol{A}$ 每行都是 n 元集 S 的一个 s-排列, 每列都是 n 元集 S 的一个 r-排列. (即每行每列元素都从 S 中取且互不相同). 则称 $\boldsymbol{A}$ 是基于集合 S 的 $r \times s$ **拉丁矩形 (Latin rectangle)**. n 元集上的 $n \times n$ 拉丁矩形叫**拉丁方 (Latin square)**.

例如, 下面的矩阵是一个 5 阶拉丁方:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \\ 4 & 5 & 1 & 2 & 3 \\ 3 & 4 & 5 & 1 & 2 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

数独问题的解是一个 9 阶拉丁方.

下面的定理是关于小的拉丁矩形一定可以扩充为大的拉丁方的一个结果.

定理 5.1.5

任一个基于 $S = \{1, \cdots, n\}$ 的 $r \times n$ 拉丁矩形 $(r < n)$ 可以扩展为一个 n 阶拉丁方.

证明: 只需证 $r < n$ 时, 基于 $S = \{1, \cdots, n\}$ 的 $r \times n$ 拉丁矩形 $\boldsymbol{A}$ 可以扩展为 $(r+1) \times n$ 拉丁矩形 $\widetilde{\boldsymbol{A}}$. 取 $S_j \subseteq S$ 如下: $i \in S_j \Leftrightarrow i$ 不在 $\boldsymbol{A}$ 的第 j 列中出现.

由于 i 在 $\boldsymbol{A}$ 的每行中出现一次, 而这些 i 处于不同列, 故恰有 $n-r$ 列不含 i, 即 i 只属于 $S_1, \cdots, S_n$ 中的 $n-r$ 个, 所以 $|S_j| = n - r$. 由推论5.1.2, $(S_1, \cdots, S_n)$ 有 SDR$(a_1, \cdots, a_n)$, 这是

$1,\cdots,n$ 的一个排列. 让 $\widetilde{\boldsymbol{A}}=\begin{pmatrix} & \boldsymbol{A} & \\ a_1 & \cdots & a_n \end{pmatrix}$, 当 $1\le j\le n$ 时, $a_j\in S_j$, 则 a_j 不在 $\boldsymbol{A}$ 的第 j 列出现, 故 $\widetilde{\boldsymbol{A}}$ 每列元素都各不相同. □

§5.2 公共代表系

设集合 T 有两个分划:

$$T=A_1\cup A_2\cup\cdots\cup A_m, \tag{5.4}$$

$$T=B_1\cup B_2\cup\cdots\cup B_m, \tag{5.5}$$

其中 $\{A_i\}_{i=1}^m,\{B_i\}_{i=1}^m$ 分别两两不交且各个 A_i,B_i 非空. 我们希望找公共代表元同时是这两个分划的代表系.

定义 5.2.1

若 m 元集 E 与每个 A_i 与每个 B_j 都有公共元, 即

$$|E\cap A_i|=1,|E\cap B_j|=1,i,j=1,2,\cdots,m.$$

则称 E 是这两个分划的**公共代表系 (SCR, system of common representatives)**.

下面定理是 T 有 SCR 的充分必要条件.

定理 5.2.1

设 (5.4)(5.5) 是 T 的两个分划, 则它们有 SCR $\Leftrightarrow$ 对每个 $I\subseteq\{1,\cdots,m\}$, 有

$$\left|\left\{1\le j\le m\middle|B_j\subseteq\bigcup_{i\in I}A_i\right\}\right|\le|I|.$$

证明: "$\Rightarrow$": 设 E 是 SCR, $J=\left\{1\le j\le m\middle|B_j\subseteq\bigcup_{i\in I}A_i\right\}$, 注意 $E\cap B_j$ 只有一个元素且 B_j 两两不交, 则

$$|J|=\left|\bigcup_{j\in J}(E\cap B_j)\right|=\left|E\cap\bigcup_{j\in J}B_j\right|\overset{(J\text{ 的定义})}{\le}\left|E\cap\bigcup_{i\in I}A_i\right|=\left|\bigcup_{i\in I}(E\cap A_i)\right|=|I|.$$

"$\Leftarrow$": 让 $S=\{A_1,\cdot,A_m\}$, $S_j=\{A_i|A_i\cap B_j\ne\varnothing,1\le i\le m\},j=1,2,\cdots,m.$

任给 $J\subseteq\{1,\cdots,m\}$, 令 $I=\{1\le i\le m|\text{有}j\in J\text{使得}A_i\cap B_j\ne\varnothing\}$, 则当 $i\in I$ 时, 有 $j\in J$ 使得 $A_i\cap B_j\ne\varnothing$, 所以 $A_i\in S_j$, 故 $\left|\bigcup_{j\in J}S_j\right|\ge|\{A_i|i\in I\}|=|I|$.

对 $j\in J$, 若 $B_j\nsubseteq\bigcup_{i\in I}A_i$, 则由 $B_j\subseteq T=\bigcup_{i\in I}A_i\cup\bigcup_{i\notin I}A_i$, 可知存在 $i\notin I$ 使得 $B_j\cap A_i\ne\varnothing$. 所以 $i\in I$, 矛盾. 所以当 $j\in J$ 时必有 $B_j\subseteq\bigcup_{i\in I}A_i$, 所以 $|I|\ge|J|$.

这样我们就证明了

$$\left|\bigcup_{j\in J}S_j\right|\ge|I|\ge|J|.$$

由 Hall 定理, $(S_1,\cdots,S_m)$ 有 SDR$(A_{i_1},\cdots,A_{i_m})$, 且 $A_{i_1},\cdots,A_{i_m}$ 两两不同, 且 $A_{i_j}\cap B_j\ne\varnothing$.

取 $a_j \in A_{i_j} \cap B_j$, 则 $E = \{a_1, \cdots, a_m\}$ 是两个分划 (5.4)(5.5) 的 SCR. □

推论 5.2.2

设 (5.4)(5.5) 是有穷集 T 的两个分划, 若 $r = |A_1| = \cdots = |A_m| = |B_1| = \cdots = |B_m|$, 则 (5.4)(5.5) 有 SCR.

证明: 当 $I \subseteq \{1, \cdots, m\}$ 时, $\left|\bigcup_{i\in I} A_i\right| = \sum_{i\in I} |A_i| = r|I|$, 则 $\left|\left\{1 \le j \le m | B_j \subseteq \bigcup_{i\in I} A_i\right\}\right| \le |I|$. (若不然, 满足 $B_j \subseteq \bigcup_{i\in I} A_i$ 的 j 个数大于 $|I|$, 从而 $r|I| > r|I|$, 矛盾) 由定理5.2.1, (5.4)(5.5) 有 SCR. □

推论 5.2.3

设 G 是有限群, H 是 G 的子群, $[G : H] = k$. 则有 $g_1 \cdots, g_k \in G$ 使 $g_1H \cup \cdots \cup g_kH$ 为 G 的左陪集分解, 同时 $Hg_1 \cup \cdots \cup Hg_k$ 是 G 的右陪集分解.

证明: 设 $a_1H \cup \cdots \cup a_kH$ 与 $Hb_1 \cup \cdots \cup Hb_k$ 分别是 G 的左、右陪集分解, 则它们也是 G 的两个分划, 且 $|a_1H| = \cdots = |a_kH| = |H| = |Hb_1| = \cdots = |Hb_k|$. 由推论5.2.2, 这两个分划有公共代表系 E, 且 $|E \cap a_iH| = 1$, 记 $g_i \in E \cap a_iH$, 则 $a_iH = g_iH$, 所以 $g_1H \cup \cdots \cup g_kH$ 是 G 的左陪集分解. 另外 $|E \cap Hb_i| = 1$, 记 $g_{i_j} \in E \cap b_jH$, 则 $b_jH = g_{i_j}H$, 所以 $Hg_{i_1} \cup \cdots \cup Hg_{i_k} = Hg_1 \cup \cdots \cup Hg_k$ 是 G 的右陪集分解. □

§5.3 0-1 矩阵

5.3.1 基本定义

对矩阵 $\boldsymbol{A} = (a_{ij})_{1\le i\le m, 1\le j\le n}$, 当 $a_{ij} \in \{0, 1\}$ 时, $\boldsymbol{A}$ 叫 **0-1 矩阵**.

给定 n 元集 $S = \{a_1, \cdots, a_n\}$ 与 S 的子集列 $M(S) = (S_1, \cdots, S_m)$, 当 $1 \le i \le m, 1 \le j \le n$ 时, 让

$$a_{ij} = \begin{cases} 1, & a_j \in S_i, \\ 0, & a_j \notin S_i, \end{cases}$$

则 $(0, 1)$-矩阵 A 叫 S 关于子集列 $(S_1, \cdots, S_m)$ 的**关联矩阵**.

反过来, 任给 $(0, 1)$-矩阵 $\boldsymbol{A} = (a_{ij})_{1\le i\le m, 1\le j\le n}$, 让 S 是 n 元集 $\{a_1, \cdots, a_n\}$, $S_i = \{a_i \in S | 1 \le j \le n且a_{ij} = 1\}$, 则 $(S_1, \cdots, S_m)$ 的子集列, 所以 $a_{ij} = 1 \Leftrightarrow a_j \in S_i$, 因此 $\boldsymbol{A}$ 是 S 关于子集列 $(S_1, \cdots, S_m)$ 的关联矩阵.

于是我们建立了 0-1 矩阵与关联矩阵的一一对应关系.

(0,1)-矩阵 $\leftrightarrow$ 关联矩阵.

0-1 矩阵问题都可以看作组合问题.

若 $(a_{ij})_{n\times n}$ 是方阵, 则**行列式**定义为 $\det(a_{ij})_{n\times n} = \sum_{\sigma\in S_n} \operatorname{sign}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}$. 对于一般的矩阵 $\boldsymbol{A} = (a_{ij})_{m\times n}$, 我们定义**积和式 (permanent)** 为

$$\operatorname{per}(\boldsymbol{A}) \triangleq \sum_{\substack{j_1,\cdots,j_m是\\ 1,\cdots,n的m\text{-}排列}} a_{1j_1} a_{2j_2} \cdots a_{mj_m}. \tag{5.6}$$

特别地, 如果 $\boldsymbol{A}=(a_{ij})_{n\times n}$ 是方阵, 则

$$\mathrm{per}(\boldsymbol{A})=\sum_{\sigma\in S_n}a_{1\sigma(1)}\cdots a_{n\sigma(n)}.$$

定理 5.3.1

设 $M(S)=(S_1,\cdots,S_m)$ 是 n 元集 S 的子集列, $m\le n$, $(0,1)$-矩阵 $\boldsymbol{A}$ 是 $M(S)$ 的关联矩阵, 则 $\mathrm{per}(\boldsymbol{A})$ 等于 $M(S)$ 的 SDR 个数.

证明: 记 $\boldsymbol{A}=(a_{ij})_{1\le i\le m,1\le j\le n}$, 则 $S=(a_1,\cdots,a_n)$. 则 $a_{ij}=1\Leftrightarrow a_j\in S_i$. 注意

$$\begin{aligned}a_{1j_1}a_{2j_2}\cdots a_{mj_m}=1&\Leftrightarrow a_{ij_i}=1(i=1,\cdots,m)\\&\Leftrightarrow a_{j_i}\in S_i(i=1,\cdots,m),\\&\Leftrightarrow (a_{j_1},\cdots,a_{j_m})\text{是}M(S)\text{的 SDR.}\end{aligned}$$

回顾积和式的定义 (5.6), 结论成立. □

定义 5.3.1

设 $\boldsymbol{A}$ 是 $m\times n$ 的 $(0,1)$-矩阵, 把 $\boldsymbol{A}$ 的行或列称为**线 (line)**, $\boldsymbol{A}$ 的一组两两不共线的 1 叫**线性无关 1 组**. $\boldsymbol{A}$ 的线性无关 1 组中所含 1 的个数叫做 $\boldsymbol{A}$ 的**项秩 (term rank)**, 记为 $\rho(\boldsymbol{A})$. 能把 $\boldsymbol{A}$ 中所有 1 覆盖住的一组线叫 $\boldsymbol{A}$ 的**线覆盖**. $\boldsymbol{A}$ 的线覆盖中, 所用的最少线数叫做 $\boldsymbol{A}$ 的**线秩 (line rank)**, 记为 $\lambda(\boldsymbol{A})$.

例 5.3.2

设 $\boldsymbol{A}_1=\begin{pmatrix}1&1&1\\0&0&0\\0&0&0\end{pmatrix}$, $\boldsymbol{A}_2=\begin{pmatrix}1&1&1\\1&0&0\\1&0&0\end{pmatrix}$, $\boldsymbol{A}_3=\begin{pmatrix}1&1&0\\1&0&1\\1&1&0\end{pmatrix}$,

则 $\rho(\boldsymbol{A}_1)=1,\rho(\boldsymbol{A}_2)=2,\rho(\boldsymbol{A}_3)=3$, 且 $\lambda(\boldsymbol{A}_1)=1,\lambda(\boldsymbol{A}_2)=2,\lambda(\boldsymbol{A}_3)=3$.

定理 5.3.3. König-Egerváry, 1931

$(0,1)$-矩阵 $\boldsymbol{A}=(a_{ij})_{\substack{1\le i\le m\\1\le j\le n}}(m\le n)$ 的线秩等于项秩.

证明: (1) 在 $\boldsymbol{A}$ 中找出 $\rho(\boldsymbol{A})$ 个两两不共线的 1, 把这些 1 盖住至少需要 $\rho(\boldsymbol{A})$ 条线, 故 $\rho(\boldsymbol{A})\le\lambda(\boldsymbol{A})$.

(2) 设 S 是 n 元集 $\{a_1,\cdots,a_n\}$, $S_i=\{a_j|1\le j\le n,a_{ij}=1\}$. 则 $\boldsymbol{A}$ 为 S 关于子集列 $M(S)=(S_1,\cdots,S_m)$ 的关联矩阵. 一个线性无关 1 组 $a_{i_1j_1}=\cdots=a_{i_rj_r}=1$ 对应于 $M'(S)=(S_{i_1},\cdots,S_{i_r})$ 的一个 SDR$(a_{j_1},\cdots,a_{j_r})$, (注意 $a_{i_sj_s}=1\Leftrightarrow a_{j_s}\in S_{j_s}$), 所以

$$\rho(\boldsymbol{A})=\max_{\substack{M'(S)\subseteq M(S)\\M'(S)\text{有 SDR}}}|M'(S)|.$$

(3) 由 (5.3) 式, 我们只需证明

$$\lambda(\boldsymbol{A})\le\rho(\boldsymbol{A})=\min\left\{m-|I|+\left|\bigcup_{i\in I}S_i\right|:I\subseteq\{1,\cdots,m\}\right\}.$$

取 $I\subseteq\{1,\cdots,m\}$ 使得 $m-|I|+\left|\bigcup\limits_{i\in I}S_i\right|$ 达到最小 $\rho(\boldsymbol{A})$ 值, 下面取由 $a_j\in\bigcup\limits_{i\in I}S_i$ 决定的那些第 j 列与 $i\in\{1,\cdots,n\}\setminus I$ 决定的那些第 i 行, 这里一共有 $m-|I|+\left|\bigcup\limits_{i\in I}S_i\right|$ 条线, 这些线覆盖住了所有 1. (对于 $a_{ij}=1$, 如果 $i\in I$, 则 a_{ij} 位于上面取到的某个第 j 列中. 如果 $i\notin I$, 那么 $i\in\{1,\cdots,n\}\setminus I$, 则 a_{ij} 位于上面取到的某个第 i 行中.) □

5.3.2 Birkhoff 定理

设 $\boldsymbol{P}$ 是 $m\times n$ 的 $(0,1)$-矩阵, 若 $\boldsymbol{PP'}$ 是 m 阶单位方阵 $\boldsymbol{I}_m$, 则称 $\boldsymbol{P}$ 为**置换矩阵**.

引理 5.3.4

设 $\boldsymbol{P}$ 是 $m\times n$ 的置换矩阵, 则 $m\leq n$.

证明: $m=r(\boldsymbol{I}_m)=r(\boldsymbol{PP'})\leq\min\{r(\boldsymbol{P}),r(\boldsymbol{P'})\}\leq r(\boldsymbol{P})\leq n$. □

引理 5.3.5

$m\times n$ 的 $(0,1)$-矩阵 $\boldsymbol{P}$ 是置换矩阵 $\Leftrightarrow$ $\boldsymbol{P}$ 的每行恰有一个 1, 每列至多一个 1.

证明: 设 $\boldsymbol{P}=\{p_{ij}\}_{1\leq i\leq m,1\leq j\leq n}$, 则

$$\begin{aligned}\boldsymbol{PP'}=\boldsymbol{I}_m&\Leftrightarrow\sum_{k=1}^{n}p_{ik}p_{jk}=\delta_{ij},(\forall 1\leq i\leq m,1\leq j\leq n)\\&\Leftrightarrow\begin{cases}\sum\limits_{k=1}^{n}p_{ik}^2=1,(i=1,2,\cdots,m),(\text{第 }k\text{ 列恰有一个 }1)\\\sum\limits_{k=1}^{n}p_{ik}p_{jk}=0,(i\neq j),(\text{第 }k\text{ 列不能有两个 }1)\end{cases}\end{aligned}$$

注: n 阶 $(0,1)$-方阵中每行每列都恰有一个 1(这是因为 $\boldsymbol{P},\boldsymbol{P'}$ 都是置换矩阵), 所以 $\boldsymbol{P}$ 中恰有 n 个 1 且两两不共线.

定理 5.3.6

设 $\boldsymbol{A}=(a_{ij})_{m\times n}(m\leq n)$ 不是零矩阵, $a_{ij}\geq 0$. $\boldsymbol{A}$ 的每行各项直和为 $\widetilde{m}$, 每列各项直和为 $\widetilde{n}$, 则有正整数 $c_1,\cdots,c_k$ 与 $m\times n$ 置换矩阵 $\boldsymbol{P}_1,\cdots,\boldsymbol{P}_k$, 使得 $\boldsymbol{A}=c_1\boldsymbol{P}_1+\cdots+c_k\boldsymbol{P}_k$, 且 $\sum\limits_{i=1}^{k}c_i=\widetilde{m}$.

证明: (1) 把 $\boldsymbol{A}$ 变成方阵: 由于 $\boldsymbol{A}$ 是非零矩阵, $\widetilde{m}>0,\widetilde{n}>0$, 让

$$\widetilde{\boldsymbol{A}}=\begin{pmatrix}\boldsymbol{A}\\\frac{\widetilde{m}}{n}\boldsymbol{J}\end{pmatrix}_{n\times n},\text{其中}\boldsymbol{J}=\begin{pmatrix}1&\cdots&1\\\vdots&&\vdots\\1&\cdots&1\end{pmatrix}_{(n-m)\times n},$$

$\widetilde{\boldsymbol{A}}$ 的每行行和为 $\frac{\widetilde{m}}{n}\times n=\widetilde{m}$, 每列列和为 $\widetilde{n}+\frac{\widetilde{m}}{n}(n-m)=\widetilde{n}-\frac{m}{n}\widetilde{m}+\widetilde{m}=\widetilde{m}$. (注意 $m\widetilde{m}=\sum\limits_{i,j}a_{ij}=n\widetilde{n}$.)

(2) 下面把 $\widetilde{\boldsymbol{A}}$ 看作 $(0,1)$-矩阵, 把非零元变成 1 来定义它的项秩 $\rho(\widetilde{\boldsymbol{A}})$ 与线秩 $\lambda(\widetilde{\boldsymbol{A}})$. 断言: $\rho(\widetilde{\boldsymbol{A}})=n$, 即 $\widetilde{\boldsymbol{A}}$ 中有 n 个非零元两两不共线. 事实上, 若 $\rho(\widetilde{\boldsymbol{A}})<n$, 则 $\lambda(\widetilde{\boldsymbol{A}})<n$, 所以可以用 $n-1$ 条线覆盖住 $\widetilde{\boldsymbol{A}}$ 的所有非零元. 于是 $\widetilde{\boldsymbol{A}}$ 的所有项之和不超过 $(n-1)\widetilde{m}(<n\widetilde{m})$, 这与所有项之和为 $n\widetilde{m}$ 矛盾.

(3) 证明方阵情形结论正确: 设 $\widetilde{\boldsymbol{P}}_1$ 是 n 阶置换方阵, 且根据引理5.3.5, 可以让 $\widetilde{\boldsymbol{P}}_1$ 中 1 的位置与 $\widetilde{\boldsymbol{A}}$ 中两两不共线的 n 个非零元位置相同. 设 c_1 是这 n 个非零元中最小的一个数, 则 $\widetilde{\boldsymbol{A}}_1 = \widetilde{\boldsymbol{A}} - c_1\widetilde{\boldsymbol{P}}_1$ 且每项非负, 而且 $\widetilde{\boldsymbol{A}}_1$ 每行行和与每列列和都是 $\widetilde{m} - c_1$. 注意 $\widetilde{\boldsymbol{A}}_1$ 中非零元个数比 $\widetilde{\boldsymbol{A}}$ 的非零元个数少 (c_1 所在位置变成 0 了), 所以可以用归纳法. 若 $\widetilde{\boldsymbol{A}}_1 \neq 0$, 继续上面的过程, 找到 $c_2 > 0$ 与 $\widetilde{\boldsymbol{P}}_2$, 使得 $\widetilde{\boldsymbol{A}}_2 = \widetilde{\boldsymbol{A}}_1 - c_2\widetilde{\boldsymbol{P}}_2$, 且 $\widetilde{\boldsymbol{A}}_2$ 中非零元比 $\widetilde{\boldsymbol{A}}_1$ 少. 有限步之后可以得到 $\widetilde{\boldsymbol{A}} = c_1\widetilde{\boldsymbol{P}}_1 + \cdots + c_k\widetilde{\boldsymbol{P}}_k$.

(4) 把 $\widetilde{\boldsymbol{A}}$ 的后 $n-m$ 行甩掉, 得到非方阵情形. 记 $\boldsymbol{P}_i$ 是由 $\widetilde{\boldsymbol{P}}_i$ 的前 m 行构成, 那么它每行恰有一个 1, 每列至多一个 1, 由引理5.3.5, $\boldsymbol{P}_i$ 是置换矩阵, 而且 $\boldsymbol{A} = c_1\boldsymbol{P}_1 + \cdots + c_k\boldsymbol{P}_k$. 容易验证 $\widetilde{m} = \sum_{i=1}^{k} c_i$. □

推论 5.3.7

设 $\boldsymbol{A}$ 是 $(0,1)$-矩阵, 行和与列和都是 k, 则 $\boldsymbol{A}$ 可以表示成 $\boldsymbol{P}_1 + \cdots + \boldsymbol{P}_k$, 其中 $\boldsymbol{P}_i$ 是置换方阵.

下面设 $\boldsymbol{A} = (p_{ij})_{n\times n}$, 其中 $p_{ij} \geq 0$ 且每条线上各项之和为 1, 则称 $\boldsymbol{A}$ 为**双重随机矩阵**.

推论 5.3.8. G.Birkhoff

设 $\boldsymbol{A}$ 是 n 阶双重随机矩阵, 则 $\boldsymbol{A}$ 可以表成有限个 n 阶置换方阵的凸组合.

设 $\boldsymbol{A} = (a_{ij})_{n\times n}$ 是 n 阶双重随机矩阵, 则

$$0 < \operatorname{per}(\boldsymbol{A}) = \sum_{\sigma\in S_n} a_{1\sigma(1)}\cdots a_{n\sigma(n)} \leq \Big(\sum_{j=1}^{n} a_{1j}\Big)\Big(\sum_{j=1}^{n} a_{2j}\Big)\cdots\Big(\sum_{j=1}^{n} a_{nj}\Big) = 1.$$

取 $\boldsymbol{A} = \frac{1}{n}\boldsymbol{J} = \frac{1}{n}\begin{pmatrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{pmatrix}_{n\times n}$, 则 $\boldsymbol{A}$ 是双重随机矩阵, 且 $\operatorname{per}(\boldsymbol{A}) = \sum_{\sigma\in S_n} \frac{1}{n^n} = \frac{n!}{n^n}$.

1926 年, van der Waerden 猜想: 若 $\boldsymbol{A}$ 是 n 阶双重随机矩阵, 则 $\operatorname{per}(\boldsymbol{A}) \geq \frac{n!}{n^n}$, 且等号成立当且仅当 $\boldsymbol{A} = \frac{1}{n}\boldsymbol{J}$. 1981 年被 G.P.Egorychev 解决.

1963 年有人提出如下猜想: 设 $\boldsymbol{A}$ 是 n 阶 $(0,1)$-矩阵, m_i 是第 i 行的行和, 则 $\operatorname{per}(\boldsymbol{A}) \leq \prod_{i=1}^{n}(m_i!)^{\frac{1}{m_i}}$. 此猜想于 1973 年被解决.

§5.4 极值集论简介

设 S 是 n 元集, $\mathscr{A}$ 是 S 的子集族, 要求 $\mathscr{A}$ 满足某些性质 (关于交、包含、并等), 问 $|\mathscr{A}|$ 的上、下界.

例 5.4.1

要求 $\mathscr{A}$ 中任意两个集合相交非空, 则 $|\mathscr{A}|$ 最大可能值是 2^{n-1} 个. 因为 $A \in \mathscr{A} \Leftrightarrow A^c \notin \mathscr{A}$, 所以 A, A^c 之一在 $\mathscr{A}$ 中.

称 $\mathscr{A}$ 是**链**, 如果 $\mathscr{A}$ 中子集有如下包含关系: $A_1 \subseteq A_2 \subseteq \cdots$.

称 $\mathscr{A}$ 是**反链**, 如果 $\mathscr{A}$ 中的子集互不包含.

定理 5.4.2. Sperner, 1928

设 $\mathscr{A}$ 是 n 元集 S 的子集构成的反链, 则 $|\mathscr{A}| \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}$.

注: 这个界可以达到: 设 $\mathscr{A} = \left\{A \subseteq S : |A| = \left\lfloor \frac{n}{2} \right\rfloor\right\}$, 则 $\mathscr{A}$ 是反链, 且 $|\mathscr{A}| = \binom{n}{\lfloor \frac{n}{2} \rfloor}$.

证明: (Lubell, 1966) 不妨设 $S = \{1, \cdots, n\}$. 对 $A \subseteq S$ 与 $\sigma \in S_n$, 如果 $A = \{\sigma(1), \cdots, \sigma(|A|)\}$, 则称 σ **由** A **开始**.

若 σ 既由 A 开始, 也由 B 开始, 则 $A \subseteq B$ 或 $B \subseteq A$. 由于 $\mathscr{A}$ 是反链, 所以对每个 $\sigma \in S_n$, 至多有一个 $A \in \mathscr{A}$ 使得 σ 由 A 开始.

对每个 $A \in \mathscr{A}$, 有 $|\{\sigma \in S_n | \sigma由A开始\}| = |A|!(n - |A|)!$, 所以

$$n! \geq |\{\sigma \in S_n | \exists A \in \mathscr{A}(\sigma由A开始)\}| = \sum_{A \in \mathscr{A}} |A|!(n - |A|)!.$$

(注意由 A 开始的 σ 与由 B 开始的 σ 不一样，没有包含关系．) 所以 $\sum\limits_{A \in \mathscr{A}} \frac{1}{\binom{n}{|A|}} \leq 1$, 所以

$$\sum_{k=1}^{n} \frac{p_k}{\binom{n}{k}} \leq 1, 其中 p_k = |\{A \in \mathscr{A} : |A| = k\}|. \tag{5.7}$$

不等式 (5.7) 叫 **LYM 不等式**. 由上述不等式, 并注意 $\binom{n}{k}$ 当 $k = \left\lfloor \frac{n}{2} \right\rfloor$ 时取最大, 则

$$|\mathscr{A}| = \sum_k p_k = \binom{n}{\lfloor \frac{n}{2} \rfloor} \sum_k \frac{p_k}{\binom{n}{\lfloor \frac{n}{2} \rfloor}} \leq \binom{n}{\lfloor \frac{n}{2} \rfloor} \sum_k \frac{p_k}{\binom{n}{k}} \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}.$$

□

下面的定理发表在 Quant.J.Math,12(1961), 313-320. 这是极值集论的起源. (Ko 是柯召)

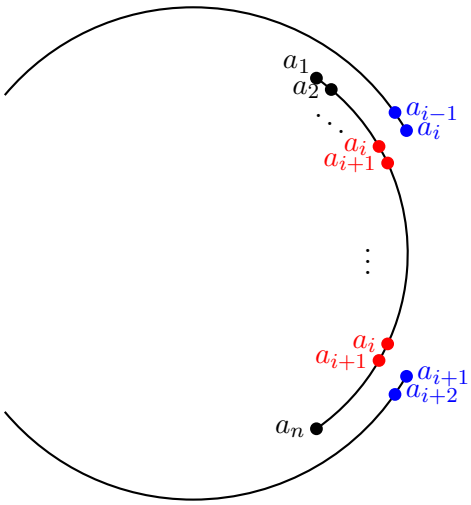
定理 5.4.3. Erdös-Ko-Rado

设 $n \geq 2k > 0$, $\mathscr{A}$ 由 $\{1, \cdots, n\}$ 的一些 k 元子集构成, 且 $\mathscr{A}$ 中子集两两相交非空, 则 $|\mathscr{A}| \leq \binom{n-1}{k-1}$.

注: 等号可以成立: 固定 $m \in S = \{1, \cdots, n\}$, 让 $\mathscr{A} = \{A \subseteq \{1, \cdots, n\} : |A| = k且m \in A\}$, 则 $|\mathscr{A}| = \binom{n-1}{k-1}$.

证明: (O.H.Katona, 1972) 将 $1, \cdots, n$ 随意排列在圆周上, 形成一个圆排列 $(i_1, i_2, \cdots, i_n)$. 考虑长为 k 的区间: $\{i_1, i_2, \cdots, i_k\}$, $\{i_2, \cdots, i_k, i_{k+1}\}$, $\cdots$, $\{i_n, i_1, \cdots, i_{k-1}\}$, 它们至多有 k 个属于 $\mathscr{A}$.

设这样的一个区间 $\{a_1, \cdots, a_k\}$ 属于 $\mathscr{A}$, 则另一个属于 $\mathscr{A}$ 的这样的区间与它相交, 从而有 $1 \leq i \leq k-1$ 使得它恰含 a_i 与 a_{i+1} 中的一个. (如下图.) 如果两个这样的不同区间都恰好含 a_i, a_{i+1} 中的一个, 则这两个区间不相交, 从而不全在 $\mathscr{A}$ 中. 故属于 $\mathscr{A}$ 的区间数不超过 $1 + |\{\{a_i, a_{i+1}\} : i = 1, \cdots, k-1\}| = k$ 个.



下面计算 $N=|\{\langle S,C\rangle : S\in\mathscr{A}, C是1,\cdots,n的圆排列, 且S是C的一个区间\}|$. 对每个 $S\in\mathscr{A}$, 使得 S 是 C 的一个区间的圆排列 C 个数是 $k!(n-k)!$, 所以

$$N=\sum_{S\in\mathscr{A}} k!(n-k)!=|\mathscr{A}|k!(n-k)!.$$

另一方面,

$$N=\sum_{1,\cdots,n圆排列}\underbrace{|\{S\in\mathscr{A}|S是C的一个区间|}_{\leq k}\leq (n-1)!k.$$

由上, $|\mathscr{A}|k!(n-k)!=N\leq (n-1)!k=n!\dfrac{k}{n}$, 故 $|\mathscr{A}|\leq \binom{n}{k}\dfrac{k}{n}=\binom{n-1}{k-1}$. □

若集族 $\mathscr{A}$ 中的集合两两相交为非空, 即 $A,B\in\mathscr{A}\Rightarrow A\cap B\neq\varnothing$, 则称 $\mathscr{A}$ 是**交族**. n 元集合 S 的一个子集族 $\mathscr{A}$ 叫**星族**, 指 $\bigcap\limits_{A\in\mathscr{A}} A\neq\varnothing$.

Chvátal 猜想: 设 $\mathscr{A}$ 是 n 元集 S 的子集的一个理想 (即若 $A\in\mathscr{A}\Rightarrow A$ 的子集都属于 $\mathscr{A}$), 让 $w(\mathscr{A})$ 为最大的 k 使得任何 $A_1,\cdots,A_k\in\mathscr{A}$ 两两相交都为非空; $s(\mathscr{A})$ 为最大的 k 使得任何 $A_1,\cdots,A_k\in\mathscr{A}$ 都有 $\bigcap\limits_{i=1}^{k} A_i\neq\varnothing$. 则 $w(\mathscr{A})=s(\mathscr{A})$. (易见 $w(\mathscr{A})\geq s(\mathscr{A})$.)

第五章习题

1. 设 $x_1,\cdots,x_n\in\mathbb{R},|x_i|\geq 1$. 任给 $c\in\mathbb{R}$, 证明:

$$\left|\left\{\langle\varepsilon_1,\cdots,\varepsilon_n\rangle\middle|\varepsilon_i\in\{\pm1\},且\sum_{i=1}^{n}\varepsilon_i x_i\in[c,c+2)\right\}\right|\leq\binom{n}{\lfloor\frac{n}{2}\rfloor}.$$

提示: 用 Sperner 定理.

第 6 章　加法组合

§6.1　$\mathbb{Z}$ 上和集

设 $A_1,\cdots,A_n$ 是 $\mathbb{Z}$ 的有穷非空子集, 把

$$A_1+\cdots+A_n=\{a_1+\cdots+a_n|a_i\in A_i\}$$

叫 $A_1,\cdots,A_n$ 的**和集 (sum set)**.

例如, 若 $A=\{0,1,\cdots,k-1\}$, $B=\{0,1,\cdots,l-1\}$, 则 $A+B=\{0,1,\cdots,k+l-2\}$, 从而 $|A+B|=k+l-1=|A|+|B|-1$.

定理 6.1.1

设 $A_1,\cdots,A_n$ 是 $\mathbb{Z}$ 的有穷非空子集, 则

$$|A_1+\cdots+A_n|\geq|A_1|+\cdots+|A_n|-n+1.$$

证明: 只需证明当 $n=2$ 时结论正确, 然后对 n 归纳即可得到欲证结论.

设 $A=\{a_1,\cdots,a_k\},B=\{b_1,\cdots,b_l\}$ 是 $\mathbb{Z}$ 的子集, $k\leq l$, 且 $a_i<a_{i+1},b_j<b_{j+1}$. 则

$$a_i+b_i<a_i+b_{i+1}<a_{i+1}+b_{i+1},i=1,2,\cdots,k-1.$$

进一步有

$$\underbrace{a_1+b_1<a_1+b_2<a_2+b_2<a_2+b_3<\cdots<a_k+b_{k-1}<a_k+b_k}_{2k-1\text{个}}<\underbrace{a_k+b_{k+1}<\cdots<a_k+b_l}_{l-k\text{个}}.$$

这样我们找到了 $A+B$ 中的 $2k-1+l-k=|A|+|B|-1$ 个不同元素, 从而 $|A+B|\geq|A|+|B|-1$.

□

命题 6.1.2

设 $A_1,\cdots,A_n$ 是 $\mathbb{Z}$ 的有穷非空子集, 则 $|A_1+\cdots+A_n|=|A_1|+\cdots+|A_n|-n+1$ 的充分必要条件是 $A_1,\cdots,A_n$ 是具有相同公差的算术级数.

证明: 以 $n=2$ 为例, 先设 $A=\{a_1,\cdots,a_k\},B=\{b_1,\cdots,b_k\}$, $|A+B|=2k-1$. 则

$$A+B=\{a_1+b_1<a_1+b_2<a_2+b_2<\cdots<a_k+b_k\},$$

(我们把 $2k-1$ 个元素都表示出来了.)

由 $a_{i-1}+b_i<\begin{matrix}a_i+b_i\\a_{i-1}+b_{i+1}\end{matrix}<a_i+b_{i+1}$, 所以 $a_i+b_i=a_{i-1}+b_{i+1}\Rightarrow a_i-a_{i-1}=b_{i+1}-b_i$.

由 $a_{i-1}+b_{i-1}<\begin{matrix}a_{i-1}+b_i\\a_i+b_{i-1}\end{matrix}<a_i+b_i$, 所以 $a_{i-1}+b_i=a_i+b_{i-1}\Rightarrow a_i-a_{i-1}=b_i-b_{i-1}$.

综上, $a_i-a_{i-1}=b_i-b_{i-1}$. □

注: 当 $A=\{a+di|i=0,1,\cdots,k-1\},B=\{b+dj|j=0,1,\cdots,l-1\}$ 时,

$$|A+B|=|\{a+b+d(i+j)|0\leq i\leq k-1,0\leq j\leq l-1\}|=k+l-1=|A|+|B|-1.$$

下面记

$$A_1\dot{+}\cdots\dot{+}A_n=\{a_1+\cdots+a_n|a_i\in A_i,\text{且}a_1,\cdots,a_n\text{两两不同}\},$$

为**异元和集**. 若 $A_1=A_2=\cdots=A_n=A$, 则把 $A_1+\cdots+A_n$ 记为 nA, 把 $A_1\dot{+}\cdots\dot{+}A_n$ 记为 $n^{\wedge}A$.

那么当 A 为有穷非空子集时, $|nA|\geq n|A|-n+1$. 令 $A=\{0,1,\cdots,k-1\}(k\geq n)$, 则

$$n^{\wedge}A=[0+1+\cdots+(n-1),(k-1)+(k-2)+\cdots+(k-n)]\cap\mathbb{N},$$

即 $n^{\wedge}A$ 为从 $\frac{n(n-1)}{2}$ 到 $kn-\frac{n(n+1)}{2}$ 的所有整数. 这样

$$|n^{\wedge}A|=kn-\frac{n(n+1)}{2}-\frac{n(n-1)}{2}+1=kn-n^2+1=n(|A|-n)+1.$$

我们有如下的定理:

定理 6.1.3. Nathanson

设 A 是 $\mathbb{Z}$ 的有穷非空子集, 则 $|n^{\wedge}A|\geq n(|A|-n)+1$.

当 $2\leq n\leq|A|-2$ 且 $|A|\neq 4$ 时, 等号成立当且仅当 A 是算术级数.

对一般的情况, 有如下定理: [cf. Acta. Math. 曹惠琴, 孙智伟, 87(1998); 孙智伟, 99(2001)].

定理 6.1.4

设 $A_1,\cdots,A_n$ 是 $\mathbb{Z}$ 的有穷子集, $|A_1|\leq\cdots\leq|A_n|$, 且 $|A_i|\geq i(i=1,2,\cdots,n)$, 则

$$|A_1+\cdots+A_n|\geq 1+\sum_{i=1}^{n}\min_{i\leq j\leq n}(|A_j|-j).$$

§6.2 Cauchy-Davenport 定理

把前面的结论推广到有限 Abel 群.

定理 6.2.1

设 G 是群, A,B 是 G 的有穷子集. 若 $|A|+|B|>|G|$, 则 $AB=\{ab|a\in A,b\in B\}=G$.

证明: 若有 $g\in G$ 使得 $g\notin AB$, 则对任意 $a\in A,b\in B$, 有 $gb^{-1}\neq a$, 从而 $gB^{-1}\cap A=\varnothing$. 但是

$$|G|\geq|A\cup gB^{-1}|=|A|+|gB^{-1}|=|A|+|B|,$$

与条件矛盾. □

与加法组合有关的问题举例:

- 记 $\square=\{n^2|n=0,1,2,\cdots\}$, Lagrange 四平方和定理: $4\square\triangleq\square+\square+\square+\square=\mathbb{N}$.
- Goldbach 猜想: 当 $n>2$ 时, $2n$ 可以写成 $p+q$, 其中 p,q 都是素数.
- 陈景润定理: 充分大的偶数可以表示成 $p+p_2$, 其中 p 是素数, p_2 是至多两个素数的乘积.

记 $\mathbb{P}=\{$全体素数$\}$, 则 Goldbach 猜想就是说 $P+P=\{4,6,8,\cdots\}$, 这就是一个和集的问题.

1930 年代, Schnirelmann 引入了 **Schnirelmann 密率**:

$$\sigma(A)=\inf_{n\geq 1}\frac{|A\cap\{1,2,\cdots,n\}|}{n},$$

H.B.Mann 证明了如下结论:

定理 6.2.2. Mann

设 A,B 是 $\mathbb{Z}$ 的含 0 子集, 则 $\sigma(A+B)\geq\min\{1,\sigma(A)+\sigma(B)\}$.

根据这个定理, 对 $\mathbb{Z}$ 的子集 A, 如果 $\sigma(A)>0$, 则当 h 足够大时, 总有 $h\sigma(A)=\sigma(A)+\cdots+\sigma(A)\geq 1$, 从而 $\sigma(hA)\geq 1$, 从而 $\sigma(hA)=1\Rightarrow hA=\mathbb{Z}^+$.

Schnirelmann 证明了下面定理的结论, 极大地推进了 Goldbach 猜想的研究:

定理 6.2.3. Schnirelmann

存在正整数 h, 使得任意充分大的整数是最多 h 个素数的和.

我们知道, 对 $\mathbb{P}_0=\{0\}\cup\mathbb{P}$, 由素数定理可知 $\sigma(\mathbb{P}_0)=0$. 但是 Schnirelmann 证明了 $\sigma(\mathbb{P}_0+\mathbb{P}_0)>0$. 根据 Mann 定理, 存在 h 使得 $h\mathbb{P}_0=\mathbb{Z}^+$. 这样大于 1 的整数都可以写成至多 h 个素数之和. □

Cauchy 于 1820 年代得到下面的结论, 但是 Davenport 于 1935 年重新发现了下述结论.

定理 6.2.4. Cauchy-Davenport

设 p 是素数, $F_p=\mathbb{Z}/p\mathbb{Z}$, $\varnothing\neq A,B\subseteq F_p$, 则

$$|A+B|\geq\min\{p,|A|+|B|-1\}.$$

注: 记 $d(A)=\dfrac{|A|}{p}$, 则 $d(A+B)\geq\min\left\{1,d(A)+d(B)-\dfrac{1}{p}\right\}$, 可以与 Mann 定理作个比较.

F.Dyson 为了简化 Mann 定理的证明, 引入了 **g-变换**, 我们即将在证明 Cauchy-Davenport 定理的时候也要用到. 设 G 是加法 Abel 群, A,B 是 G 的非空子集, $g\in G$. 让

$$A(g)=A\cup(B+g),B(g)=B\cap(A-g). \tag{6.1}$$

称 $\langle A(g),B(g)\rangle$ 是有序对 $\langle A,B\rangle$ 的 **g-变换**. 注意 $A\subseteq A(g),B(g)\subseteq B$.

引理 6.2.5

设 G 是加法 Abel 群, A,B 是 G 的非空子集, $g\in G$, 且 $A(g),B(g)$ 定义如 (6.1) 式. 则

(1)$A(g)+B(g)\subseteq A+B$;

(2)$A(g)\setminus A=g+(B\setminus B(g))$;

(3) 若 A,B 有穷, 则 $|A(g)|+|B(g)|=|A|+|B|$;

(4) 若 $g\in A,0\in B$, 则 $g\in A(g),0\in B(g)$.

证明: (1) 设 $x\in A(g),y\in B(g)$. 由于 $B(g)\subseteq B$, 则 $y\in B$.

若 $x\in A$, 则 $x+y\in A+B$; 若 $x\notin A$, 则 $x\in B+g$, 所以 $x+y=(x-g)+(y+g)\in A+B$. 这样 $A(g)+B(g)\subseteq A+B$.

(2)$A(g)\backslash A=(B+g)\backslash A=\{b+g|b\in B,b+g\notin A\}=g+\{b\in B|b\notin A-g\}=g+B\backslash((A-g)\cap B)=g+B\setminus B(g)$.

(3) 若 A,B 是有穷集, 则 $|A(g)|-|A|=|A(g)\setminus A|=|g+(B\setminus B(g))|=|B\setminus B(g)|=|B|-|B(g)|$.

(4) 显然. □

Cauchy-Davenport 定理的证明: (1) 若 $|A|+|B|>p=|\mathbb{Z}/p\mathbb{Z}|$, 由定理6.2.1, $A+B=\mathbb{Z}/p\mathbb{Z}$, 从而

$$|A+B|=p\geq\min\{p,|A|+|B|-1\}.$$

(2) 下设 $|A|+|B|\leq p$. 要证明

$$|A+B|\geq|A|+|B|-1. \tag{6.2}$$

取 $b_0\in B$, 让 $B'=B-b_0$, 则 $|A+B'|=|A+B-b_0|=|A+B|$, 且$|B|=|B'|$. 所以可以不妨设 $0\in B$(要不然就作个平移).

(i) 若 $B=\{0\}$, 则 $|A+B|=|A|=|A|+|B|-1$;

(ii) 若 $A=\{a\}$, 则 $|A+B|=|B|=|B|+|A|-1$.

(iii) 下设 $|A|\geq2,|B|\geq2,0\in B$. (反证) 若 (6.2) 式不成立, 我们取这样的反例 A,B 使得 $|B|$ 最小. 由于 $|B|\geq2$, 所以存在 $b\in B\setminus\{0\}$.

①若 $A+b\subseteq A$, 则 $A+2b\subseteq A+b\subseteq A,\cdots,A+jb\subseteq A,j=0,1,\cdots,p-1$. (注意 jb 取遍了 $\mathbb{Z}/p\mathbb{Z}$ 中的所有元素.) 取 $a\in A$, 则 $\{a+jb|j=0,1,\cdots,p-1\}\subseteq A$, 故 $|A|\geq p$, 故 $A=\mathbb{Z}/p\mathbb{Z}$, 这与 $|A|+|B|\leq p$ 矛盾.

②若 $A+b\nsubseteq A$, 则有 $g\in A$ 使得 $g+b\notin A$. 让 $A(g),B(g)$ 如 (6.1) 式, 则

$$|A(g)+B(g)|\leq|A+B|<|A|+|B|-1=|A(g)|+|B(g)|-1,$$

且 $\langle A(g),B(g)\rangle$ 也是反例. 但是 $b\in B$ 且 $b\notin A-g$, 则 $b\in B\setminus B(g)$, 故 $|B(g)|<|B|$, 这与 $\langle A,B\rangle$ 的选取 ($|B|$ 最小) 矛盾. □

不难把这个结论推广到 n 个的情形:

推论 6.2.6

设 $A_1,\cdots,A_n$ 是 $\mathbb{Z}/p\mathbb{Z}$ 的非空子集, 则

$$|A_1+\cdots+A_n|\geq\min\{p,|A_1|+\cdots+|A_n|-n+1\}.$$

等号成立条件: 取 $A_i=\{\bar{0},\bar{1},\cdots,\overline{k_i-1}\}$, 其中 $k_i\leq p$. 则

$$|A_1+\cdots+A_n|=\left|\left\{\bar{m}:0\leq m\leq\sum_{i=1}^{n}(k_i-1)\right\}\right|=\min\left\{p,\sum_{i=1}^{n}|A_i|-n+1\right\}.$$

Cauchy-Davenport 定理有更一般的版本:

定理 6.2.7. Kneser

设 A,B 是有限 Abel 群 G 的子集, 则

$$|A+B|\geq|A+H|+|B+H|-|H|, \tag{6.3}$$

其中 $H=\{h\in G|h+A+B=A+B\}$ 是 G 的稳定化子. (不难证明 $H\leq G$.)

注: 在这个定理中取 $G=\mathbb{Z}/p\mathbb{Z}$, p 是素数. 则 $H\leq G\Rightarrow H=\{0\}$ 或 $H=G$.
若 $H=\{0\}$, 则 (6.3) 式可以推出 $|A+B|\geq|A|+|B|-1$;
若 $H=G$, 则 G 中元 h 都满足 $h+A+B=A+B$, 所以 $A+B=G=\mathbb{Z}/p\mathbb{Z}$. 则 $|A+B|=p$.
因此这个定理可以推出 Cauchy-Davenport 定理.

§6.3 Erdös-Ginzburg-Ziv 定理与零和问题

Erdös-Ginzburg-Ziv 定理开创了零和问题的研究.

定理 6.3.1. Erdös-Ginzburg-Ziv, 1961

任何 $2n-1$ 个整数 (允许重复) 必可取 n 个使得其和是 n 的倍数.

注: $2n-1$ 不能换成更小的, 考虑 $\underbrace{0,\cdots,0}_{n-1},\underbrace{1,\cdots,1}_{n-1}$, 任选 n 个之和不可能是 n 的倍数.

证明: (1) 假设 EGZ 定理在 n 为素数时成立, 下证 EGZ 定理对任何 $n\in\mathbb{Z}^+$ 成立.

对 n 归纳. 当 $n=1$ 时显然. 下设 $n>1$ 且 n 更小时结论正确. 若 n 是素数, 则结论成立. 下设 n 是合数.

记 $n=uv(1<u\leq v<n)$, 设 $a_1,\cdots,a_{2n-1}\in\mathbb{Z}$, 则 $2n-1=2uv-1\geq 2v-1$. 由归纳假设, 有 $I_1\subseteq\{1,2,\cdots,2n-1\}$ 使得 $|I_1|=v$, 且 $\sum\limits_{i\in I_1}a_i\equiv 0(\mathrm{mod}\ v)$. 由于 $2n-1-v=(2n-1)v-1\geq 2v-1$, 又可以找到 $I_2\subseteq\{1,2,\cdots,2n-1\}\setminus I_1$, 使得 $|I_2|=v$ 且 $\sum\limits_{i\in I_2}a_i\equiv 0(\mathrm{mod}\ v)$. 继续找 $I_3,\cdots,I_{2u-1}\subseteq\{1,2,\cdots,2n-1\}$, 且 $I_1,\cdots,I_{2u-1}$ 两两不交, $|I_j|=v$ 且 $\sum\limits_{i\in I_j}a_i\equiv 0(\mathrm{mod}\ v), j=1,2,\cdots,2u-1$.

设 $1\leq j\leq 2n-1$ 时, $\sum\limits_{i\in I_j}a_i=q_jv$, 依归纳假设, 在 $q_1,\cdots,q_{2u-1}$ 中又可以找到 u 个, 使得其和为 u 的倍数. 设 $J\subseteq\{1,2,\cdots,2u-1\}, |J|=u$, $\sum\limits_{j\in J}q_j\equiv 0(\mathrm{mod}\ u)$. 如此,

$$\sum_{j\in J}\sum_{i\in I_j}a_i=\sum_{j\in J}q_jv\equiv 0(\mathrm{mod}\ n).$$

这样我们找到了 n 个元素, 加起来的和是 n 的倍数.

(2) 下设 $n=p$ 是素数, $a_1,\cdots,a_{2p-1}\in\mathbb{Z}$. 让 a_i' 表示 a_i 模 p 的最小非负余数,

不妨设 $0\leq a_1'\leq a_2'\leq\cdots\leq a_{2p-1}'$. 如果有 $1\leq i\leq p$ 使得 $a_i'=a_{i+p-1}'$, 则 $a_i'=a_{i+1}'=\cdots=a_{i+p-1}'$, 于是

$$a_i\equiv a_{i+1}\equiv\cdots\equiv a_{i+p-1}(\mathrm{mod}\ p)\Rightarrow a_i+a_{i+1}+\cdots+a_{i+p}-1\equiv pr\equiv 0(\mathrm{mod}\ p).$$

下设 $1\leq i\leq p$ 时, $a_i'\neq a_{i+p-1}'$, 即 $a_i+p\mathbb{Z}\neq a_{i+p-1}+p\mathbb{Z}$. 当 $1\leq i\leq p-1$ 时, 让

$$A_i=\{a_i+p\mathbb{Z},a_{i+p-1}+p\mathbb{Z}\}$$

表示 $\mathbb{Z}/p\mathbb{Z}$ 的 2 元子集. 由 Cauchy-Davenport 定理,

$$|A_1+\cdots+A_{p-1}|\geq\min\left\{p,\sum_{i=1}^{n}|A_i|-(p-1)+1\right\}=p,$$

从而 $A_1+\cdots+A_{p-1}=\mathbb{Z}/p\mathbb{Z}$. 而 $-a_{2p-1}+p\mathbb{Z}\in\mathbb{Z}/p\mathbb{Z}=A_1+\cdots+A_{p-1}$, 所以当 $1\leq i\leq p-1$ 时, 存在 $\widetilde{i}\in\{i,i+p-1\}$, 使得

$$(a_{\widetilde{1}}+p\mathbb{Z})+\cdots+(a_{\widetilde{p-1}}+p\mathbb{Z})=-a_{2p-1}+p\mathbb{Z}.$$

所以 $(a_{\widetilde{1}}+\cdots+a_{\widetilde{p-1}}+a_{2p-1})\equiv 0(\mathrm{mod}\ p)$. 这样就找到了 p 个数加起来是 p 的倍数. □

回顾域论的基础知识:

- q 元域存在 $\Leftrightarrow$ q 是素数幂次;
- 任意两个 q 元域同构, 且在同构意义下 q 元域唯一, 记为 $\mathbf{F}_q$ 或 $\mathbf{GF}(q)$.
- $\mathbf{F}_{p^n}$ 的特征为 p, 即同一元素相加 p 次为 0.
- 有限域的乘法群 $\mathbf{F}_q^*\triangleq\mathbf{F}_q\setminus\{0\}$ 是循环群.

定理 6.3.2. Chevalley-Warning

设有限域 F 的特征为素数 p, $f_1(x_1,\cdots,x_n),\cdots,f_m(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n]$. 让 $V=Z(f_1,\cdots,f_m)$ 是方程组

$$\begin{cases} f_1(x_1,\cdots,x_n)=0,\\ \vdots \qquad\qquad ,x_1,\cdots,x_n\in F\\ f_m(x_1,\cdots,x_n)=0, \end{cases} \tag{6.4}$$

的解集, 如果 $\sum_{i=1}^{m}\deg f_i<n$, 则 $p\Big||V|$. 特别地, 方程组 (6.4) 不可能有唯一解.

证明: 设 $|F|=q=p^\alpha$, 则 $F^*=F\setminus\{0\}$ 是 $q-1$ 阶循环群. 设 g 是 F 的生成元, 则当 $q-1\nmid k$ 时, $g^k\neq 1$. 注意

$$g^k\sum_{x\in F}x^k=\sum_{x\in F}(gx)^k=\sum_{y\in F}y^k,\Rightarrow(g^k-1)\sum_{x\in F}x^k=0.$$

但是当 $k=1,2,\cdots,q-2$ 时 $g^k-1\neq 0$, 所以必有 $\sum_{x\in F}x^k=0$. 由于 $\sum_{x\in F}x^0=|F|\cdot 1=p^\alpha\cdot 1=0$, 所以

$$\sum_{x\in F}x^k=0,k=0,1,\cdots,q-2. \tag{6.5}$$

若 $f_i(x_1,\cdots,x_n)\neq 0$, 则 $f_i(x_1,\cdots,x_n)^{q-1}=1$, 故当 $x_1,\cdots,x_n\in F$ 时,

$$\prod_{i=1}^{n}(1-f_i(x_1,\cdots,x_n)^{q-1})=\begin{cases}1, & (x_1,\cdots,x_n)\in V,\\ 0, & \text{此外.}\end{cases}$$

让 $S=\sum_{x_1,\cdots,x_n\in F}\prod_{i=1}^{n}(1-f_i(x_1,\cdots,x_n)^{q-1})$, 则 $S=|V|\cdot 1$, 所以 $p\Big||V|\Leftrightarrow S=0$. 下面只需证 $S=0$.

注意 $\sum_{i=1}^{n}(q-1)\deg f_i<n(q-1)$, 记 $\prod_{i=1}^{n}(1-f_i(x_1,\cdots,x_n)^{q-1})\triangleq\sum_{j_1+\cdots+j_n<n(q-1)}a_{j_1,\cdots,j_n}x_1^{j_1}\cdots x_n^{j_n}$,

则由 (6.5) 式,

$$\begin{aligned} S &= \sum_{x_1,\cdots,x_n\in F} \sum_{j_1+\cdots+j_n<n(q-1)} a_{j_1\cdots j_n} x_1^{j_1}\cdots x_n^{j_n} \\ &= \sum_{j_1+\cdots+j_n<n(q-1)} a_{j_1\cdots j_n} \Big(\sum_{x_1\in F} x_1^{j_1}\Big)\cdots\Big(\sum_{x_n\in F} x_n^{j_1}\Big) = 0. \end{aligned}$$

(因为必有一个 $j_i < q-1$.) □

用 Chevalley-Warning 定理证明 EGZ 定理后半部分:

设 $a_1,\cdots,a_{2p-1}\in F_p=\mathbb{Z}/p\mathbb{Z}$, 要找 $I\subseteq\{1,2,\cdots,2p-1\}$, 使得 $|I|=p$ 且 $\sum\limits_{i\in I}a_i=0$. 考虑

$$\begin{cases}x_1^{p-1}+\cdots+x_{2p-1}^{p-1}=0,\\ a_1x_1^{p-1}+\cdots+a_{2p-1}x_{2p-1}^{p-1}=0,\end{cases}\tag{6.6}$$

由 Chevalley-Warning 定理可知, 方程组 (6.6) 不可能有唯一解. 由于此方程组有零解, 于是存在不全为 0 的 $x_1,\cdots,x_{2p-1}\in F$ 使得 (6.6) 成立.

让 $I=\{1\le i\le 2p-1|x_i\neq 0\}$, 则 $I\neq\varnothing$. 由 (6.6) 的第一条式子, 可得 $\sum\limits_{i\in I}x_i^{p-1}=0$. 注意 $x_i^{p-1}=1$, 所以 $|I|\cdot 1=0$, 故 $p\Big||I|$. 由 $0<|I|<2p$, 故必有 $|I|=p$. 再由 (6.6) 的第二条式子, 可得 $\sum\limits_{i\in I}a_i=\sum\limits_{i\in I}a_i\underbrace{x_i^{p-1}}_{=1}=0$, 于是找到了 p 个元素构成的集合 I 使得 $\sum\limits_{i\in I}a_i=0$. □

EGZ 定理有如下的推广, 比如: A. Kemnitz 于 1983 年猜想: $\mathbb{Z}/n\mathbb{Z}\oplus\mathbb{Z}/n\mathbb{Z}$ 中任意 $4n-3$ 个元素可以找到 n 个元素加起来为 0. 在 2000 年匈牙利人 L. Rónyai 证明了 $4n-2$ 的情况成立. 在 2003 年, 德国的奥数金牌获得者 C. Reiher 证明了此猜想, 他的方法结合了代数与组合.

更多相关结果可以看: http://maths.nju.edu.cn/~zwsun/SurveyZS.pdf.

Cauchy-Davenport 定理取等号的情况:

定理 6.3.3. Vosper

设 p 是素数, A,B 是 $\mathbb{Z}/p\mathbb{Z}$ 的非空子集, $A+B\neq\mathbb{Z}/p\mathbb{Z}$, 则 $|A+B|=|A|+|B|-1$ 的充分必要条件是下面三条有一条成立:

(1)$|A|=1$ 或 $|B|=1$;

(2)$|A+B|=p-1$ 且设 $\mathbb{Z}/p\mathbb{Z}\setminus(A+B)=\{c\}$, 则 $B=\overline{c-A}$;

(3)A,B 是有相同公差的算术级数.

§6.4 组合零点及其应用

当 A 为 $\mathbb{Z}$ 的有穷非空子集时, $|n^\wedge A|\ge n|A|-n^2+1$. 特别地, $2^\wedge A=\{a+b|a,b\in A,a\neq b\}$ 至少有 $2|A|-3$ 个元素.

Erdös-Heilbronn 猜想 (1964): 设 p 是素数, A 是 $\mathbb{Z}/p\mathbb{Z}$ 的非空子集, 则 $|2^\wedge A|\ge\min\{p,2|A|-3\}$.

1994 年, J.A.Dias da Silva 与 Y.O.Hamidoune 在 [Bull. London. Math. Soc. 26(1994), 140-146] 证明了上述猜想, 他们证明了更广的情况 (一般的有限域), 见定理6.4.10. 但他们的证明用到了外代数 (Grassmann 代数) 和群表示论.

1995 年, Noga Alon, M.B.Nathanson, I.Z.Ruzsa 在 [Amer. Math. Monthly, 102(1995)250-255] [1]中, 只用多项式来证明了 Erdös-Heilbronn 猜想. Alon 对这个多项式方法作了进一步提炼, 得到了组合零点定理.

6.4.1 组合零点定理

Alon 于 1999 年证明了如下的名气很大的**组合零点定理 (Combinatorial Nullstellensatz)**:

[1]Amer. Math. Monthly 是不算很高深的杂志, 适合本科生阅读.

定理 6.4.1. Alon

设 $A_1,\cdots,A_n$ 是域 F 的有穷非空子集, $f(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n]$.

(1) 让 $g_i(x)=\prod_{a\in A_i}(x-a), i=1,2,\cdots,n$, 则下面两个命题等价:

(i) 对任何 $a_1\in A_1,\cdots,a_n\in A_n$, 有 $f(a_1,\cdots,a_n)=0$;

(ii) 有多项式 $h_1(x_1,\cdots,x_n),\cdots,h_n(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n]$, 使得

$$f(x_1,\cdots,x_n)=\sum_{i=1}^{n}g_i(x_i)h_i(x_1,\cdots,x_n)\text{且}\deg g_i+\deg h_i\le\deg f_i.$$

(2) 设 $0\le k_i<|A_i|,\sum_{i=1}^{n}k_i=\deg f$. 如果上面的 (i) 成立, 则 $[x_1^{k_1}\cdots x_n^{k_n}]f(x_1,\cdots,x_n)=0$.

证明: 先证明 (1) ⇒ (2): 若 (i) 成立, 即 f 在 $A_1\times\cdots\times A_n$ 上处处为 0. 由 (i) 可得

$$\begin{aligned}
&[x_1^{k_1}\cdots x_n^{k_n}]f(x_1,\cdots,x_n)\\
=&\sum_{i=1}^{n}[x_1^{k_1}\cdots x_n^{k_n}]g_i(x_i)h_i(x_1,\cdots,x_n)\\
=&\sum_{i=1}^{n}[x_1^{k_1}\cdots x_n^{k_n}]x_i^{|A_i|}h_i(x_1,\cdots,x_n)\qquad(\text{注意 }\sum_{j=1}^{n}k_j=\deg f\ge\deg g_i+\deg h_i),\\
=&0\qquad(\text{注意 }|A_i|>k_i,\text{故 }x^{k_i}\text{ 系数为 }0),
\end{aligned}$$

下证 (1). "$(ii)\Rightarrow(i)$": 设 $f(x_1,\cdots,x_n)=\sum_{i=1}^{n}g_i(x_i)h_i(x_1,\cdots,x_n)$, 当 $a_i\in A_i(i=1,2,\cdots,n)$ 时, $f(a_1,\cdots,a_n)=\sum_{i=1}^{n}g_i(a_i)h_i(a_1,\cdots,a_n)$, 由 $g_i(a_i)=\prod_{a\in A_i}(a_i-a)=0$, 则 $f(a_1,\cdots,a_n)=0$.

"$(i)\Rightarrow(ii)$": 先证明下面的引理:

引理 6.4.2

设 F 是域, $A_1,\cdots,A_n$ 是 F 的有穷非空子集, 若 $f(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n]$ 关于 x_i 的次数小于 $|A_i|$, $i=1,2,\cdots,n$, 且 f 在 $A_1,\cdots,A_n$ 上处处为 0, 则 f 为零多项式.

证明: 对 n 归纳. 当 $n=1$ 时, 由 $x_1\in A_1$, 则 $f(x_1)=0$. 所以方程 $f(x)=0$ 根的个数 $\ge|A_1|$, 但是 $\deg f<|A_1|$, 所以 f 是零多项式.

任给 $a_1\in A_1,\cdots,a_{n-1}\in A_{n-1}$, 可以记

$$f(x_1,\cdots,x_n)\triangleq\sum_{i=0}^{|A_n|-1}f_i(x_1,\cdots,x_{i-1})x_n^i,\tag{6.7}$$

所以 $f(a_1,\cdots,a_{n-1},x_n)=\sum_{i=0}^{|A_n|-1}f_i(a_1,\cdots,a_{i-1})x_n^i$, 当 $x_n\in A_n$ 时, $f(a_1,\cdots,a_{n-1},x_n)=0$. 所以方程 $f(a_1,\cdots,a_{n-1},x_n)=0$ 根的个数 $\ge|A_n|$, 但 $\deg f(a_1,\cdots,a_{n-1},x_n)<|A_n|$, 故 $f(a_1,\cdots,a_{n-1},x_n)$ 是零多项式, 从而 $f_i(a_1,\cdots,a_{n-1})=0$.

因此 f_i 在 $A_1\times A_{n-1}$ 上处处为 0, 而且 $f_i(x_1,\cdots,x_{n-1})$ 关于 x_j 次数 $<|A_j|, j=1,2,\cdots,n-1$. 由归纳假设, $f_i(x_1,\cdots,x_{n-1})$ 是零多项式. 再由 (6.7) 式可知 $f(x_1,\cdots,x_n)$ 是零多项式. □

回到定理证明, 设 $f(x_1,\cdots,x_n)$ 在 $A_1\times\cdots\times A_n$ 上处处为零, 记

$$f(x_1,\cdots,x_n)=\sum_{j_1+\cdots+j_n\le\deg f} f_{j_1\cdots j_n}x_1^{j_1}\cdots x_n^{j_n}, x^j=g_i(x)q_{ij}(x)+r_i^{(j)}(x), \tag{6.8}$$

其中 $\deg r_i^{(j)}(x)<\deg g_i(x)=|A_i|, \deg r_i^{(j_i)}(x)\le j, \deg g_i(x)q_{ij}(x)\le j$. 注意 (6.8) 式可以进一步化简:

$$f(x_1,\cdots,x_n)=\sum_{j_1+\cdots+j_n\le\deg f} f_{j_1\cdots j_n}\prod_{i=1}^n r_i^{(j_i)}(x_i)+\sum_{i=1}^n g_i(x_i)h_i(x_1,\cdots,x_n).$$

其中 $\deg g_i+\deg h_i\le\deg f$. 记 $\tilde f(x_1,\cdots,x_n)=\sum_{j_1+\cdots+j_n\le\deg f} f_{j_1\cdots j_n}\prod_{i=1}^n r_i^{(j_i)}(x_i)$.

当 $a_1\in A_1,\cdots,a_n\in A_n$ 时, $f(a_1,\cdots,a_n)=0$, 且 $g_i(a_i)=0$, 由上式可得 $\tilde f(a_1,\cdots,a_n)=0$, 所以 $\tilde f$ 关于 x_i 的次数 $<\deg g_i(x_i)<|A_i|$. 由引理 $\tilde f$ 是零多项式. □

6.4.2 Snevily 猜想

若 $a_1+1,a_2+2,\cdots,a_n+n$ 模 n 两两不同, 则 $\sum_{i=1}^n(a_i+i)\equiv 1+2+\cdots+n(\mathrm{mod}\ n)$, 从而 $a_1+\cdots+a_n\equiv 0(\mathrm{mod}\ n)$. 我们来看逆命题是否成立.

Cramer 猜想: 设 $a_1,\cdots,a_n\in\mathbb{Z}$, $a_1+\cdots+a_n\equiv 0(\mathrm{mod}\ n)$, 则 $\exists\sigma\in S_n$ 使得 $a_{\sigma(1)}+1,\cdots,a_{\sigma(n)}+n$ 两两不同.

1952 年, M.Hall 把上述猜想解决, 并推广到 Abel 群上:

定理 6.4.3. M.Hall

设 $G=\{b_1,\cdots,b_n\}$ 是 n 阶加法 Abel 群, $a_1,\cdots,a_n\in G$, $a_1+\cdots+a_n=0$, 则存在 $\sigma\in S_n$ 使得 $\{a_{\sigma(1)}+b_1,\cdots,a_{\sigma(n)}+b_n\}=G$.

注意, 若 $a_1+\cdots+a_n\equiv 0(\mathrm{mod}\ n)$, 且 $a_1,\cdot,a_n$ 模 n 两两不同, 则 $n|1+\cdots+n=\dfrac{n(n+1)}{2}$, 从而 n 是奇数.

Snevily 猜想 (1): *设 G 是素数阶加法 Abel 群, A,B 是 G 的 k 元子集, 则存在 A 的元素列举 $a_1,\cdots,a_k$ 与 B 的元素列举 $b_1,\cdots,b_k$, 使得 $a_1+b_1,\cdots,a_k+b_k$ 两两不同.*

Snevily 猜想 (2): *设 $0<k<n,a_1,\cdots,a_k\in\mathbb{Z}$, 则存在 $\pi\in S_k$ 使得 $a_1+\pi(1),\cdots,a_k+\pi(k)$ 模 n 两两不同.*

注: 对于 $k=n$ 的情形, 要加上 $a_1+\cdots+a_n\equiv 0(\mathrm{mod}\ n)$ 的条件, 即可得到 M.Hall 定理.

A.E.Kézdy 与 H.S.Snevily 在 [Combin. Probab. Comput. 2002] 中证明了 $k\le\dfrac{n+1}{2}$ 时, Snevily 猜想 (2) 结论正确.

定理 6.4.4

设 $0<k\le\dfrac{n+1}{2}, a_1,\cdots,a_k\in\mathbb{Z}$, 则存在 $\pi\in S_k$ 使得 $a_1+\pi(1),\cdots,a_k+\pi(k)$ 模 n 两两不同.

证明: 让 $A_1=\cdots=A_k=A=\{1,\cdots,k\}$, 当 $x_i,x_j\in A$ 时, $|x_i-x_j|\le k-1\le\dfrac{n-1}{2}<\dfrac{n}{2}$. 设 $a_1,\cdots,a_k\in\mathbb{Z}$, 让 r_{ij} 表示 a_j-a_i 模 n 在 $\left(-\dfrac{n}{2},\dfrac{n}{2}\right)$ 中的余数, 于是

$$x_i+a_i\not\equiv x_j+a_j(\mathrm{mod}\ n)\Leftrightarrow x_i-x_j\not\equiv a_j-a_i\equiv r_{ij}(\mathrm{mod}\ n)\Leftrightarrow x_i-x_j\not\equiv r_{ij}(\mathrm{mod}\ n). \tag{6.9}$$

下面只需要证存在 $x_1 \in A_1, \cdots, x_k \in A_k$ 使得

$$f(x_1, \cdots, x_k) \triangleq \prod_{1 \le i < j \le k} (x_j - x_i)(x_j - x_i - r_{ij}) \neq 0.$$

(由 (6.9) 式，取 $\pi(i) = x_i$，则 $\pi(i) + a_i$ 模 n 两两不同.)

由组合零点定理, 只需证 $[x_1^{k-1} \cdots x_k^{k-1}] f(x_1, \cdots, x_k) \neq 0$, 从而 f 在 $A_1 \times \cdots \times A_n$ 上不是处处为 0. 事实上,

$$\begin{aligned}
&[x_1^{k-1} \cdots x_k^{k-1}] f(x_1, \cdots, x_k) \\
&= [x_1^{k-1} \cdots x_k^{k-1}] \prod_{1 \le i < j \le k} (x_j - x_i)^2 \qquad \text{(Vandermonde 行列式)} \\
&= [x_1^{k-1} \cdots x_k^{k-1}] (|x_i^{j-1}|_{1 \le i,j \le k})^2 \\
&= [x_1^{k-1} \cdots x_k^{k-1}] \Big(\sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} x_i^{\sigma(i)-1} \Big) \Big(\sum_{\tau \in S_n} \operatorname{sgn}(\tau) \prod_{i=1}^{n} x_i^{\tau(i)-1} \Big) \qquad \text{(行列式展开)}.
\end{aligned}$$

再由

$$\sigma(i) - 1 + \tau(i) - 1 = k - 1 (i = 1, \cdots, k) \Leftrightarrow \tau(i) = k + 1 - \sigma(i) \triangleq \sigma'(i) \Leftrightarrow \tau = \sigma',$$

而且对 $1 \le i < j \le k$, 有 $\sigma(i) > \sigma(j) \Leftrightarrow \sigma'(i) < \sigma'(j)$, 因此 (我们只保留最高次项.)

$$[x_1^{k-1} \cdots x_k^{k-1}] f(x_1, \cdots, x_k) = \sum_{\sigma \in S_k} \operatorname{sgn}(\sigma) \operatorname{sgn}(\sigma') = \sum_{\sigma \in S_k} (-1)^{\binom{k}{2}} = k! (-1)^{\binom{k}{2}} \neq 0.$$

定理证明完成. □

定理 6.4.5. N.Alon, 2000

设 p 是奇素数, $k < p$, $a_1, \cdots, a_k \in \mathbb{Z}/p\mathbb{Z}$ 两两不同, $b_1, \cdots, b_k \in \mathbb{Z}/p\mathbb{Z}$(允许重复), 则存在 $\sigma \in S_k$, 使得 $a_{\sigma(1)} + b_1, \cdots, a_{\sigma(k)} + b_k$ 两两不同.

证明: 让 $A_1 = \cdots = A_k = \{a_1, \cdots, a_k\}$, 可以找 $x_1 \in A_1, \cdots, x_k \in A_k$, 使得

$$f(x_1, \cdots, x_k) \triangleq \prod_{1 \le i < j \le k} (x_i - x_j)((x_i + b_i) - (x_j + b_j)) \neq 0.$$

由组合零点定理, 只需证 $[x_1^{k-1} \cdots x_k^{k-1}] f(x_1, \cdots, x_k) \neq 0$. 由 $k - 1 < |A_i|, \deg f = k(k-1)$, 可得

$$[x_1^{k-1} \cdots x_k^{k-1}] f(x_1, \cdots, x_k) = [x_1^{k-1} \cdots x_k^{k-1}] \prod_{1 \le i < j \le k} (x_j - x_i)^2 = (-1)^{\binom{k}{2}} k! \neq 0. \text{(在 } \mathbb{Z}/p\mathbb{Z} \text{ 中)} \square$$

下面考虑 n 不为素数的情况, 此时 $\mathbb{Z}/n\mathbb{Z}$ 不是域, 没有办法直接用组合零点定理. 但是 S.Dasgupta, G.Károlyi, O.Serra, B.Szegedy 在 [Isreal J. Math, 126(2001), 17-28] 中提出了一个巧妙的证明. 不过这里 $b_1, \cdots, b_k$ 要求不能重复. 核心思想是不要把 Abel 群看成加法群, 它也有可能是乘法群.

定理 6.4.6

设 G 是 n 阶加法循环群, n 是正奇数, $A = \{a_1, \cdots, a_k\}, B = \{b_1, \cdots, b_k\}$ 是 G 的 k 元子集, 则有 $\sigma \in S_k$ 使得 $a_{\sigma(1)} + b_1, \cdots, a_{\sigma(k)} + b_k$ 两两不同.

证明: 注意 $2^{\varphi(n)} \equiv 1 (\bmod\ n)$. 设 F 是 $2^{\varphi(n)}$ 阶有限域, $\operatorname{ch}(F) = 2$, $F^* = F \setminus \{0\}$ 是 $2^{\varphi(n)} - 1$ 阶循环群, 它有 n 阶循环子群 G.

设 $A=\{a_1,\cdots,a_k\},B=\{b_1,\cdots,b_k\}$ 是 G 的 k 元子集, 要找 $\sigma\in S_k$ 使得 $a_{\sigma(1)}b_1,\cdots,a_{\sigma(k)}b_k$ 两两不同. (此群的运算是乘法!) 让 $A_1=\cdots=A_k=\{a_1,\cdots,a_k\}$, 要找 $x_1\in A_1,\cdots,x_kinA_k$, 使得

$$f(x_1,\cdots,x_k)\triangleq\prod_{1\le i<j\le k}(x_i-x_j)(x_ib_i-x_jb_j)\neq 0.$$

由组合零点定理, 只需证 $[x_1^{k-1}\cdots x_k^{k-1}]f(x_1,\cdots,x_k)\neq 0$. 事实上, 类似前面一样的讨论, 有

$$\begin{aligned}
[x_1^{k-1}\cdots x_k^{k-1}]f(x_1,\cdots,x_k)&=[x_1^{k-1}\cdots x_k^{k-1}]|(b_ix_i)^{j-1}|_{1\le i,j\le k}|x_i^{j-1}|_{1\le i,j\le k}\\
&=[x_1^{k-1}\cdots x_k^{k-1}]\Big(\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)\prod_{i=1}^n(b_ix_i)^{\sigma(i)-1}\Big)\Big(\sum_{\tau\in S_n}\operatorname{sgn}(\tau)\prod_{i=1}^n x_i^{\tau(i)-1}\Big)\\
&=\sum_{\sigma\in S_k}\operatorname{sgn}(\sigma)\operatorname{sgn}(\sigma')\prod_{i=1}^k b_i^{\sigma(i)-1}\\
&=\sum_{\sigma\in S_k}(-1)^{\binom{k}{2}}\prod_{i=1}^k b_i^{\sigma(i)-1}\qquad\text{(这是个积和式, 不好算!)}\\
&=(-1)^{\binom{k}{2}}\sum_{\sigma\in S_k}\operatorname{sgn}(\sigma)\prod_{i=1}^k b_i^{\sigma(i)-1}\qquad\text{(注意 }\operatorname{ch}(F)=2,\ 1\text{ 与 }-1\text{ 一样!)}\\
&=|b_i^{j-1}|_{1\le i,j\le k}=\prod_{1\le i<j\le k}(b_j-b_i)\neq 0.\qquad\text{(用到了 }b_i\text{ 两两不同)}\qquad\square
\end{aligned}$$

1982 年, 受 Jäger 所研究图论的启发, 他提出了下面在 $|F|=5$ 的情况的猜想:

Jäger-Alon-Tarsi 猜想: 设 F 是有限域, $|F|\ge 4$, $\boldsymbol{A}$ 是 F 上的 n 阶非奇异矩阵 ($\det\boldsymbol{A}\neq 0$), 则存在 $x_1,\cdots,x_n\in F$, 使得 $\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}$ 与 $\boldsymbol{A}\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}$ 各个分量非零.

1989 年, Alon 和 Tarsi 验证了 $|F|$ 不是素数时结论正确, 而且他们的证明方法是基于组合零点定理的思想.

6.4.3 组合零点定理在和集方面的应用

定理 6.4.7. 孙, Finite Fields Appl. 14(2008),470-481

设 F 是域, $f(x_1,\cdots,x_k)=a_1x_1^k+\cdots+a_nx_n^k+g(x_1,\cdots,x_n)\in F[x_1,\cdots,x_k],\deg g<k$. 任给 F 的有穷非空子集 $A_1,\cdots,A_n$, 有

$$|\{f(x_1,\cdots,x_k)|x_i\in A_i\}|\ge\min\left\{p(F),\sum_{i=1}^n\left\lfloor\frac{|A_i|-1}{k}\right\rfloor+1\right\},\text{其中}p(F)=\begin{cases}p, & \operatorname{ch}(F)=p,\\ \infty, & \operatorname{ch}(F)=0.\end{cases}$$

注: 这是 Cauchy-Davenport 定理的推广, 取 $f(x_1,\cdots,x_n)=x_1+\cdots+x_n$ 即可.

证明: 取最大的 $m\le n$ 使得 $\sum_{i=1}^m\left\lfloor\frac{|A_i|-1}{k}\right\rfloor<p(F)$. 下面我们取 A_i' 如下:

(1) 对 $0<i\le m$, 让 $A_i'\subseteq A_i$, 且 $|A_i'|=k\left\lfloor\frac{|A_i|-1}{k}\right\rfloor+1$.

(2) 如果 $m<n$, 则 $p(F)$ 是素数 p. 选 $A'_{m+1}\subseteq A_{m+1}$ 使得

$$|A'_{m+1}|=k\left(p-1-\sum_{i=1}^{m}\left\lfloor\frac{|A_i|-1}{k}\right\rfloor\right)+1<k\left\lfloor\frac{|A_{m+1}|-1}{k}\right\rfloor+1\le|A_{m+1}|.$$

(注意根据 m 的取法, $\sum_{i=1}^{m+1}\left\lfloor\frac{|A_i|-1}{k}\right\rfloor\ge p(F)\ge p-1$.)

(3) 对 $m+1<j\le n$, 取 $A'_j\subseteq A_j$ 使得 $|A'_j|=1$.

这样, 总有 $\sum_{i=1}^{n}(|A'_i|-1)=k(N-1)$, 其中 $N=\min\left\{p(F),\sum_{i=1}^{n}\left\lfloor\frac{|A_i|-1}{k}\right\rfloor+1\right\}$.

下面让 $\boxed{C=\{f(x_1,\cdots,x_n)|x_i\in A'_i\}}$, 则 $C\subseteq\{f(x_1,\cdots,x_n)|x_i\in A_i\}$. 只需证 $|C|\ge N$.

(反证) 若 $|C|\le N-1$, 则

$$\begin{aligned}
&[x_1^{|A'_1|-1}\cdots x_n^{|A'_n|-1}]\underbrace{f(x_1,\cdots,x_n)^{N-1-|C|}\prod_{c\in C}[f(x_1,\cdots,x_n)-c]}_{\text{最高次数是 }(N-1)\deg f}\\
&=[x_1^{|A'_1|-1}\cdots x_n^{|A'_n|-1}]f(x_1,\cdots,x_n)^{N-1}\qquad\text{(甩掉低次项.)}\\
&=[x_1^{|A'_1|-1}\cdots x_n^{|A'_n|-1}]\left(\sum_{i=1}^{n}a_ix_i^k\right)^{N-1}\qquad\text{(甩掉低次项.)}\\
&=\underbrace{\frac{(N-1)!}{\prod_{i=1}^{n}\left(\frac{|A'_i|-1}{k}\right)!}}_{\text{不是 }p\text{ 的倍数}}a_1^{\frac{|A'_1|-1}{k}}\cdots a_n^{\frac{|A'_n|-1}{k}}\neq0.\qquad\text{(多项式定理)}
\end{aligned}$$

由组合零点定理, 存在 $a_1\in A'_1,\cdots,a_n\in A'_n$ 使得

$$f(a_1,\cdots,a_n)^{N-1-|C|}\prod_{c\in C}[f(a_1,\cdots,a_n)-c]\neq0.$$

但这与 c 的取法矛盾!(根据 $c\in C$, 上式应该等于 0.) 由上, $|\{f(x_1,\cdots,x_n)|x_i\in A_i\}|\ge|C|\ge N$. □

引理 6.4.8

设 $A_1,\cdots,A_n$ 是域 F 的有穷非空子集, $f(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n]\setminus\{0\}$. 设 $k_i=|A_i|-1$, $\deg f\le\sum_{i=1}^{n}k_i$, 且

$$[x_1^{k_1}\cdots x_n^{k_n}]f(x_1,\cdots,x_n)(x_1+\cdots+x_n)^{\sum_{i=1}^{n}k_i-\deg f}\neq0,$$

则

$$|\{a_1+\cdots+a_n|a_i\in A_i,f(a_1,\cdots,a_n)\neq0\}|\ge\sum_{i=1}^{n}k_i-\deg f+1.$$

证明: 让 $C=\{a_1+\cdots+a_n|a_i\in A_i,f(a_1,\cdots,a_n)\neq0\}$. 若结论不成立, 即 $|C|\le K=\sum_i k_i-\deg f$, 让

$$P(x_1,\cdots,x_n)=f(x_1,\cdots,x_n)(x_1+\cdots+x_n)^{k-|C|}\cdot\prod_{c\in C}(x_1+\cdots+x_n-c),$$

则 $\deg P=\sum_{i=1}^{n}k_i$ 且

$$[x_1^{k_1}\cdots x_n^{k_n}]P(x_1,\cdots,x_n)=[x_1^{k_1}\cdots x_n^{k_n}]f(x_1,\cdots,x_n)(x_1+\cdots+x_n)^k\neq 0.$$

由组合零点定理, 存在 $a_1\in A_1,\cdots,a_n\in A_n$ 使得 $P(a_1,\cdots,a_n)\neq 0$. 但这与 c 的取法矛盾.

(若 $f(a_1,\cdots,a_n)\neq 0$, 则 $a_1+\cdots+a_n\in C$, 故应有 $P(a_1,\cdots,a_n)=0$.) □

注: 用组合零点定理的方法就是定义集合 C, 并定义多项式函数 P, 再导出矛盾.

定理 6.4.9. Alon-Nathanson-Ruzsa,1996

设 $A_1,\cdots,A_n$ 是域 F 的有穷非空子集, 且满足
$0<|A_1|<|A_2|<\cdots<|A_n|$, 则

$$|A_1\dot{+}\cdots\dot{+}A_n|\geq\min\left\{p(F),\sum_{i=1}^{n}(|A_i|-i)+1\right\},\text{其中}p(F)=\begin{cases}p, & \mathrm{ch}(F)=p,\\ \infty, & \mathrm{ch}(F)=0.\end{cases}$$

证明: 注意 $A_1\dot{+}\cdots\dot{+}A_n=\left\{x_1+\cdots+x_n\middle|x_i\in A_i,\prod_{1\leq i<j\leq n}(x_j-x_i)\neq 0\right\}$. 以及

$$[x_1^{k_1}\cdots x_n^{k_n}]\prod_{1\leq i<j\leq n}(x_j-x_i)\cdot(x_1+\cdots+x_n)^{\sum_{i=1}^{n}k_i-\binom{n}{2}}=\frac{(k_1+\cdots+k_n-\binom{n}{2})!}{k_1!\cdots k_n!}\prod_{1\leq i<j\leq n}(k_j-k_i).$$

(这个通过把 $\prod_{1\leq i<j\leq n}(x_j-x_i)$ 写成 `Vandermonde` 行列式, 再作行列式展开即可得到一个多项式. 最终得到了 $|(k_i)_{j-1}|_{1\leq i,j\leq n}$(向下乘 $j-1$ 个), 注意 $x^n=\sum_{k=0}^{n}S(n,k)(x)_k$ 可以把这个式子变成 `Vandermonde` 行列式 $|k_i^{j-1}|_{1\leq i,j\leq n}$.)

定理 6.4.10. Dias da Silva-Hamidoune,1994

设 $A_1,\cdots,A_n$ 是域 F 的有穷非空子集, $0<|A_1|<\cdots<|A_n|$, 则

$$|n^{\wedge}A|\geq\min\{p(F),n(|A|-n)+1\},\text{其中}p(F)=\begin{cases}p, & \mathrm{ch}(F)=p,\\ \infty, & \mathrm{ch}(F)=0.\end{cases}$$

证明: $|A|<n$ 的情况平凡. 下设 $|A|\geq n$. 让 $A_n=A$, 取 $A_{n-1}\subseteq A$ 使得 $|A_{n-1}|=k-1$, 取 $A_{n-2}\subseteq A$ 使得 $|A_{n-2}|=k-2,\cdots$, 取 $A_1\subseteq A$ 使得 $|A_1|=k-n+1$. (构造出不同基数的集合.) 由 ANR 定理,

$$|n^{\wedge}A|\geq|A_1\dot{+}\cdots\dot{+}A_n|\geq\min\left\{p(F),\sum_{i=1}^{n}(|A_i|-i)+1\right\}=\min\{p(F),n(k-n)+1\}.$$ □

第六章习题

1. 用组合零点定理证明 Cauchy-Davenport 定理.
2. 用组合零点定理证明 Erdös-Heilbronn 猜想.
3. 设 p 是素数, 域 F 为 $\mathbb{Z}/p\mathbb{Z}$, $A, B \subseteq F$, $C = \{a+b | a \in A, b \in B, ab \neq 1\}$, 证明:

$$|C| \geq \min\{p, |A| + |B| - 3\}.$$

第 7 章　有限射影平面与组合设计

§ 7.1　有限射影平面

一个**射影平面** π 由一些点和线构成, “点 P 在线 L 上”(“线 L 过点 P”) 是一种关联关系, 且满足下面三条公理:

(1) 两点决定一条线: 即 π 上两个不同点在唯一的直线上.

(2) 两条线决定一个点: 即 π 上任两条线有唯一的公共点.

(3) π 上的点不少于四个, 且存在四个点使得任意三点都不共线.

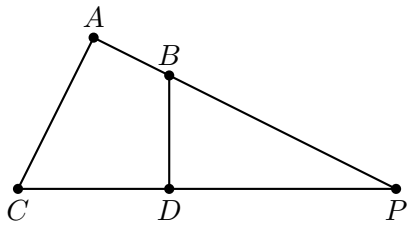
注: 三个点的射影平面认为是退化的.

命题 7.1.1

π 上至少有四条不同的线.

证明: 由公理 (3), 可设四点 A,B,C,D 满足任三点不共线. 设 AB 与 CD 交于点 P, 下证 AB,CD,AC,BD 中任三条线不共点.

若 AB,CD,AC 有公共点 P, 由于 A,B,C,D 任三点不共线, 则 P 不为 A,B,C,D. 所以 AB,AC 都经过点 P 与点 A, 从而经过 P 与 A 的直线不止一条, 这与公理 (1) 矛盾.



对偶原理: 设命题 φ 在任何射影平面都成立, 则其对偶命题 φ^*(把 φ 中的点换成线, 线换成点) 也在任何射影平面 φ 成立.

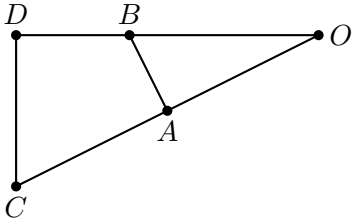
定理 7.1.2

设 π 是射影平面, P,P' 是 π 上的不同点, L,L' 是 π 上的不同线, 则

$$\{L\text{上点}\}\approx\{L'\text{上点}\}\approx\{\text{经过}P\text{的线}\}\approx\{\text{经过}P'\text{的线}\}.$$

证明: 由公理 (3), 有四点 $A,B\in L,C,D\in L'$ 使得 A,B,C,D 任三点不共线. 设 O 是 AC 与 BD 的交点. 若 $O\in L$, 则 A,O 都在 L 上, 也都在 AC 上, 与公理 (1) 矛盾. 同理不可能有 $O\in L'$. 因此 O 不在 L 也不在 L' 上. 所以 $\{L\text{上点}\}\approx\{L'\text{上点}\}$, 由对偶原理, $\{\text{经过}P\text{的线}\}\approx\{\text{经过}P'\text{的线}\}$.

若 P 不在 L 上, 则 $\{\text{经过}P\text{的线}\}\approx\{L\text{上点}\}$. 若 P 在 L 上, 由公理 (3), 在 L 之外可以找一点 P', 于是 $\{\text{经过}P\text{的线}\}\approx\{\text{经过}P'\text{的线}\}\approx\{L\text{上点}\}$. □



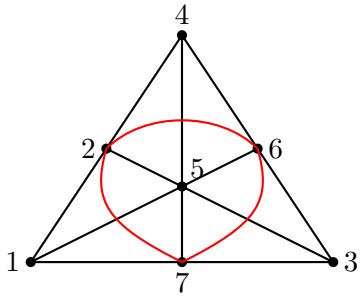
设 π 是射影平面, A,B,C,D 上任意三点不共线, 经过 A 的线至少有 AB,AC,AD, 所以每个点上至少有三条线. 由对偶原理, 每条线上至少有三个点.

定义 7.1.1

如果射影平面 π 的每条线上恰有 $n+1$ 个点, 则称 π 是n **阶射影平面**.

n 阶射影平面一共有 $n(n+1)+1$ 个点, 也有 $n(n+1)+1$ 条线, 每条线上有 $n+1$ 个点, 过每个点的线有 $n+1$ 条.

2 阶射影平面有 7 个点, 包含 7 条线 $\{1,2,4\},\{3,4,6\},\{1,3,7\},\{2,3,5\},\{1,5,6\},\{4,5,7\},\{2,6,7\}$.



定理 7.1.3

设 $n=p^a$ 是素数幂次, 则 n 阶射影平面存在.

证明: 取有限域 F_{p^a}, 形如 $y=kx+b$ 的线上有 n 个点 $(k,b\in F_{p^a})$, 形如 $x=c$ 的线上有 n 个点, 设所有斜率为 k 的线在无穷远处交于 (k), 所有斜率为 ∞ 的线在无穷远处交于 (∞), 而连接 $(1),\cdots,(n),(\infty)$ 的线 (叫**无穷远线**) 也记为一条线, 这样就得到了 n 阶射影平面, 每条线上都有 $n+1$ 个点, 且共有 n^2+n+1 条线. □

注: 当 n 不是素数幂次时, n 阶射影平面的存在性没人会证.

§7.2 正交拉丁方与 Euler 36 军官问题

回顾: 设 S 是 n 元集, 一个 $n\times n$ 矩阵叫**基于 S 的 n 阶拉丁方**, 指它的每行每列都是 S 中元的全排列.

定义 7.2.1

设 $\boldsymbol{A},\boldsymbol{B}$ 是基于 S 的 n 阶拉丁方, $\boldsymbol{A}=(a_{ij}),\boldsymbol{B}=(b_{ij})$. 若 $\begin{cases}a_{ij}=a_{st}\\ b_{ij}=b_{st}\end{cases}$ 可推出 $i=s$ 且 $j=t$, 则称 $\boldsymbol{A},\boldsymbol{B}$ **正交**, 记为 $\boldsymbol{A}\perp\boldsymbol{B}$.

注: $\boldsymbol{A}\perp\boldsymbol{B}$ 相当于 $\langle a_{ij},b_{ij}\rangle(i,j=1,2,\cdots,n)$ 这 n^2 个有序对两两不同. $\boldsymbol{A}$ 的两个地方相等, 那么 $\boldsymbol{B}$ 的这两个地方必须不等.

例 7.2.1

$\begin{pmatrix}1&2\\2&1\end{pmatrix}$ 与 $\begin{pmatrix}2&1\\1&2\end{pmatrix}$ 不正交, 而二阶拉丁方只有这两个, 所以二阶拉丁方之间都不正交.

例 7.2.2

$\begin{pmatrix}1&2&3\\2&3&1\\3&1&2\end{pmatrix}$ 与 $\begin{pmatrix}1&3&2\\2&1&3\\3&2&1\end{pmatrix}$ 正交.

定义 7.2.2

若 n 阶拉丁方 $\boldsymbol{A}_1,\cdots,\boldsymbol{A}_t$ 两两正交, 则称 $\{\boldsymbol{A}_1,\cdots,\boldsymbol{A}_t\}$ 是 n 阶拉丁方的一个**正交集**.

定理 7.2.3

设 $n\geq 2$, 基于 $S=\{1,2,\cdots,n\}$ 的 n 阶拉丁方 $\boldsymbol{A}_1,\cdots,\boldsymbol{A}_t$ 两两正交, 则 $t\leq n-1$.

证明: 设 $\boldsymbol{A}_i$ 的第一行为 $\sigma_i(1),\cdots,\sigma_i(n), i=1,2,\cdots,t$, $\sigma_i\in S_n$. 再设 $\boldsymbol{A}_j$ 的第 2 行第 1 列元素为 $\sigma_j(i_j), j=1,2,\cdots,t$.

下证 $i_1,\cdots,i_t$ 两两不同. (反证) 若 $i_k=i_l(1\leq k<l\leq t)$, 记 $\boldsymbol{A}_s=(a_{ij}^{(s)})(s=1,2,\cdots,t)$, 则 $\boldsymbol{A}_k$ 中 $a_{21}^{(k)}=a_{1i_k}^{(k)}=\sigma_k(i_k)$, $\boldsymbol{A}_l$ 中 $a_{21}^{(l)}=a_{1i_l}^{(l)}=a_{1i_k}^{(l)}$, 这与 $\boldsymbol{A}_k\perp\boldsymbol{A}_l$ 矛盾, 故 $i_1,\cdots,i_t$ 两两不同.

由拉丁方的定义, $i_1,\cdots,i_t$ 都不取 1(不然与每行每列元素不同矛盾), 所以 $i_1,\cdots,i_t\subseteq\{2,\cdots,n\}$, 但是 $i_1,\cdots,i_t$ 两两不同, 则 $t\leq n-1$. □

定义 7.2.3

如果 $\{\boldsymbol{A}_1,\cdots,\boldsymbol{A}_{n-1}\}$ 是 n 阶拉丁方正交集, 则称之为 n 阶拉丁方**完全集**.

1782 年, 皇帝让 Euler 考虑 **36 军官问题**: 有 6 个军团, 编号为 1∼ 6, 每个军团出 6 个不同级的军官各 1 人 (少校、中校、大校、少将、中将、大将), 能否把这 36 个军官排成 6×6 方阵, 使得每行、每列上 6 个人来自不同的军团, 也有不同的军衔?

每个军团有个军团编号, 也有军衔编号 (介于 $1\sim 6$ 之间), 所要求方阵各军官的军团编号构成一个基于 $\{1,\cdots,6\}$ 的拉丁方 $\boldsymbol{A}$, 各军官的军衔编号构成一个基于 $\{1,\cdots,6\}$ 的拉丁方 $\boldsymbol{B}$, 而且 $\boldsymbol{A}\perp\boldsymbol{B}$. Euler36 军官问题相当于要找一对正交的 6 阶拉丁方.

定理 7.2.4

设 $n=p^a$ 是素数幂次, $n\geq 2$, 则存在 n 阶拉丁方的完全正交集.

证明: 设 F 是 n 元域, 其元素为 $a_0=0,a_1,\cdots,a_{n-1}$. 对 $k=1,\cdots,n-1$, 让 $\boldsymbol{A}_k=(a_{ij}^{(k)})_{0\leq i,j\leq n-1}$, 其中 $a_{ij}^{(k)}=a_ka_i+a_j$, 下证 $\boldsymbol{A}_1,\cdots,\boldsymbol{A}_{n-1}$ 是两两正交的基于 F 的 n 阶拉丁方.

易证 $\boldsymbol{A}_1,\cdots,\boldsymbol{A}_{n-1}$ 都是基于 F 的 n 阶拉丁方, 只需证明正交: 即 $1\leq k<l\leq n-1$ 时 $\boldsymbol{A}_k\perp\boldsymbol{A}_l$. (反证) 如果 $a_{ij}^{(k)}=a_{i'j'}^{(k)}$ 且 $a_{ij}^{(l)}=a_{i'j'}^{(l)}$, 则

$$\begin{cases}a_ka_i+a_j=a_ka_{i'}+a_{j'}\\a_la_i+a_j=a_la_{i'}+a_{j'}\end{cases}\Rightarrow(a_k-a_l)a_i=(a_k-a_l)a_{i'}\Rightarrow a_i=a_{i'}\Rightarrow i=i'.$$

所以 $a_j=a_{j'}$, 进一步 $j=j'$. 这与拉丁方定义矛盾. 因此 $\langle a_{ij}^{(k)},a_{ij}^{(l)}\rangle$ 两两不同. □

引理 7.2.5

如果有 t 个两两正交的 n 阶拉丁方, 也有 t 个两两正交的 n' 阶拉丁方, 则有 t 个两两正交的 nn' 阶拉丁方.

证明: 略.

定理 7.2.6

设 $n=p_1^{a_1}\cdots p_r^{a_r}$, 其中 $p_1<\cdots<p_r$ 是不同素数, $a_1,\cdots,a_r\in\mathbb{Z}^+$, 让

$$t=\min_{1\le i\le r}(p_i^{a_i}-1) \tag{7.1}$$

则有 t 个两两正交的 n 阶拉丁方.

证明: 由于 $t\le p_i^{a_i}-1$, 则有 t 个两两正交的 $p_i^{a_i}$ 阶拉丁方, 由前一引理, 有 t 个两两正交的 $\prod_{i=1}^{r}p_i^{a_i}=n$ 阶拉丁方. □

注: 在 (7.1) 中, $t=1\Leftrightarrow n=2\times$ 奇数 $\Leftrightarrow n\equiv 2(\mathrm{mod}\ 4)$.

当 $n\equiv 2(\mathrm{mod}\ 4)$ 时, 是否有一对正交的 n 阶拉丁方? 当 $n=2$ 时没有, Euler 猜想 $n\ge 6$ 时也没有.

在 1900 年, Tarry 证明了 $n=6$ 没有. 但是在 1960 年, Bose, Shrikhande, Parker 证明了 $n>6$ 时有一对正交的 n 阶拉丁方.

n 阶拉丁方的完全正交集的存在性 $\Leftrightarrow n$ 阶射影平面的存在性.

Bruck-Ryser 定理: n 阶射影平面存在 $\Rightarrow n$ 可以表示成两个整数的平方和. 而数论中证明了 n 写成两个整数的平方和等价于 n 的素数分解式中 $4k+3$ 型素数出现偶数次.

利用这个定理, 可以说明 $2\times 7=14$ 阶射影平面不存在.

§ 7.3 (b,v,r,k,λ)-构形

设 $X=\{x_1,\cdots,x_v\}$ 是 v 元集 (统计中把元素称为 varieties), $X_1,\cdots,X_n$ 是 X 的 b 个子集 (统计中把 X 的子集叫 block), 如果有:

(1) $|X_i|=k, i=1,\cdots,b$.

(2) X 的每个二元子集恰好被 λ 个 X_i 所包含, 即 $|\{1\le i\le v|X_i\supset\{x,y\},x,y\in X,x\ne y\}|=\lambda$.

(3) $\lambda>0, k<r-1$.

此时称这是一个 **(b,v,r,k,λ)-构形**, 也叫**均衡不完全区组设计 (BIBD)**.

命题 7.3.1

在 (b,v,r,k,λ)-构形 X 中, $\{X_i\}_{i=1}^b$ 盖住 X 中每个元素恰好 r 次, 其中 r 满足 $r(k-1)=\lambda(v-1)$.

证明: 设 $x\in X$ 被 $\{X_i\}_{i=1}^b$ 盖住了恰好 r 次, 则

$$\sum_{\substack{y\in X\\ y\ne x}}|\{1\le i\le b|\{x,y\}\subseteq X_i\}|=\sum_{\substack{y\in X\\ y\ne x}}\lambda=\lambda(v-1).$$

另一方面,

$$\sum_{\substack{y\in X\\ y\ne x}}|\{1\le i\le b|\{x,y\}\subseteq X_i\}|=\sum_{\substack{y\in X\\ y\ne x}}\sum_{i=1}^{b}\underbrace{[\{x,y\}\subseteq X_i]}_{\text{特征函数}}=\sum_{\substack{x\in X_i\\ 1\le i\le b}}\sum_{\substack{y\in X\\ y\ne x}}1=\sum_{\substack{x\in X_i\\ 1\le i\le b}}(k-1)=r(k-1).$$

这样就给出了 (b,v,r,k,λ)-构形存在的一个必要条件. □

还可以证明:(证明略)

命题 7.3.2. Fisher 不等式

在 (b,v,r,k,λ)-构形 X 中, $b \geq v$.

注: (1) 若 $\lambda = 1$, 则 $(b,v,r,k,1)$ 构形存在可推出 $r(k-1) = v-1$ 且 $bk = vr$, 从而 $b\binom{k}{2} = \binom{v}{2}$.

(2) 若 $k = 3$ 且 $\lambda = 1$, 则 $r = \dfrac{v-1}{2}, b = \dfrac{v(v-1)}{6}$, 由 r, b 都是整数, 则 $v \equiv 1, 3 (\mathrm{mod}\ 6)$. 此时的构形叫$v$ **阶 Steiner 三元系**.

定义 7.3.1

设 $v \geq 3$. v 元集 X 的一些三元子集构成的v **阶 Steiner 三元系**指 X 的每个二元子集被这些三元子集中唯一的一个所包含.

由上面的推导, v 阶三元系存在的一个必要条件是

$$v \equiv 1, 3 (\mathrm{mod}\ 6). \tag{7.2}$$

例 7.3.3

对 $X = \{1, \cdots, 7\}$, 一个 7 阶 Steiner 三元系是

$$\{1,2,4\}, \{3,4,6\}, \{1,3,7\}, \{2,3,5\}, \{1,5,6\}, \{4,5,7\}, \{2,6,7\}.$$

J.Steinerz 在 1853 年研究四次曲线的二重切线时碰到这种三元系.

1853 年, Steiner 问: Steiner 三元系的充分必要条件是不是 $v \equiv 1, 3 (\mathrm{mod}\ 6)$, 而 1859 年, M.Reiss 证明了反方向也对!

7.3.1 Kirkman 女生问题

Kirkman 是英国的一所女子学校的校长, 他考虑如下问题: 一个班上有 15 个女生, 每天要进行散步, 把女生分成五组, 每组三个人, 求每周七天的散步安排方式使得任意两个女生在一周中恰好有一天分在同一组.

Kirkman 给出的解答如下:

星期日	{1, 2, 3},	{4, 8, 12},	{5, 10, 15},	{6, 11, 13},	{7, 9, 14}
星期一	{1, 4, 5},	{2, 8, 10},	{3, 13, 14},	{6, 9, 15},	{7, 11, 12}
星期二	{1, 6, 7},	{2, 9, 11},	{3, 12, 15},	{4, 10, 14},	{5, 8, 13}
星期三	{1, 8, 9},	{2,12,14},	{3, 5, 6},	{4, 11, 15},	{7, 10, 13}
星期四	{1, 10, 11},	{2, 13, 15},	{3, 4, 7},	{5, 9, 12},	{6, 8, 14}
星期五	{1, 12, 13},	{2, 4, 6},	{3, 9, 10},	{5, 11, 14},	{7, 8, 15}
星期六	{1, 14, 15},	{2, 5, 7},	{3, 8 ,11},	{4, 9, 13},	{6, 10, 12}

这是一个 Steiner 三元系的问题, 只不过需要满足更多条件.

Kirkman 三元系是一个 $v = 6n+3$ 阶 Steiner 三元系, 它满足如下附加条件: 它的 $b = (2n+1)(3n+1)$ 个三元子集可以分成 $3n+1$ 个分支, 使得每个分支都包含 $2n+1$ 个三元子集. $v = 6n+3$ 个 X 中元在每个分支中恰好出现一次. ($n = 2$ 就是 Kirkman 女生问题)

问题: 当 $n \geq 2$ 时, Kirkman 三元系是否存在?

高中物理教师陆家羲对 Kirkman 女生问题感兴趣, 在 1961 年, 他对一般的 n 证明了存在性, 然而当时一直未能发表, 后来被 R.Chaudburi, R.M.Wilson 发表了解法, 这对陆家羲打击很大.

7.3.2 Steiner 三元系大集问题

7 阶 Steiner 三元系

$$\{1,2,3\},\{1,4,5\},\{1,6,7\},\{2,4,6\},\{2,5,7\},\{3,4,7\},\{3,5,6\}$$

与

$$\{1,2,7\},\{1,3,4\},\{1,5,6\},\{2,3,6\},\{2,4,5\},\{3,5,7\},\{4,6,7\}$$

两两不相交. 问: 最多可以找多少个 v 阶三元系使得它们两两不相交?

设最多可以找 $D(v)$ 个 v 阶三元系使得它们两两不相交, v 元集 X 一共有 $\binom{v}{3}$ 个三元集, 而每个 v 阶 Steiner 三元系所含不交子集个数是 $b=\dfrac{v(v-1)}{6}$, 故 $D(v)\le\dfrac{1}{b}\binom{v}{3}=v-2$.

Cayley 证明了 $D(7)=2$, Kirkman 证明了 $D(9)=7$.

猜想 (Steiner 三元系大集问题): 是否对 $v\ge 9$ 且 $v\equiv 1,3(\mathrm{mod}\ 6)$, 都有 $D(v)=v-2$?

在 19 世纪, 这个问题就被提出, 但是没有任何进展. 1974 年, R.H.Denniston 借助超级计算机证明了 $D(15)=13$. 然而, 1981 年 9 月至 1983 年 4 月，美国《组合数学杂志》收到了陆家羲的六篇论文, 陆家羲证明了: 对 $v>7, v\equiv 1,3(\mathrm{mod}\ 6)$, 如果 $v\notin\{141,283,501,789,1501,2365\}$, 则 $D(v)=v-2$, 直接把这个问题基本上解决了. 这被誉为 20 世纪组合学领域的重大成就之一, 可惜陆家羲因为积劳成疾而英年早逝, 来不及深入研究这些工作.

第 8 章　考试相关

【作者温馨提示】考前建议把每章后面的习题都做一遍, 绝对有帮助.

题型: 填空题 (可能出类似于 $\sum_{k=0}^{n}\binom{n}{k}^2$ 等于多少)、解答题, 满分 100 分.

考试形式: 开卷 (2020-2021 学年)

考试时间: 最后一次上课的晚上 (不同年份的考试时间不一样, 有可能会选在考试周).

不考的内容: 整数分拆、生成函数、半序集上的莫比乌斯反演.

重点掌握内容:

- 组合恒等式: 基本技巧要会, 如反演公式、朱-Van 恒等式.
- 递归序列: 线性递推序列求通项公式 (比较好求).
- 容斥原理.
- 抽屉原理, 比如 n 个盒拿 k 个球的问题, $|\{x_1+\cdots+x_n=k|\cdots\}|$ 的估计等等.
- Ramsey 定理的含义, 重点看 Schur 定理的证明 (里面的 $x+y=z$ 可能会改一下, 做法类似.)
- 经典 Möbius 反演.
- 极值组合.
- Hall 定理.
- 组合零点: 弄简单的, 多项式是二元的, 如

$$|\{a+b|\cdots\}|\geq\min\{p,\underline{\quad\quad A\quad\quad}\},$$

  用多项式方法, 如果 A 小就用组合零点定理, 如果 A 大就把 $\{a+b\}$ 挖去一点元素, 让 A 减到 p.
- 有限射影平面, 比如举出二阶、三阶射影平面的例子.
- 更列数.

思考题

1. 设 $l,m,n\in\mathbb{N},l\geq n$, 则 $\sum_{k=0}^{n}(-1)^k\binom{n}{k}\binom{k+m}{l}=(-1)^n\binom{m}{l-n}$.
2. 设 $d,n\in\mathbb{Z}^+,d|n$, 整数 c,d 互素, 证明: $\left\{c+dq\middle|q=1,\cdots,\frac{n}{d}\right\}$ 恰好有 $\frac{\varphi(n)}{\varphi(d)}$ 个与 n 互素.
3. 证明: $\sum_{\substack{m=1\\(m,n)=1}}^{n}e^{2\pi i\frac{m}{n}}=\mu(n)$.
4. 设 $x_1,\cdots,x_n\in\mathbb{R},|x_i|\geq 1$. 任给 $c\in\mathbb{R}$, 证明:

$$\left|\left\{\langle\varepsilon_1,\cdots,\varepsilon_n\rangle\middle|\varepsilon_i\in\{\pm1\},\text{且}\sum_{i=1}^{n}\varepsilon_i x_i\in[c,c+2)\right\}\right|\leq\binom{n}{\lfloor\frac{n}{2}\rfloor}.$$

   提示: 用 Sperner 定理.

§8.1　部分习题解答

例 8.1.1

证明: 对正整数 n, 有

$$\sum_{k=1}^{n}\binom{n}{k}(-1)^k H_k^{(2)} = -\frac{H_n}{n}.$$

其中, $H_n^{(2)} = \sum_{k=1}^{n}\frac{1}{k^2}$ 是二阶调和数, $H_n = \sum_{k=1}^{n}\frac{1}{k}$ 是调和数.

证明: 由反演公式, 只需证

$$\sum_{k=1}^{n}\binom{n}{k}(-1)^{k-1}\frac{H_k}{k} = H_n^{(2)}.$$

事实上,

$$\begin{aligned}
LHS &= \sum_{k=1}^{n}\binom{n}{k}(-1)^{k-1}\frac{1}{k}\sum_{j=1}^{k}\binom{k}{j}\frac{(-1)^{j-1}}{j} \qquad 【利用\ \sum_{k=1}^{n}\binom{n}{k}\frac{(-1)^{k-1}}{k} = H_n】\\
&= \sum_{j=1}^{n}\left[\left(\sum_{k=j}^{n}\binom{n}{k}\binom{k}{j}(-1)^{k-1}\frac{1}{k}\right)\frac{(-1)^{j-1}}{j}\right] \qquad 【求和换序】\\
&= \sum_{j=1}^{n}\binom{n}{j}\frac{(-1)^{j-1}}{j}\sum_{k=j}^{n}\binom{n-j}{k-j}\frac{(-1)^{k-1}}{k} \qquad 【用\ \binom{n}{k}\binom{k}{j} = \binom{n}{j}\binom{n-j}{k-j}】\\
&= \sum_{j=1}^{n}\binom{n}{j}\frac{(-1)^{j-1}}{j}\sum_{l=0}^{n-j}\binom{n-j}{l}(-1)^{l+j-1}\int_0^1 x^{l+j-1}\mathrm{d}x \qquad 【换元\ k=j+l】\\
&= \sum_{j=1}^{n}\binom{n}{j}\frac{(-1)^{j-1}}{j}\left(\int_0^1\sum_{l=0}^{n-j}\binom{n-j}{l}(-x)^l x^{j-1}\mathrm{d}x\right)(-1)^{j-1}\\
&= \sum_{j=1}^{n}\binom{n}{j}\frac{(-1)^{j-1}}{j}\int_0^1(1-x)^{n-j}x^{j-1}\mathrm{d}x(-1)^{j-1} \qquad 【二项式定理】\\
&= \sum_{j=1}^{n}\binom{n}{j}\frac{1}{j}\frac{(n-j)!(j-1)!}{n!} \qquad 【\text{Beta 函数性质}】\\
&= \sum_{j=1}^{n}\frac{1}{j^2} = H_n^{(2)}.
\end{aligned}$$

□

例 8.1.2

设 $l,m,n\in\mathbb{N}, l\geq n$, 则 $\sum_{k=0}^{n}(-1)^k\binom{n}{k}\binom{k+m}{l} = (-1)^n\binom{m}{l-n}$.

证明: 由二项式变换反演公式, 只需证

$$\sum_{k=0}^{n}(-1)^k\binom{n}{k}(-1)^k\binom{m}{l-k} = \binom{n+m}{l}.$$

事实上, 根据朱-Vandermonde 恒等式,

$$\sum_{k=0}^{n}(-1)^k\binom{n}{k}(-1)^k\binom{m}{l-k}=\sum_{k=0}^{n}\binom{n}{k}\binom{m}{l-k}=\binom{n+m}{l}.$$

例 8.1.3

设 $d,n\in\mathbb{Z}^+,d|n$, 整数 c,d 互素, 证明: $\left\{c+dq\middle|q=1,\cdots,\frac{n}{d}\right\}$ 恰好有 $\frac{\varphi(n)}{\varphi(d)}$ 个与 n 互素.

证明: 欲证命题等价于 $\{c+dq|q=1,\cdots,n\}$ 恰好有 $\frac{d\varphi(n)}{\varphi(d)}$ 个与 n 互素. 设 d 的所有素因子为 $p_1,\cdots,p_l$, n 的所有素因子为 $p_1,\cdots,p_l,p_{l+1},\cdots,p_k$.

设 $S=\{1,2,\cdots,n\}$, 称 $a\in S$ 具有性质 P_i 指 $p_i|c+da$. 取

$$\begin{aligned}S_i&=\{a\in S|a\text{具有性质}P_i\},\\N(P_{i_1}P_{i_2}\cdots P_{i_t})&=\{a\in S|a\text{具有性质}P_{i_1},\cdots,P_{i_t}\},\\N(P'_{i_1}P'_{i_2}\cdots P'_{i_t})&=\{a\in S|a\text{不具有}P_{i_1},\cdots,P_{i_t}\text{中任何一个性质}\},\end{aligned}$$

则 $\{c+dq|q=1,\cdots,n\}$ 中与 n 互素的数共有 $|N(P'_1P'_2\cdots P'_n)|$ 个.

由于 $(c,d)=1$, 故对任意 $a\in S$, 都有 $p_i\nmid c+da$, 从而对任意的 $\{i_1,\cdots,i_t\}\subseteq\{1,2,\cdots,l\}$, 都有 $N(P_{i_1}P_{i_2}\cdots P_{i_t})=0$. 由容斥原理,

$$\begin{aligned}|N(P'_1P'_2\cdots P'_n)|&=\left|\bigcap_{i=1}^{n}\overline{S_i}\right|=|S|-\left|\bigcup_{i=1}^{n}S_i\right|\\&=n-\sum_{i=1}^{k}N(P_i)+\sum_{1\le i<j\le k}N(P_iP_j)-\cdots+(-1)^kN(P_1P_2\cdots P_k)\\&=n-\sum_{i=l+1}^{k}\frac{n}{p_i}+\sum_{l+1\le i<j\le k}\frac{n}{p_ip_j}-\cdots+(-1)^k\frac{n}{p_1\cdots p_k}\\&=n\prod_{i=l+1}^{k}\left(1-\frac{1}{p_i}\right)=d\cdot\frac{n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)}{d\prod_{i=1}^{l}\left(1-\frac{1}{p_i}\right)}=\frac{d\varphi(n)}{\varphi(d)},\end{aligned}$$

这里利用了 $\varphi(n)=n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$. □

例 8.1.4

证明: $\sum_{\substack{m=1\\(m,n)=1}}^{n}e^{2\pi i\frac{m}{n}}=\mu(n)$.

解: 设 $f(x)=e^{2\pi ix}$, $F=\sum_{m=1}^{n}f\left(\frac{m}{n}\right)$, $G=\sum_{\substack{m=1\\(m,n)=1}}^{n}f\left(\frac{m}{n}\right)$, 则 $F(n)=\begin{cases}1, & n=1,\\0, & n>1.\end{cases}$, 从而 $\mu*F=\sum_{d|n}\mu\left(\frac{n}{d}\right)F(d)=\mu(n)$. 故欲证命题等价于 $\mu*F=G$. 由 Möbius 反演, 只需要证 $F(n)=\sum_{d|n}G(d)$,

即证

$$\sum_{k=1}^{n} f\left(\frac{k}{n}\right)=\sum_{d|n}\sum_{\substack{m=1\\(m,d)=1}}^{d} f\left(\frac{m}{d}\right). \qquad (*)$$

只需要比较等号两边 $f\left(\frac{k}{n}\right)$ 出现的次数. 由于 $\frac{k}{n}$ 写成既约分数为 $\frac{\frac{k}{(n,k)}}{\frac{n}{(n,k)}}$, 取 $d=\frac{n}{(n,k)}, m=\frac{k}{(n,k)}$, 则 $(m,d)=1$ 且 $d|n$. 而如果 $(m,d)=1$ 且 $d|n$, 则 $\frac{m}{d}$ 是既约分数. 因此等号右边出现 $f\left(\frac{k}{n}\right)$ 的次数是 1. 故 $(*)$ 式成立. □

例 8.1.5

设 $x_1,\cdots,x_n\in\mathbb{R}, |x_i|\geq 1$. 任给 $c\in\mathbb{R}$, 证明:

$$\left|\left\{\langle\varepsilon_1,\cdots,\varepsilon_n\rangle\middle|\varepsilon_i\in\{\pm 1\}, \text{且}\sum_{i=1}^{n}\varepsilon_i x_i\in[c,c+2)\right\}\right|\leq\binom{n}{\lfloor\frac{n}{2}\rfloor}.$$

提示: 用 Sperner 定理.

证明: 如果 $\sum_{i=1}^{n}\varepsilon_i x_i\in[c,c+2)$, 且 $x_j\leq -1$, 把 x_j 换成 $-x_j$, 可得 $\sum_{\substack{i=1\\i\neq j}}^{n}\varepsilon_i x_i+(-\varepsilon_i)(-x_j)\in[c,c+2)$. 因此可以不妨设 $x_i\geq 1(\forall i=1,2,\cdots,n)$.

设 $A=\left\{\langle\varepsilon_1,\cdots,\varepsilon_n\rangle\middle|\varepsilon_i\in\{\pm 1\}, \text{且}\sum_{i=1}^{n}\varepsilon_i x_i\in[c,c+2)\right\}$, 定义 $\{1,\cdots,n\}$ 的子集族为

$$\mathscr{A}=\left\{B\middle|\varepsilon_i=\begin{cases}1, & i\in B,\\ -1, & i\notin B,\end{cases}, \text{且}\sum_{i=1}^{n}\varepsilon_i x_i\in[c,c+2)\right\}.$$

则 $A\mapsto\mathscr{A}$ 是一一映射,

我们下面证明 $\mathscr{A}$ 是反链, 即任意 $\mathscr{A}$ 中元素互不包含, 设 $\langle\varepsilon_1,\cdots,\varepsilon_n\rangle,\langle\eta_1,\cdots,\eta_n\rangle\in A$, 且至少有一个分量不同. 则 $\sum_{i=1}^{n}\varepsilon_i x_i,\sum_{i=1}^{n}\eta_i x_i\in[c,c+2)$.

不妨设 $\varepsilon_1=1,\eta_1=-1$. 我们证明存在 k 使得 $\varepsilon_k=-1,\eta_k=1$, 这样根据 $\mathscr{A}$ 的定义可知 $\mathscr{A}$ 是反链.

(反证) 若不存在 k 使得 $\varepsilon_k=-1,\eta_k=1$, 则必有 $\varepsilon_i\geq\eta_i(\forall 1\leq i\leq n)$, 从而

$$c+2>\sum_{i=1}^{n}\varepsilon_i x_i=\sum_{i=1}^{n}\eta_i x_i+\sum_{i=1}^{n}(\varepsilon_i-\eta_i)x_i\geq c+\sum_{\varepsilon_i\neq\eta_i}2x_i\geq c+2x_1\geq c+2,$$

得到矛盾. 所以 $\mathscr{A}$ 是反链, 由 Sperner 定理可得 $|A|=|\mathscr{A}|\leq\binom{n}{\lfloor\frac{n}{2}\rfloor}$. □