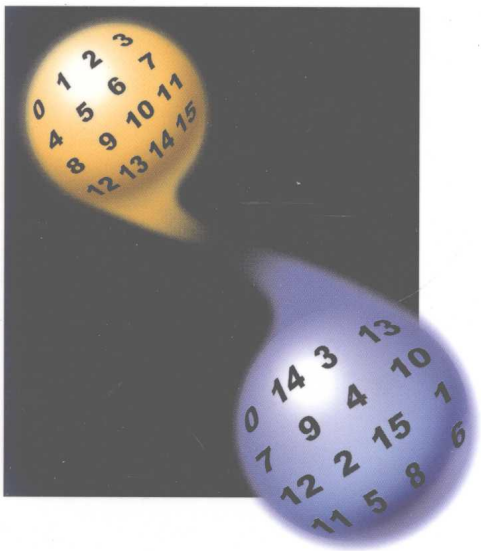
组合设计理论

Theory of Combinatorial Designs

（第二版）

沈灏 著



上海交通大學出版社

组合设计理论

（第二版）

沈　灏　著

上海交通大学出版社

内 容 提 要

本书系统论述组合设计理论。全书共分十章，全面深入地介绍了区组设计、有限几何、差集与差族、Hadamard 矩阵、成对平衡设计和可分解设计等组合设计理论主要分支的基本概念、基础理论和重要方法，还介绍了组合设计理论在纠错码理论和密码学中的若干应用。本书论证严谨、叙述简洁、语言流畅。

本书可作为数学、信息论和计算机科学等专业的研究生和高年级本科生有关课程的教材或教学参考书，也可供相关领域的研究者作参考之用。

图书在版编目(CIP)数据

组合设计理论/沈灏著. —2 版. —上海：上海交通大学出版社，2008

ISBN 978-7-313-01666-9

I. 组... II. 沈... III. 组合设计 IV. 0157.2

中国版本图书馆 CIP 数据核字(2008)第 025126 号

组合设计理论

（第二版）

沈 灏 著

上海交通大学出版社出版发行

(上海市番禺路 877 号 邮政编码 200030)

电话：64071208 出版人：韩建民

常熟市华通印刷有限公司 印刷 全国新华书店经销

开本：787mm×960mm 1/16 印张：21.25 字数：398 千字

1996 年 9 月第 1 版 2008 年 1 月第 2 版 2008 年 1 月第 2 次印刷

印数：3050

ISBN 978-7-313-01666-9/O・101 定价：42.00 元

第二版前言

组合设计理论是离散数学的一个重要分支, 是一门研究将事物按特定要求进行安排并讨论其性质的学问, 它的历史可以追溯到远古. 我国四千多年前关于“河图洛书”的美丽传说, 其中的“洛书”就是一个简单的组合设计——3阶幻方. 历史上许多有关组合设计的著名难题, 如Euler的36军官问题和Kirkman女生问题等, 以其特有的魅力, 吸引了一代又一代青年学子, 把他们领进数学研究的殿堂.

然而组合设计又是一个相对年轻的数学分支. 对于组合设计的系统研究, 始于20世纪30年代R. C. Bose等人的工作. 自20世纪60年代起, 随着关于正交拉丁方的Euler猜想, 关于组合设计的存在性猜想以及关于不相交Steiner三元系大集的存在性等著名问题的解决, 特别是关于组合设计的理论与方法在数理统计、运筹学、信息论和计算机科学中的应用日益广泛, 组合设计理论的研究进入了一个飞速发展的黄金时期, 在近50年来取得了令人瞩目的巨大进展. 组合设计的一些基本问题和历史上久悬未决的难题一个接一个被解决, 新的理论和方法不断创立和引入, 应用领域不断扩大, 组合设计的面貌发生了根本性的变化, 它在理论上已渐趋成熟.

组合设计理论是一个既有古老的历史渊源, 而又相对年轻的数学分支, 是一个生气勃勃、广有前途的研究领域. 它既有很强的理论性, 又有广泛的应用价值, 并且饶有趣味, 引人入胜. 这是一座充满珍花异草的美好园林, 足以使观赏者流连, 更能激发起青年人创造的激情, 研究数学之理, 探求数学之用, 感受数学之美.

本书第一版于1996年出版以来, 得到了国内外同行的关心与热情鼓励. 很多大学将此书用作研究生教材或教学参考书, 并在使用中不断地向作者提供宝贵的改进意见与建议. 近10年来, 组合设计的理论、方法和研究内容发生了深刻的变化. 组合设计理论不但与编码理论和密码学有着广泛和深刻的联系, 而且在实验设计与分析、计算机网络、算法设计与分析、数据结构、生物与生命科学, 甚至像光学与医疗诊断学这样的领域, 都有着实质性的应用. 为了适应在理论和应用上这种变化和发展的需要, 我们在第二版中, 对全书进行了全面的改写, 并且新增了“可分解设计”和“设计的应用”两章. 在本书中, 我们对组合设计的基本概念、基础理论以及重要的方法与技巧作了比较全面、系统和有一定深度的论述, 努力反映组合设计理论研究的新进展与新成果. 本书还精选出300余篇文献以供读者作进一步的研读和参考. 对我国数学家在组合设计理论与应用研究中所取得的成果也作了适当的介绍. 本书中还列出了一批有待解决的重要问题和猜想, 供有志者一试锋芒.

本书可用作数学、应用数学、信息论与计算机科学等专业的研究生和本科高年级学生的教材或教学参考书, 也可供有关领域专家研究时作参考之用.

本书第二版在写作过程中, 得到了不少国内外同行的关心和帮助. 常彦勋教授, 曹珍

富教授, 向青教授和殷剑兴教授提出了宝贵的修改意见. 李秀丽博士, 熊瑜博士和邓大萌副教授认真地校阅了本书的部分章节, 作者谨向他们表示由衷的感谢. 特别要感谢张媛博士、沈军博士、刘丽华博士和李伟霞博士, 他们耐心细致地为本书打印文稿, 付出了十分艰辛的劳动. 最后, 本书责任编辑韩正之教授, 他以编辑和数学行家的双重身份, 十分细致地逐字审阅原稿, 提出了一系列中肯的修改意见, 为使本书增色, 付出了大量精力, 对此, 作者谨向他致以诚挚的谢意.

著者

2007年12月

目 录

第 1 章　引论

组合设计理论的主要研究对象是各种类型的有限关联结构.作为全书的引论, 本章概要地介绍平衡不完全区组设计、成对平衡设计、可分组设计、横截设计以及t-设计等重要关联结构的基本概念, 并讨论它们之间的相互联系, 以期使读者对组合设计理论的内容、方法与特点有一个初步了解.

1.1　有限关联结构

定义 1.1.1　设V与$\mathbf{B}$为两个不相交的集合, $\mathbf{I}$为V与$\mathbf{B}$之间的二元关系, 即$\mathbf{I} \subseteq V \times \mathbf{B}$, 则称$\mathbf{D} = (V, \mathbf{B}, \mathbf{I})$为一个**关联结构**(incidence structure). V的元素叫**点** (point), $\mathbf{B}$ 的元素叫**区组**(block), $\mathbf{I}$叫**关联关系**(incidence relation). 设$p \in V$, $B \in \mathbf{B}$, 若$(p, B) \in \mathbf{I}$, 则称点p与区组B关联并记作$p\mathbf{I}B$. 若p与B不关联, 则记作$p\not\mathbf{I}B$.

有时为了强调关联结构的几何意义, 也把区组叫做**直线**(line). 此时, "$p\mathbf{I}B$" 也可读作"点p在直线B上"或"直线B经过点p".

本书只讨论有限关联结构, 即V与$\mathbf{B}$都是有限集的关联结构.当$\mathbf{D} = (V, \mathbf{B}, \mathbf{I})$ 为有限关联结构时, 常以v表示集合V 的基数, b表示集合$\mathbf{B}$的基数, 即$v = |V|$, $b = |\mathbf{B}|$, 并称v为$\mathbf{D}$的**阶**(order).

定义 1.1.2　设$V = \{p_1, p_2, \cdots, p_v\}$, $\mathbf{B} = \{B_1, B_2, \cdots, B_b\}$, $\mathbf{D} = (V, \mathbf{B}, \mathbf{I})$为有限关联结构. 对$1 \leqslant i \leqslant v$, $1 \leqslant j \leqslant b$, 令

$$a_{ij} = \begin{cases} 1, & 若 p_i \mathbf{I} B_j, \\ 0, & 若 p_i \not\mathbf{I} B_j, \end{cases} \tag{1.1.1}$$

则称$(0,1)$-矩阵

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1b} \\ a_{21} & a_{22} & \cdots & a_{2b} \\ \vdots & \vdots & \ddots & \vdots \\ a_{v1} & a_{v2} & \cdots & a_{vb} \end{bmatrix} \tag{1.1.2}$$

为$\mathbf{D}$的**关联矩阵**(incidence matrix) .

对$1 \leqslant i \leqslant v$, 令$r_i$表示$\mathbf{B}$中与点$p_i$关联的区组数; 对$1 \leqslant j \leqslant b$, 令$k_j$表示$V$中与区组$B_j$关联的点的个数; 对$1 \leqslant i, j \leqslant v$, $i \neq j$, 令λ_{ij}表示$\mathbf{B}$中同时与点p_i及p_j关联的区组数. r_i叫做点p_i的**重复度**(replication number), k_j叫做区组B_j的**容量**(**或长度**)(length), λ_{ij}叫做点p_i与p_j的**相遇数**. 于是r_i等于关联矩阵A的第i行的**行和**(row sum), 亦即第i行中1的个数, k_j为A的第j列的**列和**(column sum), 而λ_{ij}则是A的第i行与第j行的内积. 因此, 用两种方法计算A中1的个数, 可得下述等式:

$$\sum_{i=1}^{v} r_i = \sum_{j=1}^{b} k_j. \tag{1.1.3}$$

再令w_v表示元素全为1的v维行向量, A^{T}表示A的转置矩阵, 则得

$$AA^{\mathrm{T}} = \begin{bmatrix} r_1 & \lambda_{12} & \lambda_{13} & \cdots & \lambda_{1v} \\ \lambda_{21} & r_2 & \lambda_{23} & \cdots & \lambda_{2v} \\ \lambda_{31} & \lambda_{32} & r_3 & \cdots & \lambda_{3v} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda_{v1} & \lambda_{v2} & \lambda_{v3} & \cdots & r_v \end{bmatrix}, \tag{1.1.4}$$

$$w_v A = (k_1, k_2, k_3, \cdots, k_b). \tag{1.1.5}$$

有限关联结构$\mathbf{D} = (V, \mathbf{B}, \mathbf{I})$的关联矩阵与$V$及$\mathbf{B}$中元素的排列顺序有关. 因此, 同一个关联结构可有多个不同的关联矩阵. 另一方面,不同的有限关联结构可能有相同的关联矩阵.为了研究有限关联结构之间的关系以及表示同一个有限关联结构的各个关联矩阵之间的关系, 我们先引入下述概念.

定义 1.1.3 *设$\mathbf{D}_1 = (V_1, \mathbf{B}_1, \mathbf{I}_1)$与$\mathbf{D}_2 = (V_2, \mathbf{B}_2, \mathbf{I}_2)$为两个有限关联结构. 设*

$$\sigma : V_1 \cup \mathbf{B}_1 \to V_2 \cup \mathbf{B}_2$$

为满足下述条件的一个双射:

(i) $\sigma(V_1) = V_2$, $\sigma(\mathbf{B}_1) = \mathbf{B}_2$;

(ii) 对任意$p \in V_1$, 与任意$B \in \mathbf{B}_1$,当且仅当$p\mathbf{I}_1 B$时才有$\sigma(p)\mathbf{I}_2\sigma(B)$.

则称σ为$\mathbf{D}_1$到$\mathbf{D}_2$上的一个**同构映射**或**同构**(isomorphism).若存在$\mathbf{D}_1$到$\mathbf{D}_2$上的一个同构映射,则称$\mathbf{D}_1$与$\mathbf{D}_2$同构,记作$\mathbf{D}_1 \cong \mathbf{D}_2$. 当$\mathbf{D}_1 = \mathbf{D}_2 = \mathbf{D}$时,$\mathbf{D}$到自身上的同构叫做$\mathbf{D}$的**自同构**(automorphism). $\mathbf{D}$的全体自同构关于映射的合成组成一个群,叫做$\mathbf{D}$的**全自同构群**(full automorphism group), 并记作Aut($\mathbf{D}$). Aut($\mathbf{D}$)的任一子群都叫做$\mathbf{D}$的**自同构群**(automorphism group).

定义 1.1.4 *各行各列都恰有一个1的$n \times n$ $(0,1)$-矩阵叫做n阶**置换矩阵**(permutation matrix). 设A与B为两个$m \times n$ $(0,1)$-矩阵, 若存在m阶置换矩阵P及n阶置换矩阵Q, 使$PAQ = B$,则称A与B**置换相抵**(permutation equivalent).*

置换相抵关系具有自反性、对称性和传递性,因而是一个等价关系.

引理 1.1.1　同一个有限关联结构的各关联矩阵置换相抵.

证　设$\mathbf{D}=(V,\mathbf{B},\mathbf{I})$为有限关联结构,$A$为它的一个关联矩阵. 将$V$中的点重新排列,对应于将$A$的各行作相应的重新排列亦即在$A$的左边乘以一个适当的置换矩阵$P$, 将$\mathbf{B}$中的区组重新排列, 对应于将$A$中的各列作相应的重新排列亦即在$A$的右边乘以一个适当的置换矩阵$Q$,从而此时$\mathbf{D}$的关联矩阵变为$PAQ$.因此$\mathbf{D}$的对应于$V$与$\mathbf{B}$中元素不同排列的各个关联矩阵彼此置换相抵.即得结论. □

定理 1.1.1　设A与B分别为有限关联结构$\mathbf{D}_1$与$\mathbf{D}_2$的关联矩阵,则$\mathbf{D}_1$与$\mathbf{D}_2$ 同构的充分必要条件是A与B置换相抵.

证　设$\mathbf{D}_1=(V_1,\mathbf{B}_1,\mathbf{I}_1)$, $V_1=\{p_1,p_2,\cdots,p_v\}$, $\mathbf{B}_1=\{B_1,B_2,\cdots,B_b\}$ 且此时$\mathbf{D}_1$的关联矩阵为A.若A与B置换相抵,则有置换矩阵P与Q使$PAQ=B$.而PAQ是将V_1与$\mathbf{B}_1$ 中元素作适当重新排列后$\mathbf{D}_1$的关联矩阵.具有同一关联矩阵的两个有限关联结构显然是同构的,因此$\mathbf{D}_1\cong\mathbf{D}_2$. 反之,设$\mathbf{D}_1\cong\mathbf{D}_2$, $\mathbf{D}_2=(V_2,\mathbf{B}_2,\mathbf{I}_2)$, σ为$\mathbf{D}_1$到$\mathbf{D}_2$上的一个同构, 则$V_2=\{\sigma(p_1),\sigma(p_2),\cdots,\sigma(p_v)\}$, $\mathbf{B}_2=\{\sigma(B_1),\sigma(B_2),\cdots,\sigma(B_b)\}$ 且此时$\mathbf{D}_2$的关联矩阵也是A.于是A与B都是$\mathbf{D}_2$的关联矩阵,由**引理**1.1.1可知A与B置换相抵.即得结论. □

我们常将集合论中的属于关系"$\in$"用作关联关系, 并把关联结构$(V,\mathbf{B},\in)$简单地记作$(V,\mathbf{B})$, 此时$\mathbf{B}$的元素其实就是V的子集. 需要指出的是, V的一个子集在$\mathbf{B}$中可能出现不止一次, 这样的区组叫做**重复区组**(repeated block). $\mathbf{B}$ 中全体不同区组的集合$\mathbf{B}'$叫做$\mathbf{B}$的**支撑集**(support), $\mathbf{B}'$中所含区组的个数叫做**支撑数**(support size). 通常用字母b表示$\mathbf{B}$中所含的区组数, 用b'表示支撑数. 不包含重复区组的关联结构叫做**单纯**(simple)关联结构.

例 1.1.1　令$V=Z_7$为以7为模的全体剩余类的集合, 令

$$\mathbf{B}=\big\{\{0,1,3\},\ \{1,2,4\},\ \{2,3,5\},\ \{3,4,6\},\ \{4,5,0\},\ \{5,6,1\},\ \{6,0,2\}\big\}.$$

若将区组看作直线, 则$\mathbf{D}=(Z_7,\mathbf{B})$是一个由7个点和7条直线组成的关联结构, 它的关联矩阵为

$$A=\begin{bmatrix}1&0&0&0&1&0&1\\1&1&0&0&0&1&0\\0&1&1&0&0&0&1\\1&0&1&1&0&0&0\\0&1&0&1&1&0&0\\0&0&1&0&1&1&0\\0&0&0&1&0&1&1\end{bmatrix}. \tag{1.1.6}$$

这个关联矩阵可由图1.1给出的Fano构形直观表示.

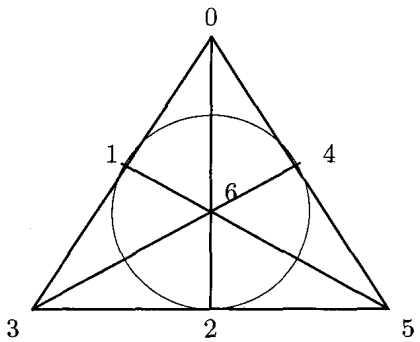


图 1.1 Fano构形

D的7个点分别由图中三角形的重心、三个顶点及三边中点表示,7条直线则分别由三角形的三条边、三条中线以及过三边中点的圆周表示.下面将会看到, 如此简单的Fano构形, 却有着多种有趣的几何学与组合论的解释: 可以把它看作一个7阶Steiner三元系, 也可看作一个循环区组设计, 还可看作一个2阶射影平面, 从图论的角度看, 它又可看作一个7阶完全图的三角形分解, 真可谓是"横看成岭侧成峰, 远近高低各不同".

例 1.1.2 令$V = Z_6$,

$$\mathbf{B} = \{\{2,4,5\},\ \{2,4,5\},\ \{0,1,5\},\ \{0,3,5\},\ \{0,1,4\},\ \{0,2,3\},\ \{1,2,3\},\ \{1,3,4\},\ \{0,1,2,4\},\ \{0,1,2,5\},\ \{0,2,3,4\},\ \{0,3,4,5\},\ \{1,2,3,5\},\ \{1,3,4,5\}\}.$$

$\mathbf{D} = (Z_6, \mathbf{B})$是一个6阶关联结构, 它共包含14个区组. **D**的关联矩阵为

$$A = \begin{bmatrix} 0&0&1&1&1&1&0&0&1&1&1&1&0&0 \\ 0&0&1&0&1&0&1&1&1&1&0&0&1&1 \\ 1&1&0&0&0&1&1&0&1&1&1&0&1&0 \\ 0&0&0&1&0&1&1&1&0&0&1&1&1&1 \\ 1&1&0&0&1&0&0&1&1&0&1&1&0&1 \\ 1&1&1&1&0&0&0&0&0&1&0&1&1&1 \end{bmatrix}. \tag{1.1.7}$$

由于用作区组B_1与B_2的是同一子集$\{2,4,5\}$,因此A的第一列与第二列相同.

下面再举一个不以$\in$为关联关系的有限关联结构的例子.用F_q表示q阶有限域.

例 1.1.3 设V由F_2上如下7个2×3矩阵组成:

$$\begin{bmatrix} 1&0&0 \\ 0&1&0 \end{bmatrix}, \begin{bmatrix} 1&0&0 \\ 0&0&1 \end{bmatrix}, \begin{bmatrix} 1&1&1 \\ 0&1&1 \end{bmatrix}, \begin{bmatrix} 0&1&1 \\ 0&0&1 \end{bmatrix}, \begin{bmatrix} 0&1&0 \\ 1&0&1 \end{bmatrix}, \begin{bmatrix} 1&1&1 \\ 1&1&0 \end{bmatrix}, \begin{bmatrix} 1&1&0 \\ 1&0&1 \end{bmatrix}.$$

$\mathbf{B}$由F_2上全体3维非零向量组成, 即

$$\mathbf{B}=\{(1\ 0\ 0),\ (0\ 1\ 0),\ (0\ 0\ 1),\ (1\ 1\ 0),\ (1\ 0\ 1),\ (0\ 1\ 1),\ (1\ 1\ 1)\}.$$

关联关系$\mathbf{I}$规定如下: 对$p\in V, B\in\mathbf{B}$,当且仅当

$$p\times B^{\mathrm{T}}=\begin{bmatrix}0\\0\end{bmatrix}\text{或}\begin{bmatrix}1\\1\end{bmatrix}$$

时$p\mathbf{I}B$,则$\mathbf{D}=(V,\mathbf{B},\mathbf{I})$是一个7阶关联结构, 它与例1.1.1中的关联结构同构.

定理 1.1.2　任一有限关联结构$\mathbf{D}=(V,\mathbf{B},\mathbf{I})$都与某个以“$\in$”为关联关系的关联结构$\mathbf{D}'=(V,\mathbf{B}')$同构.

证　设$\mathbf{B}=\{B_1,B_2,\cdots,B_b\}$, 令

$$B'_j=\{p\in V|p\mathbf{I}B_j\},\ 1\leqslant j\leqslant b,$$

则B'_j是V的子集.令$\mathbf{B}'=\{B'_1,B'_2,\cdots,B'_b\}$,则对任一$p\in V$与任一$j=1,2,\cdots,b$,当且仅当$p\mathbf{I}B_j$时$p\in B'_j$.从而$\mathbf{D}$与$\mathbf{D}'=(V,\mathbf{B}')$ 有相同的关联矩阵.由**定理**1.1.1, $\mathbf{D}$与$\mathbf{D}'$同构. □

因此,在大多数情形,我们讨论的都是以“$\in$”为关联关系的关联结构. 不过, 在某些场合, 采用一般意义下的关联关系, 将使我们在研究有关设计问题时具有较大的自由度和灵活性.

下面介绍由已知关联结构来构造新的关联结构的两个简单方法.

定义 1.1.5　设$\mathbf{D}=(V,\mathbf{B},\mathbf{I})$为有限关联结构, 令$V^*=\mathbf{B},\mathbf{B}^*=V,\mathbf{D}^*=(V^*,\mathbf{B}^*,\mathbf{I}^*)$, 关联关系$\mathbf{I}^*$以下述方式给出: 对任意$p^*\in V^*$, $B^*\in\mathbf{B}^*$, 当且仅当$B^*\mathbf{I}p^*$时有$p^*\mathbf{I}^*B^*$. 则称$\mathbf{D}^*$为$\mathbf{D}$的**对偶结构**(dual structure).

若A为$\mathbf{D}$的关联矩阵, 则A的转置阵A^{T}是$\mathbf{D}^*$的关联矩阵.显然有$(\mathbf{D}^*)^*=\mathbf{D}$.

定义 1.1.6　设$\mathbf{D}=(V,\mathbf{B},\mathbf{I})$为有限关联结构, 令$\overline{\mathbf{I}}=(V\times\mathbf{B})\setminus\mathbf{I}$, $\overline{\mathbf{D}}=(V,\mathbf{B},\overline{\mathbf{I}})$, 则$\overline{\mathbf{D}}$称为$\mathbf{D}$的**补结构**或简称**补**(complement), 亦即对任意$p\in V$与任意$B\in\mathbf{B}$, 当且仅当$p\not\mathbf{I}B$时有$p\overline{\mathbf{I}}B$.

设$v=|V|$, $b=|\mathbf{B}|$, A为$\mathbf{D}$的关联矩阵. 令J_{vb}表示$v\times b$全1阵, 则$J_{vb}-A$是$\overline{\mathbf{D}}$ 的关联矩阵.

当$\mathbf{D}=(V,\mathbf{B})$为以“$\in$”作为关联关系的关联结构时, 令$\overline{\mathbf{B}}=\{V\setminus B|B\in\mathbf{B}\}$, 则$\overline{\mathbf{D}}$与$(V,\overline{\mathbf{B}})$同构, 因此我们也可直接将$(V,\overline{\mathbf{B}})$看作$\mathbf{D}$的补结构.

例 1.1.4 设$\mathbf{D}$为由例1.1.1给出的关联结构, 则$\overline{\mathbf{D}} \cong (Z_7, \overline{\mathbf{B}})$,此处

$$\overline{\mathbf{B}} = \{\{2,4,5,6\},\{3,5,6,0\},\{4,6,0,1\},\{5,0,1,2\},\{6,1,2,3\},\{0,2,3,4\},\{1,3,4,5\}\}.$$

其关联矩阵为

$$J-A=\begin{bmatrix} 0&1&1&1&0&1&0\\ 0&0&1&1&1&0&1\\ 1&0&0&1&1&1&0\\ 0&1&0&0&1&1&1\\ 1&0&1&0&0&1&1\\ 1&1&0&1&0&0&1\\ 1&1&1&0&1&0&0 \end{bmatrix}.$$

关于关联结构的定义过于宽泛, 以致任何一个$(0,1)$-矩阵都可以作为某个有限关联结构的关联矩阵. 因此对于一般的关联结构, 很难指望能得到比较深刻的结果. 然而, 当所讨论的有限关联结构满足某些特定的条件和约束时, 它们就有可能变得既有深刻的理论意义, 又有广泛的应用价值, 而且饶有趣味, 引人入胜.

设$\mathbf{D} = (V, \mathbf{B}, \mathbf{I})$为有限关联结构. 对$p \in V$, 令$r_p$表示点$p$的重复度; 对$B \in \mathbf{B}$, 令$k_B$表示区组$B$的容量; 对$V$的任一$t$元子集$S$, 令$\lambda_S$表示与$S$中每一点都关联的区组个数. 在设计理论的研究中, 以下条件是最常用的.

(i) **正则性**(regularity): 存在常数$r > 0$,使对所有$p \in V$都有$r_p = r$.

(ii) **均匀性**(uniformity): 存在常数$k > 0$,使对所有$B \in \mathbf{B}$都有$k_B = k$.

(iii) t-**平衡性**(t-balance): 对给定的正整数t, 存在常数$\lambda > 0$,使对V的任一 t 元子集S都有$\lambda_S = \lambda$.

1-平衡性即正则性, 2-平衡性通常就叫做平衡性.在本章以后各节中, 将简要介绍几类重要的有限关联结构.

1.2 平衡不完全区组设计

同时满足正则性、均匀性和平衡性三个条件的有限关联结构叫平衡不完全区组设计, 切实言之, 有以下定义.

定义 1.2.1 设v, k, λ为给定的正整数, $\mathbf{D} = (V, \mathbf{B}, \mathbf{I})$为有限关联结构.若以下条件满足:

(i) $|V| = v$;

(ii) 对任意$B \in \mathbf{B}$,都有$k_B = k$;

(iii) 对任意$p, q \in V, p \neq q$, 都有$\lambda_{p,q} = \lambda$.

则称$\mathbf{D}$是一个**平衡不完全区组设计**(balanced incomplete block design), 简称**区组设计**(block design) 或**BIB设计**, 记作B$(k, \lambda; v)$. v叫做$\mathbf{D}$的**阶**(order), k叫做$\mathbf{D}$的**区组容量**或**区组长度**(block size), λ叫做**相遇数**或**指数**(index).

由于历史上的原因, $\lambda = 1$ 时的BIB设计通常叫做**Steiner系**(Steiner system)或**Steiner 2-设计**, 并且$\mathrm{B}(k,1;v)$也常记作$\mathrm{S}(2,k;v)$. 随之, 对一般的λ, $\mathrm{B}(k,\lambda;v)$也记作$S_\lambda(2,k;v)$.

引理 1.2.1　*设$k \geqslant 2$, $\mathbf{D} = (V,\mathbf{B})$为一个$\mathrm{B}(k,\lambda;v)$, 则*

(i) *V中任意一点p的重复度为*

$$r_p = r = \lambda(v-1)/(k-1), \tag{1.2.1}$$

(ii) **B**中所包含的区组个数为

$$b = |\mathbf{B}| = \lambda v(v-1)/k(k-1). \tag{1.2.2}$$

证　设A为**D**的关联矩阵.适当排列V与**B**中元素的顺序,不妨设p为V中第一个点且**B**的前r_p个区组与p关联.于是A具有下列形状:

$$A = \begin{bmatrix} 1\cdots 1 & 0\cdots 0 \\ A_1 & * \end{bmatrix} \tag{1.2.3}$$

其中A_1为由A的后$v-1$行与前r_p列组成的$(v-1)\times r_p$子矩阵.因**B**的前r_p个区组中的每一个都恰与V中除p之外的$k-1$点关联, 故A_1的各列的列和都是$k-1$.又因p与V中其余各点的相遇数为λ,故A_1各行的行和都是λ.用两种方法计算A_1中1的个数得$\lambda(v-1) = r_p(k-1)$, 从而$r_p = \lambda(v-1)/(k-1) = r$, 即得(i). 因此$A$的各行的行和都是$r$. 又因$A$的各列的列和都是$k$, 从而用两种方法计算$A$中 1 的个数便得$bk = vr$,由(i)即得(ii). □

由上述引理可知, 若$\mathbf{D} = (V,\mathbf{B},\mathbf{I})$为一个$\mathrm{B}(k,\lambda;v)$, 则$V$中每一点的重复度都等于某个常数$r$, 叫做此设计的**重复数**(replication number). v,b,r,k与λ叫做此设计的参数, 它们满足下述参数关系:

$$bk = vr, \tag{1.2.4}$$

$$\lambda(v-1) = r(k-1). \tag{1.2.5}$$

由此得到关于BIB设计存在的下述基本必要条件.

定理 1.2.1　*若$\mathrm{B}(k,\lambda;v)$存在, 则*

$$\lambda(v-1) \equiv 0 \pmod{(k-1)}, \tag{1.2.6}$$

$$\lambda v(v-1) \equiv 0 \pmod{k(k-1)}. \tag{1.2.7}$$

设$\mathbf{D}$为一个$\mathrm{B}(k,\lambda;v)$, A为$\mathbf{D}$的关联矩阵, 则由式(1.1.4)、式(1.1.5)及**引理**1.2.1得

$$AA^{\mathrm{T}}=\begin{bmatrix} r & \lambda & \cdots & \lambda \\ \lambda & r & \cdots & \lambda \\ \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \cdots & r \end{bmatrix}=(r-\lambda)I_v+\lambda J_v, \tag{1.2.8}$$

$$w_vA=kw_b. \tag{1.2.9}$$

此处J_v是元素全为1的$v\times v$矩阵, w_v与w_b分别是元素全为1的v维与b维行向量.反之, 若A为满足条件(1.2.8)与(1.2.9) 的$v\times b$ $(0,1)$-矩阵, 则A必可看作某个$\mathrm{B}(k,\lambda;v)$的关联矩阵.在同构意义下, 一个$\mathrm{B}(k,\lambda;v)$由它的关联矩阵唯一确定.

关联矩阵的引入, 使我们把有关的设计问题转化为一类特殊的(0,1)-矩阵问题, 从而有可能用线性代数的理论、方法与技巧来进行研究. 作为一个例子, 下面用矩阵方法来证明著名的Fisher不等式.

定理 1.2.2 (Fisher [101]) *若*$\mathrm{B}(k,\lambda;v)$*存在且*$v>k$*,则*

$$b\geqslant v. \tag{1.2.10}$$

证 设A为某个$\mathrm{B}(k,\lambda;v)$ 的关联矩阵.由式(1.2.8),经简单计算可知矩阵$B=AA^{\mathrm{T}}$的行列式为

$$\det(B)=\begin{vmatrix} r & \lambda & \cdots & \lambda \\ \lambda & r & \cdots & \lambda \\ \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \cdots & r \end{vmatrix}=(r-\lambda)^{v-1}(\lambda v-\lambda+r). \tag{1.2.11}$$

由于$v>k$,由式(1.2.5)得$r>\lambda$,因此$\det(B)\neq 0$,从而

$$b\geqslant \mathrm{rank}(A)\geqslant \mathrm{rank}(AA^{\mathrm{T}})=\mathrm{rank}(B)=v.$$

即得结论. □

利用Fisher不等式可知,$\mathrm{B}(6,1;16)$与$\mathrm{B}(10,3;25)$都不存在,尽管条件(1.2.6)与(1.2.7)都满足.

Fisher不等式(1.2.10)中等号成立的情形特别有趣味.$b=v$时的$\mathrm{B}(k,\lambda;v)$叫**对称区组设计**(symmetric block design).对称区组设计有许多重要而又深刻的性质, 这将在第2章中讨论.

关于一个BIB设计与它的补之间的关系, 有下述定理.

定理 1.2.3 *设*$\mathbf{D}$*为一个*$\mathrm{B}(k,\lambda;v)$*,则*$\mathbf{D}$*的补*$\bar{\mathbf{D}}$*是一个*$\mathrm{B}(v-k,b-2r+\lambda;v)$.

证　设A为$\mathbf{D}$的关联矩阵,J_{vb}是元素全为1的$v\times b$矩阵, 则$\bar{A}=J_{vb}-A$是$\bar{\mathbf{D}}$的关联矩阵.

由于A的各行的行和为r, 故

$$w_bA^{\mathrm{T}}=rw_v. \tag{1.2.12}$$

从而由式(1.2.8)得

$$\begin{aligned}\overline{A}(\overline{A})^{\mathrm{T}} &= (J_{vb}-A)(J_{vb}-A)^{\mathrm{T}}\\ &= J_{vb}J_{vb}^{\mathrm{T}}-(J_{vb}A^{\mathrm{T}}+AJ_{bv})+AA^{\mathrm{T}}\\ &= bJ_v-2rJ_v+(r-\lambda)I_v+\lambda J_v\\ &= (r-\lambda)I_v+(b-2r+\lambda)J_v\end{aligned} \tag{1.2.13}$$

及

$$w_v\overline{A}=w_v(J_{vb}-A)=vw_b-kw_b=(v-k)w_b, \tag{1.2.14}$$

即$\bar{A}$满足式(1.2.8)与式(1.2.9),从而$\overline{\mathbf{D}}$是一个BIB设计, 且 $\overline{k}=v-k,\overline{\lambda}=b-2r+\lambda$ 成立,即$\overline{\mathbf{D}}$是一个$\mathrm{B}(v-k,b-2r+\lambda;v)$. □

基于上述定理, 为了研究$\mathrm{B}(k,\lambda;v)$的存在性, 不妨假定$k\leqslant v/2$.当$k>v/2$时, 可以研究其补设计的存在性.

关于BIB设计的研究是从$k=3$的情形开始的. 我们把一个$\mathrm{B}(3,\lambda;v)$叫做v阶λ**重三元系**(λ-fold triple system of order v). $\lambda=1$时的三元系, 经E.Witt [277]首创, 将其叫做Steiner三元系. v阶Steiner三元系也记作$\mathrm{STS}(v)$. 例1.1.1给出的是一个$\mathrm{STS}(7)$, 由**定理**1.2.3, 它的补设计是一个$\mathrm{B}(4,2;7)$. 在历史上, 下述Kirkman 15名女生问题给出了三元系的最著名的例子.

例 1.2.1　(Kirkman [153]) 一位女教师每天带领她的15名女学生散步一次.散步时她把学生分成5组, 每组3人. 问能否设计出这样一个连续散步一周的方案, 使得任意两名学生都正好有一次被安排在同一组? 用1到15这15个数字代表15名女生, 下面给出这个问题的一个解:

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}.

这其实是一个具有可分解性的$\mathrm{STS}(15)$.