普通高等院校“十一五”规划教材

组合设计理论与编码理论

ZUHE SHEJI LILUN YU BIANMA LILUN

蒲利群　编著

国防工业出版社
National Defense Industry Press

普通高等院校“十一五”规划教材

组合设计理论与编码理论

蒲利群　编著

国防工业出版社
·北京·

内容简介

本书对组合设计和编码的基本概念、方法和理论作了比较简单的介绍，并介绍了组合设计和编码的联系。全书共分九章。第一章有限关联结构从有限关联结构出发给出了组合设计的基本概念。第二章介绍拉丁方与正交序列的一般理论。第三章介绍几类对称设计。第四章介绍有限射影几何与有限仿射几何。第五章介绍 Hadamard 矩阵与 Hadamard 2－设计。第六章到第八章介绍了编码理论中一些与设计有关系的码。第九章讨论了设计与编码的关系。

本书可作为数学系研究生的教材，也可作为通信专业本科大四的教材，或者作为从事应用数学和编码理论研究人员的参考书。

图书在版编目(CIP)数据

组合设计理论与编码理论/蒲利群编著.—北京：国防工业出版社，2009.5

普通高等院校“十一五”规划教材

ISBN 978-7-118-05987-8

Ⅰ.组… Ⅱ.蒲… Ⅲ.①组合设计－高等学校－教材 ②编码理论－高等学校－教材 Ⅳ.0157

中国版本图书馆 CIP 数据核字(2008)第 152416 号

※

国防工业出版社出版发行

(北京市海淀区紫竹院南路 23 号 邮政编码 100048)

天利华印刷装订有限公司印刷

新华书店经售

*

开本 787×1092 1/16 **印张** 8 **字数** 280 千字

2009 年 5 月第 1 版第 1 次印刷 **印数** 1—3000 册 **定价** 20.00 元

(本书如有印装错误，我社负责调换)

国防书店：(010)68428422 发行邮购：(010)68414474

发行传真：(010)68411535 发行业务：(010)68472764

前　言

组合设计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配置并讨论其性质的学问。它的历史可以追溯到很远。然而组合设计又是一门年轻的数学分支。对于组合设计的系统研究，是从20世纪30年代R. C. Bose等人的工作开始的，而从60年代起，随着关于正交拉丁方的Euler猜想等重要问题的解决，特别是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重要应用，组合设计的发展进入了一个飞速发展的时期，取得了令人瞩目的发展。组合设计与其他学科的联系日趋紧密，这不但刺激了组合数学本身的发展，而且为组合数学的研究提供了广泛的素材。本书注重讨论组合设计基础知识、基本理论以及与编码理论的联系。

本书的前五章重点介绍组合数学的基本理论。第一章是全书的引论，从关联结构的角度引出组合设计理论中最重要、最基本的概念，为以后各章的讨论作必要的准备。第二章和第五章分别介绍了拉丁方、正交序列和Hadamard矩阵，而拉丁方和正交序列是出现频率很高的名词和工具；在第七章还介绍了Hadamard码，像这样组合设计和编码的联系贯穿于全书。第三章介绍了对称设计的理论。因为对称设计与编码中的许多码有联系，可以由对称设计出发构造一些码，也可以根据码字的特点，构造对称设计。第四章介绍了射影平面和仿射平面的有关概念，读了这一章可以帮助读者理解第八章的内容。

编码理论自20世纪40年代由仙农(Shannon)，汉明(Hamming)等人创立以来，已经有40年的历史。这期间，由于工程技术的实际需要，编码理论获得了不断的发展。特别是近年来，它在卫星通信、计算机技术、保密技术以及磁盘与光盘技术方面具有许多重要应用，愈来愈受到重视。

在我国编码理论的研究始于20世纪50年代末。中国的许多教授和知名学者如蔡长年教授、周炯槃教授、胡征教授、陈太一教授等对于促进这一学科的发展和应用做出了巨大的贡献。万哲先教授、曾肯成教授等一批数学家的参与对推动编码理论的发展起到了很大的作用。

很多编码理论的教材立足于编码理论和代数知识的联系。编码和组合理论的联系散见于许多西文期刊的论文，本书介绍了组合设计理论和编码理论的基础知识，并将编码理论与组合设计的联系进行了较为系统化的阐述。本书从第六章开始介绍编码理论。因为本书的侧重点在于介绍组合设计和编码的联系，因此关于编码中的一些与信息论有联系的问题如编码理论的基本思想、译码的原则、仙农信道编码定理等未涉及。本书介绍的码基本上都与组合设计理论有联系，当然有些码是编码的基础，为了全书的独立性和完整性，也为了方便读者，也作了介绍，如第六章纠错码和循环码。第七章为五种好码的介绍。编码中的好码是指一些能够满足一些界限如Johnson界或者具有某些特点的码，如给定

码长、字母表和码重，具有较多码字的码。本章介绍的码仅仅为一小部分，是要在第九章中出现的。因为有很多码具有多重身份，如有的码既是循环码又是平方剩余码，本书在介绍时，一般选用通行的分类标准，同时考虑到本书的侧重点：组合设计和编码的联系。本书的第八章较为简单，是作为了解内容出现的。第九章是全书的总结。

本书可作为数学系研究生的教材，也可作为通信专业本科大四的教材或者作为从事应用数学和编码理论研究人员的参考书籍。阅读该书需要有有限域和信息论的一些基本知识，即使缺少这些知识储备，在阅读中补上有关的概念也不影响学习和理解。

编码理论和组合设计之间有很多联系，现在发现的仅是很少的部分，还有许多问题有待科研工作者去解决。希望这本书能够吸引更多的有识之士加入到这方面的研究中，也希望这本书能够起到抛砖引玉的作用。由于时间的关系和本人的水平有限，本书难免有不足之处，敬请各位指正。

作者

目　录

第一章　有限关联结构

这一章将概要介绍组合设计理论的基本概念和主要研究内容。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。在引入关联结构的概念之后，对一些重要的关联结构包括平衡不完全区组设计[2][29]、成对平衡设计以及 t - 设计等作了介绍，并讨论了它们的联系，以使读者能对设计理论的内容、方法和特点有一个初步的了解。

1.1　有限关联结构

组合设计理论的主要研究对象是各种有限关联结构。

定义 1.1.1　设 V 与 $\mathscr{B}$ 为两个不相交集合，I 为 V 与 $\mathscr{B}$ 之间的一个二元关系，即 $I\subseteq V\times\mathscr{B}$，则称 $\mathscr{D}=(V,\mathscr{B},I)$ 为一个关联结构。V 的元素叫做点，$\mathscr{B}$ 的元素叫做区组，I 叫做关联关系。设 $p\in V,B\in\mathscr{B}$，若 $(p,B)\in I$，则称点 p 与区组 B 关联并记作 pIB。若 p 不与 B 关联并记作 $p\not IB$。

有时为了强调关联结构的几何意义，也把区组叫做直线，此时，“pIB”也可叫做“点 p 在直线上”或“直线 B 经过点 p”。

本书只讨论有限关联结构，即 V 与 $\mathscr{B}$ 都是有限集的关联结构，当 $\mathscr{D}=(V,\mathscr{B},I)$ 为有限关联结构时，常以 v 表示 V 的基数，以 b 表示 $\mathscr{B}$ 的基数，即 $v=|V|,b=|\mathscr{B}|$，并称 v 为 $\mathscr{D}$ 的阶。

定义 1.1.2　设 $\mathscr{D}_1=(V_1,\mathscr{B}_1,I_1),\mathscr{D}_2=(V_2,\mathscr{B}_2,I_2)$ 为两个有限关联结构，设 $\sigma:V_1\cup\mathscr{B}_1\to V_2\cup\mathscr{B}_2$ 为满足下述条件的一个双设：

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

(ii) 对任意 $p\in V_1$ 与任意 $B\in\mathscr{B}_1$，当且仅当 pI_1B 时才有 $\sigma(p)I_2\sigma(B)$，则称 σ 为 $\mathscr{D}_1$ 到 $\mathscr{D}_2$ 的同构，此时称 $\mathscr{D}_1$ 与 $\mathscr{D}_2$ 为两个同构的关联结构。特别地，当 $\mathscr{D}_1=\mathscr{D}_2=\mathscr{D}$ 时，$\mathscr{D}$ 到它自身的同构称为自同构，$\mathscr{D}$ 的全体自同构关于映射的乘法组成一个群，叫做 $\mathscr{D}$ 的全自同构群，记作 $\mathrm{Aut}(\mathscr{D})$。$\mathrm{Aut}(\mathscr{D})$ 的任一子群叫做 $\mathscr{D}$ 的自同构群。

有限关联结构可以用它的关联矩阵来刻画。

定义 1.1.3　设 $V=\{p_1,p_2,\cdots,p_v\},\mathscr{B}=\{B_1,B_2,\cdots,B_b\},\mathscr{D}=(V,\mathscr{B},I)$ 为有限关联结构。对 $1\leqslant i\leqslant v,1\leqslant j\leqslant b$，令

$$a_{ij}=\begin{cases}1, & \text{若 } p_iIB_i\\ 0, & \text{若 } p_i\not IB_j\end{cases}\tag{1.1.1}$$

则 $v\times b$ 阶 $(0,1)$ - 矩阵

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

叫做 $\mathscr{D}$ 的关联矩阵。

对 $1\leqslant i\leqslant v$，令 r_i 表示 $\mathscr{B}$ 中与 p_i 关联的区组数；对 $1\leqslant j\leqslant b$，令 k_j 表示 V 中与 B_j 相关联的点的个数；对 $1\leqslant i,j\leqslant v$，$i\neq j$，令 λ_{ij} 表示 $\mathscr{B}$ 中同时与点 p_i、p_j 关联的区组数，r_i 叫做点 p_i 的重复度，k_j 叫做区组 B_j 的容量（或长度），λ_{ij} 表示 p_i、p_j 的相遇数，则 r_i 等于关联矩阵 $\boldsymbol{A}$ 的第 i 行的行和，即第 i 行中 1 的个数，k_j 等于 $\boldsymbol{A}$ 的第 j 列的列和，而 λ_{ij} 则是 $\boldsymbol{A}$ 的第 i 行与第 j 行的内积。因此，用两种方法计算 $\boldsymbol{A}$ 中 1 的个数，可以得到下面等式：

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

令 w_v 表示元素全为 1 的 v 维行向量，$\boldsymbol{A}^{\mathrm{T}}$ 表示 $\boldsymbol{A}$ 的转置矩阵，则

$$\boldsymbol{A}\boldsymbol{A}^{\mathrm{T}}=\begin{pmatrix} r_1 & \lambda_{12} & \lambda_{13} & \cdots & \lambda_{1v} \\ \lambda_{21} & r_2 & \lambda_{23} & \cdots & \lambda_{2v} \\ \vdots & \vdots & & \vdots & \\ \lambda_{v1} & \lambda_{v2} & \lambda_{v3} & \cdots & r_v \end{pmatrix} \tag{1.1.4}$$

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

有限关联结构 $\mathscr{D}=(V,\mathscr{B},I)$ 的关联矩阵与 V 及 $\mathscr{B}$ 中元素的排列顺序有关。为了讨论 $\mathscr{D}$ 的对应于 V 及 $\mathscr{B}$ 中元素不同排列的关联矩阵的关系，引入下述定义。

定义 1.1.4 各行各列都恰好有一个 1 的 $n\times n$ $(0,1)$－矩阵叫 n 阶置换矩阵。设 $\boldsymbol{A}$ 与 $\boldsymbol{B}$ 为两个 $m\times n$ $(0,1)$－矩阵，若存在 m 阶置换矩阵 $\boldsymbol{P}$ 和 n 阶置换矩阵 $\boldsymbol{Q}$，使 $\boldsymbol{B}=\boldsymbol{PAQ}$，则称 $\boldsymbol{A}$ 与 $\boldsymbol{B}$ 置换相抵。

设 $V=\{p_1,p_2,\cdots,p_v\}$ 与 $\mathscr{B}=\{B_1,B_2,\cdots,B_b\}$ 时，$\mathscr{D}$ 的关联矩阵为 $\boldsymbol{A}$，将 V 中的点重新排列，对应于将 $\boldsymbol{A}$ 的各行作相应的重新排列亦即在 $\boldsymbol{A}$ 的左边乘以一个适当的 v 阶置换矩阵 $\boldsymbol{P}$；将 $\mathscr{B}$ 中区组重新排列，对应于将 $\boldsymbol{A}$ 的各列作相应的排列，亦即在 $\boldsymbol{A}$ 的右边乘以一个适当的 b 阶置换矩阵 $\boldsymbol{Q}$。因此 $\mathscr{D}$ 的对应于 V 与 $\mathscr{B}$ 中元素不同排列的两个关联矩阵必定置换相抵。又由于具有相同关联矩阵的两个关联结构显然是同构的，因此证明了下述结论。

定理 1.1.1 设 $\boldsymbol{A}$ 与 $\boldsymbol{B}$ 分别是有限关联结构 $\mathscr{D}_1$、$\mathscr{D}_2$ 的关联矩阵，则 $\mathscr{D}_1$、$\mathscr{D}_2$ 同构的充要条件为 $\boldsymbol{A}$ 与 $\boldsymbol{B}$ 置换相抵。

定义 1.1.5 设 $\mathscr{D}=(V,\mathscr{B},I)$ 为有限关联结构。令 $\mathscr{D}^*=(V^*,\mathscr{B}^*,I^*)$，此处 $V^*=\mathscr{B}$，$\mathscr{B}^*=V$，并且对任意 $p^*\in V^*$，$\mathscr{B}^*\in\mathscr{B}^*$，当且仅当 B^*Iv^* 时有 $v^*I^*B^*$，则称 $\mathscr{D}^*$ 为 $\mathscr{D}$ 的对偶结构。若 $\mathscr{D}^*$ 与 $\mathscr{D}$ 同构，则称 $\mathscr{D}$ 为自对偶结构。

若 $\boldsymbol{A}$ 为 $\mathscr{D}$ 的关联矩阵，则 $\boldsymbol{A}^{\mathrm{T}}$ 是 $\mathscr{D}^*$ 的关联矩阵。显然 $(\mathscr{D}^*)^*=\mathscr{D}$。

对偶原理　设 Φ 为由一些关联结构组成的类，使得 Φ 在包含某关联结构 D 时，也包含了它的对偶结构 $\mathscr{D}^*$。若命题 $\mathscr{P}$ 对 Φ 中的所有关联结构都成立，则其对偶命题（即将 $\mathscr{P}$

中的点与区组互换所得到的命题)$\mathscr{P}^*$也对 Φ 中的所有关联结构都成立。

定义 1.1.6 设 $\mathscr{D}=(V,\mathscr{B},I)$为有限关联结构。令$\overline{I}=(V\times\mathscr{B})\setminus I$,则称$\overline{D}=(V,\mathscr{B},\overline{I})$为 $\mathscr{D}$ 的补结构或简称补,亦即对任意 $p\in V$ 与任意$B\in\mathscr{B}$,当且仅当 $p\not IB$ 时,有 $P\overline{I}B$。

设 $v=|V|,b=|\mathscr{B}|$,$\boldsymbol{A}$ 为 $\mathscr{D}$ 的关联矩阵。令 $\boldsymbol{J}_{vb}$表示全部元素都是1的 $v\times b$ 矩阵,则 $\boldsymbol{J}_{vb}-\boldsymbol{A}$ 是$\overline{\mathscr{D}}$的关联矩阵。

常将集合论中的包含关系"$\in$"用做关联关系,并把关联结构$(V,\mathscr{B},\in)$简单记作$(V,\mathscr{B})$,此时 $\mathscr{B}$ 的元素其实就是 V 的子集。需要指出的是 V 的子集有时在 $\mathscr{B}$ 中可能不仅出现一次,设为 s 次。此时这个子集所代表的 s 个区组仍然看做不同。因此将 $\mathscr{B}$ 中的元素看做区组时,$\mathscr{B}$ 是一个集合。而如果将 $\mathscr{B}$ 的元素看做 V 的子集时,则同一个子集可以重复出现,因此应该把 $\mathscr{B}$ 看做 V 上的一个子集族,即不但要看它包含 V 中的哪些子集,还要考虑各个子集在 $\mathscr{B}$ 中出现的重数。

例 1.1.1 令 $V=Z_7$ 为以7为模的全体剩余类的集合,令

$$\mathscr{B}=\{\{0,1,3\},\{1,2,4\},\{2,3,5\},\{3,4,6\},\{4,5,0\},\{5,6,1\},\{6,0,2\}\}$$

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

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

例 1.1.2 $V=Z_6$, $\mathscr{B}=\{\{2,4,5\},\{2,4,5\},\{0,1,5\},\{0,3,5\},\{0,1,4\},\{0,2,3\},\{1,2,3\},\{1,3,4\},\{0,1,2,4\},\{0,1,2,5\},\{0,2,3,4\},\{0,3,4,5\},\{1,2,3,5\},\{1,3,4,5\}\}$

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

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

由于用做区组 $\mathscr{B}_1$、$\mathscr{B}_2$ 的是同一个子集$\{2,4,5\}$,因此 $\boldsymbol{A}$ 的第1,2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。

例 1.1.3 设 V 由 GF(2)上如下7个2×3矩阵组成:

$$\boldsymbol{V}=\left\{\begin{pmatrix}1&0&0\\0&1&0\end{pmatrix},\begin{pmatrix}1&0&0\\0&0&1\end{pmatrix},\begin{pmatrix}1&1&1\\0&1&1\end{pmatrix},\begin{pmatrix}0&1&1\\0&0&1\end{pmatrix},\right.$$

$$\left\{\begin{pmatrix}0&1&0\\1&0&1\end{pmatrix},\begin{pmatrix}1&1&1\\1&1&0\end{pmatrix},\begin{pmatrix}1&1&0\\1&0&1\end{pmatrix}\right\}$$

$\mathscr{B}$ 由 GF(2)上全体 3 维非零向量组成,即

$$\mathscr{B}=\{\{1,0,0\},\{0,1,0\},\{0,0,1\},\{1,1,0\},\{1,0,1\},\{0,1,1\},\{1,1,1\}\}$$

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

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

时 pIB,则 $D=(V,\mathscr{B},I)$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 $D=(V,\mathscr{B},I)$都与某个以"$\in$"为关联关系的关联结构 $\mathscr{D}=(V,\mathscr{B})$同构。

证明 设 $\mathscr{B}=\{B_1,B_2,\cdots,B_b\}$,令

$$B_j'=\{p\in V\mid pIB_j\},1\leqslant j\leqslant b$$

则 B_j' 是 V 的子集。令 $\mathscr{B}'=\{B_1',B_2',\cdots,B_b'\}$,则对任一点 $p\in V$ 与任一 $j=1,2,\cdots,b$,当且仅当 pIB_j 时 $p\in B_j'$,从而 $\mathscr{D}$ 与 $\mathscr{D}'$ 有相同的关联矩阵。由定理 1.1.1,$\mathscr{D}$ 与 $\mathscr{D}'$ 同构。

因此在大多数情况下,都讨论以"$\in$"为关联关系的关联结构。不过,在某些场合下,采用一般意义的关联关系,将使我们在研究有关的设计问题时,有较大的自由度和灵活性。

关于关联结构的定义过于宽泛,以致任何一个(0,1)-矩阵都可以看做某个有限关联结构的关联矩阵。因此对一般的关联结构很难得到深刻的结果。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,它们就能变得既有深刻的理论意义又有广泛的应用价值。

设 $\mathscr{D}=(V,\mathscr{B},I)$为有限关联结构。对 $p\in V$,令 r_p 表示 p 点的重复度;对 $B\in\mathscr{B}$,令 k_b 表示区组 B 的容量;对 V 的任一 t 元子集 S,令 λ_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,以下条件是常用的。

(1) 正则性:存在常数 $r>0$,使对所有 $p\in V$,都有 $r_p=r$。

(2) 均匀性:存在常数 $k>0$,使对所有 $B\in\mathscr{B}$ 都有 $k_B=k$。

(3) t-平衡性:对任何给定的正整数 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。

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做平衡不完全区组设计。

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

(i) $|V|=v$,

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

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

则称 $\mathscr{D}$ 是一个平衡不完全区组设计,简称区组设计或BIB设计,记作 $B(k,\lambda;v)$。v 叫做 $\mathscr{D}$ 的阶,k 叫做 $\mathscr{D}$ 的区组容量,λ 叫做相遇数。

$\lambda=1$ 时的BIB叫做Steiner系或者Steiner 2-设计,并且 $B(k,1;v)$ 也常记作 $S(2,k;v)$。对于一般的 λ,$B(k,\lambda;v)$ 记作 $S_\lambda(2,k;v)$。

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

(i) V 中任意一点 p 的重复度为

$$r_p=\frac{\lambda(v-1)}{k-1} \tag{1.2.1}$$

(ii) $\mathscr{B}$ 中所包含区组的个数为

$$b=|\mathscr{B}|=\frac{\lambda v(v-1)}{k(k-1)} \tag{1.2.2}$$

证明 设 A 为 $\mathscr{D}$ 的关联矩阵。适当排列 V 与 $\mathscr{B}$ 中元素的顺序,不妨设 p 为 V 中的第一个点且 $\mathscr{B}$ 的前 r_p 个区组与 p 关联。于是 $\boldsymbol{A}$ 具有下列形状:

$$\boldsymbol{A}=\begin{bmatrix}11\cdots1 & 0\cdots0\\ \boldsymbol{A}_1 & *\end{bmatrix} \tag{1.2.3}$$

其中 $\boldsymbol{A}_1$ 为由 $\boldsymbol{A}$ 的后 $v-1$ 行与前 r_p 列组成的 $(v-1)\times r_p$ 子矩阵。由于 $\mathscr{B}$ 的前 r_p 个区组中的每一个都恰好与 V 中除 p 之外的 $k-1$ 个点关联,故 A_1 的每一列和都是 $k-1$。又因为 p 与其余各点的相遇数为 λ,故 $\boldsymbol{A}_1$ 各行的行和为 λ。用两种方法计算 $\boldsymbol{A}_1$ 中1的个数便得

$$\lambda(v-1)=r_p(k-1)$$

从而

$$r_p=\frac{\lambda(v-1)}{k-1}=r$$

即得(i)。因此 $\boldsymbol{A}$ 的各行的行和都是 r。又因 $\boldsymbol{A}$ 的各列的列和都是 k,从而用两种方法计算 $\boldsymbol{A}$ 中1的个数便得 $bk=vr$,由(i)即得(ii)。

由上述引理可知,若 $\mathscr{D}=(V,\mathscr{B},I)$ 为一个 $B(k,\lambda;v)$,则 V 中每一点的重复度都等于常数 r,r 叫做此设计的重复数,v、b、r、k、λ 满足以下关系:

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

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

由此得到关于BIB设计存在的下述必要条件。

定理 1.2.1 若 $B(k,\lambda;v)$ 存在,则

$$\lambda(v-1)\equiv 0(\mathrm{mod}(k-1)) \tag{1.2.6}$$

$$\lambda v(v-1)\equiv 0(\mathrm{mod}k(k-1)) \tag{1.2.7}$$

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

$$\boldsymbol{A}\boldsymbol{A}^{\mathrm{T}}=\begin{bmatrix}r & \lambda & \cdots & \lambda\\ \lambda & r & \cdots & \lambda\\ \vdots & \vdots & & \vdots\\ \lambda & \lambda & \cdots & r\end{bmatrix}=(r-\lambda)\boldsymbol{I}_v+\lambda\boldsymbol{J}_v \tag{1.2.8}$$

$$\boldsymbol{w}_v\boldsymbol{A} = k\boldsymbol{w}_b \tag{1.2.9}$$

此处 $\boldsymbol{J}_v$ 是元素全为 1 的矩阵，$\boldsymbol{w}_v$、$\boldsymbol{w}_b$ 分别为元素全为 1 的 v、b 维行向量。反之，若 $\boldsymbol{A}$ 为满足条件式(1.2.8)、式(1.2.9)的 $v\times b(0,1)$－矩阵，则 $\boldsymbol{A}$ 必可看做某个 $B(k,\lambda;v)$的关联矩阵。在同构意义下，一个 $B(k,\lambda;v)$由它的关联矩阵唯一确定。

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

定理 1.2.2 (Fisher 1940)若 $B(k,\lambda;v)$存在，且 $v>k$，则

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

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

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

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

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

即得结论。

利用 Fisher 不等式可知 $B(6,1;16)$与 $B(10,3;25)$都不存在，尽管它们都满足条件式(1.2.6)与式(1.2.7)。

Fisher 不等式(1.2.10)中等号成立即 $b=v$ 时 $B(k,\lambda;v)$叫做对称区组设计。

定理 1.2.3 设 $\mathscr{D}$ 为一个 $B(k,\lambda;v)$，则 $\mathscr{D}$ 的补设计 $\overline{\mathscr{D}}$ 是一个 $B(v-k,b-2r+\lambda;v)$。

证明 设 $\boldsymbol{A}$ 为 $\mathscr{D}$ 的关联矩阵，则 $\overline{\boldsymbol{A}}=\boldsymbol{J}_{vb}-\boldsymbol{A}$ 是 $\overline{\mathscr{D}}$ 的关联矩阵。此处 $\boldsymbol{J}_{vb}$ 是元素全为 1 的 $v\times b$ 矩阵。

由于 $\boldsymbol{A}$ 的各行的行和为 r，故

$$\boldsymbol{w}_b\boldsymbol{A}^{\mathrm{T}} = r\boldsymbol{w}_v \tag{1.2.12}$$

从而由式(1.2.8)得

$$\begin{aligned} \overline{\boldsymbol{A}}(\overline{\boldsymbol{A}})^{\mathrm{T}} &= (\boldsymbol{J}_{vb}-\boldsymbol{A})(\boldsymbol{J}_{vb}-\boldsymbol{A})^{\mathrm{T}} = \\ &\boldsymbol{J}_{vb}\cdot\boldsymbol{J}_{vb}^{\mathrm{T}} - (\boldsymbol{J}_{vb}\cdot\boldsymbol{A}^{\mathrm{T}} + \boldsymbol{A}\cdot\boldsymbol{J}_{bv}) + \boldsymbol{A}\boldsymbol{A}^{\mathrm{T}} = \\ &b\boldsymbol{J}_v - 2r\boldsymbol{J}_v + (r-\lambda)\boldsymbol{I}_v + \lambda\boldsymbol{J}_v = \\ &(r-\lambda)\boldsymbol{I}_v + (b-2r+\lambda)\boldsymbol{J}_v \end{aligned} \tag{1.2.13}$$

及

$$\boldsymbol{w}_v\overline{\boldsymbol{A}} = \boldsymbol{w}_v(\boldsymbol{J}_{vb}-\boldsymbol{A}) = v\cdot\boldsymbol{w}_b - k\boldsymbol{w}_b = (v-k)\boldsymbol{w}_b \tag{1.2.14}$$

即 $\overline{\boldsymbol{A}}$ 满足式(1.2.8)与式(1.2.9)，从而 $\overline{\mathscr{D}}$ 是一个 BIB 设计，且有 $\overline{k}=v-k$，$\overline{\lambda}=b-2r+\lambda$，即 $\overline{\mathscr{D}}$ 是一个 $B(v-k,b-2r+\lambda;v)$。

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

当 $k=3$ 时，称 $B(3,\lambda;v)$为 v 阶 λ 重三元系，记作 TS(v,λ)。$\lambda=1$ 的三元系称为 Steiner 三元系。下述 Kirkman15 名女生问题，给出了三元系的例子。

例 1.2.1 (Kirkman 1850)一位女教师每天带领她的 15 名女生散步一次，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}，{4,10,11}，{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}

这其实是一个可分解的性的 Steiner 三元系。

定义 1.2.2 设 $\mathcal{D}=(V,\mathcal{B},I)$为一个 $B(k,\lambda;v)$。$\mathcal{P}\subset\mathcal{B}$，若 V 中的每一点都恰好与 $\mathcal{P}$ 中唯一的一个区组关联，则称 $\mathcal{P}$ 为一个平行类。若 $\mathcal{B}$ 中全部区组能划分成 $r=\frac{\lambda(v-1)}{k-1}$个平行类，则称此 $B(k,\lambda;v)$可分解，记作 RB$(k,\lambda;v)$。$\lambda=1$ 时可分解的 Steiner 三元系 STS(v)，叫做 Kirkman 三元系，记作 KTS(v)。

例 1.2.2 用下述方法构造一个 $B(6,2;16)$，令 $V=Z_{16}$，作下列矩阵

$$\begin{bmatrix}0&1&2&3\\4&5&6&7\\8&9&10&11\\12&13&14&15\end{bmatrix}$$

对任一 $i\in Z_{16}$，令 $\boldsymbol{A}_i$ 表示由上面矩阵中与 i 位于同一行，同一列但不同于 i 的元素组成的集合，例如，$\boldsymbol{A}_0=\{1,2,3,4,8,12\}$。令 $\mathcal{B}=\{\boldsymbol{A}_i\mid i\in Z_{16}\}$，由于 Z_{16} 中任意一对不同元素都恰好包含在两个区组中，因此这是一个 $B(6,2;16)$。

下面用几何方法构造两类重要的 BIB 设计。

定理 1.2.4 设 q 为素数幂，则 $B(q+1,1;q^2+q+1)$存在。

证明 由于 q 为素数幂，故 q 阶有限域 F_q 存在。取 F_q 上的三维向量空间 $V_3(F_q)$ 中全体 1 维子空间的集合为 V，全体二维子空间的集合为 $\mathcal{B}$。把 V 中的元素作为点，$\mathcal{B}$ 中的元素作为直线。再以子空间中的包含关系作为关联关系 I，如此得到的关联结构$\mathcal{D}=(V,\mathcal{B},I)$叫做 F_q 上的一个 q 阶射影平面，记作 PG$(2,q)$。

由于 $V_3(F_q)$中 1 维子空间的个数为$\frac{q^3-1}{q-1}$，一个二维子空间包含的 1 维子空间的个数为$\frac{q^2-1}{q-1}$，并且两个不同的一维子空间同时包含在唯一的一个二维子空间中，因此 PG

$(2,q)$是一个 $v=q^2+q+1,k=q+1,\lambda=1$ 的 BIB 设计，即 $B(q+1,1;q^2+q+1)$这个设计是对称的。

定理 1.2.5 设 q 为素数幂，则 RB$(q,1;q^2)$存在。

证明 设$(V,\mathscr{B},I)$为一个 PG$(2,q)$。由于 $V_3(F_q)$中任意两个不同的二维子空间的交是一个一维子空间，因此 $\mathscr{B}$ 中任意两个不同的二维子空间的交是一个一维子空间，因此 $\mathscr{B}$ 中任意两条不同直线都有唯一的一个交点。设 $B_0=\{a_0,a_1,\cdots,a_q\}$为 $\mathscr{B}$ 中一条给定的直线。去掉 B_0 这条直线，并从 V 及其余 q^2+q 条直线上去掉 B_0 中的点，则得到一个 $B(q,1;q^2)$，叫做 F_q 上的 q 阶仿射平面，记作 AG$(2,q)$。对 $i=0,1,\cdots,q$，$\mathscr{B}$ 中除 B_0 之外包含 a_i 的 q 条直线去掉 a_i 之后组成 AG$(2,q)$的一个平行类。因此 AG$(2,q)$中的全部直线恰好划分为 $q+1$ 个平行类，从而 AG$(2,q)$是可分解的。

BIB 设计的存在性问题是组合设计理论的一个基本问题，R. M. Wilson(1975)证明了下述定理。

定理 1.2.6 给定正整数 k 与 λ，存在常数 $v_0=v_0(k,\lambda)$，使当 $v\geqslant v_0$ 时，$B(k,\lambda;v)$存在的必要条件也是充分条件。

1.3 对称 PBD 设计

先给出满足 2－平衡性条件的有限关联结构－成对平衡设计的基本概念。

定义 1.3.1 设 v 与 λ 为给定的正整数，K 为给定的正整数集合，又设 $\mathscr{D}=(V,\mathscr{B})$为有限关联结构。若以下条件满足：

(i) $|V|=v$；

(ii) 对任意 $B\in\mathscr{B}$，都有$|B|\in K$；

(iii) V 中任意一对不同的点都恰好同时包含在 λ 个区组中，则称 $\mathscr{D}$ 为一个成对平衡设计，简称 PBD 设计，记作 $B(K,\lambda;v)$，v 叫做设计的阶，λ 叫做相遇数。

当 $K=\{k\}$，即 K 只包含一个正整数时，$B(\{k\},\lambda;v)$就是上一节所定义的 BIB 设计 $B(k,1;v)$。

设 $\mathscr{D}=(V,\mathscr{B})$为一个 $B(K,\lambda;v)$，若存在区组 $B\in\mathscr{B}$ 使 $2\leqslant|\mathscr{B}|<v$，则称 $\mathscr{D}$ 为非退化的 PBD 设计 $B(k,1;v)$。

需要指出的是，对某个 $k\in K$，$\mathscr{B}$ 可能不包含容量为 k 的区组。因此当 $K_1\subseteq K_2$ 为两个正整数集时，每一个 $B(K_1,\lambda;v)$也可以看做一个 $B(K_2,\lambda;v)$。

设 $\mathscr{D}=(V,\mathscr{B})$为一个 $B(K,\lambda;v)$，$\boldsymbol{A}$ 为它的关联矩阵。现有

$$\boldsymbol{A}\boldsymbol{A}^{\mathrm{T}}=\begin{bmatrix} r_1 & \lambda & \lambda\cdots & \lambda \\ \lambda & r_2 & \lambda\cdots & \lambda \\ \vdots & \vdots & & \vdots \\ \lambda & \lambda & \lambda\cdots & r_v \end{bmatrix} \tag{1.3.1}$$

显然对所有 $1\leqslant i\leqslant v$，都有 $r_i\geqslant\lambda$。

引理 1.3.1 设 $\mathscr{D}$ 为非退化的 $B(K,\lambda;v)$。对 $1\leqslant i\leqslant v$，令 $r_i=n_i+\lambda$，则 $n_i>0$。

证明 设若不然，对某个 i 有 $n_i=0$，即 $r_i=\lambda$。因此包含点 p_i 的区组只有 λ 个。设

$p_j \in V$ 为任意另外一个点。由于 $\mathcal{D}$ 的相遇数为 λ，故每一个包含点 p_i 的区组必然包含点 p_j，从而每一个包含点 p_i 的区组都包含了 V 中所有的点。由于 $\mathcal{D}$ 的相遇数为 λ，故 $\mathcal{D}$ 不能再有其他至少包含两个点的区组，这与 $\mathcal{D}$ 的非退化性相矛盾，故得到结论。

利用上述引理，可以证明 Fisher 不等式的下述推广。

定理 1.3.1 (Lenz 1983)设 $\mathcal{D}=(V,\mathcal{B})$ 为非退化 $B(K,\lambda;v)$，又设 $|\mathcal{B}|=b$。再令 b' 用做表示区组的不同子集的个数，则

$$b \geqslant b' \geqslant v \tag{1.3.2}$$

证明 设 $\boldsymbol{A}$ 为 $\mathcal{D}$ 的关联矩阵，则由式(1.3.1)得

$$\boldsymbol{A}\boldsymbol{A}^{\mathrm{T}} = \begin{bmatrix} r_1 & \lambda & \lambda & \cdots & \lambda \\ \lambda & r_2 & \lambda & \cdots & \lambda \\ \vdots & \vdots & \vdots & & \vdots \\ \lambda & \lambda & \lambda & \vdots & r_v \end{bmatrix} = \boldsymbol{N} + \lambda \boldsymbol{J}_v \tag{1.3.3}$$

此处

$$\boldsymbol{N} = \begin{bmatrix} n_1 & & & \\ & n_2 & & \\ & & \ddots & \\ & & & n_v \end{bmatrix}, \quad n_i = r_i - \lambda, 1 \leqslant i \leqslant v \tag{1.3.4}$$

由于 $\mathcal{D}$ 非退化，故由引理 1.3.1，对所有 $1 \leqslant i \leqslant v$ 都有 $n_i > 0$。从而

$$\det(\boldsymbol{A}\boldsymbol{A}^{\mathrm{T}}) = \begin{vmatrix} n_1+\lambda & \lambda & \lambda & \cdots & \lambda \\ -n_1 & n_2 & 0 & \cdots & 0 \\ -n_1 & 0 & n_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ -n_1 & 0 & 0 & \cdots & n_v \end{vmatrix} = \begin{vmatrix} x & \lambda & \lambda & \cdots & \lambda \\ 0 & n_2 & 0 & \cdots & 0 \\ 0 & 0 & n_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & n_v \end{vmatrix} \tag{1.3.5}$$

其中

$$x = n_1 + \lambda + n_1\lambda\left\{\frac{1}{n_2} + \frac{1}{n_3} + \cdots + \frac{1}{n_v}\right\} \tag{1.3.6}$$

从而

$$\det(\boldsymbol{A}\boldsymbol{A}^{\mathrm{T}}) = x\prod_{i=2}^{v} n_i > 0 \tag{1.3.7}$$

因此

$$b \geqslant \min\{v,b\} \geqslant \min\{v,b'\} \geqslant \operatorname{rank}\boldsymbol{A} \geqslant \operatorname{rank}(\boldsymbol{A}\boldsymbol{A}^{\mathrm{T}}) = v$$

从而即得结论。

定义 1.3.2 设 $\mathcal{D}=(V,\mathcal{B})$ 为一个 $B(K,\lambda;v)$，$\mathcal{B}_1 \subset \mathcal{B}$，若 V 中每一点都恰好包含在 B_1 的 α 个区组中，则称 $\mathcal{B}_1$ 为 $\mathcal{D}$ 的一个 α－平行类。特别当 $\alpha=1$ 时，1－平行类即叫做平行类。

定理 1.3.2 设 $\mathcal{D}=(V,\mathcal{B})$ 为一个 $B(K,\lambda;v)$ 且 $v>\max K$。设 $\mathcal{B}_1,\mathcal{B}_2,\cdots,\mathcal{B}_l$ 构成

$\mathscr{B}$ 的一个划分，使对 $i=1,2,\cdots,l$，$\mathscr{B}_i$ 是一个 λ_i - 平行类。设 $|\mathscr{B}|=b$，则

$$b \geqslant v+l-1 \tag{1.3.8}$$

证明 设 $\mathscr{D}$ 的关联矩阵 $\boldsymbol{A}$ 中与区组 $\boldsymbol{B}$ 对应的列向量为 α_B，对 $1\leqslant i\leqslant l$，由于 $\mathscr{B}_i$ 为 λ_i - 平行类，故

$$\sum_{B\in\mathscr{B}_i}\alpha_B = \lambda_i \boldsymbol{w}_v^{\mathrm{T}}, \quad 1\leqslant i\leqslant l \tag{1.3.9}$$

此处 $\boldsymbol{w}_v^T$ 表示元素全为 1 的列向量。从而对 $1\leqslant i\leqslant l-1$，有

$$\lambda_l \sum_{B\in\mathscr{B}_i}\alpha_B = \lambda_i \sum_{B\in\mathscr{B}_l}\alpha_B \tag{1.3.10}$$

于是在 $\mathscr{B}_i$ 中存在一个区组 B'，它所对应的列向量 $\alpha_{B'}$ 可以表示为 $\mathscr{B}_i$ 中其余区组以及 $\mathscr{B}_l$ 中区组所对应的列向量的线性组合。因此，$\boldsymbol{A}$ 中至少有 $l-1$ 个列向量可以表示为其余向量的线性组合。因此 $\mathrm{rank}\boldsymbol{A}\leqslant b-(l-1)$。又因 $v>\max K$，故 $\mathscr{D}$ 为非退化，从而由定理 1.3.1，得 $\mathrm{rank}\boldsymbol{A}=v$ 即得结论。

1.4 t - 设计

在本节中，从另外的角度来推广 BIB 设计的概念。下面要研究的是一类满足正则性，均匀性和 t - 平衡性条件的有限关联结构。

定义 1.4.1 设 $\mathscr{D}=(V,\mathscr{B})$ 为有限关联结构。若下列条件满足：

(i) $|V|=v$，

(ii) 存在常数 k，使对所有 $B\in\mathscr{B}$，都有 $k_B=k$，

(iii) 对给定的正在整数 t，存在常数 $\lambda>0$，使对 V 的任意一个 t 元子集 S，都有 $\lambda_S=\lambda$，则称 $\mathscr{D}$ 为一个 $t-(v,k,\lambda)$ 设计，简称 t - 设计。$t-(v,k,\lambda)$ 设计常记为 $S_\lambda(t,k;v)$。

设 $\mathscr{D}=(V,\mathscr{B})$ 为一个 $t-(v,k,\lambda)$ 设计，如果 V 的每个 k 元子集都在 $\mathscr{B}$ 中出现相同的次数，则称 $\mathscr{D}$ 为平凡的 t - 设计。例如，当 $v\leqslant k+t$ 时，任意 $t-(v,k,\lambda)$ 设计都是平凡的。$t=2$ 时的设计称为 BIB，也称为 2 - 设计，或者 $2-(v,k,\lambda)$ 或者 $B(k,\lambda;v)$。

下面给出几个列子。

例 1.4.1 令 $V=Z_7\cup\{\infty\}$，

$\mathscr{B}$：{0,1,2,4}，{1,2,3,5}，{2,3,4,6}，{3,4,5,0}，{4,5,6,1}，{5,6,0,2}，{6,0,1,3}；

{0,1,5,∞}，{1,2,6,∞}，{2,3,0,∞}，{3,4,1,∞}，{4,5,2,∞}，

{5,6,3,∞}，{6,0,4,∞}

这是一个 8 阶 Steiner 4 元系，SQS(8)。如果取包含∞的 7 个区组并将∞去掉，则得到 Z_7 上的一个 STS(7)。

$\mathscr{D}=(V,\mathscr{B})$ 也是一个 2 - (8,4,7) 设计，它还是一个 1 - (8,4,7) 设计。

定理 1.4.1 对上述条件给出了合理的解释。

例 1.4.2 令 $V=\{1,2,3,4,5,6,7,8,9,10\}$，有