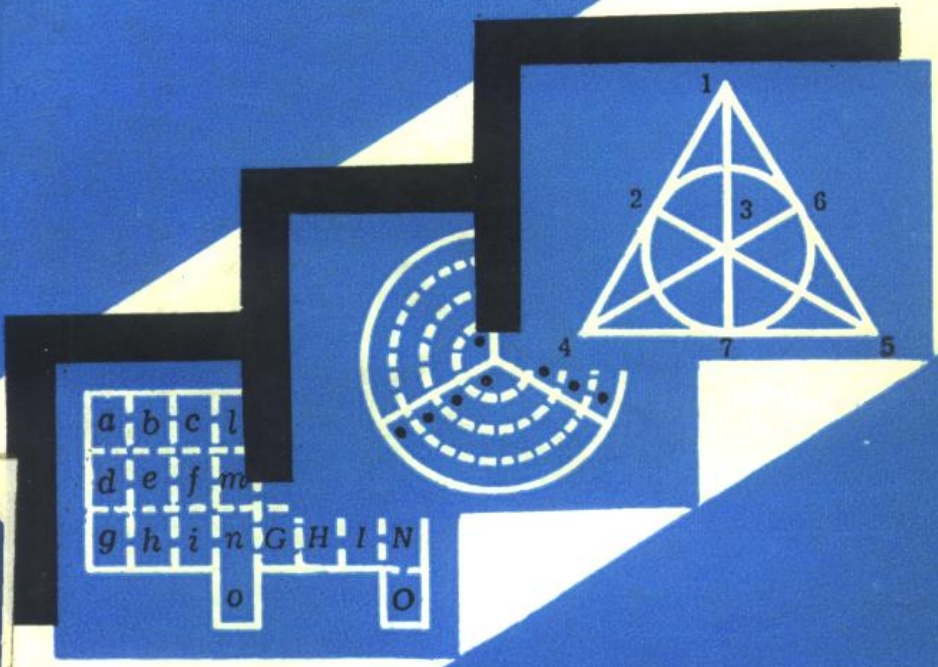
组合设计与编码

靳蕃 编著



西南交通大学出版社

组合设计与编码

靳 蕃 编著

西南交通大学出版社

内 容 提 要

本书以组合数学为基础，以编码技术为对象，重点介绍了组合编码的原理和应用。全书共分十章，循序渐进地将同余方法（数论）→组合设计（组合数学）→组合编码（编码技术）三大学科领域有机地贯串在一起。书中反映了近些年来，包括作者在内的国内外学者在组合编码技术方面的新思想和新成果，是一本运用数学理论发展信息技术，依靠信息技术拓宽数学理论的新书。

本书可以作为计算机、通信技术、信息工程、试验设计及应用数学等专业大学生、研究生的教学参考书，也可供上述有关专业广大工程技术人员使用参考。

组合设计与编码

ZUHE SHEJI YU BIANMA

靳 蕃

*

西南交通大学出版社出版发行

（四川 峨眉山市）

西南交通大学出版社印刷厂印刷

*

开本：787×1092 1/32 印张：14.6875

字数：325千字 印数：1—2500册

1990年5月第1版 1990年5月第1次印刷

ISBN 7—81022—146—9/T 053

定价：3.05元

序

随着计算机科学和现代数字通信技术的发展，保证数字信息高速可靠地进行传输和处理显得十分重要。因此差错控制编码方法日益受到人们的重视。近四十年来，出现了一些性能良好的差错控制码，如Hamming码，BCH码和Convolution码等。

《组合设计与编码》一书，除向读者介绍已有的一些常见差错控制码外，将编码技术中的组合编码方法，组合数学中的区组设计，以及数论中的同余方法有机地结合在一起。读者一方面可以从本书中熟悉数论和组合数学的基本概念和原理，另一方面可以利用这些概念和原理研究和构造各种组合编码译码方法。书中所提出的复数旋转码，就是一种具有大数逻辑快速译码特性的新型组合码。

热忱希望广大读者从本书中获得一些有益的知识，并在进一步发展和应用差错控制编码技术中作出自己的贡献。

美国里海大学 K. K. 茅诗珍（茅于明）

前 言

以数字计算机为核心的现代信息处理技术，加上以数字通信为基础的现代通信技术，构成了正在到来的信息时代的主要特征。如果说人与人之间是靠语言来表达和交换信息的话，那么，数字计算机、数字通信设备以及各种数字控制测量装置间，就全靠离散型的码字，特别是简单方便的二进制码字，来作为沟通信息的共同语言。

为了提高数字信息传输的可靠性，50年代以来，差错控制编码技术有了很大的发展，出现了许多以码率高为特点的好码，如Hamming码、Golay码、BCH码和Goppa码等。随着计算机技术的迅速发展和推广应用，在网络系统、存储系统和运算系统中，都有大量的差错控制问题有待解决。尤其是在传输、存取、运算速度不断提高的情况下，差错控制码的译码速度能否进一步提高，就是编码理论和应用技术中的一个急待解决的重要课题。于是，具有并行处理特点和大数逻辑译码可能性的组合编码技术，近年来逐渐引起人们的关注和重视。

尽管国内外已有的少数编码书籍中，介绍了个别的组合编码方法，已有的一些组合数学书籍中，也谈到了组合原理用于编码技术的前景和示例，但是，尚未见到将组合数学和编码理论实践紧密联系起来，进行系统完整阐述的论著。为此，作者在本书中的一个大胆尝试，就是打算将组合编码技

术和它的理论基础——组合设计结合起来，再加上所需的数论同余方法，构成一条以**同余方法（数论）→组合设计（组合数学）→组合编码（编码技术）**为主轴线的新体系。

本书共分10章。第1章以绪论的形式，举例说明组合设计的内容，以及编码技术、组合设计和数论这三者的衔接关系。在第2章中，读者可以用不长的时间，熟悉掌握数论中同余运算方法的基本规则和若干重要定理，为从事组合设计和编码技术的学习研究，打下必要的数学基础。

第3章和第4章分别是组合数学和差错控制主要章节的一个缩影，使读者重点着眼于组合编码方法的同时，在组合数学和差错控制这两大领域中拓宽必要的广度。

第5章中三个主要的区组设计BIBD、DBBD和SBIBD，和第6章中用平方剩余构造循环差集的原理方法，是组合编码的数学基础。掌握这部分内容将有助于进一步探索和构造新的组合码类型。

第7章哈达玛矩阵和第8章拉丁方阵，是人们所熟悉的两类组合设计形式，由它们可以直接构造出相应的组合码。

第9章所介绍的一些组合码中，包括了作者及其同事们近年来在国内外学术会议和刊物上发表的几种新型组合码。而对作者所研究的比较典型完整的复数旋转码及其应用等，则单独列为第10章加以系统地阐述。

为了便于读者学习，除每章后附有适量习题外，书末还列有三个附表和参考文献以供查阅。

“万事开头难”。要想在有限的篇幅中，按组合设计与编码这个主题的要求，组织好各个章节的内容，并把一些离散的研究成果转化为系统的阐述，其本身就是一个相当难的

组合设计问题。作者在这里所抱的宗旨是，尽最大努力把一些新的概念、思路和初步成果（那怕是还不完全成熟的），尽快地介绍给有兴趣的读者，以便有更多的人掌握组合设计与编码的原理和技巧，在这个领域中开展更为深入的研究。正因为如此，作者殷切地希望，读者能将阅读本书过程中所发现的一些缺陷、问题和宝贵的建议，及时地通知作者，以便今后的改进和提高。

在组合编码的研究以及本书的写作过程中，西南交通大学曹建猷教授始终给予了有力的支持和指导。美国里海（Lehigh）大学曾开明（K. K. Tzeng）教授热情为本书作序。西安电子科学技术大学王新梅教授提供了许多宝贵的意见和建议。西南交通大学计算机科学与工程系陈志老师协助校核原稿。我的一些同事和研究生，如彭晓红老师、范平志老师、袁毅老师等，都为组合编码研究工作作出了自己的贡献。对此，作者一并表示自己诚挚的谢意。

靳　蕃

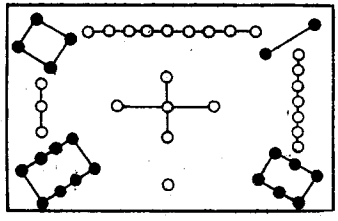
1989年5月

目　录

1 组合与编码概论

1.1 组合学的范畴

组合学（Combinatorics），也称组合数学或组合分析，它是一门既古老而又年轻的数学分支。当前世界上的一些组合数学家认为中国是组合数学的发源地。例如，约在公元前2200年的易经上，就曾描绘了据说是刻绘在黄河里神龟背上的两个数字配置图，即洛书（图 1.1）和河图（图 1.2）。



4	9	2
3	5	7
8	1	6

图 1.1 洛　书

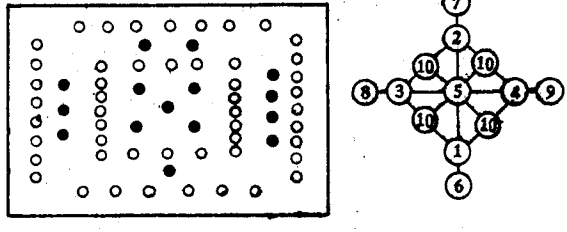


图 1.2 河　图

可以看出，如用数字代替各个点集，洛书所表示的就是一个每行、每列及每条对角线上各数和都等于15的幻方(Magic Squares)。而河图上的数字具有和中心相对称的性质，如$2+5=7$，$4+5=9$；$2+10+4=7+9$，$4+10+1=9+6$等等。实际上，这些都是若干数字的一种组合或安排。

本世纪50年代以来，由于数字式集成电路的迅猛发展，带动了以离散量为信息处理对象的数字式电子计算机技术的飞跃进步，促进了以数字信号为传输对象的数字通信技术的日益兴盛。在这种条件下，以研究离散对象在各种约束条件下的安排和配置问题的组合数学，被赋予了新的任务和内容，已经成为深受人们重视的一门独立的数学分支。组合数学在理论上与数论、集合论、代数学、概率统计等有密切关系，在信息编码、计算机科学、数字通信、物质结构、生物遗传工程、实验设计、人工智能以及社会管理科学许多领域中，都有重要的应用。甚至有人将组合概念用在发明新产品、构思新设计上，例如，将计时、测温和收音这三种功能采取不同的组合，就可以构造出带温度计的手表，带电子钟的收音机，以及兼有温度计、电子钟的三用式收音机等。

稍加注意，我们就会发现，自然界以及人类社会生产和生活中，充满着各式各样的组合问题。一定的化学成分可以组合成适合某种作物的最佳肥料，一批合适的队员可以组合成一支强劲的球队。组合电路、组合音响、组合家具等，都是因组合而显出它们的特点的。

作为组合数学来说，它所包含的内容应当是极其丰富的，而且将会随着科学技术的发展而不断地扩大它的范畴，因此给它下一个确切的定义为时尚早。目前的文献中，通常

把组合数学的内容分为下列三方面：

(1) **研究事物安排的存在性** 即把一组事物（通常是有限个事物）进行某种安排，使之满足一定的约束条件，研究这种安排是否存在。如果这种安排不总是可能时，那么就要分析在怎样的（必要的、充分的或充分且必要的）条件下，才能获得这种安排。

例如，n阶幻方就是把整数 1，2，3，…，n^2 排成 $n \times n$ 阵列，使每行、每列及两条对角线上 n 个数之和相等。

如果将这个和用 S_n 表示，由于 n 阶幻方中全部整数之总和是

$$1+2+3+\cdots+n^2=\frac{n^2(n^2+1)}{2}$$

故有

$$nS_n=\frac{n^2(n^2+1)}{2}$$

或

$$S_n=\frac{n(n^2+1)}{2} \tag{1.1}$$

显然，图 1.1 中的 3 阶幻方满足

$$S_3=\frac{3(3^2+1)}{2}=15$$

但是 $n=3$ 的幻方存在，并不意味着 n 为其他整数时幻方都存在。例如，$n=2$ 的幻方是不可能存在的，因为该幻方中任意一数字，不可能与其他三个不同的数字相加，使其和为同一数 $S_4=2(2^2+1)/2=5$。

如果能够设法构造出一组事物的某种安排，则该种安排

的存在性也就无疑义了。例如，对于 $n=2m+1$ ($m=0$, 1, 2, …) 的奇数阶幻方 $A=(a_{ij})$，其任一元素可以用公式（文献[4]）

$$a_{ij}=n(i+j+m+1)_n+(i+2j+1)_n+1 \quad (1.2)$$

来确定，式中 i, $j=0$, 1, 2, …, $2m$，括号右下注脚 n 表示对模 n 取余数。

四色问题是数学中一百多年来有名的未解决的难题之一。它的提法是，至少需用多少种颜色对一张平面地图上的各个国家（每个国家都是连通区域）着色，才能使有公共边界的国家具有不同的颜色？1890 年，P. J. Heawood 证明了用五种颜色着色就够了。直到 1976 年，两位数学家 K. Appel 和 W. Haken 作出证明，用四种颜色就可以给任何平面地图着色，他们的证明用计算机计算约需 1 200 机时，要作出 100 亿个独立的逻辑判断。由此可见，证明一种组合安排的存在性往往是一件艰巨的工作。

但是，某些初看上去很难的存在性判定问题，却可以用灵机一动的简便方法加以解决，这也是组合数学的一个特点。

瓷砖覆盖（或**棋盘覆盖**）问题就具有这样的性质。图 1.3 中的由 $6\times7=42$ 块方瓷砖组成的地面，显然可以用21块大小等于原先两块的长方形瓷砖所覆盖。如果在 1、7 两个位置上不再铺瓷砖，问剩下的地区能否用 20 块长方形瓷

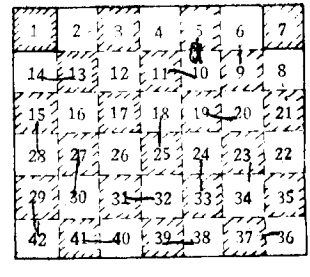


图 1.3 瓷砖覆盖问题

砖所完全覆盖（不允许瓷砖重叠）。

由于覆盖的方式种类很多，用穷举法来试探是十分费事的。下面可以用一个十分简便的方法来说明这种完全覆盖是不存在的。假定我们对原来 6×7 个方块进行黑白交替着色，图 1.3 中斜线方块表示着黑色，即共有 21 个黑色方块和 21 个白色方块。由于取消的 1、7 两方块都是黑色的，剩下地区只有 19 个黑色方块和 21 个白色方块。但是每一长方形瓷砖覆盖一个白色方块和一个黑色方块，因此 20 块长方形瓷砖理应覆盖 20 个黑色方块和 20 个白色方块。这就说明，剩下地区不可能被完全覆盖。

上面已经证明缺少两个同色方块后是不可能被完全覆盖的。那么，如果缺少的是两个不同颜色的方块，例如缺少的是 7 和 36 两个方块时，是否存在完全覆盖呢？如果缺少的是当中任何两个异色方块，情况又将是怎样的呢？

我们可以不用穷举法而按下面简单方法来证明它是可行的。设想图 1.3 中 42 个方块按顺序首尾相连成一条黑白交错的闭合环路，把闭合回路上任何两个异色方格取消，该闭合回路就一断为二（如取消的是相邻两异色方格，则变为一条），每一条必定由数目相同的异色方块组成，因而总可以被长方形瓷砖所覆盖。

（2）**事物安排的计数和分类** 如果某种安排是可能的，我们就可以来计算这类安排的数目，或者按一定的原则对它们进行分类。

图 1.4 表示一格形街道，某人从住地 A 到办公地 Z 去上班，问最短的路线有多少条。

显然，只要从 A 沿着向下的方向走到 Z 点都是最短路