全国高技术重点图书·通信技术领域

编码密码学

杨义先　林须端　著
胡正名　审

人民邮电出版社

登记证号（京）143号

内 容 简 介

本书是作者及所在课题组近十年来研究成果的总结，大部分内容在同类书籍中是首次出现。

全书共分四篇，分别对阵列编码、纠错编码、分组密码、序列密码进行了系统而深入的研究，并揭示了这四类编码形式彼此间的内在联系。

本书可供通信与电子系统、信号与信息处理和应用数学等方面的理论工作者、研究生和高年级本科生等作为专业课题研究的参考书。另外，书中许多简明的信号设计方案和密码协议对有关工程人员也有一定的参考价值。

全国高技术重点图书（通信技术领域）

编码密码学

林须端 著

胡正名 审

责任编辑：李树岭

人民邮电出版社出版发行

北京东长安街27号

中国科学院印刷厂印刷

新华书店总店科技发行所经销

*

开本：850×1168 1/32 1992年12月 第一版

印张：23 4/32页数：370 1992年12月北京第1次印刷

字数：610 千字 印数：1—5 000册

ISBN 7-115-04819-3/TN·576

定价：17.40元

《全国高技术重点图书》出版指导委员会

主　任： 朱丽兰

副主任： 刘　杲　卢鸣谷

委　员：（以姓氏笔划为序）

王大中　王为珍　王守武　牛田佳　卢鸣谷
叶培大　刘　仁　刘　杲　朱丽兰　孙宝寅
师昌绪　任新民　杨牧之　杨嘉墀　陈芳允
陈能宽　张钰珍　张效详　罗见龙　周炳琨
欧阳莲　赵忠贤　顾孝诚　谈德颜　龚　刚
梁祥丰

总干事： 罗见龙　梁祥丰

《全国高技术重点图书·通信技术领域》编审委员会

主　任： 叶培大

委　员： 陈俊亮　徐大雄　姚　彦
程时昕　陈芳烈　李树岭

前　言

今天我们已经进入信息时代。信息的传输、变换、压缩和存储等信息处理的有效性、可靠性和安全性已成为当今信息处理中极待解决的重要问题，而各种形式的编码和密码则是解决上述问题的基本理论和方法。

本世纪六十年代起，由于有限域等数学理论的引进使得编码理论，特别是纠错编码理论方面的研究成果叠出。但在七十年代后，虽然编码研究工作者们付出了艰辛的劳动，但却未能获得突破性的成果。为了进一步深入开发编码理论所蕴含的潜力，开辟新的研究领域，我们引入布尔函数和矩阵方法等数学工具，从另一新的侧面入手对各种编码形式，特别是 Walsh 编码、Hadamard 编码、最佳二进阵列、光正交码、并元码、Costas 阵列、循环码和等重码等进行了系统而深入的研究。这就是本书A、B两篇的内容。

根据加密原理的不同，现代密码学可分为分组密码和序列密码两大分支。在本书C篇中将主要介绍公开钥密码体制的基本原理和典型的密码体制代表。D篇中将对序列密码中密钥流的线性复杂度、相关免疫性和抗熵漏特性等进行深入研究。

本书是作者及所在课题组近十年来研究成果的系统总结。大部分内容在同类书籍中是首次出现。书中还提出了若干没有解决的问题和一些有价值的有待进一步研究方向，因此本书对有关通信与电子系统、信号理论与信息处理和应用数学等有关的理论工作者、研究生和高年级本科生的专业课题研究都有一定参考价值。

本书不涉及高深的数学理论，一般工程技术人员都能阅读，而且书中的许多结果都简明易懂。特别是在最佳信号设计和密码体制设计与安全性分析等方面的结果，对工程技术人员都会有一定的参

考价值。

全书共分19章。其中第1～9章和第17章由杨义先执笔，其它章节由林须端执笔，胡正名对全书的初稿进行了详细的修改并审校了全书。我们感谢课题组：李世群、罗群、吴建田、潘春燕、郭保安和朱剑英等的通力合作。感谢北京邮电学院周炯槃教授、蔡长年教授、胡正名教授、钟义信教授和吴伟陵教授的多方指导和帮助。特别感谢钮心忻、嵇丽华和钮因宽，他们在本书的整理过程中付出了艰辛的劳动。

由于水平所限，本书一定有许多不足之处，欢迎广大读者批评指正。

作　者

1992年于北京

目　　录

A篇　阵列编码

第一章　Walsh编码 …… 2

1.1　引言 …… 2

1.2　连续型 Walsh 函数 …… 3

1.2.1　Rademacher 函数 …… 3

1.2.2　Walsh 函数 …… 4

1.2.3　Walsh 函数系与三角函数系的类比 …… 9

1.3　离散型 Walsh 函数 …… 16

1.3.1　Walsh 矩阵及其快速构造 …… 16

1.3.2　Walsh 变换及其快速算法 …… 22

1.3.3　并元微积分 …… 29

1.4　信号移位及其 Walsh 频谱特性 …… 35

1.4.1　并元移位情形 …… 35

1.4.2　循环移位情形 …… 36

1.4.3　Walsh 移位情形 …… 41

1.5　Walsh 滤波 …… 47

1.5.1　Walsh 变换的纯量滤波 …… 47

1.5.2　Walsh 梳状列率滤波 …… 49

本章小结 …… 52

参考文献 …… 54

第二章　Hadamard 编码 …… 56

2.1　引言 …… 56

2.2　二维 Hadamard 矩阵 …… 58

2.2.1 二维 Hadamard 矩阵基础 ……58
2.2.2 归一 Hadamard 矩阵 ……65
2.2.3 循环 Hadamard 矩阵 ……71
2.3 四维二阶 Hadamard 矩阵 ……72
2.3.1 准备工作 ……73
2.3.2 计数与构造 ……74
2.4 n 维 2 阶 Hadamard 矩阵与 n 元H-布尔函数……81
2.4.1 n 元H-布尔函数的基本性质 ……81
2.4.2 n 维 2 阶 Hadamard 矩阵 ……92
2.5 一般高维 Hadamard 矩阵 ……98
2.5.1 存在性研究 ……99
2.5.2 高维完全正则与完全不正则 Hadamard 矩阵 …… 106
2.5.3 高维 Hadamard 矩阵的构造 …… 113
本章小结…… 117
参考文献…… 118
第三章 最佳二进阵列与三角序列…… 122
3.1 引言 …… 122
3.2 最佳二进阵列基础 …… 125
3.2.1 一维最佳二进阵列 …… 125
3.2.2 最佳二进阵列的平衡性 …… 126
3.2.3 最佳二进阵列的谱分析 …… 129
3.2.4 最佳二进阵列的构造法 …… 134
3.3 最佳二进阵列与高维 Hadamard 编码 …… 146
3.3.1 三维六阶 Hadamard 矩阵的发现 …… 147
3.3.2 构造高维 Hadamard 矩阵的新方法 …… 148
3.3.3 n 维二阶最佳二进阵列与H-布尔函数…… 150
3.4 准最佳二进阵列 …… 151
3.4.1 通用定义 …… 152
3.4.2 Fourier 频谱分析 …… 153

3.4.3 准最佳二进阵列的构造 …… 158
3.5 具有良好相关特性的实序列 …… 163
3.5.1 相关函数的物理意义 …… 163
3.5.2 第一类三角序列 …… 167
3.5.3 第二类三角序列 …… 170
3.5.4 第三类和第四类三角序列 …… 174
3.5.5 第五类三角序列 …… 175
3.5.6 第六类三角序列 …… 178
本章小结 …… 178
参考文献 …… 180
第四章 并元码与 Bent 函数 …… 182
4.1 引言 …… 182
4.2 一般并元码 …… 183
4.3 二进制并元码 …… 190
4.3.1 布尔函数的导数与 Walsh 谱 …… 190
4.3.2 二进制并元码 …… 195
4.4 Bent 函数与 Bent 序列 …… 203
4.4.1 Bent 函数 …… 203
4.4.2 Bent 序列 …… 218
4.5 Bent 函数与阵列编码之间的关系 …… 225
4.5.1 Bent 函数与 Walsh、Hadamard 编码 …… 226
4.5.2 Bent 函数与最佳二进阵列 …… 227
4.5.3 Bent 函数与并元码 …… 228
本章小结 …… 230
参考文献 …… 231
第五章 光正交码与 Costas 阵列 …… 233
5.1 引言 …… 233
5.2 光正交码及其构造 …… 234
5.2.1 预备知识 …… 234

5.2.2 递归构造法 …… 239
5.2.3 直接构造法 …… 242
5.2.4 代数构造法 …… 246
5.2.5 其它构造法 …… 249
5.3 光正交码的计数 …… 254
5.3.1 $\phi(n,\omega,\lambda)$ 的上界 …… 254
5.3.2 $\phi(n,\omega,\lambda)$ 的几个精确值 …… 265
5.3.3 其它参数的上下界 …… 270
5.4 Costas 阵列及其构造 …… 273
5.4.1 背景知识与定义 …… 273
5.4.2 Costas 阵列的构造 …… 279
5.5 Costas 阵列的极限行为 …… 288
本章小结 …… 297
参考文献 …… 299

B 篇 纠 错 编 码

第六章 线性分组码 …… 304
6.1 引言 …… 304
6.2 线性分组码基础 …… 305
6.2.1 生成矩阵与校验矩阵 …… 305
6.2.2 码间距离与码重 …… 309
6.3 Hamming 码与 R-M 码 …… 312
6.3.1 Hamming 码简介 …… 312
6.3.2 一阶 Reed-Muller 码简介 …… 316
6.3.3 高阶 Reed-Muller 码 …… 319
6.4 R-M 码与高维 Hadamard 矩阵 …… 321
6.4.1 正则 Hadamard 矩阵与一阶 R-M 码 …… 322
6.4.2 H(2,2,n) 的平衡度 …… 324

6.4.3 Hadamard 矩阵与 R-M 码 …… 326
6.5 R-M码的快速编码 …… 330
6.5.1 Y变换及其基本性质 …… 330
6.5.2 R-M码的快速编码 …… 337
本章小结 …… 338
参考文献 …… 338
第七章 循环码 …… 341
7.1 引言 …… 341
7.2 循环码基础 …… 341
7.2.1 循环码的生成多项式 …… 341
7.2.2 循环码的生成矩阵 …… 344
7.2.3 循环码的编码 …… 346
7.3 Reed-Solomon 码 …… 347
7.3.1 R-S码简介 …… 348
7.3.2 R-S码的最大周期计数 …… 351
7.3.3 随机序列计数 …… 355
7.4 循环码的周期分布 …… 357
7.4.1 R-S码的周期分布 …… 358
7.4.2 扩展R-S码的周期分布 …… 360
7.4.3 一般循环码的周期分布 …… 362
7.5 循环码在密码学中的应用实例 …… 364
本章小结 …… 366
参考文献 …… 368
第八章 等重码 …… 370
8.1 引言 …… 370
8.2 线性等重码的结构分析 …… 371
8.2.1 概念与定义 …… 371
8.2.2 结构分析 …… 375
8.3 非线性等重码的构造 …… 382

8.3.1 预备知识 …… 382
8.3.2 直接构造法 …… 384
8 3.3 间接构造法 …… 389
8.4 非线性等重码的容量上界 …… 391
8.4.1 A(n, d, w) 简介 …… 391
8.4.2 A(n, d, w) 的上界 …… 392
8.4.3 A(n, d, w) 的部分精确值 …… 396
8.5 非线性等重码的容量下界 …… 399
8.5.1 一般参数情形 …… 399
8.5.2 小参数情形 …… 401
本章小结 …… 408
参考文献 …… 409
第九章 纠错码差错控制性能分析 …… 412
9.1 引言 …… 412
9.2 不可检测错误概率 …… 413
9.2.1 基础知识 …… 413
9.2.2 几个实例 …… 417
9.3 截短 R-M 码和 SAB 码的不可检错误概率 …… 420
9.3.1 截短 R-M 码的 P(e) …… 420
9.3.2 SAB 码的 P(e) …… 427
9.4 译码错误概率 …… 440
9.4.1 背景简介 …… 440
9.4.2 译码错误概率与重量分布之间的关系 …… 442
9.4.3 几个实例 …… 445
9.5 掩蔽概率 …… 446
9.5.1 掩蔽概率简介 …… 446
9.5.2 最小最大检错准则最优码 …… 450
9.5.3 近似度量 …… 452
本章小结 …… 455

参考文献…… 456

C 篇 分组密码

第十章 古典密码…… 460
10.1 引言…… 460
10.2 古典密码系统…… 461
10.3 古典密码的破译…… 463
本章小结…… 468
参考文献…… 469
第十一章 现代密码基础理论…… 470
11.1 引言…… 470
11.2 密码系统的数学模型…… 471
11.3 密码系统理论安全性测度…… 472
11.4 密码系统的实用安全性…… 477
11.5 现代密码中计算复杂性理论基础…… 478
本章小结…… 480
参考文献…… 481
第十二章 DES 系统 …… 483
12.1 引言…… 483
12.2 DES 的算法描述 …… 484
12.3 DES 的弱点 …… 487
12.4 S-盒的设计分析 …… 490
本章小结…… 493
参考文献…… 493
第十三章 公开钥密码系统…… 495
13.1 引言…… 495
13.2 公开钥密码的基本思想…… 496
13.3 几个典型的公开钥密码系统…… 498

13.3.1 RSA 系统 …… 498
13.3.2 背包系统 …… 500
13.3.3 McEliece 系统 …… 503
13.3.4 二次剩余系统 …… 504
本章小结 …… 505
参考文献 …… 505
第十四章 密钥管理与确证系统 …… 507
14.1 引言 …… 507
14.2 密钥的管理与分配 …… 508
14.3 确证系统 …… 511
本章小结 …… 514
参考文献 …… 514

D 篇 序列密码

第十五章 序列密码原理 …… 518
15.1 引言 …… 518
15.2 序列密码的一般原理 …… 519
15.3 移位寄存器序列 …… 521
15.4 前馈序列 …… 531
15.5 用于序列密码的布尔函数计数问题 …… 538
15.5.1 满足一个条件时的计数 …… 539
15.5.2 满足多个条件时的计数 …… 544
本章小结 …… 549
参考文献 …… 549
第十六章 密钥序列随机性分析 …… 553
16.1 引言 …… 553
16.2 统计随机性与保密随机性 …… 553
16.3 随机序列的线性复杂度期望 …… 556

16.4 周期序列线性复杂度期望…… 561
16.4.1 扩域序列的线性复杂度与 GDFT …… 561
16.4.2 周期与特征互素的序列复杂度期望…… 568
16.4.3 周期为任意值N的序列复杂度期望…… 571
16.5 G(f) 序列线性复杂度分布 …… 579
本章小结…… 585
参考文献…… 586
第十七章 相关免疫与熵漏…… 589
17.1 引言…… 589
17.2 相关免疫的 Walsh 谱方法 …… 590
17.2.1 基本概念…… 590
17.2.2 Walsh 谱方法…… 593
17.3 相关免疫的布尔函数重量分析方法…… 596
17.3.1 低次情形…… 597
17.3.2 和式情形…… 600
17.3.3 其它情形…… 605
17.4 广义相关免疫…… 610
17.4.1 背景知识…… 610
17.4.2 广义相关免疫…… 612
17.5 线性逼近熵漏…… 617
17.5.1 线性逼近熵漏及其与阵列编码的关系…… 617
17.5.2 广义 e-bent 函数 …… 619
17.5.3 线性逼近熵漏…… 621
本章小结…… 628
参考文献…… 629
第十八章 线性复杂度及复杂度曲线…… 631
18.1 引言…… 631
18.2 线性复杂度计算布尔函数方法…… 631
18.2.1 周期为 2^n 序列的线性复杂度 …… 631

18.2.2 周期为 2^n 序列复杂度快速算法 …… 636
18.2.3 周期序列的布尔多项式表示 …… 637
18.2.4 一类序列线性复杂度的快速计算 …… 642
18.3 复合序列分析与卷积复合 …… 645
18.3.1 已知周期的序列安全性 …… 646
18.3.2 序列卷积复合 …… 648
18.4 线性复杂度曲线特性 …… 652
18.4.1 线性复杂度曲线的控制与特性 …… 653
18.4.2 连分式与线性复杂度曲线 …… 661
18.5 有限域上任意长度的 DFT …… 665
18.5.1 GF(q) 上任意长N的 DFT …… 665
18.5.2 任意长广义 DFT 的性质 …… 679
本章小结 …… 684
参考文献 …… 685
第十九章 序列的迹函数分析 …… 689
19.1 引言 …… 689
19.2 m-序列的结构分析 …… 689
19.3 序列相关函数的递归计算 …… 696
19.4 扩展 m-序列 …… 702
19.4.1 扩域序列的分量序列 …… 703
19.4.2 m-序列扩展 …… 704
19.4.3 随机性分析 …… 710
19.5 扩展 m-序列的相关函数 …… 716
本章小结 …… 722
参考文献 …… 722

A篇 阵列编码

"阵列编码"这一名词并无严格的数学定义，一般地讲以序列、矩阵和高维矩阵等阵列形式出现的离散编码都可称为阵列编码。由此可见阵列编码的研究领域十分广泛和丰富。在本篇（A篇）中，我们只重点研究彼此之间关系十分密切的Walsh编码、Hadamard编码、最佳二进阵列、三角序列、并元码、Bent序列、光正交码和Costas阵列等阵列编码形式。有关以上各种编码形式的内在联系的定量描述将在第1至第5章中详细叙述。在此，我们仅对这些联系作一个定性描述以便使读者能更清楚地了解本书的结构特征。①：Walsh编码是一类特殊的二维2^n阶的Hadamard编码，而一般的高维Hadamard编码则是二维情形向高维情形的推广。②：n维2阶最佳二进阵列与Bent函数和二进制并元码是彼此相互等价的，它们又都是一类特殊形式的n维2阶Hadamard矩阵。③：最佳二进阵列与三角序列与Bent序列、并元码、光正交码、Costas阵列分别是在循环相关、并元相关、光相关、非循环相关意义下的(准)最佳阵列编码形式。

希望以上内在联系的定性描述会有助于读者阅读本篇。

第一章 Walsh 编码

1.1 引 言

十九世纪末以来，以正弦函数和余弦函数为代表的频率理论在电子通信工程技术领域内统治了九十多年。至今在电子工程的许多领域中，正弦函数和余弦函数还一直被视为是这些工程发展的基础，这主要是因为在工程设计的理论和实践中经常是用频域方法来研究各种信号特征。实践和理论都表明频率理论的确非常好，特别是在通信领域中分析随机问题时，正弦和余弦函数的完备性和正交性使得解决判别问题十分方便。正弦、余弦函数最重要的特点之一是：大多数用于通信中的时间函数都可以表示为正弦和余弦函数的迭加，著名的富里叶分析就是进行这种变换的数学工具，它将时间函数变为频率函数。

但是随着数学理论的发展，人们已经认识到用正弦和余弦函数来表示时间函数，只是许多函数表示法中的一种，而且在有些情况下还不是最好的表示法。例如对方波形函数用 Walsh 函数去表示就更为简洁。因此随着电子技术的发展，特别是半导体工艺和集成电路技术的发展，人们开始寻求其它更具普遍性或在特定条件下性能更优良的完备正交函数系。就线性时不变系统而言，这些正交函数虽缺少正弦和余弦函数在线性时不变网络中的一些有用特性，但却具有另一些有用的特点使得它们在某些方面的应用更为直接和简便。以 Walsh 函数和 Haar 函数等为代表的非正弦正交函数系便是这样一类优良的函数系。它们的主要特点是仅包含两个状态，与数字逻辑特点一致而且还具有与正弦、余弦函数相似的若干性质。在本世纪六十年代末期，以 Walsh 函数为代表的非正弦正交函数的