

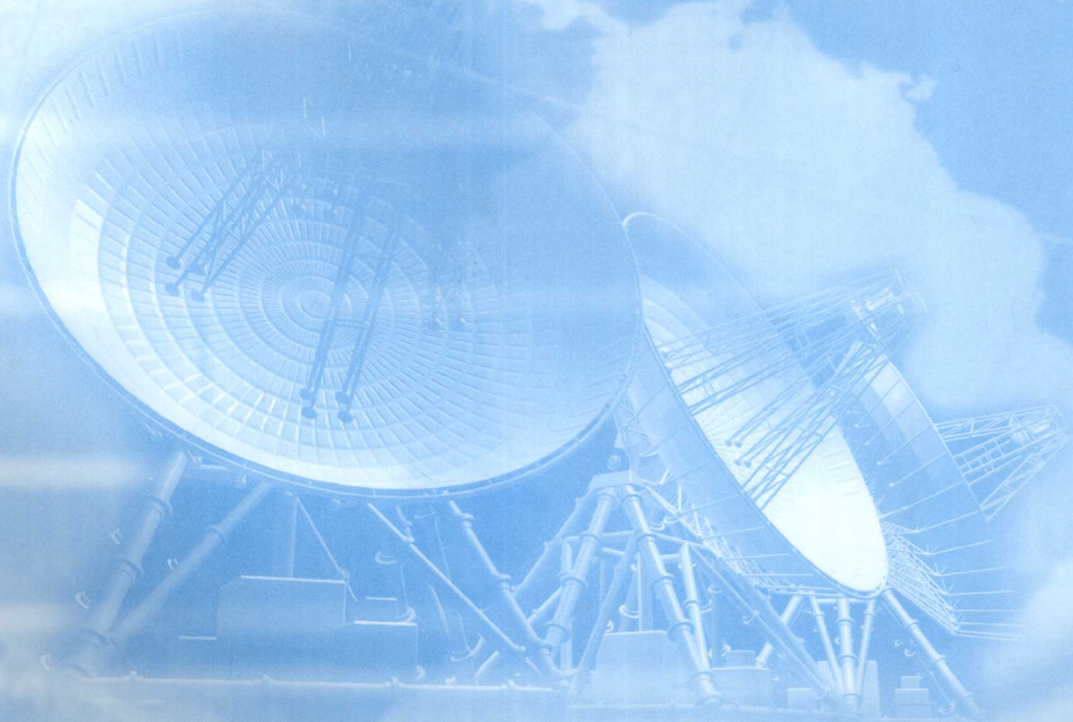
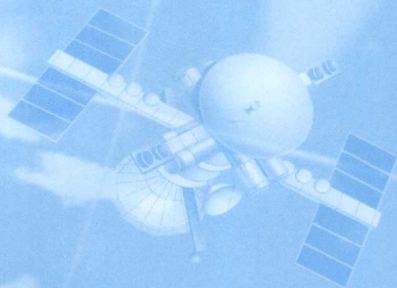


高等学校通信类教材

信道编码

(第三版)

刘玉君 编著



河南科学技术出版社

信道编码

(第三版)

刘玉君 编 著

河南科学技术出版社

内 容 提 要

本书比较详细地论述了信道编码理论和主要纠错码类的编、译码原理。内容包括：数学预备知识；线性分组码、循环码、BCH码和卷积码等主要纠错码类的编、译码原理，译码算法和实现方法；最后五章着重介绍纠突发错误编、译码技术，扰乱器，Turbo码，LDPC码和信道编码在通信信号加密和信息隐藏等方面的应用。本书可作为高等院校通信、计算机等专业的高年级本科生、研究生教材和参考书，也可供从事通信与计算机等工作的技术人员参考。

信 道 编 码

(第 三 版)

刘玉君 编著

责任编辑 李迎辉

河南科学技术出版社出版

解放军信息工程大学印刷厂印刷

787×1092毫米 16开本 30.5印张 780千字

1992年6月第1版 2006年12月第3次印刷

印数：5 001—10 000册

ISBN 7-5349-1090-0/G·252

定 价：43.00元

前 言

信道编码是 20 世纪 40 年代末提出、60 年代发展起来的一门提高数据传输可靠性的理论与技术，至今已有 50 余年的历史。随着数字通信的发展，特别是 70 年代以来，随着卫星通信和高速数据网的飞速发展，对数据传输的可靠性提出了越来越高的要求，因此，如何提高数据传输的可靠性已成为一个迫切需要解决的问题。

在有扰信道上传输数字数据时，所收到的数据将不可避免地含有差错。通常，用户提出一个差错率，当超出此差错率时，接收数据即不予使用。若采用信道编码技术，则可将差错减少到容许的限度以内。因此，信道编码是用来改善数字通信可靠性的一种信号处理技术。

代数理论为信道编码提供了理论基础，大规模集成电路和微型计算机的发展为信道编码技术的应用开拓了广阔的前景。我们将会看到，随着我国四化建设的飞速发展，信道编码技术将得到更加广泛的应用。

本书是在笔者所编著的《信道编码分析》和《信道编码》两套教材的基础上，经过多年试用和多次修改并加进了笔者多年来的研究成果编写而成的，这次修订再版，又增加了 Turbo 码、低密度校验码和信道编码在保密通信中的应用等三章，因此全书共分十二章，它们包括以下内容：

第一、二两章分别介绍了学习“信道编码”所需要的数学知识和信道编码理论中的一些基本概念。

线性分组码是信道编码中最基本的一类码，它有明显的数学结构，是讨论各类码的基础，因此，我们首先在第三章中介绍了线性分组码，并讨论了三个基本码限和两类基本线性分组码——汉明码和 RM 码。

为了使编、译码手续更为简单，多年来人们一直致力于分组码的研究，希望找到一种编、译码较易实现的分组码，而循环码就是这样的码。因此，我们在第四章介绍了循环码的基本理论及其编、译码实现电路。

BCH 码是一类纠多个随机错误的循环码，它纠错能力强，构造方便，编码简单，译码也较易实现，在编码理论中起着重要作用。因此我们在第五章对 BCH 码作了较为详细的论述，对主要的译码算法的原理和实现方法作了系统介绍，特别对 BCH 码的迭代译码原理及译码算法的改进进行了深入的讨论，并对 RS 码的频域编、译码方法及其频谱特征作了简单介绍。

1954 年里德（Reed）在译 RM 码时首先提出了大数逻辑译码的思想，以后许多编码工作者推广并发展了这一算法。1963 年梅西（Massey）首先把大数逻辑译码算法予以系统化。因此，我们在第六章中对循环码的大数逻辑译码作了系统的介绍，并对软判决的大数逻辑译码，即 APP 算法作了推广工作，提出了 L 步 APP 门限译码算法。

卷积码是区别于分组码的又一种新型信道编码，它广泛应用于卫星通信中，因此，我们在第七章中详细论述了卷积码的有关概念，对卷积码的代数译码和维特比译码算法进行了较为深入的讨论，并用不变因子分解定理，从理论上彻底解决了非系统卷积码中由生成多项式

矩阵求解监督多项式矩阵和非系统卷积码的信息恢复等问题。

许多实际信道中所产生的错误大部分是突发性的，或是突发错误与随机错误并存的。针对这类信道，需要设计专门用来纠突发错误的码类。因此，我们在第八章着重讨论了针对突发错误的编码技术，其中包括各种交错技术，如矩阵交错、卷积交错以及伪随机交错等。

实际数字通信系统的设计通常都受待传送的数据序列统计特性的影响，为了改善数据序列的统计特性，需要调制前的预编码，这就构成了数字通信系统设计中的一种专门技术——扰乱技术。本书第九章首先简要介绍了与扰乱技术有关的线性移位寄存器和 m 序列理论，然后对几种主要扰乱器作了较为详细地讨论。扰乱技术已用于 PCM 数字通信和保密通信中，所以介绍这方面的有关内容对于读者拓宽知识面和理论联系实际都是有益的。

Turbo 码是由法国学者 C. Berrou 等人在 1993 年国际通信会议 (ICC) 上提出来的，它的基本思想是利用递归系统卷积码和交织技术结合在一起，设计一种新的编码方法，Turbo 码的发现标志着信道编码理论与技术研究进入了一个崭新的阶段。因此，我们这次修订，特别增加了 Turbo 码一章，把 Turbo 码的有关概念介绍给读者。

随着 Turbo 码研究的进一步深入，人们重新发现，Gallager 早在 20 世纪 60 年代提出的低密度校验 (Low density parity check, LDPC) 码也是一种具有渐进特性的非常好的码。在较长码长条件下，LDPC 码的译码性能同样可以逼近香农限，而且 LDPC 码还具有译码算法复杂度与码的长度呈线性关系、不采用交织器等特点。我们在第十一章讨论 LDPC 码的有关概念，重点介绍几种用代数方法构造的 LDPC 码，最后较详细讨论了 LDPC 码译码的和积算法。

在目前许多通信体制中，加密与纠错往往是分开进行的。一般来说，一个完整的加密系统，首先要对数据加密，然后再对加密后的数据进行信道编码，以便保证通信的安全性和可靠性。然而这样做的结果是通信系统的计算量增大，系统处理数据的能力降低，且系统设备复杂。要克服上述种种弊端，就必须设计一种既安全又可靠的新型加密系统，它应当有机地将加密与纠错结合起来，利用信道编码进行加密就满足这样的要求，我们在最后一章讨论了信道编码在保密通信中的应用，简要介绍了用信道编码构建加密系统和信道编码信息隐藏系统的原理和方法。

为了便于读者阅读，我们在书的最后，还对各章节部分习题，给出参考答案，以便读者演练习题时参考。

笔者由衷地感谢窦瑞华、聂涛、党明瑞等教授以及我院、系、教研室、教保处的领导和同志们对本书的写作和出版所给予的支持、鼓励和帮助。特别是窦瑞华教授在百忙中认真审阅了初稿全文，改正了其中一些错误，并提出了许多具体的修改意见，笔者再次表示深切谢意。在本书这次修改重印过程中，北京理工大学安建平教授对本书修改提出了许多建设性意见，我校宋惠元教授、张水莲教授和李静、刘建洲、巩克现、杜健等同志分别对部分章节进行了认真校对，胡春松、唐冬明、王伟祥、王天宇、严玉平和徐甫等同志为本书最后三章的编写工作提供了许多帮助，在此一并致谢。

由于笔者水平有限，书中缺点在所难免，敬请广大读者批评指正。

刘玉君

2006 年 12 月

于解放军信息工程大学

目 录

第一章 数学预备知识	1
1.1 整数的可除性	1
1.1.1 整除的概念	1
1.1.2 最大公因数和最小公倍数	2
1.1.3 欧几里德算法	3
1.2 同余式和欧拉 - 费尔马定理	3
1.2.1 整数按模运算	3
1.2.2 同余式	4
1.2.3 模 n 剩余系和模 n 剩余缩系	4
1.2.4 欧拉函数及欧拉 - 费尔马定理	5
1.3 群的基本概念	7
1.3.1 群的定义	7
1.3.2 有限群及其性质	8
1.3.3 循环群及其性质	10
1.3.4 陪集的概念	11
1.4 域和域的同构	13
1.4.1 域的概念	13
1.4.2 域的性质	14
1.4.3 域的同构	15
1.4.4 域的特征和素域	15
1.5 交换环与理想	17
1.5.1 交换环的概念	17
1.5.2 子环与理想	18
1.6 $F_p[x]$ 中多项式	19
1.6.1 $F_p[x]$ 中一元多项式的运算	19
1.6.2 $F_p[x]$ 中多项式的最大公因式	19
1.6.3 $F_p[x]$ 中多项式的性质	24
1.7 欧拉 - 费尔马定理的推广	24
1.7.1 多项式的同余式	24
1.7.2 模 n 剩余系的推广	25
1.7.3 欧拉 - 费尔马定理的推广	26
1.8 多项式的周期和本原多项式	27
1.8.1 多项式的周期	27
1.8.2 本原多项式	30
1.9 有限域上线性空间	32
1.9.1 有限域上的几何向量	32
1.9.2 有限域上线性空间	33
1.9.3 线性空间的维数	34

1.9.4 线性子空间	34
1.10 $F_p[x] \bmod f(x)$ 的同余类环	35
1.10.1 $F_p[x] \bmod f(x)$ 的同余类环的概念	35
1.10.2 同余类环 $F_p[x]/(f(x))$ 的性质	36
1.11 $F_2[x] \bmod f(x)$ 的同余类域及极小多项式	38
1.11.1 $F_p[x] \bmod p(x)$ 的同余类域	38
1.11.2 有限域 $GF(2^n)$ 性质的进一步讨论	41
1.11.3 极小多项式	42
习 题	46
参考文献	48
第二章 数字通信与信道编码	49
2.1 差错控制与信道编码	49
2.1.1 信道编码的基本思想	49
2.1.2 突发错误和随机错误	50
2.1.3 差错控制的基本方式	51
2.1.4 信道编码的分类	51
2.2 信道模型和译码	53
2.2.1 信道模型	53
2.2.2 纠错译码	53
2.2.3 最大似然译码	54
2.2.4 最小距离译码	54
2.2.5 分组码的检、纠错能力	56
2.3 常用检错码	57
2.3.1 奇偶监督码	57
2.3.2 水平一致监督码	58
2.3.3 水平垂直一致监督码	58
2.3.4 群计数码	59
2.3.5 水平群计数码	59
2.3.6 等比码	60
2.3.7 交错监督码	60
2.3.8 二进制总计监督码	61
习 题	61
参考文献	62
第三章 线性分组码	63
3.1 线性分组码的基本概念	63
3.1.1 线性分组码的生成	63
3.1.2 (n, k) 线性分组码的一致监督矩阵	65
3.2 线性分组码的数学描述	67
3.2.1 线性分组码的代数结构	67
3.2.2 等价码	68
3.2.3 零化空间和对偶码	69
3.2.4 线性分组码的性质	70

3.3 线性分组码的译码	71
3.3.1 监督矩阵与最小距离的关系	71
3.3.2 标准阵列译码表	72
3.3.3 伴随式纠错译码	73
3.4 纠错能力与码限	75
3.4.1 辛格尔顿 (Singleton) 限	75
3.4.2 普洛特金 (Plotkin) 限	76
3.4.3 汉明 (Hamming) 限	76
3.5 汉明码及扩展汉明码	77
3.5.1 汉明码的构造	77
3.5.2 扩展汉明码	80
3.6 由已知码构造新码	82
3.6.1 对偶码	82
3.6.2 扩展码	82
3.6.3 删余码	82
3.6.4 增信删余码	83
3.6.5 增余删信码	83
3.7 RM 码及里德译码算法的改进	84
3.7.1 RM 码的概念	84
3.7.2 RM 码的里德译码算法	86
3.7.3 里德译码算法的改进	87
3.7.4 小数逻辑译码	88
习 题	90
参考文献	92
第四章 循环码	93
4.1 循环码的数学描述	93
4.1.1 循环码的基本概念	93
4.1.2 循环码的多项式表示	94
4.1.3 循环码与理想	94
4.2 循环码的矩阵描述和对偶码	97
4.2.1 循环码的生成矩阵	97
4.2.2 循环码的监督矩阵	99
4.2.3 对偶码	100
4.3 由生成多项式的根定义循环码	100
4.4 平方剩余码	104
4.4.1 平方剩余的概念	104
4.4.2 平方剩余码	105
4.5 多项式的乘除运算电路	106
4.5.1 乘法电路	106
4.5.2 除法电路	107
4.5.3 乘除电路	108
4.6 循环码的编码电路	109

4.6.1	r 级编码电路	109
4.6.2	k 级编码电路	110
4.7	循环码的译码电路	112
4.7.1	伴随式计算电路	112
4.7.2	错误图样检测器	113
4.7.3	梅吉特 (Meggit) 译码器的设计	113
4.7.4	非系统循环码的译码	116
4.8	缩短循环码	117
4.8.1	缩短循环码的构成	117
4.8.2	缩短循环码的生成矩阵和监督矩阵	118
4.8.3	缩短循环码的编码和译码电路	118
4.9	循环冗余码	119
4.9.1	循环冗余码的编、译码原理	119
4.9.2	循环冗余码的检、纠错能力	120
4.10	循环码的性质及其应用	121
4.10.1	循环码的主要性质	121
4.10.2	循环码性质的应用	121
4.11	准循环码和双环循环码	122
4.11.1	准循环码	122
4.11.2	双环循环码	124
4.11.3	双环循环码的编码电路	126
习 题		127
参考文献		128
第五章	BCH 码	129
5.1	BCH 码的基本概念	129
5.1.1	BCH 码的定义	129
5.1.2	BCH 码的进一步讨论	130
5.1.3	BCH 码的扩展	131
5.2	BCH 码的纠错能力	134
5.3	RS 码	135
5.3.1	RS 码的基本概念	135
5.3.2	非系统 RS 码的编码	137
5.3.3	RS 码的扩展	137
5.3.4	系统 RS 码的编码电路	138
5.3.5	缩短 RS 码	140
5.4	彼得森 (Peterson) 译码算法	140
5.4.1	彼得森译码原理	140
5.4.2	彼得森译码算法的计算机实现	144
5.5	BCH 码译码电路的设计	145
5.5.1	计算伴随式的电路设计	145
5.5.2	求错位多项式 $\sigma(x)$ 根的电路设计	146
5.6	BCH 码迭代译码原理	147

5.6.1	牛顿公式	147
5.6.2	关键方程的建立	151
5.6.3	迭代算法	152
5.6.4	迭代算法的计算机实现	156
5.7	快速迭代译码	158
5.7.1	二元 BCH 码迭代译码算法的简化	158
5.7.2	BCH 码的快速迭代译码	159
5.8	快速迭代译码的进一步改进	161
5.9	错误值计算和福尼 (Forney) 算法	165
5.9.1	福尼算法	165
5.9.2	福尼算法的简化	166
5.10	欧几里德译码算法	167
5.10.1	欧几里德译码算法原理	167
5.10.2	欧几里德算法的计算机实现和性能比较	170
5.11	RS 码的变换编码和译码	170
5.11.1	MS 多项式和有限域上的傅氏变换	170
5.11.2	RS 码的变换编码	173
5.11.3	RS 码的变换译码	174
5.12	RS 码的特征	177
5.12.1	RS 码与其对应二进制码的关系	177
5.12.2	RS 码对应的二进制码序列的特性	180
	习 题	182
	参考文献	182
第六章	循环码的大数逻辑译码	184
6.1	一步大数逻辑译码	184
6.1.1	大数逻辑译码的基本原理	184
6.1.2	一步大数逻辑译码的纠错能力	185
6.2	一步大数逻辑译码电路	186
6.2.1	I 型大数逻辑译码电路	186
6.2.2	II 型大数逻辑译码电路	188
6.3	某些一步大数逻辑可译码	189
6.3.1	极长码	189
6.3.2	差集循环码	190
6.4	L 步大数逻辑译码	193
6.4.1	L 步大数逻辑译码的概念	193
6.4.2	L 步大数逻辑译码电路的设计	195
6.5	欧氏几何码	198
6.5.1	欧氏几何的基本概念	198
6.5.2	欧氏几何码	199
6.5.3	欧氏几何码译码和 SCR 译码电路	203
6.6	APP 门限译码	205
6.6.1	离散无记忆信道 (DMC) 和距离函数	205

6.6.2 APP 门限译码	207
6.6.3 APP 门限译码的实现	210
6.6.4 L 步 APP 门限译码	211
习 题	213
参考文献	214
第七章 卷积码	215
7.1 $(n_0, 1, m)$ 卷积码的概念	215
7.1.1 卷积码的一般概念	215
7.1.2 $(n_0, 1, m)$ 卷积码的矩阵描述	216
7.2 $(n_0, 1, m)$ 卷积码的多项式表示	219
7.2.1 子生成多项式和生成多项式矩阵	219
7.2.2 卷积码的生成多项式	220
7.3 (n_0, k_0, m) 卷积码	221
7.3.1 (n_0, k_0, m) 卷积码的矩阵描述	221
7.3.2 (n_0, k_0, m) 卷积码的多项式表示	224
7.3.3 (n_0, k_0, m) 系统卷积码	224
7.4 不变因子分解定理与监督矩阵	225
7.4.1 系统码的监督矩阵	225
7.4.2 非系统卷积码的监督矩阵	229
7.4.3 不变因子分解定理和监督多项式矩阵	230
7.5 (n_0, k_0, m) 卷积码的编码电路	232
7.6 卷积码的译码	234
7.6.1 伴随式计算与实现电路	234
7.6.2 反馈译码电路的设计	235
7.7 卷积码的距离特性和纠错能力	238
7.7.1 初始截短码	238
7.7.2 距离特性和纠错能力	240
7.7.3 截断码的概念	242
7.8 卷积码的大数逻辑译码	244
7.8.1 自正交码	244
7.8.2 可正交码	247
7.9 卷积码的 APP 门限译码	251
7.10 卷积码的定译码	254
7.10.1 误差传播	254
7.10.2 定译码	256
7.11 怀纳 - 阿什 (WA) 纠一个错误卷积码	257
7.12 非系统卷积码的大数逻辑译码	259
7.12.1 伴随式计算和大数逻辑译码	259
7.12.2 $(n_0, 1, m)$ 非系统卷积码信息恢复电路	261
7.12.3 (n_0, k_0, m) 非系统卷积码的信息恢复电路	263
7.12.4 不变因子分解定理与信息恢复矩阵	264
7.13 卷积码的树图描述和栅格图	266

7.13.1	卷积码的树图描述	266
7.13.2	状态图与栅格图	268
7.14	卷积码的维特比译码	270
7.14.1	维特比译码算法的基本原理	270
7.14.2	维特比译码算法的修改	273
7.14.3	软判决的维特比译码	274
7.14.4	BSC 中维特比译码算法的性能和适用的码	276
7.15	删除卷积码	281
7.15.1	删除卷积码的概念	281
7.15.2	删除码的大数逻辑译码	283
7.15.3	常用的删除码	284
	习 题	285
	参考文献	287
第八章	纠突发错误码	288
8.1	循环码的纠突发错误能力	288
8.2	几类纠突发错误码	290
8.2.1	艾布拉姆森码和法尔码	290
8.2.2	巴顿码的构造	291
8.2.3	RS 码的纠突发错误性能	293
8.3	循环码的捕错译码	293
8.3.1	捕错译码的一般原理	293
8.3.2	纠单个突发错误码的捕错译码	296
8.4	循环码的矩阵交错编码	298
8.4.1	矩阵交错编码的原理	299
8.4.2	矩阵交错码的编、译码电路	301
8.5	分组码的卷积交错编码	301
8.5.1	交错次数 $m = pn + 1$ 的卷积交错编码	301
8.5.2	交错次数 $m = pn - 1$ 的卷积码交错编码	304
8.5.3	交错交数 m 与码长 n 互素的卷积交错编码	305
8.6	乘积码	307
8.6.1	乘积码及其纠错能力	307
8.6.2	循环乘积码	308
8.7	级连码	309
8.8	伪随机交错编码	311
8.8.1	线性冗余交错编码	311
8.8.2	伪随机交错编码	313
8.9	纠突发错误卷积码	316
8.9.1	基本概念	316
8.9.2	岩垂 (Iwadare) 码	317
8.10	扩散卷积码	319
8.10.1	自正交扩散卷积码	319
8.10.2	可正交扩散卷积码	321

8.11 卷积码的交错编码	322
8.11.1 卷积码的矩阵交错	322
8.11.2 卷积码的卷积交错	323
8.12 加拉格尔 (Gallager) 码	326
习 题	328
参考文献	329
第九章 数字数据扰乱器	330
9.1 线性移位寄存器序列的数学描述	330
9.1.1 线性移位寄存器序列与递推关系式	330
9.1.2 生成函数与生成多项式	333
9.1.3 状态转移矩阵和特征多项式	334
9.2 线性移位寄存器序列的周期性	335
9.3 $G(f)$ 中的平移等价类	338
9.4 m 序列及其伪随机性	339
9.4.1 m 序列的定义	339
9.4.2 m 序列的伪随机性	340
9.5 m 序列的移加特性和抽样特性	343
9.5.1 m 序列的移加特性	343
9.5.2 m 序列的抽样特性	345
9.6 线性移位寄存器的综合	347
9.6.1 解方程组法	348
9.6.2 迭代算法	349
9.7 伪随机扰乱器	351
9.8 自同步扰乱器	354
9.8.1 自同步扰乱器的基本原理	354
9.8.2 循环输入扰乱器的线性变换矩阵	356
9.8.3 自同步扰乱器的临界状态	358
9.8.4 带有特殊循环输入的扰乱器	359
9.9 自同步式伪随机扰乱器	361
9.10 扰乱器的主要特性	362
习 题	364
参考文献	364
第十章 Turbo 码	365
10.1 Turbo 码产生的背景与研究现状	365
10.1.1 Turbo 码的概述	365
10.1.2 Turbo 码研究现状	365
10.2 递归系统卷积码	367
10.2.1 非系统卷积码及其描述	367
10.2.2 递归系统卷积码及其描述	369
10.3 Turbo 码的编码原理	371
10.3.1 Turbo 码的并行级连结构	371
10.3.2 Turbo 码的串行级连结构	372

10.4	交织器的设计	374
10.4.1	交织器的基本原理	374
10.4.2	用于 Turbo 码的几种交织器设计	375
10.5	幻方交织器的设计	378
10.5.1	幻方的几种构成方法	378
10.5.2	幻方交织器的设计	384
10.6	Turbo 码译码的 SOVA 算法	385
10.6.1	软输出译码算法的提出	385
10.6.2	Turbo 码译码的 SOVA 算法	385
10.7	Turbo 码的迭代译码结构	386
10.8	分组 Turbo 码的编码原理	387
10.8.1	分组 Turbo 码的概念	387
10.8.2	多维分组 Turbo 码	389
10.8.3	分组 Turbo 码的译码	390
	习 题	392
	参考文献	393
第十一章	低密度校验码	394
11.1	低密度校验码产生的背景与研究现状	394
11.2	规则 LDPC 码的构造	395
11.2.1	规则低密度校验码的定义	395
11.2.2	Gallager 提出的 LDPC 码构造方法	395
11.3	LDPC 码的因子图表示	397
11.4	用循环矩阵构造的 LDPC 码	398
11.4.1	矩阵循环群	398
11.4.2	利用矩阵循环群构造的 LDPC 码	399
11.5	欧氏几何 LDPC 码	400
11.5.1	欧氏几何的有关概念	400
11.5.2	欧氏几何 LDPC 码	401
11.6	级连 LDPC 码	406
11.6.1	SPC 码	406
11.6.2	串行 LDPC 码的编码和码结构	408
11.7	LDPC 码的译码	411
11.7.1	LDPC 码的译码思想	411
11.7.2	逐个的码元检测	411
11.7.3	并行的码元检测	413
11.7.4	和积算法程序流程	415
	习题	416
	参考文献	417
第十二章	信道编码在保密通信中的应用	418
12.1	密码学概述	418
12.2	分组密码体制	419
12.3	信道编码加密系统	420

12.3.1 McEliece 公钥密码体制	421
12.3.2 M 公钥密码体制的改进和信道编码公钥密码体制	421
12.4 信道编码公钥密码体制的分析	425
12.4.1 信道编码公钥密码体制的性能分析	425
12.4.2 信道编码公钥密码体制的解含错方程组攻击法	426
12.5 信息隐藏技术	430
12.5.1 信息隐藏技术的概述	430
12.5.2 信息隐藏原理和技术指标	431
12.6 信道编码与信息隐藏技术	432
12.6.1 信道编码信息隐藏的意义	432
12.6.2 信道编码信息隐藏的原理	433
12.6.3 信道信息隐藏的预处理	433
12.6.4 信道编码信息隐藏的性能分析	434
12.7 基于 BCH 码和 RS 码的信道编码信息隐藏技术	435
12.7.1 基于 BCH 码、RS 码的信道信息隐藏的实现方案	435
12.7.2 实验数据与性能分析	436
12.7.3 信道编码私钥密码体制与信道编码信息隐藏技术	436
12.8 信道编码信息隐藏的检测技术	437
12.8.1 信息隐藏分析方法简介	437
12.8.2 信道编码信息隐藏检测技术	438
习 题	439
参考文献	441
部分习题参考答案	442
附录 英汉信道编码词汇	460

第一章 数学预备知识

信道编码理论与代数学有着密切的关系. 多项式、向量、矩阵运算以及近世代数的有关理论是研究信道编码必不可少的数学工具. 鉴于这些数学知识在有关教科书中都有详细论述, 这里仅对本书常用到的一些主要数学概念, 给以简要介绍.

1.1 整数的可除性

1.1.1 整除的概念

我们把 $1, 2, 3, \dots, n, \dots$ 称为自然数, 并用 N 表示自然数全体所成的集合, 即:

$$N = \{1, 2, \dots, n, \dots\}.$$

显然, 任意两个自然数的和与积仍然是自然数, 但两个自然数相减就不一定是自然数, 因为减法运算产生了零和负数. 通常我们把正整数、负整数的全体与零所成的集合称为整数集合, 并用 Z 表示, 即

$$Z = \{\dots, -n, \dots, -2, -1, 0, 1, 2, \dots, n, \dots\}.$$

在整数集合 Z 中可以做加、减和乘法等运算, 但除法不总是可以进行的, 因为任意两个整数作除法, 结果可能不再是整数.

定义 1.1 对于整数集合 Z 中任意两个数 a, b , 且 $a \neq 0$, 如果存在一个 $q \in Z$, 使得 $b = aq$, 则称 a 整除 b , 记为 $a|b$. 否则称 a 不能整除 b . 若 $a|b$, 也称 a 是 b 的因数, 或 b 是 a 的倍数.

下面列举有关整除的一些性质.

1° 如果 $a|b$, 则 $a|(-b)$, $-a|b$, $-a|(-b)$.

有了性质 1°, 我们今后只需考虑正整数和零的正因子和正倍数即可.

2° 如果 $a|b$ 及 $a|c$, 则 $a|(mb + nc)$, $m, n \in Z$.

该性质还可以推广到有限个的情况, 即

如果 $a|b_i, i = 1, 2, \dots, n$, 则

$$a \mid \sum_{i=1}^n k_i b_i, \quad k_i \in Z, i = 1, 2, \dots, n.$$

3° 如果 $a|b, b|c$, 则 $a|c$.

4° 如果 $a|b$, 且 $b|a$, 则 $a = b$.

5° 如果 $a|b, c \neq 0$, 则 $ac|bc$.

6° 如果 $ac|bc$, 则 $a|b$.

既然除法运算在整数集合中不总是可以进行的, 那么用整数集合 Z 中一个非零整数去除 Z 中任一整数, 就有除得尽与除不尽两种可能. 下面定理给出了用 b 去除 Z 中任一数 a 所得的结果, 这就是带余除法定理.

定理 1.1 设 a, b 是整数集合 Z 中任意两个数, 且 $a \neq 0$, 则一定存在唯一的两个整数 q 和 r , 使得

$$b = aq + r, \quad 0 \leq r < |a|. \quad (1.1.1)$$

1.1.2 最大公因数和最小公倍数

若 $a|b$, 则 $-a|b$ 及 $a|(-b)$, 因此我们只讨论正整数和零的正因数及正倍数.

定义 1.2 若 d 是 a 的因数, 又是 b 的因数, 则 d 称为 a 与 b 的公因数; 若 m 是 a 的倍数, 又是 b 的倍数, 则 m 称为 a 与 b 的公倍数.

一般情况下, a 与 b 的公因数不是唯一的, 它有有限多个, 当然这些公因数中一定有一个最大的. 然而两个数的公倍数有无限多个, 因为若 m 是 a 与 b 的公倍数, 则 $2m, 3m, \dots$ 等都是 a 与 b 的公倍数, a 与 b 的公倍数中一定有一个最小的.

定义 1.3 设 a 与 b 不全为零, 如果有一个 d 满足

$$1^\circ d|a, d|b;$$

$$2^\circ \text{ 若 } e \text{ 是 } a \text{ 与 } b \text{ 的公因数, 则有 } e|d,$$

我们就称 d 是 a 与 b 的最大公因数, 记为 $d = (a, b)$, 或者 $d = \text{GCD}(a, b)$.

最大公因数是今后经常用到的, 因此下面给出最大公因数的一些简单性质.

$$1^\circ d|a \text{ 与 } d|b \text{ 同时成立的充分必要条件是 } d|(a, b).$$

$$2^\circ \text{ 设 } (a, b) = d, \text{ 则 } (ka, kb) = kd; \text{ 若 } k|a, k|b, \text{ 则}$$

$$\left(\frac{a}{k}, \frac{b}{k}\right) = \frac{(a, b)}{k}.$$

$$3^\circ (a, b) = d \text{ 的充分必要条件是 } \left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

$$4^\circ \text{ 如果 } (a, b) = d, \text{ 则一定存在一对整数 } u, v, \text{ 使得}$$

$$ua + vb = d, \quad (1.1.2)$$

而且还可以进一步要求 u, v 适合条件

$$0 \leq u < \frac{b}{d}, \quad 0 \leq |v| < \frac{a}{d}.$$

其中 $a \cdot b \neq 0, a \neq b$, 且适合上述条件的 u, v 是唯一的.

定义 1.4 设 a, b 不全为零, 如果 a, b 的一个公倍数 m 具有如下性质: a 与 b 的任何一个公倍数都是 m 的倍数, 则 m 叫做 a 与 b 的最小公倍数, 记为 $m = [a, b]$ 或 $m = \text{LCM}(a, b)$.

定义 1.5 如果两个数 a 与 b 的最大公因数是 1, 即 $(a, b) = 1$, 则称 a 与 b 是互素的.

类似性质 4° , 我们有

$$5^\circ \text{ 如果 } (a, b) = 1, \text{ 则存在一对整数 } u \text{ 和 } v \text{ 使得}$$

$$ua + vb = 1,$$

其中 $0 \leq u < b, 0 \leq |v| < a$ ($a \neq 0, b \neq 0$, 且 a, b 不全为 1), 而且 u, v 是唯一确定的.

$$6^\circ \text{ 如果 } a|b \cdot c, \text{ 且 } (a, b) = 1, \text{ 则 } a|c.$$

$$7^\circ \text{ 如果 } a|c, b|c, \text{ 且 } (a, b) = 1, \text{ 则 } a \cdot b|c.$$

$$8^\circ \text{ 如果 } (a, c) = 1, (b, c) = 1, \text{ 则 } (a \cdot b, c) = 1.$$

定义 1.6 如果一个大于 1 的整数 a , 除了 1 和它本身以外, 没有其他因数, 则 a 称为素数, 大于 1 不是素数的数叫做合数.

素数有以下性质:

$$1^\circ \text{ 对于一个素数 } p \text{ 和任一整数 } a, p|a \text{ 或者 } (p, a) = 1, \text{ 两者必有且仅有一成立.}$$

$$2^\circ \text{ 如果一个素数 } p|a \cdot b, \text{ 则 } p|a \text{ 或者 } p|b.$$

定义 1.7 如果一个素数 $p|a$, 则 p 叫做 a 的素因子.