

高新技术专著系列

Modern Channel Coding And Modulation : Theory And Application

现代纠错编码与调制 理论及应用

吴湛击 著
王文博 审

- 信道编码和调制方法的基本理论与技术应用
- 编码调制领域最新理论与技术发展
- 作者多年的创新性研究成果



人民邮电出版社

POSTS & TELECOM PRESS

高新技术专著系列

**Modern Channel Coding
And Modulation :
Theory And Application**

**现代纠错编码与调制
理论及应用**

吴湛击 著
王文博 审

人民邮电出版社

北京

图书在版编目 (C I P) 数据

现代纠错编码与调制理论及应用 / 吴湛击著. —北京:
人民邮电出版社, 2008. 12
ISBN 978-7-115-19024-6

I. 现… II. 吴… III. 纠错码—通信理论 IV. TN911.22

中国版本图书馆CIP数据核字 (2008) 第161458号

内 容 提 要

本书系统地介绍了编解码理论的基本概念、基本方法和基本应用。全书内容可以分为 4 部分: 第一部分内容为绪论、信息论基本知识、纠错码基本理论与基本概念以及纠错码的代数基础; 第二部分内容为线性分组码、循环码、卷积码以及级联码等; 第三部分内容为 Turbo 码、LDPC 码以及统一编码和密度进化理论; 第四部分内容为现有的移动通信中的纠错码、无线信道估计与 Turbo 码补偿解码、未来移动通信中的 LDPC 码以及未来移动通信标准中的调制技术。

本书的特点是尽量避免枯燥的数学证明和深奥的理论分析, 注重强调纠错码技术的基本概念、方法和实际应用。本书可以作为通信领域工程技术人员的参考书, 也可以作为通信专业高年级本科生和研究生的教材。

现代纠错编码与调制理论及应用

-
- ◆ 著 吴湛击
审 王文博
责任编辑 陈万寿
执行编辑 杨 凌
 - ◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@ptpress.com.cn
网址 <http://www.ptpress.com.cn>
北京铭成印刷有限公司印刷
 - ◆ 开本: 700×1000 1/16
印张: 25.75
字数: 492 千字
印数: 1—3 000 册
 - 2008 年 12 月第 1 版
2008 年 12 月北京第 1 次印刷

ISBN 978-7-115-19024-6/TN

定价: 88.00 元

读者服务热线: (010)67129264 印装质量热线: (010)67129223
反盗版热线: (010)67171154

序

信道编码与调制是整个通信理论的精髓，广泛应用于宇航深空通信、个人移动通信、公用电话网、互联网和 DVD 纠错等各种场景，为信息化社会提供了高效、可靠的技术保障。

1948 年，香农 (Shannon) 发表了具有里程碑意义的《The Mathematical Theory of Communications (通信的数学理论)》一文，为信道编码技术指明了发展方向。在此后的半个多世纪中，经过 Hanming、Golay、Reed、Solomon、Massey、Berlekamp、Elias、Viterbi、Forney、Shu Lin、Gallager 等众多学者的不懈努力，纠错码理论与技术不断发展并完善。尤其是在世纪之交，C. Berrou 提出了 Turbo 码，随后 Mackay 和 Neal 重新发现了 LDPC 码，这两种编码都逼近了 BPSK 调制下的加性高斯白噪声信道容量。目前，Turbo 码已经成功应用到第三代移动通信的标准中，而 LDPC 码则是下一代移动通信和深空通信纠错技术的研究热点。在编码调制技术方面，基于分组码的多级编码调制、网格编码调制 (TCM) 和 Turbo-网格编码调制 (T-TCM) 等带宽有效的编码调制技术相继提出，提高了高频谱利用率下的功率有效性。以香农信息论为代表的纠错编码和调制理论进入了一个总结归纳的成熟期，同时也意味着下一次技术突破即将来临。未来的移动通信要求在有效的无线带宽内提高吞吐量来满足日益增长的宽带业务需求，而吞吐量是带宽有效性与功率有效性的综合体现。但是，目前的编码调制技术相对于高带宽利用率的衰落信道容量还有很大距离，其功率有效性还有很大的提高空间，这些都是学术界和产业界急需解决的问题。

纠错码领域的优秀专著与教材在国内外已有大量出版。《现代纠错编码与调制理论及应用》一书是作者在总结近 10 年来从事移动通信编码调制技术研究的基础上编写的，其主要特色有：第一，作者从理论与实际相结合的角度，列举了大量实例，深入浅出地介绍了纠错码的基础理论与基本知识；第二，结合作者近些年来在编码前沿技术领域的一些研究成果重点，深入地分析和介绍了 Turbo 码、LDPC 码以及统一编码和密度进化理论，探索了好码设计的关键方法及相关使用技术；第三，结合纠错码在无线移动通信中的实际应用进行了详细的分析与介绍，并作进一步的探讨；第四，作者结合自己的研究经历和实践经验，探索了无线信噪估计与 Turbo 码补偿解码技术，未来移动通信中的 LDPC 码以及未来移动通信标准中的调制技术，提出了一些有新意的学术见解。总之，作者博采众长，又有所创新，在广泛吸取和继承前人研究结果的基础上推陈出新，有所发展。

本书内容丰富，非常适合信息与通信及相关领域中的本科生、研究生以及无线移动通信领域中的工程技术人员学习、阅读和在工作中参考。

吴伟陵于北京邮电大学
2009 年元旦

前言

1948年，香农（Shannon）发表了具有里程碑意义的《The Mathematical Theory of Communications（通信的数学理论）》一文，提出了信道编码定理和信源编码定理，开创了信息论这门崭新的学科，从而为在通信系统中实现高效可靠的信息传输奠定了理论上的坚实基础。自香农开创信息论以来，经过数代学者持之以恒的辛勤探索，纠错编码领域取得了长足的进步与发展。尤其是在世纪交替的近10年间，Turbo码、LDPC码、RA码和Woven码等一大批性能优异的编解码方法如雨后春笋般涌现，标志着这一领域的研究成果已经进入了炉火纯青的境界。Turbo码已经成功应用到第三代移动通信的标准中，而LDPC码则是下一代移动通信和深空通信纠错技术的研究热点。最近出现的统一编解码理论——要素图与和积算法对这些形形色色的编解码算法给出了简明而深刻的统一解释。而密度进化理论则揭示了诸如Turbo码、LDPC码等迭代解码算法的收敛特性，解释了它们逼近香农限的原因，也提供了好码设计的思路与方法。但从历史的长河来看，这只是人类探索未知世界的一小步。按照波普提出的科技发展的规律，以香农信息论为代表的纠错编码理论进入了一个总结归纳的成熟期，同时也意味着下一次技术突破即将来临。我们深信于此。

本书作者从事编码调制技术领域的研究工作已经有10多年，越发感到这门技术的精妙和深邃。现代信道编码与调制技术，不仅需要精深而巧妙的数学，更需要深刻而辩证的思想。当读一篇经典论文时，重要的不是看懂技术本身，而是读懂它背后隐藏的思想。比如，诸如Turbo码和LDPC码的迭代解码的原理，其实和我们日常对话的原理是一样的。假设两个朋友（A和B）就某个话题交流，A听到了B的看法后，会结合自己已有的知识与观念进行综合判断，形成新的知识和观念，并反馈给B。同样，B听到A的反馈后，也会结合自己已有的知识与观念进行综合判断，并形成新的判断，再反馈给A。如此，两个人之间不断地进行反馈和交谈，这其实就是一个迭代解码的过程。最终，两个人可能达成一致意见，这就是解码收敛；但也可能仍然存在分歧，这就是解码发散。所以，只有我们能够读懂这些思想，才能深刻地理解技术本身。而最终各类科学技术都是普遍联系、融会贯通的。比如，本人一直致力于研究的统一编解码理论——要素图与和积算法，就揭示了各种各样的线性分组码（如LDPC码）和Turbo码之间的编解码规律的内在统一性。更一般地，要素图与和积算法还能揭示编码与各种滤波理论（如卡尔曼滤波、维纳滤波）、信号处理的一些经典算法（如快速傅里叶变换）甚至人工智能领域中的经典算法（如置信度传播BP算法）的内在统一性。这其实已经上升到了一个理性抽象的哲学高度。只有我们真正掌握了这些理论和思想，才能高屋建瓴地把握这些纷繁复

.....

杂的技术，并更好地用理论来指导技术的推陈出新。这门技术的难点也就在于此：不仅需要精深的数学抽象，而且更需要深刻的思想创新。所以，基于信息论的现代信道编码与调制，与其说是一种技术，不如说是一门艺术。

在本书的写作过程中，得到了吾师吴伟陵教授的悉心指导。而在本人读博士期间，也从吴老师的言传身教中获益匪浅，所以才能厚积薄发，有了写作此书的基础。特别令人感动的是，吴老师还在非常繁忙的工作中拨冗亲自为本书作序。在此，谨向吾师表达最诚挚的谢意。

同时，本书也得到了王文博老师的指导。在本人任教期间，得到了王老师多方面的关怀和帮助，才得以在王老师任责任教授的无线信号处理与网络实验室(WSPN)里能够潜心钻研，写作此书。在本书的写作过程中，王老师也给了许多中肯的意见和建议。在此，也向王老师表达由衷的谢意。

本书的研究工作也得到了国家自然科学基金(No. 60702050)的资助，在此表示感谢。同时，本书的一些研究成果也得益于普天信息技术研究院的资助，感谢胡炜、雷旭、郑辰等几位博士的交流合作。在本人求学期间，与梁双春、孟德香、吴江、叶卓映、吴强、程型清等博士同学经常切磋交流，并且受益匪浅。在本人指导的科研项目中，还得到了杨洪文、刘丹谱、彭木根、彭涛、张兴、孙卓、景晓军、李绍胜、君长川、林雪红等教师的有力支持和帮助，同时也有与欧阳子月和李璐颖等研究生共同研究的辛勤所得。

在本人参加国家 IMT-Advanced 的标准化活动中，得到了沈嘉、林辉、孙韶辉等博士的支持，深表谢意。另外，也特别感谢 Marc Fossorier、Daniela Tuninetti、Jinhong Yuan 等海外知名学者对本人研究工作的支持与鼓励。

感谢姐姐吴蔚爽对我多年来的关心和鼓励；感谢爱人高辉对我生活的关照以及对我研究工作的支持。

最后，将本书献给我的父母——吴浩生和李素萍，感谢父母多年的辛苦养育和全力支持。

当然，对于本书中的不足之处，也恳请读者批评斧正，不吝赐教。

路漫漫其修远兮，吾将上下而求索。

吴湛击

wuzhanji@163.com

wuzhanji@bupt.edu.cn

目 录

第 1 章 绪论

- 1.1 纠错码理论的历史回顾 2
- 1.2 近十年来纠错码理论的突破性发展 4

第 2 章 信息论基础

- 2.1 熵和互信息的概念 8
- 2.2 信道容量的概念 11
- 2.3 纠错码与信道容量的关系 13

第 3 章 纠错码的基本概念

- 3.1 差错控制的基本概念 20
- 3.2 差错控制系统 21
- 3.3 纠错码的基本概念 23
 - 3.3.1 编码效率 23
 - 3.3.2 编码增益 24
 - 3.3.3 信息码元与监督码元 24
 - 3.3.4 许用码组与禁用码组 24
 - 3.3.5 编码距离 24
- 3.4 检错纠错能力与最小码间距离 $d_{\min}$ 的关系 25
- 3.5 差错控制编码的效用 27

3.6 纠错码的分类 28

第4章
纠错码的代数基础

4.1 整数的基本知识 31

4.2 代数系统的基本概念 32

4.3 多项式剩余类环 34

 4.3.1 关于多项式的几个定义 34

 4.3.2 多项式的运算规则 35

 4.3.3 多项式剩余类构成有限域 36

4.4 有限域代数的基础知识 36

4.5 中国剩余定理(孙子定理) 39

第5章
线性分组码

5.1 线性分组码的基本概念 42

5.2 码的校验矩阵与生成矩阵 43

5.3 线性分组码的伴随式与解码方法 44

5.4 最大距离码与完备码 46

5.5 汉明码与格雷码 47

5.6 哈达玛码(Hadamard Code)与瑞德-穆勒码(Reed-Muller Code) 48

5.7 线性分组码的性能限 52

5.8 线性分组码在第三代移动通信系统中的应用 54

 5.8.1 编码器结构 55

 5.8.2 解码算法 58

 5.8.3 仿真验证 64

 5.8.4 结论 65

第6章
循环码

6.1 循环码的基本概念 67

6.2 循环码的多项式描述 67

6.3	循环码的矩阵描述	69
6.4	缩短循环码与循环冗余校验码	71
6.5	Fire (费尔) 码和 QR (平方剩余) 码	72
6.6	BCH 码和 R-S 码	75
6.7	多项式乘法电路	77
6.7.1	多项式乘法电路	77
6.7.2	多项式除法电路	79
6.7.3	多项式乘法电路	80
6.7.4	循环码的编码电路	82
6.8	循环码的解码	83
6.8.1	梅杰特解码器	84
6.8.2	捕错解码器	88
6.8.3	缩短循环码的解码	90
6.9	BCH 码和 R-S 码的编码构造	92
6.9.1	BCH 码的构造方法	94
6.9.2	R-S 码的构造方法	98
6.10	BCH 码和 R-S 码的解码方法	100
6.10.1	关键方程的引入	100
6.10.2	多项式的欧几里德算法	102
6.10.3	BCH/R-S 码的解码步骤	105
6.10.4	仿真结果	109
6.11	删除信道下的解码	112

第7章 卷积码

7.1	卷积码的基本概念	119
7.2	卷积码的描述	120
7.2.1	卷积码的矩阵描述	120
7.2.2	卷积码的树图描述	125
7.2.3	卷积码的状态图描述	126
7.2.4	卷积码的网格图描述	126
7.2.5	卷积码的多项式表示	128
7.3	卷积码的维特比解码算法	128

7.3.1	维特比解码算法的基本原理	128
7.3.2	维特比解码算法的性能	132
7.4	卷积码的距离特性	134
7.5	卷积码距离谱的信号流图法	136
7.5.1	线性状态方程法	138
7.5.2	图解变换法	139
7.6	卷积码的性能分析	140
7.7	卷积码在通信中的应用	145

第8章

交织码、级联码与 TCM 和 PCM

8.1	交织	147
8.1.1	块交织	148
8.1.2	比特翻转交织	148
8.1.3	权位倒置交织器的提出	149
8.2	级联码	151
8.3	网格编码调制 (TCM)	152
8.3.1	8PSK 4 状态的 TCM	152
8.3.2	一般的 TCM	155
8.4	CPM 调制和解调技术	158
8.4.1	CPM 信号的一般表达式及其线性近似模型	158
8.4.2	GSM 中的调制技术——GMSK 调制	160
8.4.3	无线信道下的 CPM 信号的最佳解调技术——MLSE 均衡 解调技术	161

第9章

Turbo 码

9.1	Turbo 码的编码方法	165
9.2	Turbo 码的解码方法	166
9.2.1	MAP、Log_MAP 和 Max_Log_MAP 算法	168
9.2.2	SOVA 算法	171
9.2.3	各种算法小结	174

9.3 Turbo 码的分量码与交织器的设计	175
9.4 Turbo 码解码质量的估值技术	177
9.4.1 对误帧率的估值算法研究	177
9.4.2 对误码率的估值算法研究	180
9.4.3 仿真比较性研究	181
9.4.4 结论	184
9.5 Turbo 码的自适应迭代算法	184
9.5.1 自适应迭代解码算法的研究综述	185
9.5.2 新的自适应迭代算法	186
9.5.3 仿真比较性研究	189
9.5.4 结论	193
9.6 Turbo 码在第三代移动通信中的应用	194
9.6.1 Turbo 码在 cdma2000 中的应用	194
9.6.2 Turbo 码在 WCDMA 系统中的应用	200
9.6.3 卷积 Turbo 码在 WiMAX 系统中的应用	204
9.6.4 协议中 Turbo 码的比较研究	210
9.7 本章总结	213

第 10 章

LDPC 码

10.1 LDPC 码的提出和再发现	215
10.2 Gallager 码编码原理	217
10.3 Gallager 码解码原理	218
10.4 非规则 LDPC 码的编码构造方法	220
10.4.1 监督矩阵的构造方法	222
10.4.2 从监督矩阵到生成矩阵的编码方法	224
10.5 LDPC 码的迭代算法——和积算法	226
10.5.1 初始化	226
10.5.2 迭代过程	227
10.6 LDPC 码的性能分析和数学建模	229
10.6.1 Gallager 码的性能分析	229
10.6.2 Luby 对非规则 LDPC 码的性能分析	231

10.7	LDPC 码的高效解码实现方法	232
10.7.1	基于似然比值的 LDPC 解码实现方法	233
10.7.2	新的差分解码算法及其简化算法的提出	236
10.7.3	仿真测试和对比	238
10.7.4	结论	241
10.8	多进制 LDPC 码	241
10.8.1	多进制 LDPC 码的构造	242
10.8.2	多进制 LDPC 码的解码	243
10.8.3	$GF(q)$ 域上的 LDPC 码的解码性能	246
10.8.4	结论	250
10.9	本章总结	250

第 11 章

统一编解码与密度进化理论

11.1	要素图与和积算法	252
11.1.1	计算单个边缘函数	254
11.1.2	计算所有边缘函数	255
11.2	前/后向算法的要素图解释	258
11.2.1	前/后向算法的要素图表示	258
11.2.2	Turbo 码的迭代解码的要素图表示	260
11.3	LDPC 码和 RA 码的要素图解释	261
11.3.1	LDPC 码	261
11.3.2	RA 码	261
11.3.3	二进制变量和校验式的简化	262
11.4	密度进化的分析方法	264
11.4.1	密度进化模型和高斯近似	265
11.4.2	解码收敛的动态模型	267
11.5	本章总结	271

第 12 章

移动通信系统中的信道编码

12.1	GSM 系统的信道编码	273
------	-------------	-----

12.1.1	GSM 的信道编码方案	273
12.1.2	全速率语音信道(TCH/FS)的信道编码	274
12.2	IS-95 系统中的信道编码	276
12.2.1	检错 CRC	277
12.2.2	前向纠错码(FEC)	277
12.2.3	交织编码	278
12.3	cdma2000 系统的信道编码	282
12.3.1	检错 CRC	282
12.3.2	前向纠错码 FEC	283
12.3.3	交织编码	285
12.4	WCDMA 系统的信道编码	287
12.4.1	信道编码/复用流程	287
12.4.2	WCDMA 系统中的信道检错、纠错编码	289
12.4.3	WCDMA 系统中不同业务数据的编码/复用过程	291
12.5	协议比较	293

第 13 章

无线信道估计与 Turbo 码的补偿解码

13.1	Nakagami 衰落信道下的信噪比(半盲)估值及其在 Turbo 解码中的应用	296
13.1.1	系统模型及 Nakagami 衰落随机变量的两个定理	296
13.1.2	Nakagami 信道下 SNR 估值的新算法	301
13.1.3	Turbo 解码信道补偿估值算法及其对解码精度的灵敏性 仿真对比测试	308
13.1.4	结论	314
13.2	Nakagami 衰落信道下的信道状态(全盲)估值算法及其在 Turbo 解码中的应用	315
13.2.1	研究综述	316
13.2.2	Nakagami 信道下 SNR 估值的新算法及全盲估值算法	318
13.2.3	Turbo 解码信道补偿估值算法及其对解码精度的灵敏性 仿真对比测试	327
13.2.4	结论	329
13.3	本章总结	331

第 14 章

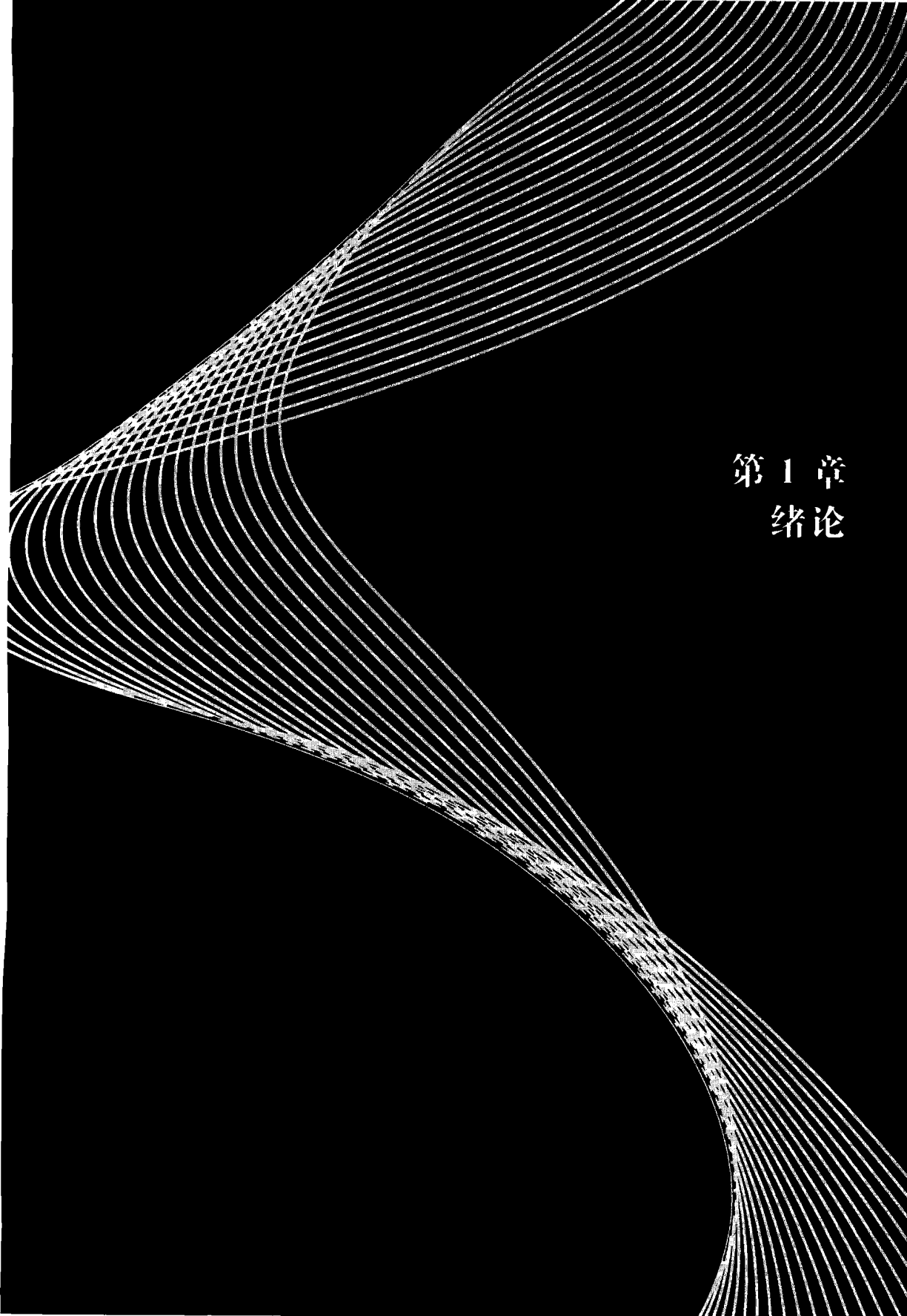
未来移动通信标准中的低密度校验码

14.1	802.16e LDPC 码部分协议介绍	333
14.2	中兴关于 LDPC 码的提案内容介绍	337
14.2.1	LDPC 母码编码器介绍	339
14.2.2	用于低于母码码率的 LDPC 缩短编码方式	340
14.2.3	用于高于母码码率的 LDPC 打孔编码方式	341
14.3	三菱关于 LDPC 码的提案内容介绍	343
14.3.1	三菱 LDPC 码的构造和描述	343
14.3.2	适用于多码率的 RC-LDPC 码	346
14.4	我们提出的一种增强型的 LDPC 码	347
14.5	仿真结果	349
14.5.1	802.16e 仿真结果图	349
14.5.2	中兴仿真结果图	353
14.5.3	3 种方案比较图	355
14.5.4	我们提出的增强型 LDPC 码的仿真性能	357
14.6	结论	364

第 15 章

未来移动通信标准中的调制技术

15.1	简介	366
15.2	OFDM	367
15.3	旋转调制 (Rotation-modulation) 技术	372
15.3.1	普通调制方式	373
15.3.2	旋转调制技术	373
15.3.3	OFDM 调制的旋转调制符号映射与时频二维交织	374
15.3.4	最大似然解调器	375
15.4	LDPC-OFDM 仿真系统	375
15.5	结论	386
	参考文献	387



第 1 章 绪论

1. 1

纠错码理论的历史回顾

通信的主要目的是保障消息传递的可靠性、有效性和安全性。然而，可靠性和有效性往往是相互矛盾的。不失一般性，增加更多发送信息的冗余度可以使通信更可靠，但是浪费了系统带宽，有效性降低了。纠错码理论就是在解决这对矛盾的过程中不断向前发展的。事实上，纠错码的本质是寻找增加冗余度的一种最有效的方法，从而在接收信息受到一定干扰的条件下仍然能够可靠地恢复原始的发送信息。

一个简化的数字通信系统如图 1-1 所示。为了克服传输过程中的各种各样的干扰，往往要人为地加入一些冗余度，使其具有自动检错或纠错能力，这种能力由图中的纠（检）错编码器完成。在此模型中，信源是指经过信源编码器后的二（多）进制信息序列。信道是包括发射机、实际信道（或称传输媒质）和接收机在内的广义信道（又称编码信道），它的输入是二（多）进制数字序列，输出一般也是二（多）进制数字序列。在接收端由纠（检）错解码器最大限度地恢复信源信息（最大似然解码），并传递给信宿做后继处理。

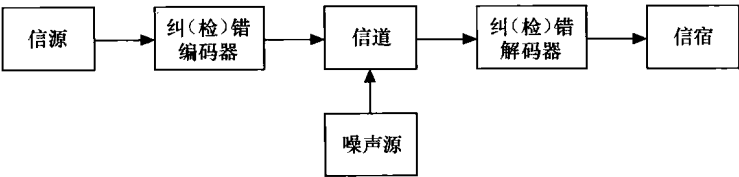


图 1-1 数字通信系统的简化模型

1948 年，香农（Shannon）发表了具有里程碑意义的《The Mathematical Theory of Communications（通信的数学理论）》一文 [144]，提出了信道编码定理和信源编码定理，开创了信息论这门崭新的学科，从而为在通信系统中实现高效可靠的信息传输奠定了理论上的坚实基础。香农信道编码定理表述如下。

每个离散无记忆信道都有一个非负数 C （称为信道容量）与之相联系，并具有如下性质：对于任意给定的 $\epsilon > 0$ 和 $R < C$ ，总存在码率为 R 的码字和解码算法使得解码错误概率小于 ϵ 。大于信道容量的码率不可能实现无差错通信。

可以采用随机分组码证明上述定理，为此需要引入 3 个基本条件：码字长度趋于无穷，随机编码，最大似然解码。香农还给出了在加性高斯白噪声下的信道容量：

$$C = W \log_2 \left[1 + \frac{P_s}{WN_0} \right] \quad (\text{bit})$$