

# 差错控制编码

(原书第2版)

## Error Control Coding

(Second Edition)

(美) Shu Lin Daniel J. Costello, Jr. 著

晏坚 何元智 潘亚汉 等译

## Error Control Coding

Second Edition



Shu Lin · Daniel J. Costello, Jr.

电子与电气工程丛书

# 差错控制编码

(原书第2版)

Error Control Coding

(Second Edition)



(美) Shu Lin Daniel J. Costello, Jr. 著

晏坚 何元智 潘亚汉 等译



机械工业出版社  
China Machine Press

本书系统讲解了差错控制编码系统的基础理论和实际应用, 主要内容包括: 用于可靠数字传输和存储的编码、线性分组码、循环码、二进制 BCH 码、大数逻辑可译码与有限几何码、线性分组码的网格、卷积码、基于网格的软判决译码算法、Turbo 编码、低密度单奇偶校验码、网格编码调制等。本书包含大量实例和习题, 讲解深入浅出, 分析细致透彻, 是差错控制编码领域中的经典教材。

本书适合作为高等院校低年级研究生或高年级本科生编码理论课程的教材或参考书, 也可供相关技术人员参考。

Simplified Chinese edition copyright © 2007 by Pearson Education Asia Limited and China Machine Press.

Original English language title: *Error Control Coding*, Second Edition (ISBN 0-13-042672-5) by Shu Lin, Daniel J. Costello, Copyright © 2004.

All rights reserved.

Published by arrangement with the original publisher, Pearson Education, Inc., publishing as Pearson Education.

本书封面贴有 Pearson Education(培生教育出版集团)激光防伪标签, 无标签者不得销售。

版权所有, 侵权必究。

本书法律顾问 北京市展达律师事务所

**本书版权登记号: 图字: 01-2004-4411**

**图书在版编目(CIP)数据**

差错控制编码(原书第2版)/(美)林舒(Lin, S.), (美)科斯特洛(Costello, D.J.)著; 晏坚等译. -北京: 机械工业出版社, 2007.6

(电子与电气工程丛书)

书名原文: *Error Control Coding Second Edition*

ISBN 978-7-111-20804-4

I. 差… II. ①林… ②科… ③晏… III. 信道编码 - 编码理论 - 高等学校 - 教材  
IV. TN911. 22

中国版本图书馆 CIP 数据核字(2007)第 011787 号

机械工业出版社(北京市西城区百万庄大街 22 号 邮政编码 100037)

责任编辑: 秦燕梅

北京京北制版厂印刷·新华书店北京发行所发行

2007 年 6 月第 1 版第 1 次印刷

184mm × 260mm · 52 印张

定价: 88.00 元

凡购本书, 如有倒页、脱页、缺页, 由本社发行部调换

本社购书热线: (010)68326294

# 译者序

由林舒(Shu Lin)教授和 D. J. 科斯特洛(Costello)教授撰写的《差错控制编码基础和应  
用》一书于1983年出版,作为一本深入浅出的普及型专业教材获得了巨大的成功。该书以通  
俗易懂的方式介绍了纠错码的理论和相关应用,它的中译本由西安电子科技大学的王育民教  
授和王新梅教授翻译,早已为国内读者所熟悉。20年后,林舒教授和科斯特洛教授对全书  
进行了全面的修订和更新,补充了纠错编码领域的大量最新发展内容,于2004年推出了第  
2版。

诚如作者在第2版前言中所述,在过去的20年间,纠错码理论和应用都取得了许多突  
破性的进展,最新的纠错编码技术已经非常逼近香农所指出的理论极限。纠错编码技术的发  
展深刻地影响了实际系统的设计,在高速调制解调、移动通信、卫星及空间通信、数据存储  
等领域得到了广泛的应用,例如低密度单奇偶校验(LDPC)码就已经被欧洲下一代数据广播  
标准 DVB-S2 和 IEEE 的 10G 以太网标准 10GBASE-T 所采用。在第2版中增加了全新的七  
章,分别对软译码、编码调制、Turbo 码和 LDPC 码等内容进行了详尽的阐述,基本覆盖了  
近年来编码研究领域的最新进展,具体的内容安排可参见作者撰写的前言部分。

总体上,第2版保留了第1版的基本特色,在较少的数学背景知识基础上,以通俗易懂  
的方式阐述问题的本质,着重于基本概念的理解和应用。每章末尾的习题和参考材料对读者  
加深概念理解很有帮助,这使得本书非常适合作为编码理论课程的入门教材。同时,书中  
给出的大量应用举例、性能仿真曲线及已知的最优码列表,使得本书也适合于作为从事数字  
系统设计的工作者的一本综合参考书。

由于本书的第2版仍保留了第1版的部分材料,尤其是在基础理论、分组码与卷积码的  
讨论和分析等方面。为保持与第1版的一致,在第2版的翻译过程中大量参考了王育民教授  
和王新梅教授译著的本书第1版中译本,在此特别做以说明并向王育民教授和王新梅教授表  
示谢意。

本书的翻译工作是集体的成果,晏坚、何元智、潘亚汉和陈华完成了主要章节的翻译以  
及全书的修订,此外,参与翻译工作的还有李倩、李斌、姜博、万鹏、郭代和翟立君。在本书  
的翻译过程中,得到了清华大学电子工程系曹志刚教授的悉心指导,在此致以诚挚的  
谢意。

由于本书篇幅较长,时间仓促,加之译者水平有限,错误和不妥之处当属难免,恳请读  
者批评指正。

晏 坚

2007年2月于清华园

# 前 言

本书首先归功于香农在 1948 年所做的“通过有噪传输信道实现可靠通信”的先驱性工作。香农的中心论题是：如果系统的信息传输速率小于信道容量，则通过选择适当的编译码技术就能实现可靠通信。由汉明、格雷等人于 19 世纪 40 年代后期所开创的设计好码和有效译码方法的工作，后来受到了许多研究者的关注。这方面的大多数工作在本质上是高度数学化的，因而对其深入理解需要有丰富的近世代数和概率论的背景知识。这对许多希望将这些技术应用于实际系统的工程师和计算机科学工作者来说无疑是一种障碍。本书的目的之一，就是用最少的数学基础知识，使读者能够理解和运用这些相当复杂的技术。

19 世纪 50 年代和 60 年代的编码研究主要致力于发展有效的编译码器。1970 年，有位作者首次出版了一本名为《纠错码入门》(An Introduction to Error - Correcting Codes)的书，这本书介绍了最初 20 年间分组码和卷积码技术的基础知识，以通俗易懂的方式阐述问题，并不追求数学上的严谨性。本书于 1983 年出版了第 1 版，同样着重于编码理论的基础知识，并增加了对 70 年代所发展的许多编码理论实际应用的介绍。第 1 版的主要内容还包括对分组码检错能力的深入分析，并对卷积码的软译码算法进行了着重讨论。

到了 20 世纪 80 年代和 90 年代，随着一些理论研究的进展及显著的实际应用，编码领域取得了突破性的发展。其中三个方面的发展尤其突出：二进制卷积码和分组码应用于扩展(非二进制)调制符号；可实际应用的分组码软译码算法取得发展；发现了用于分组码和卷积码的软输入、软输出迭代译码算法。这些新的进展革命性地改变了实际系统的编码方式，影响了高速数据调制解调器、数字移动蜂窝电话、卫星及空间通信、高密度数据存储等系统的设计。本版增加了七章新的内容，覆盖了这些专题：两章关于网格编码调制和分组编码调制技术，三章关于分组码的软译码技术，两章关于 Turbo 码和低密度单奇偶校验码及迭代译码。

由于本书的重点是介绍编码的基础理论，而新的技术内容又如此之多，一些特定的专题在本书中无法全部涵盖，例如代数几何码和删除校正码的新发展就没有被涉及。另外，虽然本书中所研究的编码技术可以被应用于数据存储系统，但是并没有直接讨论存储信道的特点。类似地，也未能对衰落信道的编码进行深入的讨论。除了前面提到的新增加的章节外，所有第 1 版的章节在第 2 版中都经过彻底的修订和更新。下文给出各个章节的简要介绍，并突出了区别于第 1 版的改动。

第 1 章对数据通信和存储系统中所采用的差错控制编码进行了综述。简单讨论调制解调的目的是想在一个完整的系统中将编码的作用定位到适当的地位。增加了两节新的内容，用于介绍编码调制、编码增益及香农限的概念。第 2 章从近世代数的观点来介绍一些为理解后面各章节内容所必需的概念，这些都可以被高年级大学生和实践工程师，以及计算机科学工作者所理解。

第 3 章到第 10 章详细介绍了分组码的基本原理。第 3 章介绍线性分组码，还包括对线性码检错能力的分析。第 4 章介绍了几类重要的线性分组码，其中增加了关于里德-穆勒(Reed-Muller)码的新内容。第 5 章介绍循环码的基本结构和性能，以及基于校正子的译码方法。第 6 章详细讨论了一类重要的码——BCH 码，其中包括了 BCH 译码器的软件和硬件实现，以及采用 BCH 码的错误检测。第 7 章包括里德-所罗门(Reed-Solomon)码及其相关的扩充内容，增加了欧氏代数和频域译码的材料。第 8 章详细讨论了大数逻辑可译码，包括重

要的欧氏几何码和射影几何码。第9章和第10章完全是新增加的内容。第9章发展了分组码的网格结构理论,为第14章介绍基于网格的软译码算法打下基础。第10章由 Marc Fossorier 教授执笔,详细讨论了分组码的基于可靠性的软译码算法,并介绍了迭代译码技术。

第11章到第13章介绍卷积码的基础知识。第11章介绍了卷积码,以编码器的状态图作为研究码的结构特性和距离特性的基础,并增加了关于反馈编码器和输入-输出重量枚举函数的新内容。第12章介绍卷积码的最优译码算法,重点介绍用于硬解调判决和软解调判决的(最大似然)维特比译码算法,增加了关于软输出维特比算法、(最大后验概率)BCJR 算法及打孔和咬尾码调整技巧的介绍,另外还包括了基于编码器重量枚举函数的详细性能分析。第13章介绍面向卷积码的次优译码算法,重点介绍序列译码算法——ZJ(堆栈)算法和费诺算法,以及大数逻辑译码算法。我们对序列译码的计算性能这一难题进行了讨论,但是并未做详细的证明。新增的内容包括基于软判决的序列译码算法和大数逻辑译码算法。

在第14章中,将第12章介绍的卷积码的软译码算法推广到分组码。这一章全新的内容大量使用了第9章中介绍的分组码的网格结构。

第15章到第19章则涵盖了自从本书第1版出版后在该研究领域的重要进展。第15章介绍级联编码、多级译码及码分解的重要概念,它们构成了后面四章所介绍的新编码技术的基础。第16章到第19章是全新的内容。第16章介绍并行级联领域,或称 Turbo 编码,及其相关的基于第12章中介绍的 BCJR 算法的迭代译码技术,其中还包括基于均匀交织技术和 EXIT 表概念的性能分析。第17章全面介绍了低密度单奇偶校验码及其代数的、随机的和组合的构造方法,另外还讨论了几种译码算法并给出了对软判决置信度传播译码的完整推导。编码调制问题在第18章和第19章中讨论。第18章介绍网格编码调制的基本原理,其中包括旋转不变码和多维信号集的章节。第19章介绍分组编码调制,其中包括了多级调制和多级解调的重要概念。

本书的结尾处用了三章的篇幅介绍突发错误纠正和自动请求重传 (ARQ) 策略。第20章和第21章介绍了针对突发错误及衰落信道中经常遇到的突发和随机组合错误的纠正方法,其中包括了分组(见第20章)和卷积(见第21章)的纠突发错误码。第23章主要介绍用于双向通信信道的 ARQ 差错控制方法,讨论了纯 ARQ(采用错误检测的重传)和混合 ARQ(联合使用错误检测和错误纠正的重传)。

从内容上看,本书无论是作为教材,还是作为从事差错控制系统设计的工程师和计算机科学工作者的一本综合参考书,都有裨益。书中的三个附录包括了用于构造大多数分组码的代数基础。全书给出了许多不同译码方式下已知的最优分组码和卷积码的列表。这些对于设计者寻求某一特定应用中的最优码是有价值的。在这一版中,对这些表中定义的最优码的生成多项式和奇偶校验多项式采用了统一的八进制表示。书中还包括许多实际系统所采用的码的例子和特定编码系统的计算机仿真性能曲线。在每一章的末尾,作者都设计了一组作业习题。虽然有些问题深一些,但大多数问题是书中所讲内容的相对直接的应用。教师可从出版社获得部分题目的题解。每章的末尾还给出了参考文献。虽然我们不准备编辑完整的编码理论参考书目,但所列的参考目录可提供书中所涉及论题的细节。

本书可作为高年级本科生、研究生第一年或全日制研究生有关编码理论课程的入门教材,也可以作为想了解编码的基础知识及如何设计差错控制系统的工程师和计算机科学工作者的自学指南。

作为编码理论课程的教材,本书可分为两学期讲授。第一学期可包括第1~10章有关分组码的部分,第二学期讲授其余有关卷积码和高级的分组码专题。另一种可行的方案是第一

学期讲授第 1~8 和 11~13 章, 包括分组码和卷积码的基础知识, 第二学期可以针对提高的专题。也可以选择本书中的部分内容在一个学期的课程中完成。分组码的课程可由第 1~7 章和第 8~10、14~15、17、19~20 及 22 章中的选择性专题组成, 而第 1、11~13、16、18 和 21 章的内容可组成完整的卷积码的课程。

这里, 我们要向 Marc Fossorier 教授表示真挚的谢意。他除了完成第 10 章的撰写外, 还花费了大量的时间反复阅读了各个章节的手稿。我们也要感谢许多研究生和博士后助理, 他们提出了许多建议并在本书的准备中提供帮助, 包括进行计算机仿真、绘图、制表并将手稿转为 LaTeX 格式。他们包括: Yu Kou、Cathy Liu、Rose Shao、Diana Stojanovic、Jun Xu、Lei Chen、Oscar Takeshita、Gil Shamir、Adrish Banerjee、Arvind Sridharan、Ching He、Wei Zhang 和 Ali Pusane。特别值得一提的是, Yu Kou、Cathy Liu 和 Adrish Banerjee 对最后的手稿进行了校阅。

我们对国家自然科学基金 (National Science Foundation) 和国家宇航局 (National Aeronautics and Space Administration, NASA) 对我们在编码领域的研究所给予的全力支持表示感谢。没有他们的协助, 我们在编码方面的兴趣绝不可能发展到写这本书的地步。我们还要向在本书写作过程中提供设备和帮助的夏威夷大学玛诺亚分校 (University of Hawaii, Manoa), 加利福尼亚大学戴维斯分校 (University of California, Davis), 圣母大学 (University of Notre Dame) 和德国的洪堡基金会 (Humboldt Foundation) 表示感谢。

最后, 我们要对我们的妻子、孩子和孙子们在本书的写作过程中不断的关怀和支持表示深深的谢意。

林舒 (Shu Lin)

加利福尼亚大学戴维斯分校 (University of California, Davis)

夏威夷大学玛诺亚分校 (University of Hawaii, Manoa)

D. J. 科斯特洛 Jr. (Daniel J. Costello, Jr.)

圣母大学 (University of Notre Dame)

# 目 录

译者序	
前言	
第 1 章 用于可靠数字传输和存储的编码	1
1.1 引言	1
1.2 码的类型	2
1.3 调制和编码	3
1.4 最大似然译码	6
1.5 错误类型	9
1.6 差错控制策略	9
1.7 性能的衡量	10
1.8 编码调制	14
参考文献	15
第 2 章 代数引论	17
2.1 群	17
2.2 域	21
2.3 二元域算术	25
2.4 伽罗华域 $GF(2^m)$ 的构造	28
2.5 伽罗华域 $GF(2^m)$ 的基本性质	31
2.6 伽罗华域 $GF(2^m)$ 算术的计算举例	35
2.7 向量空间	36
2.8 矩阵	40
习题	41
参考文献	43
第 3 章 线性分组码	44
3.1 线性分组码概述	44
3.2 校正子与差错检测	48
3.3 分组码的最小距离	51
3.4 分组码的检错和纠错能力	52
3.5 标准阵与校正子译码	55
3.6 BSC 上线性码的漏检误码率	60
3.7 单奇偶校验码、重复码及自偶码	62
习题	63
参考文献	65
第 4 章 重要的线性分组码	66
4.1 汉明码	66
4.2 一类纠单个差错并检测两个差错的码	68
4.3 里德-穆勒码	70
4.4 里德-穆勒码的其他构造方法	75
4.5 码的平方构造法	79
4.6 (24, 12) 格雷码	84
4.7 乘积码	86
4.8 交织码	87
习题	89
参考文献	89
第 5 章 循环码	91
5.1 循环码的描述	91
5.2 循环码的生成矩阵与校检矩阵	96
5.3 循环码的编码	98
5.4 校正子计算和差错检测	100
5.5 循环码的译码	103
5.6 循环汉明码	108
5.7 捕错译码	111
5.8 改进的捕错译码	116
5.9 (23, 12) 格雷码	117
5.9.1 Kasami 译码器	117
5.9.2 系统搜索译码器	119
5.10 缩短的循环码	120
5.11 循环乘积码	123
5.12 准循环码	123
习题	126
参考文献	128
第 6 章 二进制 BCH 码	130
6.1 二进制本原 BCH 码	130
6.2 BCH 码的译码	137
6.3 求解错误位置多项式 $\sigma(X)$ 的迭代算法	139
6.4 求解错误位置多项式 $\sigma(X)$ 的简化迭代算法	141
6.5 求解错误位置数和纠错	143
6.6 错误和删除的纠正	144
6.7 伽罗华域运算的实现	144



6.8 纠错的实现 .....	149	网格构造 .....	240
6.8.1 校正子的计算 .....	149	9.6 网格的复杂度和对称性 .....	244
6.8.2 求解错误位置多项式 $\sigma(X)$ .....	150	9.7 网格的分段和并行分解 .....	249
6.8.3 错误位置数的计算和纠错 .....	150	9.8 低重量子网格 .....	252
6.9 二进制 BCH 码的重量分布和错误 检测 .....	151	9.9 笛卡尔积 .....	254
6.10 附注 .....	153	习题 .....	258
习题 .....	154	参考文献 .....	259
参考文献 .....	154	第 10 章 基于可靠性的线性分组码软 判决译码算法 .....	262
第 7 章 非二进制 BCH 码、RS 码及其 译码算法 .....	156	10.1 软判决译码 .....	262
7.1 $q$ 进制线性分组码 .....	156	10.2 可靠性量度与基于可靠性的一般 译码方法 .....	265
7.2 $GF(q)$ 上的本原 BCH 码 .....	157	10.3 译码码字的最优性充分条件 .....	267
7.3 里德-所罗门(RS)码 .....	158	10.4 广义最小距离译码算法与 Chase 译码算法 .....	270
7.4 非二进制 BCH 码和 RS 码的译码: Berlekamp 算法 .....	161	10.4.1 GMD 译码算法 .....	270
7.5 欧几里德译码算法 .....	166	10.4.2 Chase 译码算法 .....	271
7.6 频域译码 .....	169	10.4.3 Chase 和 GMD 译码算法 的推广 .....	271
7.7 错误和删除的纠正 .....	174	10.5 加权删除译码 .....	273
习题 .....	178	10.6 一种基于迭代处理最不可靠位的 最大似然译码算法 .....	276
参考文献 .....	179	10.7 缩减列表校正子译码算法 .....	278
第 8 章 大数逻辑可译码与有限 几何码 .....	180	10.8 最可靠独立位置重复处理译码 算法 .....	280
8.1 一步大数逻辑译码 .....	180	10.8.1 最可靠和最不可靠基 .....	280
8.2 一类一步大数逻辑可译码 .....	187	10.8.2 基于优先级的搜索译码算法 .....	281
8.3 其他的一步大数逻辑译码 .....	192	10.8.3 分级统计译码算法 .....	286
8.3.1 极长码 .....	192	10.8.4 基于校正子的分级统计 译码算法 .....	290
8.3.2 差集码 .....	194	10.9 加权大数逻辑译码 .....	290
8.4 多步大数逻辑译码 .....	196	10.9.1 二进制对称信道(BSC)上 RM 码 的大数逻辑译码 .....	291
8.5 欧氏几何 .....	202	10.9.2 基于可靠性信息的大数 逻辑译码 .....	291
8.6 欧氏几何码 .....	205	10.10 一步大数逻辑可译码的基于可靠性 的迭代译码 .....	293
8.7 二重 EG 码 .....	212	10.10.1 基于 MAP 的迭代译码 .....	293
8.8 射影几何与射影几何码 .....	216	10.10.2 基于置信度传播的迭代译码 .....	294
8.9 附注 .....	221	习题 .....	296
习题 .....	221	参考文献 .....	297
参考文献 .....	223	第 11 章 卷积码 .....	300
第 9 章 线性分组码的网格 .....	225	11.1 卷积码的编码 .....	300
9.1 码的有限状态机模型和网格表示 .....	225		
9.2 二进制线性分组码的比特级网格 .....	227		
9.3 标记状态 .....	234		
9.4 比特级网格的结构性质 .....	237		
9.5 基于奇偶校验矩阵的状态标记和 网格构造 .....	240		

11.2	卷积码的结构特点	322	14.4.1	基于比特级网格图的 MAP 译码算法	468
11.3	卷积码的距离特性	334	14.4.2	双向和并行 MAP 译码	471
	习题	337	14.4.3	计算复杂度	472
	参考文献	339	14.5	基于分段网格的 MAP 译码	473
第 12 章	卷积码的最优译码	341	14.5.1	算法	473
12.1	维特比算法	341	14.5.2	计算复杂度和存储要求	475
12.2	卷积码的性能界	347	14.6	Max-Log-MAP 译码算法	478
12.3	构造好的卷积码	355	14.6.1	基于比特级网格的 Max-log-MAP 译码	478
12.4	维特比算法的实现和性能	359	14.6.2	基于分段网格的 Max-log-MAP 译码	480
12.5	软输出维特比算法(SOVA)	368	14.6.3	log-MAP 算法	483
12.6	BCJR 算法	372		习题	484
12.7	打孔卷积码和咬尾卷积码	384		参考文献	485
	习题	394	第 15 章	级联编码、码分解与多阶段译码	488
	参考文献	396	15.1	单级级联码	488
第 13 章	卷积码的次优译码	399	15.2	多级级联码	491
13.1	ZJ(堆栈)序列译码算法	399	15.3	多阶段软判决译码	494
13.2	Fano 序列译码算法	409	15.4	码的分解	495
13.3	序列译码的性能特点	412	15.5	迭代多阶段 MLD 算法	497
13.4	用于序列译码的码的构造	420	15.6	以卷积码作为内码的级联编码方案	501
13.5	大数逻辑译码	423	15.7	二进制码级联	502
13.6	大数逻辑译码的性能特点	440		习题	503
13.7	大数逻辑可译码的构造	445		参考文献	504
13.7.1	自正交码	445	第 16 章	Turbo 编码	505
13.7.2	可正交码	449	16.1	Turbo 编码简介	506
	习题	450	16.2	Turbo 码的距离特性	515
	参考文献	452	16.3	Turbo 码性能分析	531
第 14 章	基于网格的软判决译码算法	455	16.4	Turbo 码的设计	535
14.1	维特比译码算法	455	16.5	Turbo 码的迭代译码	543
14.2	递归最大似然译码算法	457		习题	557
14.2.1	网格分段的量度表	458		参考文献	558
14.2.2	一个 RMLD 算法	462	第 17 章	低密度单奇偶校验码	561
14.2.3	最优网格分段	463	17.1	LDPC 码简介	561
14.3	基于低重量子网格的次优迭代译码算法	464	17.2	线性分组码的泰纳图	564
14.3.1	生成候选码字	464	17.3	LDPC 码的几何构造法	566
14.3.2	最优性测试和搜索区域	464	17.4	EG-LDPC 码	567
14.3.3	基于最小重量网格搜索的迭代译码算法	465	17.5	PG-LDPC 码	571
14.3.4	计算复杂度	466	17.6	LDPC 码的译码	574
14.3.5	算法的改进	467			
14.4	MAP 译码算法	468			

17.6.1 大数逻辑译码 .....	575	19.4.1 单级级联编码调制系统 .....	715
17.6.2 比特翻转译码算法 .....	575	19.4.2 多级级联编码调制系统 .....	716
17.6.3 加权大数逻辑译码与加权 比特翻转译码 .....	576	19.5 乘积编码调制 .....	719
17.6.4 和积算法 .....	577	19.6 非对称错误保护的多级编码调制 .....	720
17.6.5 有限几何 LDPC 码的 性能 .....	580	习题 .....	727
17.7 基于行分裂与列分裂的码构造 方法 .....	583	参考文献 .....	727
17.8 拆散泰纳图中的环 .....	588	第 20 章 纠突发错误码 .....	730
17.9 缩短的有限几何 LDPC 码 .....	592	20.1 引言 .....	730
17.10 Gallager LDPC 码的构造方法 .....	594	20.2 纠单个突发错误循环码的译码 .....	731
17.11 掩码 EC-Gallager LDPC 码 .....	597	20.3 纠单个突发错误码 .....	732
17.12 使用循环分解构造的准循环码 .....	601	20.3.1 Fire 码 .....	732
17.13 基于 $GF(p')$ 域上有限几何的 LDPC 码构造 .....	604	20.3.2 短有效纠突发错误码 .....	736
17.14 随机 LDPC 码 .....	607	20.3.3 采用交织方法构造的纠突发 错误码 .....	737
17.15 非规则 LDPC 码 .....	608	20.3.4 采用乘积方法构造的纠突发 错误码 .....	738
17.16 图论 LDPC 码 .....	612	20.4 纠定段突发错误码 .....	738
17.17 基于均衡不完全区组设计构造 LDPC 码 .....	616	20.5 纠突发和随机错误码 .....	739
17.18 基于具有 2 个信息符号的缩短 RS 码构造 LDPC 码 .....	619	20.5.1 由 RS 码导出的码 .....	740
17.19 LDPC 码与 Turbo 码的级联 .....	623	20.5.2 级联码 .....	741
习题 .....	624	20.5.3 能同时纠正突发和随机错误 的修正 Fire 码 .....	741
参考文献 .....	625	习题 .....	742
第 18 章 网格编码调制 .....	629	参考文献 .....	743
18.1 网格编码调制简介 .....	630	第 21 章 纠突发错误卷积码 .....	745
18.2 TCM 码的构造 .....	646	21.1 突发错误纠错能力的界 .....	745
18.3 TCM 性能分析 .....	654	21.2 纠突发错误卷积码 .....	746
18.4 旋转不变 TCM .....	658	21.2.1 Berlekamp-Preparata 码 .....	746
18.5 多维 TCM .....	669	21.2.2 Iwadare-Massey 码 .....	750
习题 .....	698	21.3 交织卷积码 .....	753
参考文献 .....	700	21.4 同时纠突发和随机错误的卷积码 .....	755
第 19 章 分组编码调制 .....	703	21.4.1 扩散码 .....	755
19.1 距离概念 .....	703	21.4.2 突发发现码 .....	758
19.2 多级分组调制码 .....	704	21.4.3 突发捕获码 .....	760
19.3 多级 BCM 码的多阶段译码 .....	711	习题 .....	763
19.3.1 第一阶段译码 .....	711	参考文献 .....	764
19.3.2 第二阶段译码 .....	711	第 22 章 自动请求重传 (ARQ) 策略 .....	765
19.3.3 第三阶段译码 .....	711	22.1 基本 ARQ 方法 .....	765
19.4 级联编码调制 .....	715	22.2 采用有限容量接收缓存器的选择 重传 ARQ .....	769
		22.2.1 传输和重传过程 .....	770

22.2.2 接收端的运行和错误恢复过程 .....	771	22.6.5 可靠性 .....	787
22.2.3 常态运行 .....	771	22.7 采用卷积码的混合 ARQ 系统 .....	787
22.2.4 阻塞态运行 .....	772	22.8 一个级联编码调制混合 ARQ 系统 ...	788
22.2.5 吞吐效率 .....	774	22.8.1 系统中所采用的码 .....	788
22.3 混合模式重传 ARQ .....	775	22.8.2 级联编码调制 FEC 子系统及重传 .....	789
22.4 混合 ARQ 方法 .....	776	22.8.3 一个特定系统 .....	791
22.5 一类半速率可逆码 .....	779	习题 .....	792
22.6 采用有限容量接收缓存器的 II 型混合选择重传 ARQ .....	781	参考文献 .....	792
22.6.1 发送和重传过程 .....	781	附录 A 伽罗华域的表 .....	796
22.6.2 常态下接收端的运行 .....	782	附录 B $GF(2^m)$ 中元素的最小多项式 ...	807
22.6.3 阻塞态下接收端的运行 .....	783	附录 C 长度至 $2^{10} - 1$ 的二进制本原 BCH 码的生成多项式 .....	810
22.6.4 吞吐效率 .....	784		

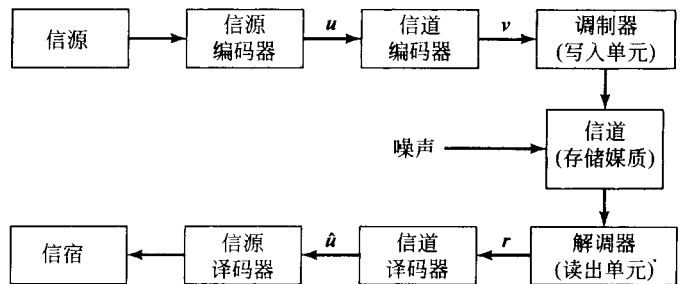
# 第1章 用于可靠数字传输和存储的编码

## 1.1 引言

近年来，对高效可靠的数字传输和存储系统的需求日益增长。这种需求随着在商业、政府和军事领域面向数字信息的交换、处理和存储的大规模高速数据网的出现而变得更加迫切。这类系统的设计要求通信与计算机技术的融合，系统设计者所关心的一个主要问题就是如何控制差错以使得数据能够可靠重现。

1948年，香农在一篇具有里程碑意义的论文<sup>[1]</sup>中曾经证明，只要信息传输速率低于信道容量，通过对信息适当进行编码，可以在不牺牲信息传输或存储速率的情况下，将有噪声信道或存储媒质引入的差错减到任意低的程度。自从香农的著作发表以来，人们为了在噪声环境下控制差错而在设计有效的编译码方法方面做出了大量的努力。近年来的发展趋势是实现目前高速数字系统所要求的可靠性，并且差错控制编码的应用已经成为现代通信系统和数字存储系统设计中不可分割的一部分。

数字信息的传输与存储有很多共同之处。两个过程都是要把数据从信源传送到信宿（或者用户）。一个典型的传输（或存储）系统可以用图1-1所示的框图来表示，信源（information source）可能是一个人或是一台机器（例如一台计算机或者数据终端）。被传送到目的地的信源输出可以是连续波形，也可以是离散的符号序列。信源编码器（source encoder）将信源的输出转换为二进制数字（比特）序列，这些序列称为信息序列（information sequence） $u$ 。对于连续信源，该过程还包括模拟/数字（A/D）转换。信源编码器被理想化地设计成：（1）为表示信源输出所要求的比特率最低；（2）信源的输出可以从信息序列 $u$ 确切地重现。信源编码不在本书的讨论范围内，对于这个重要论题的详细介绍，请参考文献[2]，[3]，[4]和[5]。



信源编码器（source encoder）将信源的输出转换为二进制数字（比特）序列，这些序列称为信息序列（information sequence） $u$ 。对于连续信源，该过程还包括模拟/数字（A/D）转换。信源编码器被理想化地设计成：（1）为表示信源输出所要求的比特率最低；（2）信源的输出可以从信息序列 $u$ 确切地重现。信源编码不在本书的讨论范围内，对于这个重要论题的详细介绍，请参考文献[2]，[3]，[4]和[5]。

信道编码器（channel encoder）将信息序列 $u$ 变换成离散的编码序列（encoded sequence） $v$ ，称之为码字（codeword）。尽管在某些应用中采用非二进制码，但在大多数情况下 $v$ 是二进制序列。本书的主要内容之一，就是设计和实现信道编码器，以抵抗传输或存储码字所面临的噪声环境的影响。

离散符号并不适合在物理信道上传输，也不适合记录到数字存储媒质上。调制器（modulator）或写入单元（writing unit）将信道编码器输出的每个符号转换为持续时间为 $T$ 秒的适合传输（或记录）的波形。这些波形进入信道（channel）或存储媒质（storage medium）并受到噪声的干扰。典型的传输信道包括电话线、移动蜂窝电话、高频无线电、遥测、微波和卫星链路、光缆等。典型的存储媒质包括磁芯和半导体存储器、磁带、磁鼓和磁碟、光盘、光存

储单元等。这些例子中的每种都受到不同类型的噪声干扰。在电话线路上, 干扰可能来自于开关脉冲噪声、热噪声或者来自其他线路的串音。对于磁碟(或光盘), 表面的缺陷和灰尘微粒都能被看做是噪声干扰。解调器(demodulator)或读出单元(reading unit)处理收到的每一个持续时间为  $T$  秒的波形, 然后产生离散(量化)或者连续(非量化)的输出。相对于编码序列  $v$ , 解调器的输出序列称之为接收序列(received sequence)  $r$ 。

信道译码器(channel decoder)将接收序列  $r$  变换为二进制序列  $\hat{u}$ , 称为估计信息序列(estimated information sequence)。译码策略基于信道编码规则和信道(或存储媒质)的噪声特性而定。尽管噪声可能导致某些译码错误(decoding errors), 但在理想情况下,  $\hat{u}$  将是信息序列  $u$  的重现。本书的另一个主要内容就是设计和实现使译码误码率最小的信道译码器。

信源译码器(source decoder)将估计信息序列  $\hat{u}$  变换为对信源输出的估计(estimate), 并将该估计传送到信宿(destination)。当信源是连续信源时, 这一过程还包括数字/模拟(D/A)转换。在一个精心设计的系统中, 除非信道(或存储媒质)干扰太严重, 否则这个估计将会是对信源输出的准确重现。

为把注意力集中于信道编码器和信道译码器, 可以: 1) 将信源和信源编码器合并成一个输出为  $u$  的数字信源(digital source); 2) 将调制器(或写入单元)、信道(或存储媒质)及解调器(或读出单元)合并成一个输入为  $v$ 、输出为  $r$  的编码信道(coding channel); 3) 将信源译码器和信宿合并成一个输入为  $\hat{u}$  的数字信宿(digital sink)。经过合并后的简化框图如图 1-2 所示。

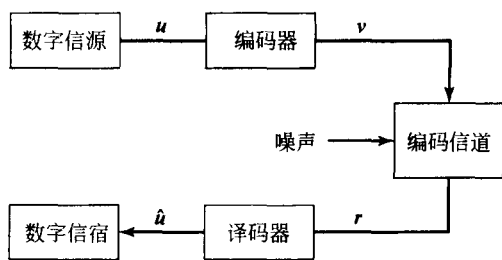


图 1-2 编码系统的简化模型

本书讨论的主要工程问题是设计和实现成对的信道编码器/译码器, 使得: 1) 信息可以在有噪环境下尽可能快(或尽可能高密度)地传输(或记录); 2) 信息在信道译码器的输出端能够可靠地重现; 3) 将实现编码器和译码器的代价降低到可接受的范围内。

## 1.2 码的类型

当前通用的码有两种不同的类型: 分组码(block codes)和卷积码(convolution codes)。分组码编码器把信息序列划分成每组含  $k$  个信息比特(符号)的消息分组。一个消息分组可用二进制  $k$  维向量  $u = (u_0, u_1, u_2, \dots, u_{k-1})$  表示, 称为一个消息(message)。在分组编码中, 符号  $u$  用来表示  $k$  比特消息而不是整个信息序列。总共有  $2^k$  个可能的不同消息。编码器把每个消息  $u$  独立地变换成  $n$  维离散符号向量  $v = (v_0, v_1, v_2, \dots, v_{n-1})$  (分组码中, 符号  $v$  用来表示一个  $n$  符号组而不是整个编码序列), 称之为码字(codeword)。因此, 对应于  $2^k$  个可能的不同消息, 编码器的输出端有  $2^k$  个可能的不同码字。这  $2^k$  个长度为  $n$  的码字的集合称为  $(n, k)$  分组码(block code)。比值  $R = k/n$  称为码率(code rate), 可解释成每个传送符号所含有的进入编码器的信息比特数。由于  $n$  符号输出码字只取决于对应的  $k$  比特输入消息, 即每个消息是独立编码的, 从而编码器是无记忆的, 且可用组合逻辑电路来实现。

对二进制码, 每个码字  $v$  也是二进制的。因此, 为使二进制码可用, 即对每个消息都能够分配不同的码字, 应有  $k \leq n$  或  $R \leq 1$ 。当  $k < n$  时, 可对每个消息附加  $n - k$  个冗余比特来构成码字。这些冗余比特将使码具有抵抗信道噪声的能力。对于固定码率  $R$ , 在保持比值  $k/n$  不变的条件下, 可通过增加分组码长度  $n$  和信息比特数  $k$  来添加更多的冗余比特。如何选择这些冗余比特, 以实现在有噪信道上的可靠信息传输是设计编码器的一个主要问题。

表 1-1 给出了一个  $k=4, n=7$  的二进制分组码的例子。第 3 章到第 10 章, 及第 14、15、17、19 和 20 章主要研究在有噪环境下用于控制差错的分组码的分析、设计和译码。

表 1-1  $k=4, n=7$  的二进制分组码

消 息	码 字	消 息	码 字
(0000)	(0000000)	(0001)	1010001
(1000)	(1101000)	(1001)	0111001
(0100)	(0110100)	(0101)	1100101
(1100)	(1011100)	(1101)	0001101
(0010)	(1110010)	(0011)	0100011
(1010)	(0011010)	(1011)	1001011
(0110)	(1000110)	(0111)	0010111
(1110)	(0101110)	(1111)	1111111

卷积码编码器同样接受  $k$  比特分组的信息序列  $u$ , 并产生  $n$  符号组的编码序列(码序列) $v$ (卷积码编码中, 符号  $u$  和  $v$  用来表示分组的序列而非单个分组)。但是, 每一个编码分组不仅取决于当前单位时间对应的  $k$  比特消息组, 而且与前  $m$  个消息组有关。此时, 编码器的存储级数(memory order)为  $m$ 。编码器所产生的所有可能的输出编码序列的集合构成了一个码。比值  $R = k/n$  称为码率(code rate)。由于编码器有存储单元, 因而必须采用时序逻辑电路实现。

对二进制卷积码, 当  $k < n$  或  $R < 1$  时, 在信息序列中加入用于抵抗信道干扰的冗余比特。通常  $k$  和  $n$  都是较小的整数, 当固定  $k$  和  $n$  从而码率  $R$  也被固定时, 增大码的存储级数  $m$  可以增大冗余度。在有噪信道上如何利用存储器来实现可靠传输是设计卷积码编码器的主要问题。图 1-3 给出了一个  $k=1, n=2$  和  $m=2$  的二进制前馈卷积码编码器的例子。为说明码字是如何产生的, 考虑信息序列  $u = (1101000\dots)$ , 最左边的二进制位将首先进入编码器。使用模二和(异或加)准则, 并假定多路选择器以上一行的输出作为第一个编码比特, 容易看出编码序列为:  $v = (11, 10, 10, 00, 01, 11, 00, 00, \dots)$ 。第 11~13 章, 第 16、18 和 21 章着重于介绍在噪声环境下控制差错的卷积码的分析、设计和译码。

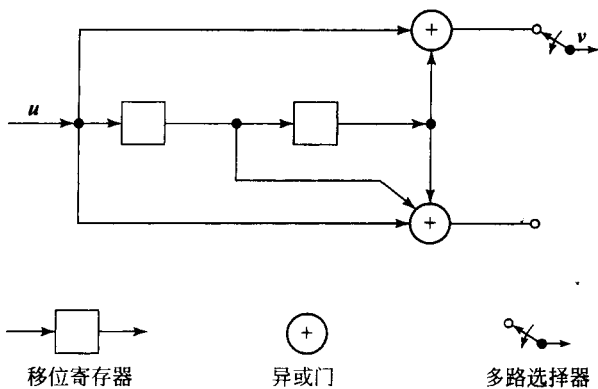


图 1-3  $k=1, n=2$  和  $m=2$  的二进制前馈卷积编码器

### 1.3 调制和编码

在通信系统中, 对编码器的每个输出符号, 调制器必须选定一个适于传输的、持续时间为  $T$  秒的波形。在二进制码的情况下, 调制器必须产生两个信号中的一个: 对应于编码信号“1”的  $s_1(t)$  或对应于编码信号“0”的  $s_2(t)$ 。对于宽带信道, 信号的最优选择是

$$\begin{aligned}
 s_1(t) &= \sqrt{\frac{2E_s}{T}} \cos 2\pi f_0 t, \quad 0 \leq t \leq T \\
 s_2(t) &= \sqrt{\frac{2E_s}{T}} \cos(2\pi f_0 t + \pi) = -\sqrt{\frac{2E_s}{T}} \cos 2\pi f_0 t, \quad 0 \leq t \leq T
 \end{aligned}
 \tag{1-1}$$

其中载波信号频率  $f_0$  是  $1/T$  的整数倍,  $E_s$  是每个信号的能量。由于载波  $\cos 2\pi f_0 t$  的相位随着编码器输出的变化而取  $0$  或  $\pi$ , 这种调制被称为二进制相移键控 (binary-phase-shift-keying, BPSK)。图 1-4 给出了对应于表 1-1 中码字  $\nu = (1101000)$  的 BPSK 调制波形。

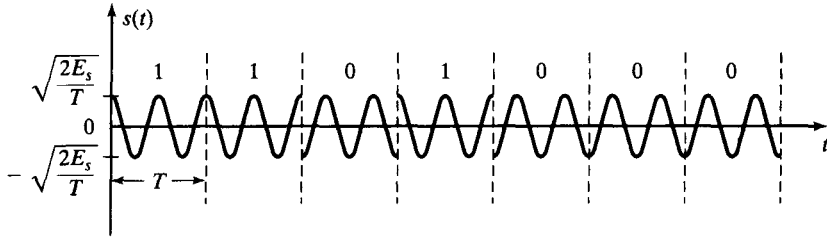


图 1-4 对应于码字  $\nu = (1101000)$  的 BPSK 调制波形

一种广泛存在于各种通信系统中的噪声干扰是加性白色高斯噪声 (additive white Gaussian noise, AWGN)<sup>[2][6][7]</sup>。若传输的信号为  $s(t)$  ( $=s_1(t)$  或  $s_2(t)$ ), 则接收信号为

$$r(t) = s(t) + n(t) \quad (1-2)$$

式中  $n(t)$  是一个高斯随机过程, 其单边功率谱密度 (power spectral density, PSD) 为  $N_0$ 。在许多系统中还存在其他形式的噪声<sup>[7]</sup>。例如, 在一个存在多径传输影响的通信系统中, 可在特定的时间间隔上观测到接收信号的衰落现象 (强度减弱)。可以用信号  $s(t)$  乘以噪声比例因子来建立这种衰落的模型。

在每个  $T$  秒的间隔上, 解调器须产生一个相应于接收信号的输出。该输出可以是一个实数, 或者是预先选定的离散符号集中的一个元素, 这取决于解调器的设计。最优解调器通常包含一个匹配滤波器或者相干检测器, 后面再有一个采样开关, 每隔  $T$  秒对输出进行采样。对于带相干检测的 BPSK 调制, 其采样输出是一个实数:

$$y = \int_0^T r(t) \sqrt{\frac{2E_s}{T}} \cos 2\pi f_0 t dt \quad (1-3)$$

未经量化的解调器输出序列可以直接送到信道译码器进行处理。在这种情况下, 信道译码器必须能够处理未经量化的输入, 也即必须能够处理实数。更为常用的一种译码方法是将实数检测器的输出  $y$  量化为有限的  $Q$  个离散输出符号中的一个。在这种情况下, 信道译码器为离散输入, 即必须能够处理离散值。大多数编码通信系统采用某种形式的离散处理。

为了用  $M = 2^l$  个信道信号来传输信息, 首先将二进制编码器的输出序列以  $l$  比特为一个字节进行分段。每个字节被称为一个符号, 因此存在  $M$  种不同的符号。接下来, 每种符号被映射为传输信号集  $S$  的  $M$  种信号中的一种。每种信号都是周期为  $T$  的脉冲波形, 这样就构成了  $M$  进制调制。 $M$  进制调制的一个例子就是  $M$  进制相移键控 ( $M$ -ary phase-shift-keying, MPSK), 其信号集由  $M$  个正弦信号组成。这些信号具有相同的能量  $E_s$  和  $M$  种等间隔的不同相位。这样的一个信号集可以由下式给出:

$$s_i(t) = \sqrt{\frac{2E_s}{T}} \cos(2\pi f_0 t + \phi_i), \quad 0 \leq t \leq T$$

式中  $\phi_i = 2\pi(i-1)/M$ ,  $1 \leq i \leq M$ 。由于这些信号具有恒定的包络, 因此 MPSK 也被称为恒包络调制 (constant-envelope modulation)。当  $M=2$ ,  $M=4$  和  $M=8$  时, 分别称为 BPSK, 4-PSK (也称为 QPSK) 和 8-PSK。这些是数字通信中经常使用的调制类型, 图 1-5 给出了它们的信号星座图。其他类型的  $M$  进制调制将在第 18 章和第 19 章中讨论。

如果在给定时间间隔内检测器的输出仅和该间隔内传输的信号有关, 而与任何以前传输



的信号无关，则称此信道是无记忆 (memoryless) 的。在这种情况下， $M$  进制输入的调制器、物理信道和  $Q$  进制输出的解调器组合在一起，可以用一个离散无记忆信道 (discrete memoryless channel, DMC) 来建模。离散无记忆信道可用一组转移概率 (transition probabilities)  $P(j|i)$  ( $0 \leq i \leq M-1, 0 \leq j \leq Q-1$ ) 来完全描述，其中  $i$  代表调制器输入的符号， $j$  代表解调器输出的符号，而  $P(j|i)$  是发送为  $i$ ，接收为  $j$  的概率。例如，考虑这样一个通信系统：1) 采用二进制调制 ( $M=2$ )；2) 噪声的幅度分布是对称的；3) 解调器的输出量化为  $Q=2$  个电平。在这种情况下可以得到一个特别简单而实际上极为重要的信道模型，称为二进制对称信道 (binary symmetric channel, BSC)。图 1-6(a) 给出了二进制对称信道的转移概率图。请注意转移概率  $p$  完全描述了这个信道。

转移概率  $p$  可以由所采用的信号、噪声的概率分布、解调器输出的量化阈值等已知信息来计算。当 BPSK 调制用于 AWGN 信道，采用最优相干检测和二进制输出量化时，二进制对称信道的转移概率就是在等概率输入信号条件下的非编码 BPSK 的误比特率，由

$$p = Q(\sqrt{2E_b/N_0}) \quad (1-4)$$

给出，其中  $Q(x) \triangleq \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-y^2/2} dy$  是高斯统计的互补误差函数 (complementary error function)，或简称  $Q$  函数。 $Q(x)$  的一个上界为

$$Q(x) \leq \frac{1}{2} e^{-x^2/2}, \quad x \geq 0 \quad (1-5)$$

它在后面计算二进制对称信道的误码性能时将会用到。

当采用二进制编码时，调制器仅有二进制 ( $M=2$ ) 输入。类似地，当解调器的输出采用二进制量化 ( $Q=2$ ) 时，译码器也只有二进制输入。在这种情况下，我们称解调器采用硬判决 (hard decision)。由于实现较为简单，无论是分组码还是卷积码的许多编码数字通信系统都采用具有硬判决译码 (hard-decision coding) 的二进制编码。但是，当  $Q > 2$  (或输出未经量化) 时，我们称解调器采用的是软判决 (soft decision)。在这种情况下，译码器必须接受多电平 (或连续

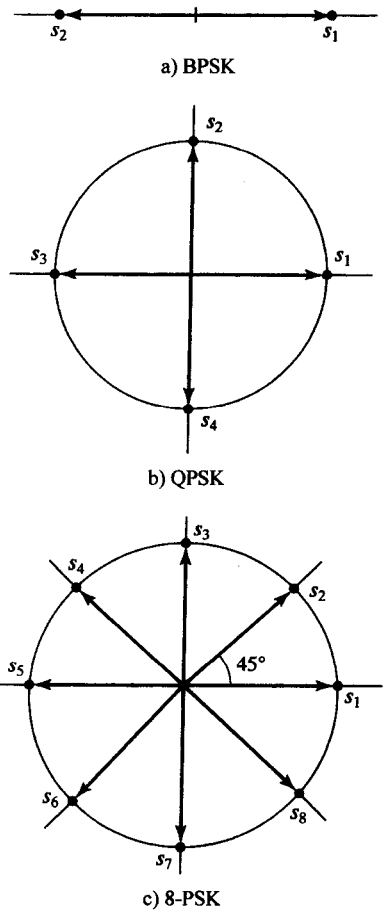


图 1-5 BPSK, QPSK 和 8-PSK 的信号星座图

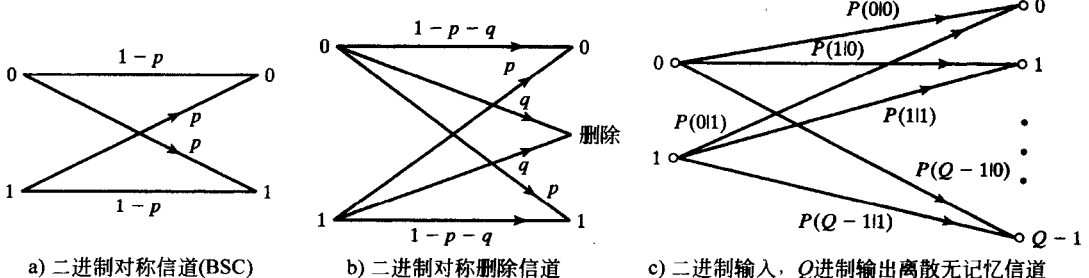


图 1-6 转移概率图