信息与通信工程研究生规划教材

现代编码理论

Modern Coding Theory

赵晓群　编著

華中科技大學出版社
http://www.hustp.com

作者所在院校












信息与通信工程研究生规划教材

策划编辑 王新华 刘锦东 责任编辑 江 津

◇现代数字信号处理
◇数字图像处理与分析
◇信号估计与检测
◆现代编码理论
◇网络信息安全理论与技术
◇密码学与通信安全基础
◇光通信理论与技术
◇量子光通信
◇网络视频通信
◇专用集成电路设计
◇ULSI阵列处理

上架建议：电信类

ISBN 978-7-5609-4457-9

定价：34.80 元

信息与通信工程研究生规划教材

现代编码理论

Modern Coding Theory

赵晓群 编 著

华中科技大学出版社
中国·武汉

图书在版编目(CIP)数据

现代编码理论/赵晓群　编著. —武汉:华中科技大学出版社,2008 年 8 月
ISBN 978-7-5609-4457-9

Ⅰ.现…　Ⅱ.赵…　Ⅲ.编码理论-研究生-教材　Ⅳ.O157.4

中国版本图书馆 CIP 数据核字(2008)第 041146 号

现代编码理论　　赵晓群　编著

责任编辑:江　津　　封面设计:潘　群
责任校对:汪世红　　责任监印:周治超

出版发行:华中科技大学出版社(中国·武汉)
武昌喻家山　　邮编:430074　　电话:(027)87557437

录　　排:华中科技大学惠友文印中心
印　　刷:华中科技大学印刷厂

开本:850mm×1065mm　1/16　　印张:19.75　　字数:427 000
版次:2008 年 8 月第 1 版　　印次:2008 年 8 月第 1 次印刷　　定价:34.80 元
ISBN 978-7-5609-4457-9/O·434

信息与通信工程研究生规划教材
编　委　会

内 容 提 要

本书全面、系统地阐述了编码理论的原理、技术和应用。本书是在汲取了国内外相关教材、专著的优点，结合信道编码的基本理论与工程应用以及作者的教学经验和科研成果的基础上编写的。全书内容深入浅出，既保持理论的完整性、系统性，又概念清楚、易读好懂，同时注重编码理论与应用的新发展。

全书共分 9 章，详细介绍了信道与编码的基本原理，初等数论和近世代数中与信道编码相关的主要内容，经典的线性分组码、循环码、BCH 码、卷积码的结构和特性，以及 Turbo 码、LDPC 码、网格编码调制等现代编码理论的重要内容。

本书适合作为高等院校信息与通信工程专业的研究生和高年级本科生教材，对于从事信息科学和技术领域工作和研究的人员也极具参考价值。

Abstract

This book gives a comprehensive and systemic elaboration on the principles, technologies and applications of coding theory. Absorbing the merits of the relevant teaching materials and monographs at home and abroad, this book is based on the combination of fundamental theory and practical application of channel coding and the author's experience in teaching. This book is a useful simplification of the profound theory, which not only keeps the integrality and systematicness of the theory, but also has a clear concept and good readability. Meanwhile it also emphasizes the new development of coding theory and application.

This book has nine chapters. It introduces the fundamental principles of channel and encoding, primary coverage related to channel coding in elementary number theory and modern algebra and structures and features of classical linear block codes, cyclic codes, BCH codes, convolutional codes, Turbo codes, LDPC codes and Trellis-Coded Modulation (TCM), which are all of great significance in modern coding theory.

This book is suited to be a teaching material for graduate and advanced undergraduate students of information and communication engineering in a college or university and it's also of great value to researchers engaged in science and technology of information and communication.

总　序

随着信息时代的到来，人类已经生活在信息的“海洋”之中，信息和通信已渗入我们生活的各个方面。近年来，我国的电信产业以10%以上的年增长率迅猛发展，“中国制造”的通信产品广泛进入了全球市场。另一方面，信息和通信领域的理论与技术获得了迅速发展，不少技术难题已取得实质性突破，技术进步和产业发展相互推动、相互促进。

产业的发展带来了对人才，特别是高层次专业人才的巨大需求。信息与通信工程是我国工科门类中应用前景广阔、招生量比较大的学科，对我国的现代化建设起着非常重要的作用。其中的通信与信息系统更是近几年硕士研究生报考的热门专业之一。随着硕士研究生的不断扩招，研究生教育成为一个突出的问题。鉴于通信学科的迅猛发展，广大科技工作者和硕士、博士研究生迫切需要学习与掌握信息和通信的现代理论与技术。目前本专业的研究生教材已有一些，其中亦不乏典范之作，但专门针对研究生读者成系列出版的尚为少见。其中的一个原因是各校研究生课程设置自成体系，各校之间不尽相同，这为研究生教材的建设和推广造成了困难。

有鉴于此，来自清华大学等十多所高校、科研单位的教授和专家相约聚首，对通信专业研究生课程体系设置进行探讨，尝试从各校现有的课程体系中提取共同性的知识结构框架，并结合他们多年的教学实践积累，编写一套针对通信专业研究生，兼顾高年级本科生的系列教材，为研究生教育做一点工作。

本系列研究生教材针对性强，知识覆盖较为全面，相信该系列教材的出版将会为读者系统掌握通信科学、信息科学的基础理论与技巧，以及本领域的先进技术方法和现代技术手段提供相对便捷的途径，对培养具有从事通信科学、信息科学以及相关领域的科研与开发和教学工作能力的人才提供有力的手段，对本专业研究生教学起到积极的推动作用。

本系列教材的作者均来自信息和通信学科实力较强的院校，不仅有较为丰富的教学经验，而且在研究方向和地域分布上具有一定的代表性。我有感于他们对教育事业的热忱、对教书育人的执著，遂为之序。

中国工程院院士　李乐民

2007年8月

前　言

1948年，信息论和编码理论的奠基人 C. E. Shannon 在他的不朽名著《A Mathematical Theory of Communication》中，首次阐明了在有扰信道中实现可靠通信的方法，提出了著名的有噪信道编码定理，奠定了信道编码理论的基石。今天的信道编码不单是一个理论问题，它已经成为现代电子、通信领域不可或缺的一项标准技术。数字通信或存储系统要求实现语音、图像和数据等大容量数据的可靠传输或存储，这些技术的实现均离不开高效的信道编码技术。

信道编码理论是应用数学的重要组成部分，也是一项实用的工程技术。它受到了代数学家和通信工程师的广泛关注，在理论发展和工程需求的双重推动下，已经得到了一大批性能优良的编码和译码方法，并在电子、通信工程中获得了广泛应用。

信道编码已走过了近60年的发展历程，其主要发展过程大致分为以下几个阶段。

20世纪50年代至60年代初期，主要研究各种有效的编码、译码方法，奠定了线性分组码的理论基础；提出了著名的 BCH 码和 RS 码的编码、译码方法以及卷积码的序列译码；得到了纠错码的基本码限。

20世纪60年代中期至70年代初期，极大地发展了多项有效的编码、译码算法，如门限译码、迭代译码、软译码和卷积码的 Viterbi 译码等。同时注重了信道编码的实用化问题，讨论了与实用有关的各种问题，如码的重量分布、译码错误概率和不可检错误概率的计算以及信道模型化等。这些重要的理论研究为信道编码的应用打下了坚实的基础。在此期间，代数编码方法，特别是以有限域理论为基础的线性分组码理论趋于成熟。

20世纪70年代初期至80年代是信道编码理论与应用发展的极其重要的时期。在理论上，代数编码理论进一步得到完善，并发现一批有重要理论和应用意义的代数码和代数几何码，其中一类子码的性能几乎达到了著名的 Shannon 限，是一种最佳码，这在信道编码历史上具有划时代的意义。与此同时，微电子技术的发展为信道编码的应用打下了坚实的物质基础，因而与实用技术相关的各种技术及有关问题得到了极大的关注，并在工程中取得了巨大成功。

可以认为，以上的成就是经典的编码理论的主要部分。从20世纪80年代起，以提高通信信道的频带和功率利用率，以及实现接近于 Shannon 限的实用编码、译码技术成为研究的热点，其相应的成果构成了现代编码理论的重要内容。

1982年提出的著名的网格编码是一种不降低频带和功率利用率，而以设备的复杂化为代价换取编码增益的方法。在传输媒体成本高于终端设备成本而成为通信成本的第一考虑因素时，这种方法是非常吸引人的。1993年提出的 Turbo 码方案，由于很好地应用了 Shannon 信道编码定理中的随机编码思想，并结合先进的次最优的软输入、软输出的迭代译码技术，而获得了接近 Shannon 理论限的译码性能，在编码理论界引起了轰动。Turbo 码是第一次从实践中证明信道编码定理的正确性的码类。因此，网格编码和 Turbo 码已成为自信息论创立以来最重大的研究进展。受到 Turbo 码的先进的译码思想启发，1996年人们又发现早在1960年

提出的低密度校验码(LDPC码)在和积译码算法下也是一个好码,具有更低的线性译码复杂度。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、数字移动蜂窝通信、卫星及空间通信、高密度数据存储等系统的设计。

在现有的编码理论的教材中,系统论述现代编码理论的教材不多,这就需要一本既包括经典的编码理论又能够反映编码理论的最新进展,且适于信息与通信工程学科的教材。为此,我们编写了本书以适应教学的需要。

本书共分为四部分。

第一部分介绍学习信道编码所需的必要的数学基础,包括第2章和第8章8.3节的一部分。这部分内容介绍了数论的初步知识,以及群、环、域、线性空间和矩阵等的基本概念,详细讨论了有限域的性质和构造,以及代数几何的基本知识。

第二部分包括第1、3、4、5章。这部分内容介绍了线性分组码的基本概念和主要码类,如Hamming码、循环码、BCH码、RS码、不等保护能力码等的基本原理与构造方法。此外,这部分还介绍了各种译码方法,如最小Hamming距离译码、最大似然译码、迭代译码、软译码、纠错纠删译码等。

第三部分主要介绍卷积码的基本概念及其有关的译码方法。这部分由第6章组成。

第四部分是现代编码理论的主要内容,由第7、8和9章组成。这部分内容介绍了Turbo码和LDPC码的编译码原理与结构、主要译码算法、码的性能特点和性能限等,以及网格编码等。

本书的内容较多,在教学过程中,可根据具体情况进行取舍。书中有*号的章节为较深或较新的内容,可视情况选学。

在本书的编写过程中,得到了同济大学的领导和老师们的大力支持。本书的责任编辑为本书的编辑出版付出了大量心血。在此,对以上为本书的写作提供帮助的相关人士表示深切谢意。

最后要感谢妻子段晓英女士和家人们,她(他)们关心作者的生活,承担起全部家务,为作者创造了安宁的写作环境。

本书得到了同济大学"十一五"规划研究生教材出版基金的资助。

鉴于作者水平有限,书中难免有错误和不妥之处,敬请专家和读者不吝赐教,在此表示衷心感谢。

赵晓群

2008年3月于同济大学

目　录

第1章 概 述

随着微电子技术、通信技术和计算机技术的发展，新的通信业务和信息业务不断涌现，用户对信息传输的质量要求不断提高。由于通信信道固有的**噪声**和**衰落特性**，或者存储媒介的缺陷等原因，信号在信道传输（或存/取）过程中，必然会受到影响从而产生**失真**。通常需要采用**差错控制编码**技术来检测和纠正由失真引起的传输错误。差错控制编码主要用于实现信道纠错，因此，又称为**纠错编码**或**信道编码**。最早的差错控制编码主要是用于深空通信和卫星通信，随着数字移动通信、数字电视以及高分辨率数字存储设备的出现，编码技术的应用已经不仅仅局限于科研和军事领域，而是在各种实现信息交流和存储的设备中得到了广泛的应用。

1948年信息论和编码理论的奠基人C. E. Shannon[44]提出了著名的**有噪信道编码定理**。该定理给出了在数字通信系统中实现可靠通信的方法，以及在特定信道上实现可靠通信的信息传输速率的上限。同时，该定理还给出了有效的差错控制编码的存在性证明，从而促进了信道编码理论的快速发展。

本章首先介绍数字通信系统的基本结构和信道模型；然后在此基础上重点介绍差错控制编码的分类，以及差错控制编码在数字通信系统中的地位和作用；最后简述最大似然译码的基本原理和信道编码定理。

1.1 数字通信系统模型

采用某种方法、借助某种媒介将**信息**从甲地传送到乙地的过程叫做**通信**。通信的目的是要把对方不知道的**消息**及时可靠地（有时还必须秘密地）传送给对方。在数字通信系统中，**可靠性**与**有效性**（也称为快速性）往往是一对矛盾。若要求有效，则必然使每个**数据符号**所占的**时间**缩短、**波形**变窄、**能量**减少，这样在受到干扰后产生错误的可能性就会增加，传送消息的可靠性就会降低；若要求可靠，则使传送消息的速率变慢。因此，如何较合理地解决可靠性与有效性这一对矛盾是正确设计通信系统的关键问题之一。**通信理论**（包括纠错编码）就是在解决这对矛盾的过程中不断发展起来的。

所有数字通信系统，如通信、雷达、遥控遥测、数字存储系统和计算机内部运算以及计算机之间的数据传输等，都可归结成图1-1的模型。模型中各部分的功能如下。

信源发出的消息（如语言、图像、文字、传感器输出的数据等）经**信源编码器**转换成离散的数字信息序列 $\boldsymbol{u}=\{u\}$，通常 $\boldsymbol{u}$ 为**二元序列**，也可为**多元序列**。为了使传输有效，信源编码器还去掉了一些与传输信息无关的**多余度**（**冗余度**）。有时为了保密，在信源编码器后还可接上**加密器**。为了抗击传输过程中的各种干扰，往往要人为地增加一些多余度，使其具有自动检错或纠错能力，该功能由图中的**信道编码器**（**纠错编码器**）完成。**发射机**（**调制器**）的功能是把信道编码器送出的**码字**（**码序列**），通过调制变换成适合于信道传输的信号。数字信号在信道传输