面向21世纪

高等学校信息工程类专业系列教材

编 码 理 论

Coding Theory

田丽华 编著

西安电子科技大学出版社
http://www.xduph.com

面向21世纪高等学校信息工程类专业系列教材

编码理论

Coding Theory

田丽华 编著

西安电子科技大学出版社
2003

内容简介

本书以信息系统的知识性、研究性、实用性、先进性、综合性的内容为主线，系统地介绍了编码理论的基本原理及应用。主要内容包括：编码理论研究的对象、目的和内容；无失真信源编码和限失真信源编码原理及方法；相关信源编码及方法；信道编码的基本原理及线性分组码、循环码、卷积码、秩距离码等纠错码的编、译码原理和方法；密码系统和密码体制的基本原理及各种实现策略；基于纠错码的密码体制、身份认证、数字签名；现代编码原理及方法等。

本书物理概念清晰、通俗易懂、由浅入深、循序渐进，可作为信息工程、计算机类各专业本科生和研究生的教材或参考书，也可供从事电子、信息、通信、计算机、自动化等专业工作的科技人员参考。

★ 本书配有电子教案，需要者可与出版社联系，免费索取。

图书在版编目(CIP)数据

编码理论＝Coding Theory/田丽华编著.
—西安：西安电子科技大学出版社，2003.8
(面向21世纪高等学校信息工程类专业系列教材)
ISBN 7-5606-1256-3
Ⅰ.编… Ⅱ.田… Ⅲ.编码理论-高等学校-教材 Ⅳ.0157.4

中国版本图书馆CIP数据核字(2003)第045981号

责任编辑 云立实 徐德源
出版发行 西安电子科技大学出版社(西安市太白南路2号)
电 话 (029)8242885 8201467 邮 编 710071
http://www.xduph.com E-mail：xdupfxb@pub.xaonline.com
经 销 新华书店
印刷单位 陕西华沐印刷科技有限责任公司
版 次 2003年8月第1版 2003年8月第1次印刷
开 本 787毫米×1092毫米 1/16 印张17.375
字 数 408千字
印 数 1～4000册
定 价 19.00元
ISBN 7-5606-1256-3/TN·0228(课)

XDUP 1527001-1

序

第三次全国教育工作会议以来，我国高等教育得到空前规模的发展。经过高校布局和结构的调整，各个学校的新专业均有所增加，招生规模也迅速扩大。为了适应社会对“大专业、宽口径”人才的需求，各学校对专业进行了调整和合并，拓宽专业面，相应地教学计划、大纲也都有了较大的变化。特别是进入21世纪以来，信息产业发展迅速，技术更新加快。面对这样的发展形势，原有的计算机、信息工程两个专业的传统教材已很难适应高等教育的需要，作为教学改革的重要组成部分，教材的更新和建设迫在眉睫。为此，西安电子科技大学出版社聘请南京邮电学院、西安邮电学院、重庆邮电学院、吉林大学、杭州电子工业学院、桂林电子工业学院、北京信息工程学院、深圳大学、解放军电子工程学院等10余所国内电子信息类专业知名院校长期在教学科研第一线工作的专家教授，组成了高等学校计算机、信息工程类专业系列教材编审专家委员会，并且面向全国进行系列教材编写招标。该委员会依据教育部有关文件及规定对这两大类专业的教学计划和课程大纲，目前本科教育的发展变化和相应系列教材应具有的特色和定位以及如何适应各类院校的教学需求等进行了反复研究、充分讨论，并对投标教材进行了认真评审，筛选并确定了高等学校计算机、信息工程类专业系列教材的作者及审稿人，这套教材预计在2004年全部出齐。

审定并组织出版这套教材的基本指导思想是力求精品、力求创新、优中选优、以质取胜。教材内容要反映21世纪信息科学技术的发展，体现专业课内容更新快的要求；编写上要具有一定的弹性和可调性，以适合多数学校使用。体系上要有所创新，突出工程技术型人才培养的特点，面向国民经济对工程技术人才的需求，强调培养学生较系统地掌握本学科专业必需的基础知识和基本理论，有较强的本专业的基本技能、方法和相关知识，培养学生具有从事实际工程的研发能力。在作者的遴选上，强调作者应在教学、科研第一线长期工作，有较高的学术水平和丰富的教材编写经验；教材在体系和篇幅上符合各学校的教学计划要求。

相信这套精心策划、精心编审、精心出版的系列教材会成为精品教材，得到各院校的认可，对于新世纪高等学校教学改革和教材建设起到积极的推动作用。

系列教材编委会

2002年8月

高等学校计算机、信息工程类专业系列教材编审专家委员会

主　任：杨　震（南京邮电学院副院长、教授）
副主任：张德民（重庆邮电学院通信与信息工程学院院长、教授）
　　韩俊刚（西安邮电学院计算机系主任、教授）
　　李荣才（西安电子科技大学出版社总编辑、教授）

计算机组

组　长：韩俊刚（兼）
成　员：（按姓氏笔画排列）
　　王小民（深圳大学信息工程学院计算机系主任、副教授）
　　王小华（杭州电子工业学院计算机分院副院长、副教授）
　　孙力娟（南京邮电学院计算机系副主任、副教授）
　　李秉智（重庆邮电学院计算机学院院长、教授）
　　孟庆昌（北京信息工程学院教授）
　　周　娅（桂林电子工业学院计算机系副主任、副教授）
　　张长海（吉林大学计算机科学与技术学院副院长、教授）

信息工程组

组　长：张德民（兼）
成　员：（按姓氏笔画排列）
　　方　强（西安邮电学院电信系主任、教授）
　　王　晖（深圳大学信息工程学院电子工程系主任、副教授）
　　胡建萍（杭州电子工业学院电子信息分院副院长、副教授）
　　徐　祎（解放军电子工程学院电子技术教研室主任、副教授）
　　唐　宁（桂林电子工业学院通信与信息工程系副主任、副教授）
　　章坚武（杭州电子工业学院通信工程分院副院长、教授）
　　康　健（吉林大学通信工程学院副院长、教授）
　　蒋国平（南京邮电学院电子工程系副主任、副教授）

总 策 划：梁家新
策　　划：马乐惠　云立实　马武装　马晓娟
电子教案：马武装

前　言

编码理论起源于现代通信技术与电子计算机技术中差错控制研究的实际需要。编码理论是用概率论、随机过程和数理统计等方法来研究信息的存储、传输和处理中一般规律的学科，所以使人们越来越重视学习和掌握信息系统的编码技术。目前，编码方法繁多，发展也相当迅速，随着针对不同应用目的而制定的各种编码的国际标准的相继推出，再加上数学、工程技术以及计算机软、硬件性能的深入发展和提高，使得编码的理论和技术得到了前所未有的发展和应用。所谓编码，广义地说就是信号的变换，是信息处理的主要手段。编码的主要目的是提高系统对某一方面的要求以及优化系统某一方面的性能指标。通信系统的性能指标主要为有效性、可靠性、安全性和经济性，优化就是使这些指标达到最佳。除了经济性外，这些指标都是编码理论的研究对象，根据信息论的各种编码定理和通信系统的性能指标，编码问题可分解为信源编码、信道编码和密码编码三类。

经典信源编码方法主要依据信源本身固有的统计特性。现代编码压缩技术的研究突破了传统香农理论的框架，注重对感知特性的利用，使得压缩效率得以极大的提高，尤其是随着数学理论，如小波变换、分形几何理论、数学形态学等以及相关学科，如模式识别、人工智能、神经网络、感知生理心理学等的深入发展，新颖高效的现代压缩方法相继产生。信源编码的主要目的是提高通信系统的有效性，信道编码的主要目标是研究如何提高信息传送的可靠性。信道中的干扰使通信质量下降，也就是使信息传送不可靠。对于模拟信号，表现在收到的信号的信扰比下降；对于数字信号，表现在误码率增大。密码编码是通信系统中的另一类编码问题，发送端的明文信息经编码后成为密文，当授权者收到后，可用已具有的密钥正确地译成明文；对于非授权者，因没有密钥而无法取得该信息，这样就保证了通信的安全性。

为了满足信息工程、计算机类各专业的学生及相关专业科技人员的迫切需要，本书系统地介绍了编码理论的基本原理及应用，以该技术领域的知识性、研究性、实用性、先进性、综合性的内容为主线，尽量将编码理论发展的新成果及其应用编入教材，合理而系统地安排各章节；在叙述上，注重基本概念、基本理论和基本方法的论述，物理概念清晰、通俗易懂、由浅入深、循序渐进、示例丰富，便于读者学习。

本书分8章介绍编码理论。在绪论中介绍编码的概念、编码理论研究的对象、目的和内容；在介绍无失真信源编码和限失真信源编码的内容时，首先复习信息熵与互信息的概念及信源编码原理，然后介绍霍夫曼码、费诺码、香农-费诺-埃利斯码、游程编码、算术编码、预测编码、变换编码等各种信源编码方法，接着介绍限失真信源编码原理及编码方法，

讨论各种编码方法的局限性和实现时将遇到的问题；关于信道编码，首先介绍信道编码的基本概念及原理，然后介绍线性分组码、循环码、卷积码、秩距离码等几种纠错码的编、译码原理和方法；关于通信系统的保密，介绍了密码系统和密码体制的基本概念和原理，认证系统及各种实现策略；关于纠错码与通信系统的保密，介绍了基于纠错码的密码体制、身份认证的基本原理及认证方案、数字签名及签名方案；本书的结束部分简单介绍了现代编码原理及方法。

本书可作为信息工程、计算机类各专业的本科生和研究生的教材或参考书，也可供从事电子、信息、通信、计算机、自动化等专业的科技人员参考。为帮助读者掌握分析和解决问题的能力，书中列举了许多例题，各章均配有大量习题。书末附有一些参考书目和参考文献，以供读者查阅。书中有些加宽加深的内容，对本科生讲授时，可作适当取舍，只讲授基本内容，复杂的数学证明可以省略。

全书共8章，田丽华副教授在原有教学讲义的基础上，编写了第1章～第6章，李月教授编写了第7章，刘红璐副教授编写了第8章；书中的所有图形均由蔡东杰副教授设计并绘制；博士生导师王珂教授审阅了原稿，并提出了许多建设性的意见；邓小英参加了部分文稿的编写、整理和录入工作。

在此对本书编写过程中所有给予热情帮助的前辈、同行及学生们：王新梅、王树勋、康健、云立实、杨晓萍、夏辉、韩爽、刑立圆等表示真诚的感谢，对本书中引用的参考文献的所有作者表示衷心的感谢。

对于书中的缺点和错误，作者殷切希望广大读者批评指正。

作　者

2003年2月12日

目 录

第 1 章 绪论 …… 1
1.1 编码理论的基本概念 …… 1
1.2 编码理论的发展 …… 2
1.3 编码理论研究的内容和目的 …… 6
习题 …… 9
第 2 章 无失真信源编码 …… 10
2.1 信息量、熵和互信息量 …… 11
2.2 信源编码定理 …… 15
2.2.1 信源编码的基本概念 …… 15
2.2.2 变长码 …… 18
2.2.3 克拉夫特(Kraft)不等式 …… 21
2.2.4 信源编码定理 …… 22
2.2.5 统计匹配码 …… 24
2.3 霍夫曼码及其他编码方法 …… 25
2.3.1 霍夫曼(Huffman)码 …… 25
2.3.2 m 元霍夫曼码 …… 28
2.3.3 霍夫曼码的最佳性 …… 30
2.3.4 费诺(Fano)编码 …… 30
2.3.5 香农-费诺-埃利斯码 …… 32
2.4 算术编码 …… 36
2.4.1 积累概率的递推公式 …… 37
2.4.2 算术编码原理 …… 38
2.4.3 算术编码的码长 …… 41
2.4.4 递推公式的应用 …… 42
2.4.5 不做乘法的算术编码 …… 46
2.5 游程编码 …… 49
2.5.1 游程和游程序列 …… 49
2.5.2 游程编码 …… 49
2.6 改进的霍夫曼码 …… 51
2.6.1 文件传真基本特性 …… 51
2.6.2 文件传真的游程编码 …… 52
2.6.3 修正霍夫曼码 …… 52
2.7 通用编码 …… 56
2.7.1 分段编码 …… 56
2.7.2 段匹配码 …… 57
2.7.3 LZW 算法 …… 59
习题 …… 61
第 3 章 相关信源编码 …… 65
3.1 预测编码 …… 65
3.1.1 预测编码的基本原理 …… 65
3.1.2 预测方法 …… 67
3.1.3 预测编码的基本类型 …… 68
3.1.4 DPCM 编译码原理 …… 70
3.2 变换编码 …… 72
3.2.1 变换编码的基本原理 …… 73
3.2.2 卡胡南-列夫变换(KLT) …… 74
3.2.3 离散余弦(DCT)变换 …… 76
3.2.4 变换编码方法的特性 …… 77
3.2.5 子带编码 …… 79
习题 …… 81
第 4 章 限失真信源编码 …… 83
4.1 连续信源的熵和互信息 …… 84
4.2 信息率失真理论 …… 85
4.2.1 失真函数 …… 85
4.2.2 平均失真 …… 87
4.2.3 信息率失真函数 …… 89
4.3 标量量化编码 …… 91
4.3.1 均匀量化 …… 91
4.3.2 最优量化 …… 92
4.4 矢量量化编码 …… 93
4.5 语音压缩编码 …… 94
4.5.1 波形编码基本原理 …… 94
4.5.2 参量编码 …… 95
4.5.3 混合编码 …… 96
4.6 图像压缩编码 …… 96
4.6.1 静止图像压缩编码 …… 98

4.6.2 活动图像压缩编码 …… 98
4.6.3 视频压缩编码 …… 100
4.6.4 H.261 建议 …… 102
4.6.5 JPEG 标准 …… 103
4.6.6 MPEG 标准 …… 106
习题 …… 110
第 5 章 信道编码 …… 112
5.1 信道编码的基本概念 …… 112
5.2 信道编码的基本原理 …… 113
5.3 线性分组码 …… 114
5.3.1 线性分组码的基本概念 …… 114
5.3.2 线性码生成矩阵和一致监督矩阵 …… 115
5.3.3 线性码的检错、纠错能力 …… 119
5.3.4 汉明码 …… 122
5.3.5 线性分组码的编码 …… 126
5.3.6 线性分组码的译码 …… 127
5.4 循环码 …… 134
5.4.1 循环码的基本概念 …… 134
5.4.2 循环码的生成矩阵和监督矩阵 … 136
5.4.3 循环码的编码 …… 142
5.4.4 循环码的译码 …… 142
5.4.5 循环码的捕错译码和大数逻辑译码 …… 146
5.4.6 BCH 码和 RS 码 …… 150
5.4.7 Goppa 码 …… 153
5.5 卷积码 …… 154
5.5.1 卷积码的基本概念和编码的基本原理 …… 155
5.5.2 卷积码的生成矩阵和监督矩阵 … 157
5.5.3 卷积码的编码 …… 159
5.6 秩距离码 …… 164
5.6.1 秩距离的基本概念 …… 164
5.6.2 秩距离码的监督矩阵和生成矩阵 …… 165
5.6.3 秩循环码 …… 167
5.7 突发错误的纠正 …… 168
5.7.1 基本概念 …… 168
5.7.2 纠突发错误的码 …… 168
5.8 级连码、交织码及 TCM 码 …… 169
5.9 纠错码的应用 …… 173
5.9.1 自动请求重传方式(ARQ) …… 174
5.9.2 前向纠错方式(FEC) …… 174
5.9.3 纠错码在 GSM 中的应用 …… 174
习题 …… 175
第 6 章 通信系统的保密 …… 178
6.1 密码系统和密码体制 …… 179
6.1.1 明文、密文和密钥 …… 179
6.1.2 密码编码和密码分析 …… 180
6.1.3 古典密码体制 …… 183
6.1.4 保密性与随机性 …… 184
6.1.5 复杂性理论 …… 188
6.2 认证技术 …… 190
6.2.1 消息认证系统 …… 191
6.2.2 消息认证码和消息认证 …… 195
6.2.3 身份认证 …… 197
6.2.4 数字签名 …… 198
6.3 认证方案 …… 200
6.3.1 RSA 签名方案 …… 200
6.3.2 不可否认签名 …… 201
6.3.3 身份认证方案 …… 202
6.3.4 基于离散对数和二次剩余的门限数字签名体制 …… 203
6.4 数据加密体制 …… 206
6.4.1 数据加密标准 DES …… 206
6.4.2 DES 密码的演化设计 …… 208
6.4.3 公开密钥密码 …… 214
6.5 模拟信号加密 …… 216
6.5.1 模拟置乱加密体制 …… 217
6.5.2 数字化加密 …… 218
习题 …… 219
第 7 章 纠错码与通信系统的保密 …… 221
7.1 基于纠错码的公钥密码体制 …… 221
7.1.1 M 公钥密码体制 …… 221
7.1.2 N 公钥密码体制 …… 222
7.1.3 M 公钥密码体制与 N 公钥密码体制的关系 …… 222
7.1.4 M_r 公钥密码体制 …… 223
7.1.5 M 公钥的安全性 …… 224
7.1.6 M 公钥的变型 …… 226
7.1.7 增加 M 公钥的传信率 …… 227
7.2 基于纠错码的私钥密码体制 …… 227
7.2.1 Rao 私钥密码体制 …… 228
7.2.2 Rao-Nam 私钥密码体制 …… 228
7.2.3 L-W 私钥密码体制 …… 229
7.2.4 MC 分组加密纠错体制 …… 232

7.2.5 基于级连码的私钥密码体制 …… 232
7.3 基于纠错码的身份认证 …… 234
7.3.1 方案的基本原理 …… 234
7.3.2 方案的安全性分析 …… 235
7.3.3 方案的一个变型 …… 235
7.4 基于纠错码的数字签名 …… 236
7.4.1 基于纠错码的 Xinmei 数字签名方案 …… 236
7.4.2 Xinmei 签名方案的安全性 …… 237
7.4.3 修正 Xinmei 方案 …… 239
7.4.4 对 AW 方案和 Xinmei 方案的通用伪造攻击 …… 241
7.4.5 签名、加密和纠错相结合的公钥体制 …… 242
习题 …… 245
第 8 章 现代编码技术 …… 246
8.1 传统信源编码的应用 …… 246
8.2 现代信源编码技术 …… 250
8.2.1 分形编码 …… 250
8.2.2 模型编码 …… 252
8.2.3 小波编码 …… 252
8.3 密码学研究现状及趋势 …… 254
8.3.1 公钥密码 …… 254
8.3.2 分组密码 …… 255
8.3.3 序列密码 …… 256
8.3.4 Hash 函数 …… 257
8.3.5 密钥管理 …… 258
8.3.6 PKI 和 VPN …… 258
8.3.7 量子密码 …… 258
8.4 多媒体信息伪装 …… 259
8.4.1 信息隐藏 …… 260
8.4.2 数字水印 …… 261
8.4.3 数字指纹 …… 263
8.4.4 叠像术 …… 263
8.4.5 潜信道 …… 264
8.5 人工神经网络 …… 265
习题 …… 266
参考文献 …… 267

第1章 绪 论

编码理论起源于现代通信技术与电子计算机技术中差错控制研究的实际需要。美国数学家香农(C. E. Shannon)在1948年发表的著名论文《通信的数学理论》，开创了一门在现代科学技术中具有重大意义的崭新的学科——信息论。编码理论是信息论的一个专门分支。目前，编码方法繁多，发展也相当迅速，随着根据不同应用目的而制定的压缩编码的国际标准的相继推出，再加上数学、工程技术以及计算机体系结构、软硬件性能的发展和提高，使得编码的理论和技术得到了前所未有的发展和应用。

1.1 编码理论的基本概念

各种通信系统，如电报、电话、电视、广播、遥测、遥控、雷达和导航等，虽然它们的形式和用途各不相同，但本质是相同的，都是信息的传输系统。为了便于研究信息传输和处理的共同规律，将各种通信系统中具有共同特性的部分抽取出来，概括成一个统一的理论模型，如图1-1所示。通常称它为通信系统模型。

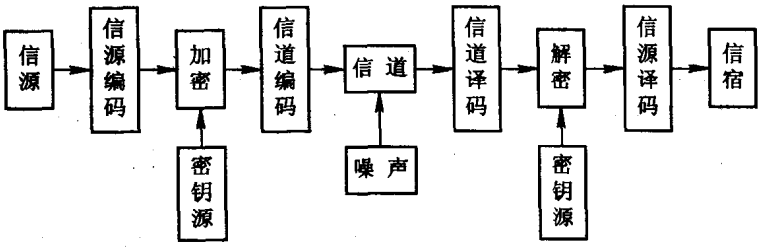

图1-1 通信系统模型

图1-1所示的通信系统模型也适用于其他的信息流通系统，如生物有机体的遗传系统、神经系统、视觉系统等，甚至人类社会的管理系统都可概括成这个模型。人们通过系统中消息的传输和处理来研究信息传输和处理的共同规律。信息传输或通信的目的是要把收方不知道的信息及时、可靠、完整、安全而又经济地传送给指定的收方。该模型按功能可分为信源、编码器、信道、译码器、信宿五部分。信源是产生消息和消息序列的源，它可以是人、生物、机器或其他事物，它是事物各种运动状态或存在状态的集合。信源发出的消息有语音、图像、文字等，人的大脑思维活动也是一种信源。信源的输出是消息，消息是具体的，但它不是信息本身。另外，信源可能出现的状态(即信源输出的消息)是随机的、不确定的，但又有一定的规律性。编码器可分信源编码器、信道编码器、保密编码器三种。

信源编码是对信源输出的消息进行适当的变换和处理，把信息变换成信号，目的是为了提高信息传输的效率，使传输更为经济、有效，还要去掉一些与被传信息无关的多余度；信道编码是为了提高信息传输的可靠性而对消息进行的变换和处理；保密编码是为保证信息的安全性。在信息传输或处理过程中，除了指定的接收者外，还有非指定的或非授权的用户，他们通过各种技术手段企图窃取机密信息。因此，为了保证被传送信息的安全和隐私，必须对信源的输出进行加密或隐藏，同时还要求信息传递过程中保证信息不被伪造和篡改。通信系统中的传输媒质有电缆、明线、光纤和无线电波的传播空间等，信号通过这些媒质时，是很不安全的。存在着各种天然和人为干扰使被传信号产生错误。除此以外，非指定用户或敌人还会通过各种方法(如搭线、电磁波接收、声音接收等)对所传输的信号进行侦听(称被动攻击)。更有甚者，有些非法入侵者主动对系统进行骚扰，采用删除、更改、增添、重放、伪造等手段，向系统注入信号或破坏被传的信号，以达到欺骗别人，有利于自己的目的，这种攻击称为主动攻击。因此，保护系统中所传消息的真实性、完整性，是一个更为困难的问题，也是密码系统所必须完成的另一个更为艰巨的任务。由于在传输信息的媒质中总是存在有各种人为或天然的干扰和噪声，因此，为了提高整个通信系统传输信息的可靠性，就需要对加密器输出的信息进行一次纠错编码，人为地增加一些多余信息，使其具有自动检错或纠错功能。这种功能由图 1－1 中的信道编码器完成。当然，对于各种实际的通信系统，还应包括换能、调制、发射等各种变换处理。信道是指通信系统把载荷消息的信号从甲地传输到乙地的媒介。在狭义的通信系统中，实际信道有明线、电缆、波导、光纤、无线电波传播空间等，这些都属于传输电磁波能量的信道。当然，对广义的通信系统来说，信道还可以是其他的传输媒介。信道除了传送信号以外，还有存储信号的作用，在信道中还存在噪声和干扰，为了分析方便起见，把在系统其他部分产生的干扰和噪声都等效地折合成信道干扰，看成是由一个噪声源产生的，它将作用于所传输的信号上。这样，信道输出的已是叠加了干扰的信号。由于干扰或噪声往往具有随机性，所以信道的特性也可以用概率空间来描述。译码就是把编码器输出的编码信号进行反变换。一般认为这种变换是可逆的。译码器也可分成信源译码器和信道译码器及保密译码器三种。信宿是消息传送的对象，即接收消息的人或机器。图 1－1 给出的模型只适用于收发两端单向通信的情况。它只有一个信源和一个信宿，信息传输也是单向的。更一般的情况是：信源和信宿各有若干个，即信道有多个输入和多个输出，另外信息传输也可以双向进行，例如广播通信是一个输入、多个输出的单向传输的通信，而卫星通信则是多个输入、多个输出的多向传输的通信。

1.2 编码理论的发展

1948 年，香农在《通信的数学理论》的论文中，用概率测度和数理统计的方法系统地讨论了通信的基本问题，得出了几个重要而带有普遍意义的结论。香农理论的核心是：在通信系统中采用适当的编码后能够实现高效率和高可靠性的信息传输，并得出了信源编码定理和信道编码定理。从数学观点看，这些定理是最优编码的存在定理。但从工程观点看，这些定理不是结构性的，不能从定理的结果直接得出实现最优编码的具体途径。然而，它

们给出了编码的性能极限，在理论上阐明了通信系统中各种因素的相互关系，为人们寻找最佳通信系统提供了重要的理论依据。

当已知信源符号的概率特性时，可计算它的信息熵，用熵来表示每个信源符号所载有的信息量。编码定理不但证明了必存在一种编码方法，使码的平均长度可任意接近但不能低于信息熵，而且还阐明达到该目标的途径，就是使概率与码长匹配。信源编码定理出现后，编码方法就趋向于合理化。从无失真信源编码定理出发，1948 年，香农在论文中提出并给出了简单的编码方法(香农编码)，1952 年，费诺(Fano)提出了一种费诺码，同年霍夫曼(D. A. Huffman)构造了一种霍夫曼编码方法，并证明了它是最佳码。霍夫曼码是有限长度的块码中的最好的码，亦即代码总长度最短的码。1956 年，麦克米伦(B. McMillan)首先证明了惟一可译变长码的克拉夫特(Kraft)不等式。

霍夫曼码在实际中已有所应用，但它仍存在一些块码及变长码所具有的缺点。例如，概率特性必须精确地测定，它若略有变化，就需更换码表，以及对于二元信源，常需多个符号合起来编码，才能取得好的效果等。因此在实用中常需做一些改进，同时也就有研究非块码的必要性。算术码就是一种非块码，它是从整个序列的概率的匹配来进行编码的。其实此概念也是香农首先提出的，后经许多学者改进，已进入实用阶段。1968 年前后，埃利斯(P. Elias)发展了香农-费诺码，提出了算术编码的初步思路。而里斯桑内(J. Rissanen)在 1976 年给出和发展了算术编码，1982 年他和兰登(G. G. Langdon)一起将算术编码系统化，并省去了乘法运算，使其更为简化、易于实现。

对概率特性未知或不确知的信源进行有效的编码，上述方法已无能为力。20 世纪 70 年代就有学者提出通用编码。要测定信源的精确概率特性，尤其对高阶条件概率是非常困难的；何况有时信源的概率特性根本无法测定，或是否存在也不知道。例如地震波信号就是如此，因为无法取得大量实验数据。当信源序列是非平稳的时，其概率特性随时间而变更，要测定这种信源的概率特性也近乎不可能。因此总希望能有一种编码方法，通用于各类概率特性的信源。

1977 年由齐弗(J. Ziv)和兰佩尔(A. Lempel)提出了 LZ 算法，它是适用于通用信源的编码算法之一。1978 年他们俩又提出了改进算法，而且齐弗也证明此方法可达到信源的熵值。1990 年，贝尔(T. C. Bell)等在 LZ 算法基础上又做了一系列变化和改进，现在 LZ 码已广泛应用于文本的数据压缩中。

通用编码中最困难的问题是准则问题。这与概率匹配问题不同，此时已不能确定最佳的标准。当概率特性已知时，信源编码定理给出了极限值，达到这个界的就是最佳码。当概率特性未知时，就无法确定这个上界。一般认为它的概率特性是存在的，只是未能测量而不确知而已。这样就可与该概率特性下的极限熵相比较，来确定某种通用编码是否渐近最佳。由此可见，通用编码不但在实用上而且在理论上都需要进一步探讨。

前面介绍的无失真信源编码适用于离散信源或数字信号，不适用于连续信源或模拟信号，如语音图像等信号的数字处理。因为连续信源的每个样值所能载荷的信息量是无限大，而数字信号的值则为有限，对连续信源不引入失真是不可能的。并且连续信号所对应的信宿一般是人，当失真在某一限度以下时是不易被感觉到的，因此是容许的。限失真信源编码的研究较信道编码和无失真信源编码落后约 10 年左右。1948 年，香农在其论文中已体现出了关于率失真函数的思想。1959 年他发表了“保真度准则下的离散信源编码定

理”，首先提出了率失真函数及率失真信源编码定理。1971 年伯格尔的《信息率失真理论》是一本较全面地论述有关率失真理论的专著。率失真信源编码理论是信源编码的核心问题，是频带压缩、数据压缩的理论基础。

连续信源编成代码后就无法无失真地恢复原来的连续值，此时只能根据率失真理论进行限失真编码。从率失真函数 $R(D)$ 出发的限失真编码定理虽给出了最佳编码的存在性，也就是在保证平均失真小于允许失真 D 的情况下，最佳码的码率可以压缩到略大于 $R(D)$，但未能给出像概率匹配那样具体的编码途径。限失真编码实际上就是最佳量化问题。最佳标量量化通常不能达到率失真函数所规定的值。以后就提出矢量量化，就是多个信源符号合成一个矢量并对它进行编码。从理论上说，在某些条件下，用矢量量化来编码可达到上述的 $R(D)$ 值，但在实现上还是非常困难的，有待进一步的研究成果来改进。对于有记忆信源，条件熵必然不大于无条件熵，而且常远小于后者。这就是说，解除符号间的相关性可进一步压缩码率。以上这些编码方法，都以无记忆信源为目标，对记忆信源尚可改进。最简单的方法是多个符号合成为一个新符号，并设新符号组成的序列是独立序列，这样就可用上述方法进行编码。这种方法并不理想。合并的符号数少时，新符号间的相关性不能解除；合并符号数多时，复杂性将大为提高，而且对实时处理十分不利。因此曾提出许多解除相关性的编码方法。比较有效的有预测编码和变换编码：前者利用前几个符号来预测后一个符号的值，预测值与实际值之差，亦即预测误差作为待编码的符号，这些符号间的相关性就大为减弱，这样可提高压缩比；后者是样值空间的变换，例如从时域变到频域，在某些情况下，可减弱相关性，取得良好的压缩比。预测编码和变换编码已在实际中有所应用。从理论上说，怎样才能把有记忆信源转换成无记忆序列，尚无理想的方法，更没有不十分复杂而能实际应用的方法。

以上简述了根据香农两个编码定理发展起来的各种信源编码方法，也就是从概率论形成的语法信息出发，去掉冗余而达到压缩码率的目的。

现在，编码理论与技术不仅在通信、计算机以及自动控制等电子学领域中得到直接的应用，而且还广泛地渗透到生物学、医学、生理学、语言学、社会学和经济学等各领域。在编码理论与自动控制、系统工程、人工智能、仿生学、电子计算机等学科互相渗透，互相结合的基础上，形成了一些综合性的新兴学科。尤其是随着数学理论，如小波变换、分形几何理论、数学形态学等以及相关学科，如模式识别、人工智能、神经网络、感知生理心理学等的深入发展，世界范围内的有关专家一直在追求、寻找现有压缩编码的快速算法，同时，又在不断探索新的科学技术在压缩编码上的应用，因此新颖高效的现代压缩方法相继产生。

小波变换 WT 的小波函数系的时宽、带宽面积很小，且在时间和频率轴上都很集中，也就是说展开系数即小波变换系数的能量集中，并且不同频带之间的小波变换系数相关联。据此，有人提出零树(Zerotree)矢量量化方法，它可以达到几百倍的压缩比，且可按不同的压缩比编码，灵活性大。在压缩编码向着智能化和高速化方向发展的今天，神经网络和模型基编码成为当今研究的热点之一。神经网络(NN，Neural Networks)之所以很适合编码，是因为 NN 具有大规模并行处理及分布式信息存储的优势，有良好的自适应性、自组性和容错性，有很强的学习功能、联想记忆功能。NN 的强映射能力和非线性特性，使它可以学习具有相当接近输入信号特征空间基带的能力。因此，用来解决最佳变换的方法是

很有效的。应用 BP 算法的多层非线性感知网曾成功地用于 DPCM 编码。利用 Kohonon 的自组织映射进行矢量量化的码本设计取得了极大的成功。用 SOFM 算法所生成的码本就很少依赖于初始码本，且生成的码本的拓扑结构能用来进一步提高编码效率和降低计算复杂度。然而，现有的一些用于编码的神经网络模型都是在模拟人脑功能的思想下建立的，没有考虑信源的特点和肉眼的视觉机理，因此压缩效果不太理想。从理论上讲，神经网络可以模拟肉眼的信息处理过程。这种模拟不限于网络结构方面，还包括网络的学习机制；但大多数神经网络的学习算法中，使用的只是均方误差或 P 阶矩误差失真准则，也没有考虑人类视觉系统的特性。另外，神经网络还未能发挥其强大的信息表征和处理功能，这些与神经网络理论研究还很不成熟，尚未形成完整的理论体系有关，有待于进一步研究。而基于模型基的编码(Model Based Coding)策略着重利用景物中的物体结构模型，在一定程度上利用了景物的三维信息。也就是说，它使用结构化的信源模型来表示信源信号，其主要优点是用结构的方式来描述信源内容。它的应用领域自然有别于波形编码。模型编码的关键之处就是如何建模。可以建立三维(3D)模型，也可以建立二维(2D)模型。3D 模型又可分为面向物体的模型(Object Oriented Model)和基于语义的模型(Semantic Based Model)(即参数化的模型)，但是，建模的问题还有待于深入研究。基于语义的方法可以有效地利用景物中已知物体的知识，以实现非常高的压缩比，但它也仅能处理已知的物体，并需要较复杂的信源分析与识别技术。而面向物体的方法可以处理一般的对象，已知的或未知的，显然有更广泛的应用前景；但其未能充分利用景物的知识，或只能在低层次上运用物体知识，编码效率也就无法同前者相比拟。

在研究信源编码的同时，另外一部分科学家从事信道编码(纠错码)的研究工作。这一工作已取得了很大的进展，并已经形成一门独立的分支——纠错码理论。1950 年汉明(R. W. Hamming)发表的论文《检错码与纠错码》是开拓编码理论研究的第一篇论文。这篇论文主要考虑在大型计算机中如何纠正所出现的单个错误。1952 年费诺(R. M. Fano)给出并证明了费诺不等式，并给出了关于香农信道编码逆定理的证明；1957 年沃尔夫维兹采用了类似典型序列的方法证明了信道编码强逆定理；1961 年费诺又描述了分组码中码率、码长和错误概率的关系，并提供了香农信道编码定理的充要性证明；1965 年格拉格尔(R. G. Gallager)发展了费诺的证明结论并提供了一种简明的证明方法；1972 年阿莫托(S. Arimoto)和布莱哈特(R. Blahut)分别发展了信道容量的迭代算法。1948 年香农首先分析并研究了高斯信道问题；1964 年霍尔辛格(J. L. Holsinger)发展了有色高斯噪声信道容量的研究；1969 年平斯克尔(M. S. Pinsker)提出了具有反馈的非白噪声高斯信道容量问题；1989 年科弗尔(T. M. Cover)对平斯克尔的结论给出了简洁的证明。从能够纠正单个错误的汉明码过渡到能够纠正多个错误的所谓 BCH 码，整整经历了 10 年的时间。因此，可以说 20 世纪 60 年代是代数编码理论发展的鼎盛时期。20 世纪 70 年代出现了高帕码(Goppa Codes)，从而又把编码理论推向了一个新的高峰。到了 20 世纪 80 年代，茨伐斯曼(Tsfasman)等人运用代数几何的方法推广了高帕码的思想，指出存在 $GF(m)$ 上的一列码。这一令人吃惊的结果给编码理论的进一步发展带来了新的希望。汉明码出现后，人们把代数方法引入到纠错码的研究，形成了代数编码理论。由此找到了大量可纠正多个错误的好码，而且提出了可实现的编译码方法。但代数编码的渐近性能很差，不能实现香农信道编码定理所指出的结果。因此，1960 年前后提出了卷积码的概率译码，并逐步形成了一系列概率译码理论。

尤其以维特比(Viterbi)译码为代表的译码方法被美国卫星通信系统所采用，使香农理论成为真正具有实用意义的科学理论。香农1961年的论文《双路通信信道》开拓了网络信息论的研究。1970年以来，随着卫星通信、计算机通信网的迅速发展，网络信息理论的研究异常活跃，成为当前信息论的中心研究课题之一。1971年艾斯惠特(R. Ahlswede)和1972年廖(H. Liao)找出了多元接入信道的信道容量区。接着，1973年沃尔夫(J. K. Wolf)和斯莱平(D. Slepian)将它推广到具有公共信息的多元接入信道中。科弗尔(T. M. Cover)、艾斯惠特(R. Ahlswede)于1983年分别发表文章讨论相关信源在多元接入信道的传输问题。1972年科弗尔提出了广播信道的研究。伯格曼斯(P. Bergmans)(1973)、格拉格尔(R. G. Gallager)(1974)、科弗尔(1975)、马登(K. Marton)(1979)、伊·盖马尔(A. ElGamal)(1979)和范·德·缪伦(E. C. Van der Meulen)(1979)等分别研究了广播信道的容量区问题。近20多年来，这一领域研究活跃，使得网络信息论的存在理论已日趋完善。

随着人类进入信息时代，信息的传递、存储和交换日益骤增。现代化的通信网、计算机信息网，以及各种类型数据库和电子数据交换系统，特别是因特网的迅速发展，使得信息的安全和保密问题与越来越多的人密切相关。个人、公司、集团、政府部门、军事部门的一些有价值的敏感信息在大规模分布式计算机网的环境下，一方面为合法用户提供了极大的方便，另一方面也为非法用户提供了更多介入机密信息的机会。保密学是一门研究通信安全和保护信息资源的既古老而又年青的科学和技术，它包括密码编码学和密码分析学两方面。密码编码学是信息安全技术的核心，密码编码学的主要任务是寻求产生安全性高的有效密码算法和协议，以满足对消息进行加密或认证的要求。密码分析学的主要任务是破译密码或伪造认证信息，实现窃取机密信息或进行诈骗破坏活动。这两个分支既相互对立又相互依存，正是由于这种对立统一关系，才推动了密码学自身的发展。香农在1949年发表的《保密通信的信息理论》论文中，首先用信息论的观点对信息保密问题作了全面的论述。由于保密问题的特殊性，直至1976年迪弗(Diffe)和海尔曼(Hellman)发表了《密码学的新方向》一文，提出了公开密钥密码体制后，保密通信问题才得到广泛研究。尤其当今，信息的安全和保密问题更加突出和重要。人们把线性代数、初等数论、矩阵等引入保密问题的研究，已形成了独树一帜的分支——密码学理论。

1.3 编码理论研究的内容和目的

研究通信系统的目的就是要找到信息传输过程的共同规律，以提高信息传输的可靠性、有效性、保密性和认证性，以达到信息传输系统最优化。所谓可靠性高，就是要使信源发出的消息经过信道传输以后，尽可能准确地、不失真地再现在接收端。而所谓有效性高，就是经济效果好，即用尽可能短的时间和尽可能少的设备来传送一定数量的信息。以后会看到，提高可靠性和提高有效性常常会发生矛盾，这就需要统筹兼顾。例如，为了兼顾有效性(考虑经济效果)，有时就不一定要求绝对准确地在接收端再现原来的消息，而是可以允许一定的误差或一定的失真，或者说允许近似地再现原来的消息。所谓保密性就是隐蔽和保护通信系统中传送的消息，使它只能被授权接收者获取，而不能被未授权者接收和理解。所谓认证性是指接收者能正确判断所接收的消息的正确性和完整性，而不是伪造的和

被篡改的。有效性、可靠性、保密性、认证性和经济性构成了现代通信系统对信息传输的全面要求，其中前四项正是本书要研究的主要内容。如果研究信息传输有效性时，可只考虑信源与信宿之间的信源编(译)码，将其他部分都看成一无干扰信道。如果研究信息传输可靠性时，将信源、信源编码和加密编码都等效成一个信源，而将信宿、信源解码和解密译码都等效成一信宿。如果考虑信息传输的保密性和认证性时，将信源和信源编码等效成一信源；将信道编码、信道、噪声源和信道译码等效成一无干扰信道；而将信源译码和信宿等效于信宿。根据信息论的各种编码定理和上述通信系统的指标，编码问题可分解为信源编码、信道编码、密码编码三类。

信源编码的主要目标是压缩每个信源符号的平均比特数或信源的码率。信源编码可分为经典编码方法和现代编码方法两大类。经典编码方法又可分为无失真信源编码和限失真信源编码。

从经典信源编码理论出发，不难得到信源编码的两种基本途径：其一是设法改变信源的概率分布，使其尽可能地非均匀，再用最佳编码方法使平均码长逼近信源熵；其二是联合信源的冗余度也寓于信源间的相关性之中，去除它们之间的相关性，使之成为或差不多成为不相关信源。基于途径一的编码方法有霍夫曼编码、算术编码、游程编码等，其压缩效率都以信息熵为上界；基于途径二的编码方法有预测编码、变换编码、混合编码、矢量量化等，同时也大都受信息熵的约束。虽然经典方法依据了信源本身固有的统计特性和利用人视觉系统的某些特性进行压缩编码，但是利用得还不够充分，且伴随着感知生理心理学的发展。人们越来越清楚地认识到：人的视觉感知特点与统计意义上的信息分布并不一致，即统计上为表征特征所需的更多的信息量，对视觉感知可能并不重要。从感知角度来讲，无需详细表征这部分特征。这时，编码技术的研究就突破了传统香农理论的框架，注重对感知特性的利用，使得编码压缩效率得以极大提高，因此称其为现代压缩编码方法。

信道编码的主要目标是提高信息传送的可靠性。信道中的干扰常使通信质量下降，也可说使信息传送不可靠。对于模拟信号，这表现在收到的信号的信扰比下降；对于数字信号，这表现在误码率增大。信道编码的主要方法是增大码率或频带，也就是增大所需的信道容量。这恰与信源编码相反。例如，为了提高模拟信号的信扰比，可采用大频偏的调频方式，这类信号的频带将远大于一般的调幅或单边带信号，就需要更大容量的信道。对于数字信号，尤其是二进制信号，通常可在信息位之后，按一定的规律附加一些监督位。这样就可在接收端检出错误并要求重发，或直接纠正某些差错。采用了检错或纠错措施后，显然降低了误码率，也就是提高了信息传送的可靠性。同时，由于增加了监督位，码率将有所扩展，因而将占用较大的信道容量。也有一些信道编码方法并不要求增大容量来提高可靠性，例如在数字调制技术中，相干解调的误码率可低于非相干解调，采用部分相应技术也有此等作用。格状码调制(TCM)技术，把多电平调制和纠错码结合起来，在保持一定有效性的条件下，可较大地提高可靠性。用这些方法提高可靠性的代价是使设备复杂化。信道编码的理论基础是信息论中的信道编码定理。该定理指出，当传送的信息率低于信道容量时，误码可接近零。这就是说，理想的信道编码器应能在码率接近信道容量时，保证可靠通信。而现有技术还远未能达到这一目标。

复用技术也可认为是信道编码。从理论基础来说，这是另一类问题。它并不是为了提高可靠性，而是为了充分利用信道。这种技术在通信中有重要意义。新的复用方式尚在发