21 面向CENTURY

高等学校信息工程类专业规划教材

编码理论

（第二版）

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规划教材

编码理论

(第二版)

田丽华 编著

西安电子科技大学出版社

2007

内容简介

本书系统地介绍了信源的压缩编码、信道的纠错编码及通信系统加密等内容的基本原理及应用，同时也简单地介绍了学习本书所需的信息论、数论及近代代数的相关知识。

全书共16章，主要内容包括：编码理论研究的对象、目的和内容；无失真信源编码原理及编码方法；信道纠错编码的基本原理和编码方法；密码系统的基本原理和编码方法；公钥密码体制中的RSA、ElGamal和椭圆曲线密码体制的表述及安全性分析；消息认证的相关知识；基于纠错码的密码体制、身份认证以及现代编码原理与方法等。

本书力求物理概念清晰，通俗易懂，由浅入深，重点突出，对基本概念和基本原理的阐述清晰明了，实用性强，可作为电子信息类、通信工程类、计算机类等专业本科生和研究生的教材或参考书，也可供相关专业的科技人员参考。

图书在版编目(CIP)数据

编码理论/田丽华编著. —2版. —西安：西安电子科技大学出版社，2007.9
面向21世纪高等学校信息工程类专业规划教材
ISBN 978-7-5606-1256-0

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(2007)第069605号

责任编辑 任 婧 云立实
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)88242885 88201467 邮 编 710071
http://www.xduph.com E-mail:xdupfxb@pub.xaonline.com
经 销 新华书店
印刷单位 陕西天意印务有限责任公司
版 次 2007年9月第2版 2007年9月第4次印刷
开 本 787毫米×1092毫米 1/16 印 张 21.75
字 数 514千字
印 数 14 001～18 000册
定 价 28.00元
ISBN 978-7-5606-1256-0/TN·0228
XDUP 1527022-4

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，相应的教学计划、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大学、西安邮电学院、重庆邮电大学、吉林大学、杭州电子科技大学、桂林电子科技大学、北京信息科技大学、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，对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。

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、好中选优、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

高等学校计算机、信息工程类专业规划教材编审专家委员会

主　任：杨　震（南京邮电大学校长、教授）
副主任：张德民（重庆邮电大学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）

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（杭州电子科技大学计算机学院教授）
　　孙力娟（南京邮电大学计算机学院副院长、教授）
　　李秉智（重庆邮电大学计算机学院教授）
　　孟庆昌（北京信息科技大学教授）
　　周　娅（桂林电子科技大学计算机学院副教授）
　　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、教授）
　　胡建萍（杭州电子科技大学信息工程学院院长、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（桂林电子科技大学通信与信息工程学院副教授）
　　章坚武（杭州电子科技大学通信学院副院长、教授）
　　康　健（吉林大学通信工程学院副院长、教授）
　　蒋国平（南京邮电大学自动化学院院长、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

信息论是20世纪40年代末期由美国数学家C. E. Shannon等人创立的，经过几十年的发展，现已成为信息科学的基础理论。

信息论本身既是一门工程科学，也是一门应用科学，是一门不断发展的学科。信源编码、信道纠错编码及密码学这三大课题是信息论的核心内容，针对其中的任何一个课题，都有很多优秀的论著。本书试图用有限的篇幅将信源编码、信道纠错编码及密码学的所有重要原理有机地结合起来进行讲述，力图使本书的内容具有知识性、研究性、实用性、先进性和综合性；注意做到结构严谨、合理而系统地安排章节；概念清晰、通俗易懂，便于读者学习；通过突出其在信息传输系统中的应用，帮助读者了解其产生理论和解决问题的实际背景，以及提高工科学生的学习兴趣。

本书要求学生具有初等数学基础，要学过概率论、随机过程、线性代数等知识。另外，对数论、离散数学及近代代数中的初等数学知识，本书做了简单的介绍，供读者学习时参考。本书可独立于“信息论”课程进行教学，因为本书对学习中所需的信息论的相关知识进行了必要的介绍。

本书共16章，系统地介绍了信源的压缩编码、信道的纠错编码及通信系统加密等的基本原理及应用。除了第14章及8.2节以外的绝大多数内容适合于本科教学，其中第4章可以不讲，供学生学习相关内容时自学。书中有些加宽、加深的内容，对本科生讲授时可作适当取舍，或只讲授基本内容，如BCH码、Goppa码、秩距离码、Turbo码、AES算法、IDEA算法、EIGamal算法及椭圆曲线加密算法等。

本书是在作者多年教学经验和研究实践的基础上编写而成，书中的所有图形均由蔡东杰副教授设计并绘制。

本书可作为电子信息类、通信工程类、计算机类等专业的本科生和研究生的教材或参考书，也可供相关专业的科技人员参考。

近几十年来，国内外有不少信息编码方面的优秀教科书和专著，本书的编写得益于作者以前对于这些著作的学习。此外，在编写本书过程中还参阅了许多文献、资料，在此向这些著作的作者深表谢意。最后，要感谢在本书编写过程中所有给予过热情帮助的前辈、同行及学生们：王新梅、王珂、康键、云立实、杨晓萍、王国鸿、张巍、周文慧等。

限于作者的水平，本书中不妥和谬误之处难免，欢迎读者将发现的错误、遗漏以及其他的建议发送到E-mail：tlh85@sina.com。

作　者

2007年8月

第一版前言

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1～6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

美国数学家香农(C. E. Shannon)在1948年发表的论文《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。信源编码、信道编码、保密编码三大编码构成了信息论的核心内容。目前，编码方法繁多，其发展也相当迅速。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本身体系结构软、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。

1.1 信息传输系统

1.1.1 信息传输的目标

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，从而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。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。提高可靠性和提高有效性常常会发生矛盾，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，可以允许有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，验证消息的完整性，确认消息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。

1.1.2 信息传输系统模型

各种现代数字通信系统如电报、电话、无线电、电视、广播、因特网、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。通常称它为信息传输系统模型。

图1-1所示的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，人体、动物的神经网络系统和视觉系统等，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。

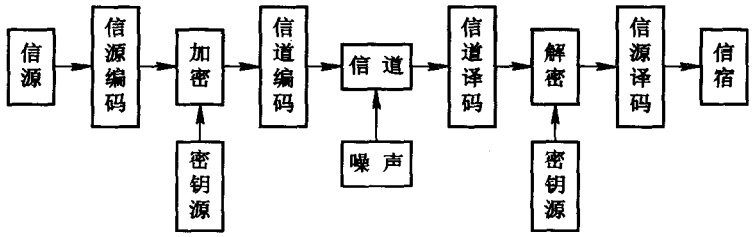

图 1-1　信息传输系统模型

1. 信源

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，信源输出的消息是随机的、不确定的，但又有一定的规律性。信源输出的消息有多种形式，可以是离散的或连续的、平稳的或非平稳的、无记忆的或有记忆的。

2. 编码器

编码器可分为信源编码器、信道编码器和保密编码器三种。信源编码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；保密编码保证了信息的安全性。由于传输信息的媒质如电波、电缆等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，使信息传输系统具有自动检错或纠错功能。当然对于各种实际的通信系统，编码器还应包括换能、调制、发射等各种变换处理功能。

3. 信道

信道是信息传输和存储的媒介，是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，信道输出的是已叠加了干扰的信号。由于干扰或噪声往往具有随机性，因此信道的特性也可以用概率空间来描述。

4. 译码器

译码是编码的反变换。一般认为这种变换是可逆的。译码器也可分成信源译码器、信道译码器和保密译码器三种。

5. 信宿

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通信，因特网是多个输入、多个输出的多向传输通信，卫星通信网也是多个输入、多个输出的多向传输通信。

1.2 信息编码的发展

根据信息论的各种编码定理和信息传输系统的指标，编码可分解为信源编码、信道编码、保密编码三类。

1.2.1 信源压缩编码的发展

1948 年，香农在《通信的数学理论》一文中，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，用它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，使代码的平均长度可任意接近但不能低于信息熵，而且还阐明达到这一目标的途径，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最好的码，亦即它是代码总长度最短的码。1949 年，克拉夫特(L. G. Kraft)提出了 Kraft 不等式，指出了即时码的码长必须满足的条件。后来，麦克米伦(B. McMillan)在 1956 年证明惟一可译码也满足此不等式。到 1961 年，卡拉什(J. Karush)简化了麦克米伦的证明方法。

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；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，霍夫曼码在实用中常需作一些改进，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匹配的角度来进行编码的。其实，此概念也是香农首先提出的，后经许多学者改进，已逐渐进入实用阶段。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。

若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。对有些信

源，要确知信源的统计特性相当困难，尤其是高阶条件概率；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。人们总希望能有一种编码方法通用于各类概率特性的信源，通用编码就是在信源统计特性未知时对信源进行编码，且使编码效率很高的一种码。

1977 年，以色列学者兰佩尔(A. Lempel)和奇费(J. Ziv)提出了一种语法解析码，习惯上称之为 LZ 码。到 1978 年，他们又对这种基于字典的方法提出了改进算法，分别称为 LZ77 和 LZ78。1984 年，韦尔奇(T. A. Welch)以 LZ 编码中的 LZ78 算法为基础修改成一种实用的算法，后定名为 LZW 算法。LZW 算法保留了 LZ78 算法的自适应性能，压缩效果也大致相同；但 LZW 算法的显著特点是逻辑性强，易于硬件实现，且价格低廉，运算速度快。LZW 算法已经作为一种通用压缩方法，广泛应用于二元数据的压缩。

前面介绍的无失真信源编码只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的，而数字信号的值则是有限的，所以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人感觉到的。同时，信宿不论是人还是机器都存在一定的灵敏度和分辨力，超过信宿的灵敏度和分辨力所传送的信息是毫无意义的，也是完全没有必要的。比如语音信源，当分层量化超过 $2^8=256$ 级时，人耳就很难分辨，所以没有必要在量化时超过 256 级。对图像信源亦是如此，人们看电影时可以充分利用人眼的视觉暂留效应，当放映机放速达 25 张每秒以上时，人眼就能将离散的照片在人脑内反映成连续画面。若放速大大超过 25 张每秒，则对普通画面是毫无意义的。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十年左右。1948 年，香农在其论文中已体现出了关于率失真函数的思想，在 1959 年，他发表的《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，直到今天它仍是信息论研究的课题。

连续信源编成代码后就无法无失真地恢复成原来的连续值，此时只能根据率失真理论进行限失真编码。限失真编码实际上就是最佳量化问题。最佳标量量化常不能达到率失真函数所规定的 $R(D)$ 值。后来人们又提出了矢量量化的概念，即将多个信源符号合成一个矢量并对它进行编码。从理论上讲，在某些条件下，用矢量量化来编码可以达到上述的 $R(D)$ 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。1955 年，埃利斯提出了预测编码方法，经过改进，现已经成为美国军用通信语言压缩的标准算法。预测编码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。变换编码是指样值空间的变换，例如从时域变到频域。在某些情况下，变换编码可减弱符号间的相关性，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，目前尚无理想的方法，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信源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中的应用，因此，新颖、高效的现代压缩方法相继产生。

1.2.2 信道纠错编码的发展

在一部分科学家研究信源编码的同时，另外一部分科学家从事有关信道编码(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，沃尔夫维兹采用类似典型序列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 Code)，从而又把编码理论推向了一个新的高峰，到了 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中，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，有些人于 1960 年左右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，使得香农理论成为真正具有实用意义的科学理论。

香农在 1961 年发表的论文《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。一方面，艾斯惠特(R. Ahlswede)(1971 年)和廖(H. Liao)(1972 年)找出了多元接入信道的信道容量区，在 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)和艾斯惠特也于 1983 年分别发表文章讨论相关信源在多元接入信道中的传输问题。另一方面，在 1972 年，科弗尔提出了广播信道的研究，伯格曼斯(P. Bergmans)(1973 年)、格拉格尔(1974 年)、