

● 高等学校教材

信息论 与编码理论

■ 王育民 李 晖 梁传甲 编著



高等教育出版社
HIGHER EDUCATION PRESS

高等学校教材

信息论与编码理论

王育民、李晖、梁传甲 编著



高等教育出版社

内容提要

信息论与编码理论是研究信息传输和信息处理的基础理论。信息论对实际通信系统的设计已产生了深刻的影响,通信工程师在信息论方面的理论基础对他们事业的发展有重要的作用。这本教材总结了西安电子科技大学自1960年创办信息论专业以来为通信工程学院各专业和其他工程专业开设信息论和编码理论课程的经验,特别是总结了改革开放以来的二十几年中为本科生和研究生开设此课的经验。书中较详细地讨论了信息论的基本理论,对信息论中新发展的若干重要课题(如率失真理论、多用户信息论、算术编码、LZ编码、Turbo码和LDPC码等)都做了专题讨论,同时,还涉及了信息论和编码理论这一学科的近况。这对于需要获得信息论基本知识的有关专业的学生和在这些领域从事研究、开发工作的工程技术人员都将是有益的。

本书可作为有关专业高年级本科生和研究生的教材。在给高年级本科生讲授时,可以只讲一些基本内容,书中标有*号的章节主要供研究生阅读,各章后面都附有一些难易程度不等的习题,可根据需要选用。书末附有较详尽的参考文献,可供阅读时参考。

图书在版编目(CIP)数据

信息论与编码理论/王育民,李晖,梁传甲编著.北京:
高等教育出版社,2005.12
ISBN 7-04-017665-3

I.信... II.①王...②李...③梁... III.①信息
论-高等学校-教材②信源编码-编码理论-高等学
校-教材③信道编码-编码理论-高等学校-教材
IV.TN911.2

中国版本图书馆CIP数据核字(2005)第118610号

| | | | |
|------|----------------|------|---|
| 出版发行 | 高等教育出版社 | 购书热线 | 010-58581118 |
| 社 址 | 北京市西城区德外大街4号 | 免费咨询 | 800-810-0598 |
| 邮政编码 | 100011 | 网 址 | http://www.hep.edu.cn |
| 总 机 | 010-58581000 | | http://www.hep.com.cn |
| 经 销 | 北京蓝色畅想图书发行有限公司 | 网上订购 | http://www.landradio.com |
| 印 刷 | 北京市南方印刷厂 | | http://www.landradio.com.cn |
| 开 本 | 787×960 1/16 | 版 次 | 2005年12月第1版 |
| 印 张 | 25.75 | 印 次 | 2005年12月第1次印刷 |
| 字 数 | 480 000 | 定 价 | 32.00元 |

本书如有缺页、倒页、脱页等质量问题,请到所购图书销售部门联系调换。

版权所有 侵权必究

物料号 17665-00

I

众所周知,信息是构成任何系统的三大要素之一,另外两个要素是物质和能量。信息虽然是无形的和抽象的,但它是系统的灵魂。

1948年,C. E. Shannon 发表了他的划时代文章《通信的数学理论》,宣告了一门崭新的学科——信息论的诞生。文章给出了可以概括一切通信系统的数学模型;用概率统计这一数学工具描述了模型中各组成部分(信源、信道、信宿、干扰源、编码器和译码器);给出了信息量的定义,使人们可以定量地研究信息的传输、处理和存储。

Shannon 信息论不仅建立了信源和信道编码定理,给出了有效性的极限,而且为人们明确地指出了实现有效而可靠通信的必由之路是数字化和编码。这是通信技术领域革命的数学或理论基础,而半导体和计算机技术则是这一革命的物理或物质基础。值得指出的是,信息论和晶体管同时诞生在 Bell 实验室。

Shannon 所给出的编码定理的证明是非构造性的,所给出的证明也不够严格,但他的“数学直观出奇地正确”[A. N. Kolmogrov(1963)]。经过无数科技工作者 50 年来的努力奋斗,人们不仅在数学上已严格地证明了 Shannon 编码定理,而且发现了各种具体可构造的有效编码理论和方法,可以实现 Shannon 指出的极限。现在已可实现几乎无差错地经由高斯(Gaussian)信道传信,其传信率可达信道容量的 80% [A. J. Viterbi(1998)],对于非白高斯信道,Shannon 的注水定理和多载波调制(MCM)技术也可接近于理论限实现有效和可靠的通信。这在当代 CDMA、MCM/COFDM、TCM(Trellis Coded Modulation)、BCM(Block Coded Modulation)、Turbo 码、LDPC(Low Density Parity Codes)、空时编码、各种均衡技术、对消技术以及信息存储编码调制技术中都充分体现了 Shannon 定理的作用。

通过近五十年的努力,人们不仅在理论上发展了 Shannon 信息论,

而且在实际中逐步实现了某些信道下的 Shannon 理论所指出的理想传信。信息论这一抽象而完美的理论,在几十年后有如此巨大、丰硕的技术成果,实在令人惊叹!

信息论对实际通信系统的设计已产生了深刻的影响,通信工程师在信息论方面的基础对他们事业的发展有重要的作用。

自 1948 年以来,已过了半个多世纪。IEEE 的信息论学会曾在 1973 年发表了一系列文章,纪念信息论诞生 25 周年,出版了 Shannon 著作集。在 1998 年又举行了一系列纪念活动,纪念信息论诞生 50 周年,并出版了专集。伟大的 Shannon 于 2001 年 2 月 24 日在纽约谢世。

50 年后的今天,通信、计算机和半导体技术的发展已将人类社会推进到一个崭新的信息时代。信息在现代社会中的作用愈来愈大,社会对信息的需求愈来愈大。通信、广播、影视、出版等正在从模拟到数字,从单一媒体到多媒体,从人工、机械化到智能化,从局部联网到全球通信网。

20 世纪七八十年代完成了通信与计算机技术的结合(C & C)。Internet 的出现,为人类交换信息,促进科学、技术、文化、教育、生产的发展,提高现代人的生活品质提供了极大的便利,大大加速了人类信息化社会的进程,加之 90 年代开始了通信、计算机和消费电子(Communications Computer Consumer electronics,3C)的三结合,信息高速公路或全球信息基础设施(GII)的提出和建设,构成了人类生存的信息环境——信息空间(Cyberspace)。这个虚拟空间的形成和发展将人类社会推进到了一个新的发展阶段——信息化社会阶段,为人们提供了更方便、更舒适的工作和生活环境,它对人类社会的发展将产生巨大的影响。

信息化社会导致经济全球化和知识化。互联网已成为社会资源重新分配的基本工具。

信息化社会导致第三次军事革命,联合作战和信息化作战成为重要作战形式,数字化部队和数字化战场也跟着诞生。

信息化社会中,人们的一切活动都将在信息空间中进行竞争和接受检验。

信息化社会中,许多有形的东西开始向数字的、无形的方向转变。

信息化社会也使人们越来越忙碌、越来越浮躁,在信息的大洋中有弄潮儿,也有溺水者。

在信息化社会中,一个国家、一个地区、一个单位乃至一个家庭和个人,除了要有能力在物理空间中生存外,还必须建设好信息基础设施,学会在无形的数字化信息空间中生存,否则,它在现代信息社会的激烈竞争中,就会落后和失败。预计到 2025 年,所有的传输都将数字化,灵巧的个人终端将为人们提供各种各样的服务,个人终端将通过几十米至几千米的无线信道与光纤等骨干网连通,通向世界。

人类已进入 21 世纪。数字化、信息化、网络化正在冲击、影响、改变我们社会生活的各个方面。从科学研究、生产制造、产品流通、商业运作、超市购物、医疗服务、教育培训、出版印刷、媒体传播到文化生活、娱乐休闲、人际交往、法律规范、伦理道德、军事作战……无一不将受到信息网络的挑战,无一不在信息技术这一最新高科技生产力的作用下迅速变化。

为了表彰信息论的创始人 Shannon 的伟大功绩,2000 年 10 月 6 日 IEEE Information Society 的 25 名成员,在 Claude Shannon 儿童时代的老家 Michigan 的 Gaylord 举行了 Shannon 塑像的落成典礼。塑像底座正面刻文如下:

Claude Elwood Shannon

Father of Information Theory

Electrical engineer, Mathematician, and native son of Gaylord. His creation of information theory, the mathematical theory of communication, in the 1940s and 1950s inspired the revolutionary advances in digital communications and information storage that have shaped the modern world.

This statue was donated by the Information Theory Society of the Institute of Electrical and Electronics Engineers, whose members follow gratefully in his footsteps.

Dedicated October 6, 2000

Edgene Daub, Sculptor

著名信息论和编码学者 Dr. Richard Blahut 在 Shannon 塑像落成典礼上的题词中说:“在我看来,两三百年之后,当人们回过头来看我们这个时代的时候,他们可能不会记得谁曾是美国的总统,他们也不会记得谁曾是影星或摇滚歌星,但是仍然会知晓 Shannon 的名字,学校里仍然会讲授信息论。”

II

距离我们在西安电子科技大学出版社出版《信息与编码理论》一书已有 17 年之久,该书第九章的作者,我们的良兄益友梁传甲教授也已过早地于 1992 年 10 月 11 日逝世,我们的老师、西安电子科技大学信息论专业的创始人——陈太一工程院院士也已于 2004 年 5 月 6 日辞世。本书的改版也是对他们两位的纪念。

III

随着我国教育事业的迅速发展,大学有关专业比较普遍地开设了信息论课程,特别是自各校广泛招收研究生以来,信息论几乎成了信息科学与技术、通信与信息系统、信号与信息处理、计算机和应用数学等有关专业普遍选修的课程。

在这种形势下,我们在多次编写信息论、编码理论教材的基础上,重新编写了这本教材,以期能适应科学技术和我国教育形势的新发展。

这本教材总结了我校自1960年创办信息论专业以来,为信息工程系各专业和其他工程专业开设信息论和编码理论课程的经验,特别是总结了改革开放以来为本科生和研究生开设此课的经验。书中较详细地讨论了信息论的基本理论,对信息论中新发展的若干重要课题(如率失真理论、多用户信息论等)都做了专题讨论,并反映信息论和编码理论这一学科的近况。这对于需要获得信息论基本知识的有关专业的同学和在这些领域从事研究、开发工作的工程技术人员都将是有益的。

本书可作为有关专业高年级本科生和研究生的教材。在给高年级本科生讲授时,可以只讲一些基本内容。书中标有*号的章节主要供研究生阅读。若只了解一般信息论的基本内容,第6、7、8章有关纠错码的部分可以从略。各章后面都附有一些难易程度不等的习题,可根据需要选用。书末附有较详尽的参考文献,可供阅读时参考。

李晖博士参加了本书的改写工作,他的贡献是在第3.4节增加了算术码和LZ压缩算法,增写了全新的第8章——接近Shannon极限的编码,对原书有关内容进行重新整理和改写,构成第5、6、7、9和10章。

本书在编写中参考了一些有关著作,特别应当提到的有Gallager(1968)、Fano(1961)、Golomb(1964)、Lin & Costello(1982)、McEliece(2002)、Viterbi & Omura(1979)、Kolesnik & Poltalev(1982)、有本卓(1977)以及周炯槃(1983)等教授的著作。

本书得到国家自然科学基金项目和西安电子科技大学研究生教材基金的资助,胡予濮、王莹、吴蔚以及西安电子科技大学信息论课程组的各位老师编写过程中提供了帮助,提出了宝贵意见。在出版过程中还得到高等教育出版社的大力支持和鼓励,作者在此表示衷心感谢。

作者

于西安电子科技大学

2005.2

○ 目 录

| | |
|------------------------------------|----|
| 第 1 章 引论 | 1 |
| 1.1 通信系统模型 | 1 |
| 1.2 Shannon 信息论的中心问题 | 4 |
| 1.3 Shannon 信息论的局限性 | 5 |
| 1.4 信息的广义性 | 7 |
| 第 2 章 信息量和熵 | 9 |
| 2.1 离散变量的非平均信息量 | 9 |
| 2.1.1 非平均互信息 | 10 |
| 2.1.2 条件互信息与联合事件的互信息 | 14 |
| 2.1.3 离散变量的非平均自信息量 | 16 |
| 2.2 离散集的平均自信息量——熵 | 18 |
| 2.2.1 熵和条件熵 | 18 |
| 2.2.2 熵的性质 | 21 |
| 2.3 熵的唯一性定理 | 25 |
| 2.4 离散集的平均互信息量 | 28 |
| 2.5 连续随机变量的互信息和微分熵 | 32 |
| 2.5.1 连续随机变量的互信息 | 32 |
| 2.5.2 连续随机变量的熵 | 34 |
| 2.5.3 微分熵的极大化 | 37 |
| 2.6 凸函数与互信息的凸性 | 39 |
| 2.6.1 凸函数概念及其性质 | 39 |
| 2.6.2 互信息的凸性 | 43 |
| 2.7 随机过程的信息量和熵 | 45 |
| 小结 | 48 |
| 习题 | 48 |
| 第 3 章 信源编码——离散信源无失真编码 | 53 |
| 3.1 信源及其分类 | 53 |
| 3.2 离散无记忆信源的等长编码 | 55 |

| | |
|----------------------------|------------|
| 3.3 离散无记忆信源的不等长编码 | 62 |
| 3.4 最佳不等长编码 | 69 |
| 3.4.1 Huffman 编码 | 69 |
| 3.4.2 算术编码 | 73 |
| 3.4.3 LZ 编码 | 76 |
| 3.5 平稳源编码 | 79 |
| 3.6 马尔可夫源 | 87 |
| 小结 | 96 |
| 习题 | 97 |
| 第 4 章 信道及其容量 | 102 |
| 4.1 信道分类 | 102 |
| 4.2 离散无记忆信道 | 103 |
| 4.2.1 有关 DMC 的容量定理 | 104 |
| 4.2.2 对称 DMC 容量的计算 | 107 |
| 4.2.3 一般 DMC 容量的计算 | 112 |
| 4.3 离散无记忆信道容量的迭代算法 | 113 |
| 4.4 离散有记忆信道 | 117 |
| 4.5 信道的组合 | 121 |
| 4.6 时间离散的无记忆连续信道 | 125 |
| 4.6.1 可加噪声信道 | 126 |
| 4.6.2 平均功率受限可加噪声信道 | 127 |
| 4.6.3 平行可加高斯噪声信道 | 129 |
| 4.7 波形信道 | 131 |
| 小结 | 134 |
| 习题 | 135 |
| 第 5 章 信道编码定理 | 139 |
| 5.1 信道编码和译码 | 139 |
| 5.1.1 信道编码 | 139 |
| 5.1.2 译码准则 | 140 |
| 5.1.3 离散序列的译码 | 141 |
| 5.1.4 连续序列的译码 | 143 |
| 5.2 Fano 不等式和信道编码逆定理 | 146 |
| 5.3 联合典型序列及信道编码定理 | 149 |
| 5.4 错误概率上限 | 153 |
| 5.4.1 并集限 | 153 |

| | | |
|--------------|----------------------------|------------|
| 5.4.2 | Bhattacharyya(巴塔恰亚)限 | 154 |
| 5.4.3 | Gallager(加拉格)限 | 155 |
| 5.4.4 | 随机码集合平均错误概率上限 | 156 |
| 5.4.5 | DMC 的译码错误概率上限 | 158 |
| 5.4.6 | 时间离散连续信道错误概率上限 | 160 |
| 5.5 | 等能量正交编码信号 | 162 |
| | 小结 | 165 |
| | 习题 | 167 |
| 第 6 章 | 线性分组码 | 171 |
| 6.1 | Galois 域 | 171 |
| 6.1.1 | 域运算 | 171 |
| 6.1.2 | $GF(p^m)$ 的构造 | 172 |
| 6.1.3 | 有限域的特征和元素的级 | 175 |
| 6.1.4 | 最小多项式 | 176 |
| 6.2 | 线性分组码 | 176 |
| 6.3 | 线性分组码的生成矩阵和校验矩阵 | 177 |
| 6.3.1 | 生成矩阵 | 177 |
| 6.3.2 | 校验矩阵 | 179 |
| 6.3.3 | 码的扩展和缩短 | 180 |
| 6.4 | 一些特殊的线性分组码 | 181 |
| 6.4.1 | Hamming(汉明)码 | 181 |
| 6.4.2 | Hadamard 码 | 181 |
| 6.4.3 | Golay 码 | 182 |
| 6.5 | 伴随式和最小汉明距离译码 | 183 |
| 6.5.1 | 分组码的标准阵译码 | 183 |
| 6.5.2 | 最小距离与纠错能力 | 186 |
| 6.6 | 循环码 | 188 |
| 6.6.1 | 循环码的数学描述 | 188 |
| 6.6.2 | 循环码的译码 | 194 |
| 6.7 | BCH 码 | 197 |
| 6.7.1 | BCH 码的定义和性质 | 197 |
| 6.7.2 | BCH 码的译码 | 198 |
| 6.8 | Reed-Solomon 码 | 202 |
| 6.9 | 分组码的性能限 | 203 |
| 6.10 | 线性分组码的性能限 | 207 |
| | 小结 | 208 |

| | |
|--------------------------------------|------------|
| 习题 | 209 |
| 第 7 章 卷积码 | 212 |
| 7.1 卷积码的基本概念 | 212 |
| 7.2 Viterbi 译码 | 229 |
| 7.3 序列译码 | 241 |
| 7.4 卷积码集合平均错误概率限 | 247 |
| 7.5 级联码 | 253 |
| 小结 | 256 |
| 习题 | 256 |
| 第 8 章 接近 Shannon 极限的编码 | 258 |
| 8.1 Turbo 码的构造 | 258 |
| 8.1.1 递归系统卷积码(RSC) | 260 |
| 8.1.2 Turbo 码的距离谱 | 260 |
| 8.1.3 Turbo 码交织器的设计 | 263 |
| 8.2 Turbo 码的译码 | 265 |
| 8.2.1 APP 译码器 | 267 |
| 8.2.2 MAP 译码算法 | 267 |
| 8.2.3 SOVA 译码算法 | 274 |
| 8.2.4 Turbo 码的迭代译码特性 | 276 |
| 8.3 Turbo 码的性能限 | 279 |
| 8.4 低密度校验码的定义 | 281 |
| 8.4.1 LDPC 码的定义 | 281 |
| 8.4.2 LDPC 码的 Tanner 图表示 | 281 |
| 8.4.3 LDPC 码的构造 | 283 |
| 8.5 低密度校验码的译码 | 284 |
| 8.5.1 硬判决译码 | 284 |
| 8.5.2 最佳 APP 译码 | 285 |
| 8.5.3 LDPC 译码的和积算法 | 289 |
| 8.5.4 对数域和积算法 | 291 |
| 8.5.5 最小和算法 | 293 |
| 8.6 低密度校验码的性能 | 294 |
| 小结 | 297 |
| 习题 | 298 |
| 第 9 章 信源编码——无记忆信源的有失真编码 | 300 |
| 9.1 一般概念与定义 | 300 |

| | |
|-----------------------------------|------------|
| 9.2 率失真函数的基本性质与有失真时的逆信源编码定理 | 303 |
| 9.2.1 基本性质 | 303 |
| 9.2.2 有失真时的逆信源编码定理 | 306 |
| 9.3 无记忆信源 $R(D)$ 的计算 | 306 |
| 9.4 $R(D)$ 上、下限的估计 | 313 |
| 9.4.1 $R(D)$ 的下限 | 313 |
| 9.4.2 $R(D)$ 的上限 | 316 |
| 9.5 有失真时的离散无记忆信源编码定理 | 318 |
| 9.6 连续幅度无记忆信源 | 325 |
| 小结 | 328 |
| 习题 | 328 |
| 第 10 章 多用户信息论 | 331 |
| 10.1 多用户通信及多用户信道的分类 | 331 |
| 10.2 相关信源独立编码 | 335 |
| 10.3 相关源协同编码 | 341 |
| 10.4 多元接入信道(MAC) | 348 |
| 10.5 广播信道 | 355 |
| 小结 | 363 |
| 习题 | 364 |
| 参考文献 | 367 |

第 1 章 引 论

本章介绍通信系统模型、信息论研究的对象和基本方法。

1.1 通信系统模型

“信息论”或者称为“通信的数学理论”，是研究信息的传输、存储和处理的科学。通信的基本问题是在彼时(存储情况)或彼地(通信情况)精确地或近似地再现此时、此地发出的消息。信息论研究的主要问题是通信系统设计中如何实现有效性和可靠性。

各种通信系统(包括存储系统),如电报、电话、图像、计算机、导航、雷达乃至生物系统,虽然它们的形式和用途各不相同,但从信息传输、存储和处理的角度来看,本质上有许多共同之处。对有收发两端的单向传信系统,一般可概括为图 1.1.1 所示的模型。

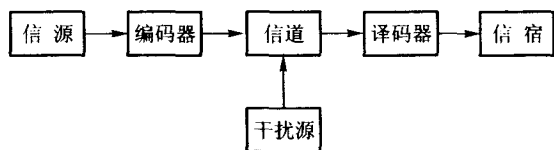


图 1.1.1 通信系统模型

信源是产生消息的源。消息可以是文字、语言、图像等,它可以是离散的,也可以是连续的,但都是随机发生的,即在收到这些消息之前不可能确切地知道它们的内容,否则通信将失去意义。可以用随机变量或随机过程来描述消息。信源研究的主要问题是消息的统计特性和信源产生信息的速率。

编码器是将信源发出的消息变换成适于信道传送的信号的设备。一般包含 3 个部分,即信源编码器、纠错编码器和调制器。信源编码器是在一定的准则下,对信源的输出进行变换,目的在于求得有效性;纠错编码器是对信源编码器的输出进行变换,用以提高对于信道干扰的抗击能力;调制器将信源编码器的输出变成适合于信道传输要求(带宽/波段、功率/通信时间等)的信号形式。不一定每个系统的编码器都含有这 3 个部分,有的只有其中的两个或一个组成部分,

也有的将其中的两个合并起来由一个组成部分实现。纠错编码器和调制器的组合又称做信道编码器,因为它们主要是针对信道的情况进行设计的,目的在于充分利用信道的传信能力可靠地传送信息,参看图 1.1.2。

信道是将信号从发端传送到收端的媒质或通道,它是包括收、发设备在内的物理设施。信道的种类很多,如架空明线、电缆、表面波、声纳、光束、电离层反射、对流层散射、卡片、磁盘、磁鼓、书籍等都可看做是信道。

干扰源是我们为了分析方便,将整个通信系统中各部分引入的各种干扰,如衰落、多径、码间干扰、非线性失真、可加噪声等都集中表示为一个方框作用于信道。这种干扰源的统计特性是划分信道的重要因素,并且是决定信道传输能力的决定因素。信道的中心课题是研究信道的统计特性和它的传信能力,即信道容量。实际干扰可分成两大类。一类是由外界引入的随机干扰,如天电干扰、设备内部的噪声,它们与信道输入信号统计无关,信道的输出就是输入和干扰的和,所以这种干扰又称之为加性干扰;另一类干扰是信号在传输过程中由于物理条件的变化(如温度、电离层位置随机变化等)引起信号参量(如频率色散、幅度衰减、相位偏移等)随机变化,此时信道的输出信号是输入与某些随机变量相乘的结果,所以又将这种干扰称之为乘性干扰。实现有效和可靠通信的主要困难是什么?是系统中的干扰。如何克服这类困难,也就是如何抗干扰是通信理论研究的中心课题。信息论要对干扰进行数学上的定量描述,以确定它们对传信能力影响的大小,从而给出有干扰下信道的传信能力。

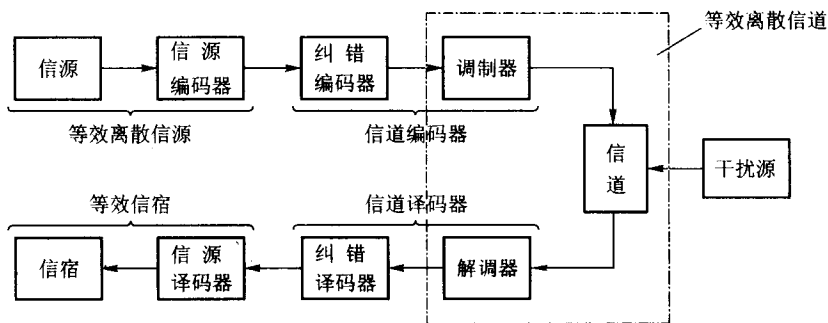


图 1.1.2 通信系统模型的细分

译码器是编码的逆变换,它要从受干扰的信号中最大限度地提取出有关信源输出消息的信息,应尽可能精确地恢复信源的输出,并将它们递送给信宿。中心问题是研究各种可实现的解调和译码方法。

信宿是信息的接收者,可以是人或物,且与信源处于不同地点或存在于不同

时刻。它要对传过来的消息提出可接受的条件,即提出一定的准则,发端将以此来确定对信源处理时所保留的最小信息量。至于信宿本身的主观因素,在 Shannon 信息论中不加过问。

系统的模型不是不变的,它根据实际情况而定。图 1.1.2 就是将图 1.1.1 中的编码器和译码器做了更细致的划分,目的是使信源编码的研究主要与信源及信宿发生关系,此时信道编码器、译码器和信道的组合可等效为一个离散无扰信道。而信道编码的研究可与信源、信宿无关,而只与信道有关,此时对于信道编码器来说信源和信源编码器组合成一个等效离散源,它的输出可近似地看成是无记忆、等概的数字序列。这种划分可使信源编码集中于解决传输的有效性,而信道编码则集中于解决抗信道干扰和失真问题,即解决传输可靠性问题,从而简化了研究。这样划分是否会对发挥通信系统的传信潜力有根本性的限制呢?研究表明,在很一般的条件下,对大多数理论结果没有太大限制。这样划分也不一定总是合理的,有时将信源编码和信道编码统一进行设计可能更有效些,有人已进行了这方面的探讨 [Davisson(1973)],如信源和信道联合编码、加密与纠错联合设计的研究。

图 1.1.1 和 1.1.2 给出的模型适用于两个用户(或终端)之间的单向通信情况。在网络通信情况下,可能有很多分开的信源、信道和信宿相互进行信息交换。为了研究网络通信系统中的信息传输和处理问题,要对上面给出的单路系统进行拓广,而引入多用户通信系统,并将单路通信的信息论发展成为多用户信息理论,这是由 Shannon 所开创的 [Shannon(1961)] 在 20 世纪的七八十年代得到广泛研究的信息论的一个新分支。本书第 10 章中将介绍其中的一些基本结果。

上面多次提到了信息、消息和信号,在结束本节时,我们想澄清这 3 个不同但又密切相关的概念。

信息是一种抽象的、存于具体消息(信息的载体)之中的东西。它是无形的,但是可以定量描述的(至少有些类信息是可以定量描述的),它又与具体信宿的接收消息空间有关。信息的产生、传送、接收、处理、存储等都离不开物质的运动,但它不是物质运动本身,而是借助于物质运动递送系统所关心的系统状态和变化的不确定性的。

信息、物质和能量被认为是构成一切系统的三大要素,信息是系统中传送(或存储、处理)的对象,它包含在消息之中。消息是比较具体的概念,但不是物理的,如语言、文字、数字、图像等。消息中载有信息,但同一信息可以由不同的消息载荷。例如,同一信息可以用不同类型的消息(语言、图像、文字等)表达。信号是表示消息的物理量,如电信号可通过幅度、频率、相位的变化表示不同的消息。可以用不同类型的信号,如声、光、电等信号传递同一消息。

1.2 Shannon 信息论的中心问题

Shannon 信息论的基本任务是为设计有效而可靠的通信系统提供理论依据。通信的基本目的是在接收端精确地或以给定的失真度重现信源的输出。信源编码器的作用是根据失真度准则对信源的输出进行划分,给每一类以不同的表示,即码字。信源译码器的任务是根据收到的信源表示恢复出信源所属的类。显然,精确度要求越高,失真度要求越低,对信源的划分就要越细,因而为表示信源所需的信息量或码长就越大。在给定信源和失真度条件下,要多大信息速率才行?或对给定信源保留一定的信息速率下,可以达到的最小失真是多少?这是信息论所关心的信源编码问题,也是通信“可行性”研究的一个问题。另一个问题是如何实现这一理论结果,即找出实际可行的信源编码和译码方法。

信息论研究的另一个主要问题是信道编码问题。它和信源编码问题类似,但它不是研究最有效地表示信源输出的,而是研究在保证信息传输可靠性(如错误概率小于给定值)的条件下最有效地利用信道的传信能力的。设送入信道的信息速率为 R ,信道容量为 C ,信道编码基本定理告诉我们,若 $R < C$,则可以将速率为 R 的信息以任意高的可靠性送至接收端;若 $R > C$,则不可能。这是信道编码和“可行性”问题。信道编码的另一个问题是寻找实际可行的编、译码方法。

信息论在研究信源和信道编码定理时所用的方法都是随机编码的方法,它是证明定理的重要工具,但为非构造性的,因此不能提供具体的可实现的编、译码方法。由 Hamming(1950)开始的可构造的编码理论在 20 世纪 50 年代末和 60 年代得到了很大的发展,成为信息论中的一个重要分支——纠错编码理论 [Peterson(1961)]。信源编码理论在 20 世纪 70 年代有了很大发展,形成速率失真理论 [Shannon (1959) 和 Berger (1971)] 和数据压缩技术 [Davisson & Gray (1976) 以及 Gilbert (1991)]。

上述信息论的基本问题在 Shannon(1948)的早期著作中都已系统地提出并给出了启发式的证明。Shannon 信息论的最大特点是将概率统计的观点和方法引入到通信理论研究中,揭示了通信系统中传送的对象是信息,并对信息给出科学的、定量的描述,指出通信系统设计的中心问题是在随机噪声干扰下如何有效而可靠地传送信息,实现这一目标的途径是编码(信源编码和信道编码),并且从理论上证明了可以达到的最佳性能限。

除了 Shannon 之外,在差不多同时,还有几位学者也明确地提出用统计观点研究信息问题。如统计学家 R. A. Fisher 从古典统计理论出发,给出了信息的定义 [Kullback (1959)]。N. Wiener(1948, 1949)从控制论和噪声中提取信息的最

佳滤波器设计角度研究信息。在通信理论中, Wiener 的过滤接收理论被看做是通信理论中的一个重要分支。V. A. Kotelnikov(1956)也用概率统计的方法研究接收信号的检测与估值、模拟调制和数字调制信号的最佳解调问题,这一方向被称做是最佳接收理论。Shannon 的信息论是从整个通信系统的最佳化来研究信息的传送和处理问题的。Shannon 信息论研究的是消息或数据的群体行为,而不是孤立的个别消息或数据的行为,正如我们从宏观来看物质或材料时,我们所关心的是大量原子或分子的群体行为一样。

当我们关心个别消息的传输问题时,或当我们不掌握整个消息空间的统计特性时,我们就需要求助于其他的信息定义或理论了。

在同一时期有这样多的学者都以概率统计的观点研究信息的产生、传送和处理,发表了具有划时代意义的著作,这绝非偶然的事,它是通信理论和通信技术发展的必然结果。有关信息产生和发展的情况可参阅 Cherry(1951)、Pierce(1973)、Slepain(1973)、Viterbi(1973)、Wyner(1974)、Wolf(1973)、Kotz(1966)、Dobrushin(1961,1972)、Price(1984)、池田止戈夫 & 广田修(1983)、Ephremides & Messey(1998)、Verdú(1998)、Gallager(2001)、Shannon(1993)以及 Liversidge(1991)等。

1.3 Shannon 信息论的局限性

1948年,Shannon 在其著名的“通信的数学理论”论文中不仅系统地总结和高度概括了人类对于通信的认识,而且为通信的发展照亮了前进的道路,指出了实现有效而可靠通信的必由之路是数字化和编码。通信的数学理论成为几十年来数字化革命的理论基础,在推动人类步入信息化社会的进程中起了巨大的推动作用。

但几十年来信息论的理论发展和实际应用走过了曲折而艰辛的道路。信息论时而表现出充满活力,欣欣向荣;时而又显得对实际通信问题束手无策,令年轻学子感到心寒和畏惧,使人远离它而显得冷清。在学术界,信息论的“死”与“活”的争论一直存在着。究其根本原因,可以从 Shannon 的通信系统模型上来认识。Shannon 的模型是很理想的抽象,它既高度概括了实际中各类通信系统的本质,又远远不能面面俱到地刻画人类的实际通信问题。

1. 信源框

Shannon 的通信系统模型将信源用一个框表示,引入概率统计工具来描述信源产生消息的规律,如用简单概率空间、平稳过程、各态历经过程、有限阶马氏过程等。如果实际信源确如这种数学描述,那么这种方法就应该是有效地、确切地表述了实际信源,否则这种表述只能是近似的,甚至是根本无效的。