



教育部高等学校电子信息类专业教学指导委员会规划教材

高等学校电子信息类专业系列教材

普通高等教育“十五”国家级规划教材

“十二五”江苏省高等学校重点教材



信息与通信工程

**I**nformation Theory and Coding  
(Third Edition)

# 信息论与编码

(第3版)

曹雪虹 张宗橙 编著

Cao Xuehong Zhang Zongcheng



清华大学出版社





教育部  
类专业教学指导委员会规划教材  
高等学校电子信息类专业系列教材



普通高等教育“十五”国家级规划教材

“十二五”江苏省高等学校重点教材

(2014-1-134)

Information Theory and Coding  
(Third Edition)

# 信息论与编码

(第3版)

曹雪虹 张宗橙 编著

Cao Xuehong Zhang Zongcheng

清华大学出版社  
北京

## 内 容 简 介

本书重点介绍由香农理论发展而来的信息论的基本理论以及编码的理论和实现原理。全书分8章,在介绍有关信息度量的基础上,重点讨论信源熵、信道容量、率失真函数,以及无失真信源编码、限失真信源编码、信道编码和加密编码中的理论知识及其实现原理,还简单介绍了网络信息理论。

本书注重概念,采用通俗的文字,联系目前实际通信系统,用较多的例题和图示阐述基本概念、基本理论及实现原理,尽量减少繁杂的公式定理证明。在各章的最后还附有内容小结和大量习题,书后附有部分习题答案,便于读者学习,加深对概念和原理的理解。

本书可作为理工科高等院校信息工程、通信工程及相关专业的本科生教材,也可供信息、通信、电子工程等有关专业的科技人员作为参考书。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

### 图书在版编目(CIP)数据

信息论与编码/曹雪虹,张宗橙编著.—3版.—北京:清华大学出版社,2016

高等学校电子信息类专业系列教材

ISBN 978-7-302-44019-2

I. ①信… II. ①曹… ②张… III. ①信息论—高等学校—教材 ②信源编码—高等学校—教材  
IV. ①TN911.2

— 中国版本图书馆 CIP 数据核字(2016)第 123386 号

责任编辑:文 怡

封面设计:李召霞

责任校对:梁 毅

责任印制:宋 林

出版发行:清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址:北京清华大学学研大厦 A 座 邮 编:100084

社 总 机:010-62770175 邮 购:010-62786544

投稿与读者服务:010-62776969, [c-service@tup.tsinghua.edu.cn](mailto:c-service@tup.tsinghua.edu.cn)

质量反馈:010-62772015, [zhiliang@tup.tsinghua.edu.cn](mailto:zhiliang@tup.tsinghua.edu.cn)

课件下载: <http://www.tup.com.cn>, 010-62795954

印 装 者:北京密云胶印厂

经 销:全国新华书店

开 本:185mm×260mm 印 张:15.75 字 数:392千字

版 次:2004年3月第1版 2016年6月第3版 印 次:2016年6月第1次印刷

印 数:1~3000

定 价:39.00元

产品编号:068920-01

# 再版说明

本教材于2004年3月首次出版,于2009年2月再版,是普通高等教育“十五”国家级规划教材,入选“十二五”江苏省高等学校重点教材。

随着电子信息类本科专业在全国高校中开设的数量不断增加,“信息论与编码”作为这些专业必修的核心课程,教材的需求量不断上升,销售面不断扩大,教材目前已被国内包括985、211高校在内的200多所高校采用,累计印刷26次,累计销售超过15万册。

十多年来,我们得到了广大教师和同学们的热诚关心和帮助,他们对教材提出了许多宝贵的意见和建议,在此表示衷心的感谢。为了紧跟科学技术和信息理论的飞速发展,我们对教材的内容进行了部分增减,对某些不妥之处进行了修改完善,形成了第3版。

真诚欢迎广大读者对书中的错误和不当之处予以批评指正。

编者

2016年3月

# 前言

## FOREWORD

当前信息产业发展很快,需要大量从事信息、通信、电子工程类专业的人才,而“信息论与编码”是这些专业的基础,必须掌握,它可以指导理论研究和工程应用。

由于“信息论与编码”介绍的是信息论基础和编码理论,内容本身理论性很强,本书针对电子信息类相关专业的本科生及相关专业的工程技术人员,重点介绍有关信息理论的基本知识,注重基本概念,用较通俗的文字解释其物理意义,辅以大量的例题和图示说明,并且联系当前实际通信技术来讲述,使读者研读本书后概念清晰,有目标地应用在实际工作中。

本书共分8章,第1章是绪论。第2章介绍信息论的一些基本概念,包括自信息量、互信息量、离散信源熵、熵的性质以及连续信源熵、最大熵定理等,对信源的信息给出定量描述,并解释冗余度的由来及作用。这一章是后续章节的基础。

第3章介绍信道的分类及其表示参数,讨论各种信道能够达到的最大传输速率,即信道的容量及其计算方法。

第4章介绍失真函数和信息率失真函数的定义及性质,给出在一定失真限度内信源必须输出的最小传输速率。

第5章介绍信源编码,首先给出无失真信源编码定理和限失真信源编码定理,其中无失真信源编码定理包括定长编码定理和变长编码定理,并详细阐述最佳无失真编码中的香农码和哈夫曼码的编码方法及其性能比较。最后简单提及常用的几种信源编码方法。

第6章介绍信道编码,在阐述信道编码定理、差错控制与信道编译码的基本原理之后,详细介绍最基本,也是最常用的几种信道编码方法,包括线性分组码、卷积码、级联码等。

第7章在介绍密码体制的基础知识及其与熵的关系后,简述具有代表性的秘密密钥加密算法 DES、IDEA 和公开密钥加密算法 RSA、MD5 等,还引入信息安全性概念以及数字签名、防火墙等技术。

第8章简单介绍网络信息理论,包括网络信道的分类、多址接入信道的容量和相关信源编码等。

本书由曹雪虹主编。第6章由张宗橙编写,其余各章由曹雪虹编写。在编写过程中,得到了徐澄圻教授、胡建彰教授的大力帮助,在此表示衷心的感谢。

限于编者的水平,书中不妥或谬误之处在所难免,殷切希望读者指正。

编者

2016年3月

# 目 录

## CONTENTS

第 1 章 绪论	1
1.1 信息论的形成和发展	1
1.2 信息理论研究的内容	2
1.3 通信系统的模型	4
1.4 信息论的应用	7
思考题	10
第 2 章 信源与信息熵	11
2.1 信源的描述与分类	11
2.1.1 无记忆信源	11
2.1.2 有记忆信源	13
2.1.3 马尔可夫信源	14
2.2 离散信源熵和互信息	20
2.2.1 自信息量	20
2.2.2 离散信源熵	22
2.2.3 互信息	26
2.2.4 数据处理中信息的变化	30
2.2.5 相对熵	32
2.2.6 熵的性质	32
2.3 离散序列信源的熵	35
2.3.1 离散无记忆信源的序列熵	35
2.3.2 离散有记忆信源的序列熵	36
2.4 连续信源的熵和互信息	40
2.4.1 幅度连续的单个符号信源熵	40
2.4.2 波形信源的熵	42
2.4.3 最大熵定理	42
2.5 信源的冗余度	43
本章小结	45
习题	47

<b>第 3 章 信道与信道容量</b> .....	52
3.1 信道的基本概念 .....	52
3.1.1 信道的分类 .....	52
3.1.2 信道的数学模型 .....	53
3.1.3 信道容量的定义 .....	56
3.2 离散单个符号信道及其容量 .....	57
3.2.1 无干扰离散信道 .....	57
3.2.2 对称离散无记忆信道 .....	58
3.2.3 准对称离散无记忆信道 .....	61
3.2.4 一般离散无记忆信道 .....	63
3.3 离散序列信道及其容量 .....	64
3.4 连续信道及其容量 .....	66
3.4.1 连续单符号加性信道 .....	66
3.4.2 多维无记忆加性连续信道 .....	67
3.4.3 限时限频限功率加性高斯白噪声信道 .....	70
3.5 多输入多输出信道及其容量 .....	72
3.5.1 MIMO 信道模型 .....	72
3.5.2 MIMO 信道容量 .....	73
3.6 信源与信道的匹配 .....	74
本章小结 .....	75
习题 .....	76
<b>第 4 章 信息率失真函数</b> .....	79
4.1 信息率失真函数的概念和性质 .....	79
4.1.1 失真函数和平均失真 .....	79
4.1.2 信息率失真函数 $R(D)$ .....	81
4.1.3 信息率失真函数的性质 .....	83
4.1.4 信息率失真函数与信道容量 .....	87
4.2 离散信源和连续信源的 $R(D)$ 计算 .....	87
本章小结 .....	90
习题 .....	90
<b>第 5 章 信源编码</b> .....	92
5.1 编码的概念 .....	93
5.2 无失真信源编码定理 .....	95
5.2.1 定长编码 .....	96
5.2.2 变长编码 .....	98
5.3 限失真信源编码定理 .....	102

5.4 常用信源编码方法简介 .....	103
5.4.1 哈夫曼编码 .....	103
5.4.2 算术编码 .....	108
5.4.3 LZ 编码 .....	111
5.4.4 游程编码 .....	112
5.4.5 矢量量化编码 .....	114
5.4.6 预测编码 .....	115
5.4.7 变换编码 .....	117
本章小结 .....	120
习题 .....	121
<b>第 6 章 信道编码</b> .....	<b>124</b>
6.1 有扰离散信道的编码定理 .....	124
6.1.1 差错和差错控制系统分类 .....	124
6.1.2 矢量空间与码空间 .....	128
6.1.3 随机编码 .....	130
6.1.4 信道编码定理 .....	132
6.1.5 联合信源信道编码定理 .....	134
6.2 纠错编译码的基本原理与分析方法 .....	137
6.2.1 纠错编码的基本思路 .....	137
6.2.2 译码方法——最优译码与最大似然译码 .....	140
6.3 线性分组码 .....	142
6.3.1 线性分组码的生成矩阵和校验矩阵 .....	142
6.3.2 伴随式与标准阵列译码 .....	145
6.3.3 码距、纠错能力、MDC 码及重量谱 .....	149
6.3.4 完备码 .....	151
6.3.5 循环码 .....	153
6.4 卷积码 .....	157
6.4.1 卷积码的基本概念和描述方法 .....	157
6.4.2 卷积码的最大似然译码——维特比算法 .....	163
6.4.3 卷积码的性能限与距离特点 .....	170
本章小结 .....	173
习题 .....	173
<b>第 7 章 加密编码</b> .....	<b>176</b>
7.1 加密编码的基础知识 .....	176
7.1.1 加密编码中的基本概念 .....	176
7.1.2 加密编码中的熵概念 .....	179
7.2 数据加密标准(DES) .....	181



7.2.1	换位和替代密码	181
7.2.2	DES 密码算法	183
7.2.3	DES 密码的安全性	186
7.2.4	DES 密码的改进	188
7.3	国际数据加密算法	189
7.3.1	算法原理	190
7.3.2	加密解密过程	190
7.3.3	算法的安全性	192
7.4	公开密钥加密法	192
7.4.1	公开密钥密码体制	193
7.4.2	RSA 密码体制	194
7.4.3	报文摘要	196
7.4.4	公开密码体制的优缺点	199
7.5	通信网络中的加密	200
7.5.1	模拟通信加密	200
7.5.2	数字通信加密	200
7.6	信息安全和确认技术	202
7.6.1	信息安全的基本概念	202
7.6.2	数字签名	203
7.6.3	防火墙	205
7.6.4	密码学的应用实例	206
	本章小结	209
	习题	209
<b>第 8 章</b>	<b>网络信息理论简介</b>	<b>211</b>
8.1	概论	211
8.2	网络信道的分类	212
8.3	网络信道的信道容量域	214
8.3.1	离散多址接入信道	214
8.3.2	高斯多址接入信道	218
8.3.3	广播信道	220
8.4	网络中相关信源的信源编码	221
8.4.1	相关信源编码	221
8.4.2	具有边信息的信源编码	224
	本章小结	227
	习题	227
<b>附录</b>	<b>本书所用主要符号及含义</b>	<b>230</b>
	<b>部分习题参考答案</b>	<b>232</b>
	<b>参考文献</b>	<b>241</b>



科学技术的发展使人类跨入了高速发展的信息化时代。在政治、军事、经济等各个领域,信息的重要性不言而喻,有关信息理论的研究正越来越受到重视。

人们在自然和社会活动中,获取信息并对其进行传输、交换、处理、检测、识别、存储、显示等操作,研究这些内容的科学就是信息科学。信息论(information theory)是信息科学的主要理论基础之一,它主要研究可能性和存在性问题,为具体实现提供理论依据。与之对应的是信息技术(information technology),它主要研究怎样实现的问题。

本章首先介绍信息论的形成和发展、信息论研究的内容及信息的基本概念,接着结合通信系统模型介绍模型中各部分的作用、编码的种类和研究内容,最后介绍信息论的应用。

### 1.1 信息论的形成和发展

信息论理论基础的建立,一般来说开始于香农(Shannon)在研究通信系统时所发表的论文。随着研究的深入与发展,信息论有了更为宽广的内容。

信息在早些时期的定义是由奈奎斯特(Nyquist)和哈特利(Hartley)在 20 世纪 20 年代提出来的。1924 年奈奎斯特解释了信号带宽和信息速率之间的关系;1928 年哈特利最早研究了通信系统传输信息的能力,给出了信息度量方法;1936 年阿姆斯特朗(Armstrong)提出了增大带宽可以加强抗干扰能力。这些工作都给香农很大的影响,他在 1941—1944 年对通信和密码进行深入研究,并用概率论的方法研究通信系统,揭示了通信系统传递的对象就是信息,并对信息给以科学的定量描述,提出了信息熵的概念。他还指出通信系统的中心问题是在噪声下如何有效而可靠地传送信息,而实现这一目标的主要方法是编码等。这一成果于 1948 年以 *A mathematical theory of communication* (通信的数学理论)为题公开发表,这是一篇关于现代信息论的开创性的权威论文,为信息论的创立作出了独特的贡献,香农因此成为信息论的奠基人。

20 世纪 50 年代信息论在学术界引起了巨大的反响。1951 年美国 IRE 成立了信息论组,并于 1955 年正式出版了信息论汇刊。20 世纪 60 年代信道编码技术有了较大进展,成

为信息论的又一重要分支。信道编码技术把代数方法引入纠错码的研究,使分组码技术发展到了高峰,找到了大量可纠正多个错误的码,而且提出了可实现的译码方法。20世纪70年代卷积码和概率译码有了重大突破,提出了序列译码和Viterbi译码方法,并被美国卫星通信系统采用,这使香农理论成为真正具有实用意义的科学理论。1982年温伯格(Ungerboeck)提出了将信道编码和调制结合在一起的网格编码调制方法,该方法无需增大带宽和功率,以增加设备的复杂度换取编码增益,受到了广泛关注,在目前的通信系统中占据统治地位。

信源编码的研究落后于信道编码。香农在1948年的论文中提出了无失真信源编码定理,也给出了简单的编码方法——香农码。1952年费诺(Fano)和哈夫曼(Huffman)分别提出了各自的编码方法,并证明其方法都是最佳编码法。1959年香农的文章*Coding theorems for a discrete source with a fidelity criterion*(保真度准则下的离散信源编码定理)系统地提出了信息率失真理论和限失真信源编码定理。这两个理论是数据压缩的数学基础,为各种信源编码的研究奠定了基础。1971年伯格(Berger)给出了更一般性的率失真编码定理。随着传输内容和传输信道的发展,人们针对各种信源的特性,提出了大量实用高效的信源编码方法。

到20世纪70年代,有关信息论的研究,从点与点间的单用户通信推广发展到多用户系统的研究。1972年盖弗(Cover)发表了有关广播信道的研究,以后陆续进行了有关多接入信道和广播信道模型及其信道容量的研究。近40多年来,这一领域的研究活跃,大量的论文被发表,使多用户信息论的理论日趋完整。

此外,香农在1949年发表了论文“保密通信的信息理论”,首先用信息论的观点对信息保密问题作了全面的论述。但由于通信保密研究当时主要用于政府和军方,成果很少对外公布,因此公开发表的论文也很少。直到1976年迪弗(Diffie)和海尔曼(Hellman)发表了论文“密码学的新方向”,提出了公钥密码体制之后,保密通信问题才得到公开、广泛的研究。尤其是现在,信息安全已成为一个关系到信息产业发展的重大问题。因此,密码学以及信息安全已经成为各国科学家研究的重点和热点。

可见,信息论主要研究的是通信的一般理论,在信息可以量度的基础上,研究有效地、可靠地、安全地传递信息的科学,它涉及信息量度、信息特性、信息传输速率、信道容量、干扰对信息传输的影响等方面的知识。

## 1.2 信息理论研究的内容

信息理论是信息科学的基础,强调用数学语言来描述信息科学中的共性问题及解决方案。目前,这些共性问题分别集中在狭义信息论、一般信息论和广义信息论中。

狭义信息论主要总结了香农的研究成果,因此又称为香农信息论。它在信息可以度量的基础上,研究如何有效、可靠地传递信息。有效、可靠地传递信息必然贯穿于通信系统从信源到信宿的各个部分,狭义信息论研究的是收、发端联合优化的问题,而重点在各种编码。它是通信中客观存在的问题的理论提升。

一般信息论研究从广义的通信引出的基础理论问题,除了香农信息论外,还包括其他人

的研究成果,其中最主要的是维纳(Wiener)的微弱信号检测理论。微弱信号检测又称最佳接收,是为了确保信息传输的可靠性,研究如何从噪声和干扰中接收信道传输的信号的理论。它主要研究两个方面的问题:从噪声中去判决有用信号是否出现和从噪声中去测量有用信号的参数。该理论应用近代数理统计的方法来研究最佳接收的问题,系统和定量地综合出存在噪声和干扰时的最佳接收机结构,并推导出这种系统的极限性能。除此之外,一般信息论的研究还包括噪声理论、信号滤波与预测、统计检测与估计理论、调制理论、信号处理与信号设计理论等。可见它总结了香农、维纳以及其他学者的研究成果,是广义通信中客观存在的问题的理论提升。

无论是狭义信息论还是一般信息论,讨论的都是客观问题,然而,当讨论信息的作用、价值等问题时,必然涉及主观因素。广义信息论研究包括所有与信息有关的领域,如心理学、遗传学、神经生理学、语言学、社会学等。因此,有人对信息论的研究内容进行了重新界定,提出从应用性、实效性、意义性或者从语法、语义、语用方面来研究信息,分别与事件出现的概率、含义及作用有关,其中意义性、语义、语用主要研究信息的意义和对信息的理解,即信息所涉及的主观因素。广义信息论从人们对信息特征的理解出发,从客观和主观两个方面全面地研究信息的度量、获取、传输、存储、加工处理、利用以及功用等,理论上说是最全面的信息理论,但由于主观因素过于复杂,很多问题本身及其解释尚无定论,或者受到人类知识水平的限制目前还得不到合理的解释,因此广义信息论还处于正在发展的阶段。

信息在传输、存储和处理的过程中,不可避免地要受到噪声或其他无用信号的干扰,信息理论就是为了可靠、有效地从数据中提取信息,提供必要的根据和方法。这就必须研究噪声和干扰的性质以及它们与信息本质上的差别,噪声与干扰往往具有按某种统计规律的随机特性,信息则具有一定的概率特性,如度量信息量的熵值就是概率性质的。因此,信息论、概率论、随机过程和数理统计学,就是信息论应用的基础和工具。

本书讲述的信息理论的基本内容是与通信科学密切相关的狭义信息论,涉及信息理论中很多基本问题。例如:

- (1) 什么是信息? 如何度量信息?
- (2) 在信息传输中,基本的极限条件是什么?
- (3) 对于信息的压缩和恢复的极限条件是什么?
- (4) 从环境中抽取信息的极限条件是什么?
- (5) 设计怎样的设备才能达到这些极限?
- (6) 实际上接近极限的设备是否存在?

信息论主要应用在通信领域,在含噪信道中传输信息的最优方法到今天还不是十分清楚,特别是在数据的信息量大于信道容量的情况下更是一无所知,这是经常遇到的情况。因为从信源提取的信息常常是连续的,即信号的信息含量为无限大。在一般信道中传输这样的信号不可能不产生误差的。引入信道容量和信息量的概念以后,这类问题便可以得到满意的解释,并可给出最佳效果的通信系统。因而信息论为设计这样的系统提供了理论依据。

在通信理论中经常会遇到信息、消息和信号这3个既有联系又有区别的名词,下面将对它们定义并作比较。

信息是指各个事物运动的状态及状态变化的方式。人们从对周围世界的观察得到的数据中获得信息。信息是抽象的意识或知识,它是看不见、摸不到的。当由人脑的思维活动产

生的一种想法仍被存储在脑子里时,它就是一种信息。

**消息**是指包含信息的语言、文字和图像等,例如我们每天从报纸、电视节目和互联网中获得的各种新闻及其他消息。在通信中,消息是指担负着传送信息任务的单个符号或符号序列。这些符号包括字母、文字、数字和语言等。单个符号消息的情况,例如用  $x_1$  表示晴天,  $x_2$  表示阴天,  $x_3$  表示雨天; 符号序列消息的情况,例如“今天是晴天”这一消息由 5 个汉字构成。可见消息是具体的,它载荷信息,但它不是物理性的。

**信号**是消息的物理体现,为了在信道上传输消息,就必须把消息加载(调制)到具有某种物理特征的信号上去。信号是信息的载荷子或载体,是物理性的,如电信号、光信号等。

在通信系统中传送的本质内容是信息,发送端需将信息表示成具体的消息,再将消息载至信号上,才能在实际的通信系统中传输。信号到了接收端(信息论中称为信宿)经过处理变成文字、语音或图像等形式的消息,人们再从中得到有用的信息。在接收端将含有噪声的信号经过各种处理和变换,从而取得有用信息的过程就是信息提取,提取有用信息的过程或方法主要有检测和估计两类。载有信息的可观测、可传输、可存储及可处理的信号,均称为数据。

信息的基本概念在于它的不确定性,任何已确定的事物都不含有信息。信息的特征有:

- (1) 接收者在收到信息之前,对其内容是未知的,所以信息是新知识、新内容;
- (2) 信息是能使认识主体对某一事物的未知性或不确定性减少的有用知识;
- (3) 信息可以产生,也可以消失,同时信息可以被携带、存储及处理;
- (4) 信息是可以量度的,信息量有多少的差别。

各类通信系统,如电话、广播、电视、雷达、遥测等传送的是各种各样的消息。消息的形式可以不同,但它们都是能被传递的,能被人们感觉器官(眼、耳、触觉等)所感知的,而且消息表述的是客观物质和主观思维的运动状态或存在状态。在各种通信系统中,其传输的形式是消息。但消息传递过程的一个最基本、最普通却又不十分引人注意的特点是:收信者在收到消息以前不知道消息的具体内容。在收到消息以前,收信者无法判断发送者将会发来描述何种事物运动状态的具体消息;他更无法判断是描述这种状态还是那种状态。再者,即使收到消息,由于干扰的存在,他也不能断定所得到的消息是否正确和可靠。总之,收信者存在着“不知”、“不确定”或“疑问”。通过消息的传递,收信者知道了消息的具体内容,原先的“不知”、“不确定”和“疑问”消除或部分消除了。因此,对收信者来说,消息的传递过程是一个从不知到知的过程,或是从知之甚少到知之甚多的过程,或是从不确定到部分确定或全部确定的过程。如果不具备这样的特点,那就根本不需要通信系统了。试想,如果收信者在接到电话之前就已经知道电话的内容,那还要电话系统干什么呢?

### 1.3 通信系统的模型

图 1-1 是目前较常用的、也较完整的通信系统物理模型。下面介绍模型中各部分的作用及需要研究的核心问题。

#### 1. 信源

信源是向通信系统提供消息  $u$  的人和机器。信源本身十分复杂,在信息论中我们仅对

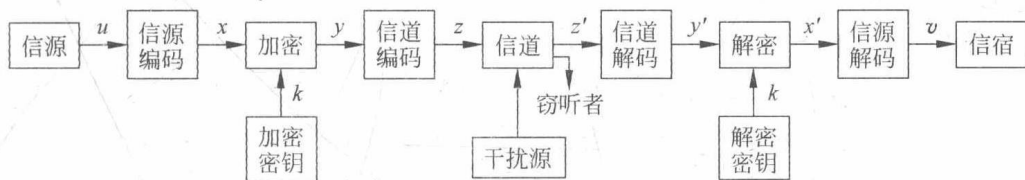


图 1-1 通信系统的物理模型

信源的输出进行研究。信源输出的是以符号形式出现的具体消息，它载荷信息。信源输出的消息可以有多种形式，但可归纳成两类：离散消息，例如由字母、文字、数字等符号组成的符号序列，或者单个符号；连续消息，例如语音、图像和在时间上连续变化的电参数等。因为通信系统的接收者（信宿）在收到消息之前并不知道信源所发出消息的内容，所以一般地说信源发出的是随机性的消息。但因信源发出的消息都携带着信息，消息的变化具有一定规律性，因此严格地说信源发出的消息并不是完全随机性的。信源的核心问题是它包含的信息到底有多少，怎样将信息定量地表示出来，即如何确定信息量。

## 2. 信宿

信宿是消息传递的对象，即接收消息的人或机器。根据实际需要，信宿接收的消息  $v$  的形式可以与信源发出的消息  $u$  相同，也可以不相同，当两者形式不相同， $v$  是  $u$  的一个映射。信宿需要研究的问题是能收到或提取多少信息。

## 3. 信道

信道是传递消息的通道，又是传送物理信号的设施。信道可以是一对导线、一条同轴电缆、传输电磁波的空间、一条光纤等传输信号的介质。信道的问题主要是它能够传送多少信息，即信道容量的大小。

## 4. 干扰源

干扰源是整个通信系统中各个干扰的集中反映，用来表示消息在信道中传输时遭受干扰的情况。对于任何通信系统而言，干扰的性质和大小是影响系统性能的重要因素。

## 5. 密钥源

密钥源是产生密钥  $k$  的源。信道编码器输出信号  $x$  经过  $k$  的加密运算后，就把明文  $x$  变换为密文  $y$ 。若窃听者未掌握发送端采用的密钥  $k$ ，则很难从窃听到的信号  $z'$  解出明文  $x$ 。而接收端的信宿因知道事先已约定好的密钥  $k$ ，因此能从收到的信号  $z'$  中解出明文  $x$ 。对于二进制的代码而言，加密相当于  $y = z \oplus p$  运算（其中序列  $p$  通常是受密钥控制的伪随机序列），而解密则相当于  $x' = y' \oplus p$  运算。这里  $x'$ 、 $y'$ 、 $z'$  之所以不同于发送端的  $x$ 、 $y$ 、 $z$ ，是因为考虑到信号  $z$  在信道中传输时所受到的干扰影响。但在正常通信条件下，总会有  $x' \approx x$ 、 $y' \approx y$ 、 $z' \approx z$  的结果。

一般地说，通信系统的性能指标主要是有效性、可靠性、安全性和经济性。通信系统优化就是使这些指标达到最佳。除了经济性外，这些指标正是信息论的研究对象，可以通过各种编码处理来使通信系统的性能最优化。根据信息论的各种编码定理和上述通信系统的指标，编码问题可分解为三类：信源编码、信道编码和加密编码。

### 1. 信源编码

信源编码器的作用有两个，一是把信源发出的消息变换成由二进制码元（或多进制码

元)组成的代码组,这种代码组就是基带信号;另一个作用是通过信源编码可以压缩信源的冗余度(即多余度),以提高通信系统传输消息的效率。信源编码可分为无失真信源编码和限失真信源编码。前者适用于离散信源或数字信号;后者主要用于连续信源或模拟信号,如语音、图像等信号的数字处理。从提高通信系统的有效性意义上说,信源编码器的主要指标是其编码效率,即理论上所需的码率与实际达到的码率之比。一般来说,效率越高,编译码器的代价也将越大。信源译码器的作用是把信道译码器输出的代码组转换成信宿所需要的消息形式,它的作用相当于信源编码器的逆过程。

## 2. 信道编码

信道编码器的作用是在信源编码器输出的代码组上有目的地增加一些监督码元,使之具有检错或纠错的能力。信道译码器具有检错或纠错的功能,它能对落在其检错或纠错范围内的错传码元进行检错或纠错,以提高传输消息的可靠性。信道编码包括调制解调和纠错检错编译码。信道中的干扰常使通信质量下降,对于模拟信号,表现在收到的信号的信噪比下降;对于数字信号,就是误码率增大。信道编码的主要方法是增大码率或频带,即增大所需的信道容量。这恰与信源编码相反。

## 3. 加密编码

加密编码是研究如何隐蔽消息中的信息内容,以便它在传输过程中不被窃听,提高通信系统的安全性。将明文变换成密文,通常不需要增大信道容量,例如在二进码信息流上叠加一密钥流。但也有些密码要求占用较大的信道容量。

在实际问题中,上述三类编码应统一考虑,以提高通信系统的性能。这些编码的目标往往是相互矛盾的。提高有效性必须去掉信源符号中的冗余部分,此时信道误码会使接收端不能恢复原来的信息,这就需要相应提高传送的可靠性,不然会使通信质量下降;反之,为了可靠而采用信道编码,往往需扩大码率,也就降低了有效性。安全性也有类似情况。编成密码,有时需扩展码位,这样就降低了有效性;有时也会因收、发两端不同步而使授权用户无法获得信息,必须重发而降低有效性,或丢失信息而降低可靠性。从理论上说,若能把3种编码合并成一种码来编译,即同时考虑有效性、可靠性和安全性,可使编译码器更理想化,在经济上也可能更优越。这种三码合一的设想是当前众所关心的课题;但从理论上和技术上的复杂性看,要取得有用的结果,还是相当困难的。值得注意的是,信息论分析的问题是存在性问题,即符合条件的编码是否存在,但并没有给出寻找编码的方法。

本书讨论编码问题,着重介绍信源和信道的编码定理。限于课时,主要从概念上解释这些定理的结论,并没有从严格意义上加以证明。而对于加密编码,仅介绍了保密通信中的一些基本知识。这里首先举几个例子来说明编码的应用,例如电报常用的摩尔斯(Morse)码就是按信息论的基本编码原则设计出来的。又如,在一些商品上面有一张由粗细条纹组成的标签,从这张标签可以得知该商品的生产厂家、生产日期和价格等信息,这些标签是利用条形码设计出来的,非常方便,非常有用,应用越来越普遍。再如,计算机的运算速度很高,又要保证它几乎不出差错,相当于要求它在100年的时间内不得有一秒钟的误差,这就需要利用纠错码来自动、及时地纠正所发生的错误。每出版一本书,都给定一个国际标准书号(ISBN),这大大方便了图书的销售、编目和收藏工作。可以说,人们在日常生活和生产实践中,正在越来越多地使用编码技术。

顺便指出:不是所有的通信系统都采用如图1-1所示的那样全面的技术。例如点对点

的有线电话,只要有一对电话机和一条电话线路(铜线)就够了,语音基带信号通过电话机变成相应的电信号(模拟信号),就能在电话线上传送。接收端的电话机再把电信号恢复成人耳能听得清的语音。如果是点对点的无线电话,则在发送端需要一台发信机,把模拟信号调制到射频上,再用大功率发射机经天线发射出去,然后在无线信道中传输。在接收端则应使用收音机把收到的调制射频信号解调恢复为发送端的原始语音。若在这样的系统中增加加密和解密装置,就构成无线保密通信系统。在干扰大、信道容量有限的通信系统中,需要采用信源编码和信道编码技术,以提高传输消息的有效性和可靠性。

## 1.4 信息论的应用

信息论从它诞生的那时起就吸引了众多领域学者的注意,他们竞相应用信息论的概念和方法去理解和解决本领域中的问题。例如,信息论在生物学、医学、经济、管理、图书情报等领域都有不同程度的应用,这使信息论成为一门新兴的横断科学。在这里,简要介绍一下信息论在生物学、医学、管理科学、经济学中的应用。

### 1. 信息论在生物学中的应用

生命体本身是一个复杂的信息传递、存储、处理、加工和控制的系统。理论上说,信息论应该与生物学有着密切关系。近几十年来,生物学的发展非常迅速,人们对生命现象的研究,已经从整体深入到细胞、亚细胞、分子水平和量子水平上,以揭示生命现象的本质。尤其是在遗传信息方面的研究取得了重大进展和成效,从此确立了信息论在生物学研究方面的重要作用和地位。

特别是20世纪90年代以来,伴随着分子结构测定技术的突破和各种基因组测序计划的展开,生物学数据大量出现,如何分析这些数据,从中获得生物结构、功能的相关信息成为困扰生物学家的一个难题。生物信息学就是在此背景下发展起来的综合运用生物学、数学、统计学、物理学、化学、信息科学以及计算机科学等诸多学科的理论和方法的前沿和交叉学科。

目前,国际上公认的生物信息学的研究内容大致包括以下几个方面:

- (1) 生物信息的收集、储存、管理和提供;
- (2) 基因组序列信息的提取和分析;
- (3) 功能基因组相关信息分析;
- (4) 生物大分子结构模拟和药物设计;
- (5) 生物信息分析的技术与方法研究;
- (6) 应用与发展研究。

### 2. 信息论在医学中的应用

医学是研究人的生命活动的本质,研究疾病发生发展的规律,研究诊断和防治疾病,恢复和保护人的身体健康的科学。信息论在医学上的应用,大大促进了医学的现代化。

从信息论的观点看,有机体不断接收与输出信息,以维持正常的生命活动。在有机体中,信息熵标志着系统组织结构复杂的有序状态,由于新陈代谢的作用,有机体内部有序结构不断遭到破坏,这时熵增加,反之机体不断从外界接收信息——负熵,在机体内合成高度



的有序结构,使熵降低。因此运用信息理论来分析生命系统,可以把生命系统看作是接收信息和传递信息的调节控制系统。

在正常的无疾病的有机体系统中,信息的接收、传递、输出均有正常的秩序,各个环节有着正常的对应关系。人体机能的控制调节,也是通过信息的传输交换过程来实现的。在正常情况下,信息是畅通无阻的。人在生病时,信道发生堵塞,信息产生异常,例如:有内分泌疾病时就会使正常信息缺乏,当有细菌侵入人体时就会受异常信息干扰;当信息代码有错乱或信息通信发生堵塞时,机体就会失去控制能力。必须查出是哪方面的信息异常,确定如何排除干扰,恢复机体系统的信息的正常流通及接收信息等功能,保证信息通畅无阻。诊断是信息的收集、分析、综合、作出判断后对症下药的过程。这一切都是为了得到更多的信息,使信息流通,把原来看不见听不到的信息转变为人类感官所能接收的信息。

治疗实际上是提供药物、能量及其所携带的信息,补足缺乏信息,纠正错误的信息,疏通信息的通道。例如,阿氏综合症就是心房室发出的节流信息,传不到心肌细胞造成心律慢的疾病;传染病则是异种蛋白或毒素带来了异常信息,扰乱了机体的正常调节功能;信息代码错乱,如 DNA 模板的错误,可能产生不正常功能的蛋白质,形成了癌细胞。信息通道堵塞也可产生疾病,例如,有些病人能用语言正确地表达自己的思想,却不能理解别人的话;而有些病正相反,能理解别人的话,却不能用语言表达自己的意思。用信息论的方法研究,发现神经系统存在着信息流,神经系统的功能是分别接收各种不同的信息。不同通道对应不同的功能,假若与某种功能相对应的信息通道受到损害,那么信息流就会阻塞中断,出现上述问题,此时疏通信息流的通道,使信息正常流动,就能恢复健康。

### 3. 信息论在管理科学中的应用

在现代化管理中,信息论已成为与系统论、控制论等并列的现代科学的主要方法论之一。信息价值、信息量、信息反馈、信息时效性、真实性、信息处理、传递以及信息论与信息科学是现代化管理的运动命脉。实际上,现代化管理与信息已融为一体,并形成一种特殊形态的信息运动形式,即管理系统信息流。

管理系统是一个复杂的大系统,在管理活动中贯穿着两种“流”,一是物流,二是信息流。物流是系统内输入资源,经过形态、性质变化而输出产品的运动过程。伴随着物流而产生的设计图纸、工艺文件、计划等大量资料,则形成了信息流。物流是管理系统活动的原生运动。信息流是伴随着物流而产生的,它引导物流有规律地运动,以达到最优的经济效果。

管理系统反映了管理世界中各种管理形态的特征和变化的组合,规定了它们的数量与质量的关系,制约着主管者的分析、判断、估测等管理逻辑思维,推导出相应的决策,以指挥和组织管理活动按照预定的目标和利益发展。

在整个管理世界里,管理信息依据不同的分类方法,可以分为各种不同的类别,而在这繁多的种类中,总的可分为两大形式:管理自然信息和管理社会信息。管理自然信息指的是管理系统以时间、效益形式呈现的自身形态、结构、运动过程与主体(主要是管理者)同样以时间、效益形式呈现的形态、结构、运动过程相互作用而在人脑中留下的与该管理系统同态的响应。管理社会信息指的是一切经过管理者利用语言、文字、符号、图像等加工过的管理自然信息。管理方面的知识、情报、指令、告示、法律等全都属于管理社会信息。

对于任何管理者来说,他随时都将会同时面临着这两种信息,并深刻地影响着自己的管理活动。就某个管理者而言,这里的管理社会信息也可以是经由前人或别人加工过的管理