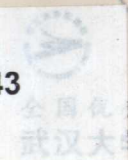


信息与计算科学专业系列丛书
面向21世纪本科生教材

信息论基础

石峰 莫忠息 编著



3 全国优秀出版社
武汉大学出版社

面向21世纪本科生教材

信息论基础



全国优秀出版社
武汉大学出版社

图书在版编目(CIP)数据

信息论基础/石峰,莫忠息编著. —武汉:武汉大学出版社,2002.7

信息与计算科学专业系列丛书

面向 21 世纪本科生教材

ISBN 7-307-03380-1

I. 信… II. ①石… ②莫… III. 信息论
IV. G201

中国版本图书馆 CIP 数据核字(2001)第 078069 号

责任编辑:顾素萍 责任校对:刘凤霞 版式设计:支 笛

出版发行:武汉大学出版社 (430072 武昌 珞珈山)

(电子邮件:wdp4@whu.edu.cn 网址:www.wdp.whu.edu.cn)

印刷:湖北省通山县印刷厂

开本:850×1168 1/32 印张:9.125 字数:229 千字

版次:2002 年 7 月第 1 版 2002 年 7 月第 1 次印刷

ISBN 7-307-03380-1/G·557 定价:14.00 元

版权所有,不得翻印;凡购买我社的图书,如有缺页、倒页、脱页等质量问题,请与当地图书销售部门联系调换。

信息与计算科学专业系列丛书

编审委员会

主任委员 费浦生

委 员 陆君安 郑慧娆 胡宝清
莫忠息 黄象鼎

出 版 说 明

1998 年, 教育部颁布了经调整后的高等学校新的专业目录, 从 1999 年秋季开始, 各院校开始按新的专业设置进行招生。信息与计算科学专业是在这次调整中设置的, 是以信息处理和科学与工程计算为背景的, 由信息科学、计算科学、运筹与控制科学等交叉渗透而形成的一个新的理科专业。目前, 社会对这方面的人才需求越来越多, 开办这个专业的院校也越来越多。因此, 系统地出版一套高质量的相关教材是一项当务之急。

由于信息与计算科学专业是一个新设的专业, 有关该专业的人才培养模式、培养目标、教学计划、课程体系、教材建设等一系列专业建设问题, 各院校目前正在积极的研究和探索之中。为了配合全国各类高校信息与计算科学专业的教学改革和课程建设, 推进高校信息与计算科学专业教材的出版工作, 在有关专家的倡议和有关部门的大力支持下, 我们组织成立了信息与计算科学专业系列教材编委会, 制订了教材出版规划, 并将该系列教材纳入武汉大学出版社“面向 21 世纪本科生教材”系列之中。

编委会一致认为, 规划教材应该能够反映当前教学改革的需要, 要有特色和一定的前瞻性。规划的教材由个人申报或有关专家推荐, 经编委会认真评审, 最后由出版社审定出版。对这批教材的编写力求做到教学改革力度大、有创新精神、有特色风格、深入浅出、可读性好、实用性强, 以满足全国各类高校 21 世纪初信息与计算科学专业及相关专业的教学需要。

本系列教材将陆续出版, 首批四部为《信息论基础》、《数值计算方法》、《数字信号处理》和《计算机图形与图像处理技术》。

限于我们的水平和经验，这批教材在编审、出版工作中还可能存在不少的缺点和不足，希望使用本系列教材的教师、同学和其他广大读者提出批评和建议。

武汉大学信息与计算科学专业系列教材编委会

前 言

随着科学技术的迅速发展、知识体系的不断更新，信息的概念已在自然科学、人文与社会科学中被广泛地采用，信息理论越来越受到人们的重视。实际上，我们目前所处的时代早已被称为信息时代。香农信息理论，是一个业已成熟的科学体系，是研究信息理论的基础。

长期以来，信息论的教材均是为通信工程或概率统计等专业的学生而编写的，需要读者具有较多的相关专业的知识。为使其他专业的学生能尽早掌握信息理论的基本原理和方法，也使信息论的思想、原理和方法在更为广泛的范围之内得到推广和应用，本书尽量用较少的概率统计知识和通信工程知识，尽可能以离散的情形来讨论有关问题。

本教材着重介绍香农信息理论的基本概念、基本分析方法和主要结论，同时，还介绍组合信息和算法信息知识。由于 Shannon 提出的信息论是一种基于统计意义上的信息理论，这一理论对通信技术的发展产生了持久而又深刻的影响，但它对信息技术的其他某些方面，如人工智能、机器学习等，则指导作用很少，所以人们对更为广泛意义下的信息的研究一直没有停止。到目前为止，较为成熟的研究成果有：E. T. Jaynes 在 1957 年提出的最大熵原理的理论；S. E. K. Kullback 在 1959 年首次提出后又被 J. S. Shore 等人发展的鉴别信息和最小鉴别信息原理的理论；A. N. Kolmogorov 在 1965 年提出的关于信息度量定义的三种方法——概率法、组合法和计算法；A. N. Kolmogorov 于 1968 年阐明并

被 J. Chaitin 在 1987 年系统发展的关于算法信息的理论。这些成果大大丰富了信息理论的概念、方法和应用范围。首先，它把信息的统计定义进一步推广并对非统计意义下的信息给出了一种度量。其次，信息度量的意义已不再局限于信源编码和信道编码，而是已经系统地发展成为信息处理的一种准则。如最大熵原理和最小鉴别信息原理在目前的估计理论中占据着重要的地位。基于此，本书对这些基本概念和成果也作了较为详细的介绍。

传统的信息论包含三个方面：信息论基础、编码理论、密码理论。由于信息论的基本原理和方法与编码理论息息相关，我们在介绍信息理论的基本知识时，处处涉及到编码理论，虽然在第 5 章的最后提到了重复码和 Hamming 码，但那仅仅只是为了加深读者对有关编码的感性认识，在第 6 章我们专门对较为成熟的线性码作了简单而又系统的介绍。由于现代密码学是基于信息理论的，所以我们对密码学作了一点介绍。

全书共分 10 章。第 1 章主要介绍香农信息理论的基本概念、基本内容、发展简史以及通信系统模型。第 2 章讨论信源的特点和分类，信息的度量，以及信息熵、条件熵、联合熵等。第 3 章介绍互信息。第 4 章主要介绍有关信源编码的一些基本概念和 Huffman 最优编码。第 5 章主要介绍离散信道编码问题、信道编码定理，并对 Hamming 码作了简单的介绍。第 6 章系统地从理论上对线性码作了介绍。第 7 章介绍有关率失真理论。第 8 章介绍两个应用得非常广泛的极大熵原理和最小鉴别信息原理，它们是估计理论中两个重要的原理，也是两个重要的方法。非统计意义下的信息理论（组合信息与算法信息）在第 9 章中作了介绍，同时给出通用编码方法的代表——Lempel-Ziv 编码方法。第 10 章介绍密码学的基础知识。

本书前 5 章和第 7 章是信息理论的基本内容，力求系统、全面地介绍有关信息的基本概念，如信源和信宿、信道和编码的基本概念和理论。作者认为本书第 2 章所讲述的一些基本概念和问

题是最基本的，特别是熵的概念，初学者应该细心研读，准确理解。这一章内容掌握得好，其余部分的内容也就容易理解和掌握了。学习这部分内容的数学基础要求是学习过数学分析和概率论的基本内容。当然，最好对随机过程的一般理论和分析方法也有所了解。

第6章、第8章到第10章的内容是专题研讨部分，读者可根据需要选读有关内容。作者力求反映国内外在这些专题研究的主要成果。这部分内容主要是为了扩大读者的知识面。教师在讲授信息论理论基础课程时可只作简略介绍或只选讲其中部分内容。

全书第1~5、7~9章由石峰编写，第6章和第10章由莫忠息编写。虽然在编写过程中参考了大量的教科书和有关专著，但由于编者的学识有限，书中错误在所难免，敬请读者批评和指正，编者不胜感激。

编 者

2002年5月

目 录

前 言	1
第 1 章 概 论	1
1.1 信息理论的基本内容	1
1.2 信息理论的发展简史	4
1.3 控制论、信息论与系统论	8
1.4 信息理论的应用	11
第 2 章 信息与熵	16
2.1 信源熵	16
2.2 联合熵与条件熵	22
2.3 熵函数的惟一性	27
2.4 熵函数的性质	31
2.5 连续型随机变量的熵	36
习 题	41
第 3 章 互信息	43
3.1 平均互信息	43
3.1.1 事件的互信息	43
3.1.2 多随机变量下条件互信息与联合事件的互信息	45
3.1.3 平均互信息	46
3.2 互信息与其他熵之间的关系	46
3.2.1 互信息的等价定义	46

3.2.2	熵之间的关系	48
3.3	多个随机变量的互信息	48
3.3.1	两组随机变量之间的互信息	49
3.3.2	条件互信息	49
3.3.3	随机向量中各随机变量之间的互信息	50
3.4	互信息函数的性质	51
3.5	连续型随机变量的互信息	53
	习题	54
第4章	离散信源的无错编码	57
4.1	信源与信源编码简介	57
4.1.1	信源	57
4.1.2	信源的分类	58
4.1.3	信源编码	59
4.2	无记忆信源的渐近等同分割性与 定长编码定理	61
4.2.1	渐近等同分割性(AEP)	61
4.2.2	定长编码定理	64
4.3	离散无记忆信源的变长编码	66
4.3.1	前缀码与 Kraft 不等式	67
4.3.2	Huffman 编码与最优编码定理	74
4.3.3	常用变长编码	81
4.4	离散平稳信源及其编码定理	84
4.4.1	平稳信源的熵率及冗余度	85
4.4.2	平稳信源的编码定理	88
4.5	马尔可夫信源及其编码	90
4.5.1	马尔可夫信源	90
4.5.2	马尔可夫信源的编码	93
	习题	96

第 5 章 离散无记忆信道的编码理论	100
5.1 信道容量	100
5.1.1 信道容量的定义和例子	101
5.1.2 离散无记忆信道容量的有关性质	104
5.1.3 某些简单情况下信道容量的计算	109
5.1.4 转移概率可逆时信道容量的计算	114
5.1.5 离散无记忆信道容量的迭代计算	115
5.1.6 达到信道容量时输入输出字母概率分布的 惟一性	120
5.2 信道编码	123
5.2.1 信道编码概述	124
5.2.2 联合典型序列	130
5.3 信道编码定理	132
5.3.1 信道编码定理的证明	133
5.3.2 Fano 不等式和逆编码定理	135
5.3.3 信源-信道联合编码	139
5.4 高斯信道	141
5.4.1 高斯信道容量	142
5.4.2 高斯信道编码定理	143
5.4.3 高斯信道编码定理的逆定理	144
5.5 信道编码实例	146
5.5.1 重复码	146
5.5.2 Hamming 码	148
习题.....	150
第 6 章 线性码	154
6.1 线性分组码的定义及表示	154
6.2 系统编码和校验矩阵	156
6.3 系统编码及其最优译码的实现	161

6.4	线性码的差错概率及纠错能力	165
第7章	信源的率失真函数与熵压缩编码	174
7.1	熵压缩编码和信源的率失真函数	174
7.2	率失真函数的基本性质	177
7.3	对离散信源求解率失真函数的迭代算法	182
7.4	连续无记忆信源的信息率失真函数	185
7.4.1	基本性质	185
7.4.2	差值失真度量下率失真函数的下界	188
7.4.3	差方失真度量下的率失真函数	191
7.5	标量量化	197
7.6	限失真信源编码定理	199
	习题	205
第8章	最大熵原理与最小鉴别信息原理	207
8.1	最大熵原理	207
8.1.1	最大熵原理的提出	207
8.1.2	最大熵原理的合理性	209
8.1.3	最大熵谱估计	213
8.2	鉴别信息	215
8.2.1	鉴别信息的定义	215
8.2.2	鉴别信息的性质	218
8.3	最小鉴别信息原理	222
8.3.1	最小鉴别信息原理	223
8.3.2	独立分量分析	224
	习题	225
第9章	组合信息与算法信息	227
9.1	自适应统计编码	227
9.2	组合信息	230

9.2.1 基于组合的信息度量	230
9.2.2 Fitingof 通用编码	232
9.3 算法信息	235
9.3.1 Kolmogorov 算法熵	237
9.3.2 算法熵的不可计算性	241
9.3.3 Lewpel-Ziv 通用编码	243
习题	244
第 10 章 密码学引论	245
10.1 古典密码学	245
10.1.1 古典密码举例	246
10.1.2 古典密码分析	248
10.2 基于信息论的密码学	250
10.2.1 完全保密	251
10.2.2 惟一解距离	255
10.2.3 实用安全性	258
10.3 数据加密标准(DES)	259
10.3.1 DES 的描述	259
10.3.2 DES 的讨论	266
10.4 其他	267
10.4.1 公开钥密码系统	267
10.4.2 认证系统	267
10.4.3 数字签名	268
10.4.4 密钥的管理	269
10.4.5 电子货币	269
参考文献	271

第 1 章 概 论

当今,信息已经成为现代社会的一项重要资源.信息的要领在自然科学和社会科学中均已被广泛地采用.研究信息的产生、获取、检测、传输、处理、识别及其应用的信息科学技术,在近几十年里得到了迅速发展.目前社会上流行的一些提法,如“信息、材料、能源是现代科学的三大支柱”、“信息、物质、能量是构成一切系统的三大要素”等,充分说明了人们对信息的重要性的认识.

1.1 信息理论的基本内容

信息科学是研究信息的产生、获取、度量、变换、传输、处理、识别及其应用的一门科学,也是源于通信实践发展起来的一门新兴应用科学.它所研究的问题是带有根本性的、基础性的问题;所给出的方法也是具有普遍性的、令人信服的、可以解决实际问题的方法;所得结论是严谨的、经得起考验的结论.

信息理论的基本问题是信源和信宿、信道以及编码问题.

信息的获取或产生主要依赖于信息源,简称信源.信源大致可分为三大类:一是自然信源,包括来自于物理、化学、天体、地学、生物等方面的自然的信息.获取信息的主要工具是传感器和传感设备,其种类繁多,型式不一,不胜枚举,主要有物理型(热、光、磁、电、声、力)传感器、化学型(气体、化合等)传感器和生物型(神经、感觉、嗅觉、视觉、听觉、触觉等)传感器.二是社会信源,包括政治、军事、管理、金融、商情以及各种情报等.采集信息

主要靠社会调查,利用统计方法加以整理.三是知识源.古今中外记录下来的知识和专家的经验都蕴含大量的信息.

在信息理论中,信息和消息是紧密相关的两个不同的概念.一般认为,消息是信息的载体,如语言、文字、各种符号、声音、图片等,而信息蕴含在消息之中.同一个消息,比如说当天新闻联播的一篇报道,不同的人从中获取的信息是不一样的;一封家书,对于收信人而言可抵万金,但对旁人来说可能是废纸一张.因此信息是一个奇妙的东西,它是有别于物质和能量的一种存在.信息可由一个人掌握,也可由多人所知晓.信息的本质和它的科学定义是当前科学界,乃至哲学界热衷研究的课题,但是它的重要性是毋庸置疑的.

信息的核心问题是它的度量问题.从目前的研究来看,要对通常意义下的信息给出一个统一的度量是困难的.至今最为成功的,也是最为普及的信息度量是由信息论创始人 Shannon 在他的光辉著作《通信的数学理论》中提出的、建立在概率统计模型上的信息度量.他把信息定义为“用来消除不确定性的东西”.用概率的某种函数来描述不确定性是自然的,所以,Shannon 用

$$I(A) = -\log P(A)$$

来度量事件 A 发生所提供的信息量,称之为事件 A 的自信息,其中 $P(A)$ 为事件 A 发生的概率.这个定义与人们的直觉经验相吻合.如果一个随机实验有 N 个可能的结果或一个随机消息有 N 个可能值,若它们出现的概率分别为 $p_1, p_2, \dots, p_N$,则这些事件的自信息的平均值

$$H = - \sum_{i=1}^N p_i \log p_i$$

作为这个随机实验或随机消息所提供的平均信息也是合理的. H 也称为熵,是借用统计物理中的一个名词.因为在物理学中,熵是描述系统的不规则性或不确定性的一个物理量.

由于信息论是源于通信实践发展起来的一门新兴应用科学,

故通信系统的基本模型也是信息理论的基本模型,该模型如图1.1所示。

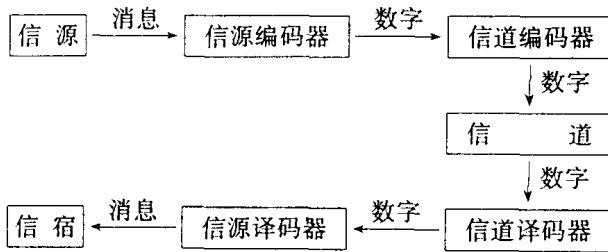


图1.1 基本的通信系统模型

信源是产生消息(或消息序列)的源。消息通常是符号序列或时间函数。消息取值服从一定的统计规律,所以信源的数学模型可以是离散的随机序列或连续的随机过程。

所谓编码,就是用符号来表达信息,即进行信源编码;还需要将符号转换成信道所要求的信号,即进行信道编码。译码是编码的反变换。

信源编码器把信源产生的消息变换成数字序列。在不允许编码失真的情况下,信源编码器的目的是在保证能从其输出数字序列并能准确无误地恢复输入消息序列的前提下,提高输出数字序列的效率,也就是保证在不失真的条件下,对输入消息序列进行压缩。或者,在允许失真的情况下,信源编码器的目的是对给定的信源,在保证消息平均失真不超过某个给定允许值 D 的条件下,对输入消息序列进行压缩。

信道在实际通信系统中是指传输信号的媒介或通道,如电缆、光缆、电离层、人造卫星等。在信息论的模型中也把发送端和接收端的调制、解调器等归入到信道中,并把系统中各部分的噪声和干扰都归入到信道中。在信道的输入、输出模型中,根据噪声和干扰的统计特征,用输入、输出的条件概率(或称转移概率)来