

21^{世纪}

高等学校电子信息类规划教材



信息论与编码

平西建 童 莉 编著
巩克现 马金全

1.2-43
1



西安电子科技大学出版社
<http://www.xduph.com>

21

TN911.2-43

1

子信息类规划教材

信息论与编码

平西建 童 莉

编著

巩克现 马金全



西安电子科技大学出版社

2009

内 容 简 介

本书系统地讨论了 Shannon 信息理论中的基本概念和相关问题,介绍了信道、信源编码的一般原理和基本方法。全书主要内容分为 8 章,包括绪论、离散无记忆信源与信息熵、离散无记忆信道与互信息、信道与信道容量、有噪信道编码、离散信源及其信息冗余、无失真信源编码和限失真信源编码。

本书可作为信息工程、通信工程、网络工程和计算机应用等相关专业高年级本科生及研究生的教材或教学参考书,也可作为从事信息理论、信息技术和通信系统研究的科研及工程技术人员的参考用书。

★ 本书配有电子教案,有需要者可登录出版社网站,免费提供。

图书在版编目(CIP)数据

信息论与编码/平西建等编著. —西安:西安电子科技大学出版社,2009.2

21 世纪高等学校电子信息类规划教材

ISBN 978-7-5606-2182-1

I. 信… II. 平… 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(2008)第 208018 号

策 划 薛 媛

责任编辑 许青青 薛 媛

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

网 址 www.xduph.com 电子邮箱 xdupfxb001@163.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 2009 年 2 月第 1 版 2009 年 2 月第 1 次印刷

开 本 787 毫米×1092 毫米 1/16 印 张 15.75

字 数 370 千字

印 数 1~4000 册

定 价 23.00 元

ISBN 978-7-5606-2182-1/TN·0481

XDUP 2474001-1

*** 如有印装问题可调换 ***

本社图书封面为激光防伪覆膜,谨防盗版。

前 言

随着信息技术的发展,信息的表示、存储、传输和处理成为多媒体技术、通信技术、信息处理、模式识别、网络工程以及计算机应用等领域的关键技术和热点研究课题。信息理论应用概率论、随机过程和数理统计等方法研究信息的描述、传输与处理中的一般规律以及基本关系,还可用于研究信息系统的有效性和可靠性,是信息科学研究和各类信息系统开发中具有重要指导作用的基础理论。

本书主要讨论 Shannon 信息理论中的基本概念和问题,主要内容分为 8 章。第 1 章介绍了信息理论的主要研究内容、发展历史和现状。第 2、3 章讨论 Shannon 信息理论中两个最重要的基本概念,即信息熵和互信息的定义与性质,通过深入分析平均互信息与信源概率分布和信道转移概率分布的凸性关系,引出了信息系统的可靠性和有效性问题。第 4、5 章讨论了信道和信息系统的可靠性问题,首先依据互信息的上凸性关系,引出了给定信道的传输信息能力并给出信道容量的定义,阐述了 Shannon 有噪信道编码定理,然后针对有噪信道中信息可靠传输的要求,比较系统地介绍了纠错编码的基本概念和线性分组码、循环码、BCH 码及卷积码等信道编码的构造原理。第 6~8 章讨论了信源和信息系统的有效性问题。在分析离散无记忆信源及其扩展信源、平稳信源和马尔可夫信源统计关系的基础上,分析并度量了信源的信息冗余,引出了信息系统的有效性问题,针对无失真表示信源信息的应用,讨论了无失真信源编码定理和编码方法。依据互信息的下凸性关系和失真度量方法,讨论了信息率失真函数的定义和性质,阐述了限失真信源编码定理,并介绍了限失真信源编码的基本原理与方法。作为学习上述内容的预备知识,书后附录中介绍了凸函数、Jensen 不等式和线性代数基础(群、环、域)等知识。

本书在内容编排上力图将信息理论与信息系统的最优化问题有机结合,注重信息论的基本概念与信息系统的可靠性、有效性等应用技术原理之间的联系,使相关专业的读者能够运用信息理论的基本概念分析信息系统的最优化问题,系统地了解信道、信源编码的一般原理和基本方法,为读者进一步学习信息与通信工程、网络工程、计算机应用等领域的专业课程,从事图像、语音等多种媒体数据的处理、编码技术研究和信息系统开发工作打下良好的基础。

本书作者长期从事“信息论与信源编码”和“信道编码”课程的教学工作,为了满足信息工程、通信工程、网络工程和计算机应用等相关专业人才培养的教学需要,在多年使用的《信息论基础与信源编码原理》、《信道编码》等教材的基础上编写了本书。本书由平西建、董莉、巩克现、马金全共同完成。刘玉君、肖永隆、邵美珍等老师在前期的教学和教材编写中做了大量的工作,张涛、周利莉、许漫坤对本书的编写提出了有益的建议,汪然、王绪和刘学谦等多名在校研究生参与了书稿的整理工作并绘制了部分插图。

我国信息科学界的不少著名学者在信息理论方面有很好的著作，这些著作对于作者从事信息论课程的教学和在相关技术领域的学术研究以及本书的编写都给予了很大的帮助。西安电子科技大学出版社的薛媛和许青青编辑为本书的出版做了大量的工作。

在此谨向对本书给予帮助和支持的所有人员表示感谢。

由于作者水平和时间所限，书中难免有不妥之处，诚恳期望读者赐教和指正。

作 者

2008 年 10 月

目 录

第 1 章 绪论	1
1.1 信息的定义与性质	1
1.1.1 信息的定义	1
1.1.2 信息的性质	4
1.2 信息论的主要研究内容	5
1.3 信道编码的研究内容与发展简史	7
1.4 信源编码的研究内容与发展简史	9
1.4.1 数据压缩的必要性	9
1.4.2 数据压缩的可能性和基本方法	10
1.4.3 信源编码研究的发展简史与现状	10
第 2 章 离散无记忆信源与信息熵	12
2.1 离散无记忆信源	12
2.2 自信息和熵	14
2.2.1 自信息	14
2.2.2 信源的信息熵	17
2.3 熵函数的性质	19
2.4 联合事件的熵及其关系	26
2.4.1 联合事件的概率空间与概率关系	26
2.4.2 联合熵、无条件熵和条件熵	27
2.4.3 各种熵之间的关系	28
2.5 连续信源的信息测度	32
2.5.1 连续信源的差熵	33
2.5.2 差熵的基本性质	35
习题 2	36
第 3 章 离散无记忆信道与互信息	39
3.1 单符号离散无记忆信道及其转移概率	39
3.2 信道疑义度	40
3.3 范诺不等式	43
3.4 互信息的定义	46
3.4.1 符号间的互信息	46
3.4.2 平均互信息	49
3.5 平均互信息的基本性质	51
3.6 平均互信息的凸性	53
3.7 信息系统的可靠性和有效性问题	58

3.8 连续信道的平均互信息	63
3.8.1 单符号连续信道的平均互信息	63
3.8.2 连续信道平均互信息的性质	64
习题 3	67
第 4 章 信道与信道容量	69
4.1 信道的描述和分类	70
4.1.1 信道的描述	70
4.1.2 信道的分类	70
4.1.3 离散无记忆信道	72
4.1.4 高斯白噪声加性波形信道	74
4.2 信道容量的定义	75
4.2.1 信息传输率	75
4.2.2 信道容量	75
4.3 离散信道的信道容量	77
4.3.1 对称信道的信道容量	77
4.3.2 准对称信道的信道容量	79
4.3.3 可逆矩阵信道的信道容量	83
4.4 离散无记忆信道容量的迭代算法	88
4.5 连续信道的信道容量	94
4.5.1 单符号高斯加性信道	95
4.5.2 高斯白噪声加性信道的信道容量	96
习题 4	97
第 5 章 有噪信道编码	98
5.1 最简单的编码方法	98
5.2 联合 ϵ 典型序列	101
5.3 有噪信道编码与 Shannon 第二编码定理	104
5.4 Shannon 理论对信道编码的指导意义	107
5.4.1 二进制离散无记忆信道下的极限	107
5.4.2 AWGN 信道下的理论极限	107
5.5 线性分组码	109
5.5.1 线性分组码的编码	109
5.5.2 最小距离译码	112
5.5.3 伴随式译码	114
5.5.4 分组码最小距离的边界	117
5.6 卷积码	119
5.7 Turbo 码	120
习题 5	122
第 6 章 离散信源及其信息冗余	123
6.1 信源的描述与分类	123

6.1.1 信源的描述	123
6.1.2 信源的分类	123
6.2 离散无记忆信源的扩展信源	125
6.3 离散平稳信源	128
6.4 马尔可夫信源	133
6.5 信源的信息冗余	139
习题 6	142
第 7 章 无失真信源编码	145
7.1 信源编码的作用与构成	145
7.2 等长信源编码的相关概念和编码定理	147
7.2.1 等长码和编码效率	147
7.2.2 信源符号序列的划分	149
7.2.3 等长信源编码定理	153
7.3 变长码的基本概念	155
7.3.1 平均码长与编码效率	156
7.3.2 变长码的结构与分类	157
7.3.3 码的树形图表示	159
7.3.4 字首码存在性定理	161
7.4 变长信源编码定理	162
7.5 最佳编码定理与统计编码方法	168
7.6 变长编码基本方法	172
7.6.1 霍夫曼编码	172
7.6.2 香农-范诺编码	175
7.6.3 算术编码	177
7.6.4 变长码的抗信道误码能力分析	179
习题 7	180
第 8 章 限失真信源编码	183
8.1 失真函数与平均失真	184
8.2 信息率失真函数及其性质	187
8.2.1 D 失真许可准则与 D 失真许可信道	187
8.2.2 信息率失真函数	188
8.2.3 $R(D)$ 的基本函数关系	189
8.2.4 信息率失真函数的性质	195
8.3 信息率失真函数的计算	198
8.3.1 信息率失真函数的一般计算方法	198
8.3.2 r 元等概信源和汉明失真函数的 $R(D)$	203
8.3.3 信息率失真函数的参量表示	206
8.4 保真度准则下的信源编码定理	210
8.4.1 信源编码定理及其逆定理	210
8.4.2 编码定理的意义	216
8.5 限失真信源编码的基本原理	218

8.5.1 限失真信源编码的必要性和可行性	218
8.5.2 保真度准则	219
8.5.3 预测编码方法	220
8.5.4 正交变换编码方法	224
8.5.5 矢量量化编码方法	227
习题 8	229
附录 A 凸函数与颜森(Jensen)不等式	231
A.1 一元函数的凸性	231
A.2 一元函数凸性的定义	232
A.3 函数凸性的判别	232
A.4 Jensen 不等式	232
A.5 凸域和凸函数	233
A.6 凸域中的 Jensen 不等式	234
附录 B 线性代数基础	235
B.1 群、域与环	235
B.2 有限域基础	236
B.3 有限域上的线性代数	236
部分习题参考答案	240

第1章 绪 论

信息科学和工程以信息为研究对象,以信息的运动规律和利用信息的原理为主要研究内容,以扩展人类的信息处理能力为主要研究目标,是当代具有强大生命力和推动力的新兴学科。作为半个多世纪科学技术进步的主要标志之一,信息科学和工程广泛地应用于通信理论与技术、计算机科学与技术、电子工程、遥感遥测技术和人工智能等各个领域。信息科学和工程的一个重要的基础理论——信息论,是在长期的信息与通信工程实践中,与概率论、随机过程和数理统计等近代数学学科相结合而建立并发展起来的,它主要研究各类电子信息系统和通信系统中信息的描述、传输和处理的一般规律与基本关系。研究信息系统的有效性和可靠性理论的目的是实现系统的最优化。在今天的“信息化社会”中,信息理论对于各类实用信息系统的研制与应用都具有重要的指导作用。作为信息论的主要分支,信源编码着重研究信源的统计特性和信源的编码理论与数据压缩技术,是提高信息系统有效性的技术手段;信道编码研究如何检测和纠正信息通过有噪信道传输后发生的错误,是提高信息系统可靠性的技术手段。信道编码、信源编码是各类电子信息系统研究和开发中的关键技术课题。

本章我们首先引出信息理论中最基本、最重要的概念——信息,简述信息理论及其主要应用领域——信源编码的主要研究内容、历史发展及现状。

1.1 信息的定义与性质

人类在日常生活和社会活动中,一时一刻也离不开信息的交流。特别是在今天的信息社会中,人们要有效地工作、明智地行动必须拥有充分的信息。但是,究竟什么是“信息”呢?“信息”有什么属性?怎样度量?这些概念通常却是含糊不清的。自从信息论这一学科诞生以来,“信息”这一名词便在工程上有了比较明确的概念,成为一个基本的技术术语。

1.1.1 信息的定义

“信息”是一个常用词,在日常生活中泛指“消息”、“信号”、“情况”、“情报”、“知识”等。例如,人们从报纸或电视新闻中得到某些消息,便说得到了信息;司机根据红绿灯信号得到车辆行驶信息,等等。随着信息的开发和利用,“信息”也逐渐显示出其巨大的威力,为人类和人类社会的进步带来明显的经济效益和社会效益。因此,在日常生活和社会活动中“信息”又被赋予各种动人的比喻,如企业家认为“信息就是效益”,商人认为“信息就是利润”,军人认为“信息就是胜利”等。可见,通常的“信息”概念仅仅是从实用角度出发在某个侧面为“信息”建立的非常粗浅、非常模糊且具有很强主观性的概念,这些概念对于不同

的人在不同的时间、地点和条件下,其意义、程度有很大的差异。因此,关于信息的这些含糊不清的概念必须进行加工、概括、提升和开拓。在我们的专业学习中,信息通常是指代表着某一个抽象的有待传送、交换、存储以及提取和识别的内容,它有严格、确切的含义,有一定的数学模式并能定量地度量。

信息论的主要奠基人香农(C. E. Shannon)以通信系统为物理模型,用概率测度和数理统计的方法研究通信系统中的基本问题,并于1948年在《贝尔系统技术》杂志上发表了著名论文《通信的数学理论》,奠定了信息论的理论基础。在这篇论文中他将信息定义为“用来消除不确定性的东西”。

图1-1给出了一个一般的通信系统。在这样的通信系统中,发信者(信源)发出的信息在某种物理媒介(信道)中传输并被收信者(信宿)接收。例如在由人与人的信息交流活动所构成的信息系统中,传输的是人体各种感觉器官(如眼、耳、鼻、舌等)所能感知的光、声和字符等信号;在电信系统中,消息(符号)便为不同频率、不同相位、不同强弱的电信号。因此,我们可以将这种一般的通信系统表述为传输消息(符号)的系统。

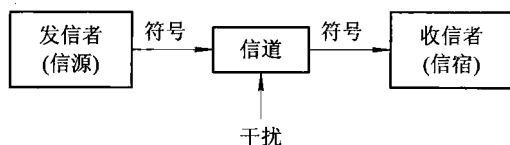


图 1-1 一般的通信系统

在图1-1所示的通信系统中,显然存在着一个能够使发信、收信双方都能理解的符号表(如某种文字、语音、图像、图形或电信号)。然而,通信过程是一个随机的、不确定的过程,即谁使用此通信系统、在什么时间发出何种具体符号是不能够事先预料的,而且通信过程中不可避免的干扰也是随机出现的。这些随机性因素使得这种消息或符号的传递过程有一个最基本、最普遍却又十分不引人注意的特点,就是收信者在收到符号之前不知道发信者发出的是哪一个符号,即对于收信者而言具有一定的随机性或不确定性。只有通过通信过程,收信者才能知道是谁向他发出符号,发出的是何种符号,消除关于发信者及其发出何种符号的不确定性。由此可知,信息的传递过程对于接收者而言是一个由不确定到确定的过程,而实现由不确定到确定的转变,所依赖的只能是接收者由通信过程所获得的信息。所以,信息确实是用来消除不确定性的东西,这也就是香农信息定义的含义。

对于一次实际的通信过程,由于信道中存在着随机性的干扰,因此接收者在通信完成之后可能完全消除了关于信源的不确定性,也可能只消除了部分不确定性,甚至仍然具有同样的不确定性。根据香农信息定义,接收者由这一通信过程所获得的信息量是不同的,即可能获得了信源输出的全部信息,也可能只获得部分信息甚至是没有得到信息。所以,香农信息定义一方面指明了信息与消息、信号、情况、情报的差异,即消息、信号、情况、情报只是携带着信息,是信息的载体,并不是信息本身,信息则是这个载体所携带的内容。另一方面,香农信息定义指明了信息是可以度量的,即消息、信号、情况、情报所携带的信息量的大小与接收者通过通信过程消除或减少对于该事物的不确定程度有关。只要原有的不确定性程度有所减少,接收者便由此次通信得到了一定的信息。

香农信息定义揭示了信息的含义,为信息、通信系统的定量分析打下了良好的基础。

但是,该定义只是从信息的功能上对信息加以描述,只是说出了信息能够做什么,有什么用,并没有正面回答信息是什么。

关于信息的定义,学术界有多种描述,但是尚无一种适用范围广、得到普遍公认的定义形式。这说明人们对于信息的研究还没有达到完全揭示本质的程度。但是人们在这一领域所从事的研究、所提出的各种定义仍然在一定程度或从一定的侧面触及到了信息的某些实质问题。例如,控制论的创始人维纳(N. Wiener)1948年在《控制论——动物和机器中的通信与控制问题》一书中指出:“信息就是信息,不是物质,也不是能量”。1950年,他又在《人有人的用处》中提出:“信息就是人和外界互相作用的过程中相互交换的内容和名称”。维纳的定义表明,人与客观世界除了物质、能量的交换之外,还有信息的交换。人类通过语言、文字、图像等各种手段交换信息,学习有关彼此的知识,使人类社会成为一个有机的整体。由此可知,信息及其信息的交换确实也是一种客观存在。同时也应当注意到,信息的交换不仅发生在人与外界相互作用的过程中,在没有人参与的许多相互作用的过程中同样包含信息的交换。

从更一般的意义上可以认为,信息反映了一切事物的存在和运动方式的描述。此时信息的定义表述为:事物运动(包括客观世界和主观世界以及人脑的思维活动)所表现出来的各种状态和方式。

在这种定义下,维纳所说的“人与外界……相互交换的内容”不是别的,正是“事物运动的状态和方式”,即人从外界得到的信息是外界事物的运动状态和方式,而人给外界的信息则是人的思维运动的状态和方式,是人的意志和命令。对于香农定义中的所谓不确定性,则正是对于事物运动的状态和方式所具有的不确定性,即不知道事物处于什么运动状态中,不知道事物正在以什么方式运动。要消除这种不确定性,就需要知道事物运动的状态和方式,需要得到信息。因此,信息——事物运动的状态和方式,就是用来消除不确定性的东西。可见,这一定义不仅统一了多种定义的概念,而且从更一般的意义上较好地揭示了信息的本质。

近十几年来,以计算机、信息处理、网络、通信和微电子技术的发展、应用和普及为标志的信息技术得到了迅猛发展。人类已经进入信息时代,我们对于信息及其在人类的生活和社会活动中的作用有了更加明确、深刻的认识,“信息”已经成为人类在“数字化生存”中的一项基本要素,决定了人在现代社会中的生存方式和生存质量。

由上面的分析我们可以归纳出以下三点:

- (1) 信息不是物质或能量,它是自然世界和人类社会中的另一种基本要素;
- (2) 信息具有客观存在的属性,是客观事物运动状态和方式的表征,不完全取决于人的主观认识;
- (3) 信息又与主观认识有关,是客观事物在人脑中的反映。

在信息处理学科中,信息常表示为对数据含义的一种解释,而数据则是那些可以记录下来、反映事物运动状态和方式的符号,包括数值、曲线、图像、语音等。在信息的处理过程中,输入的是数据,处理后的输出结果仍然是数据,而信息则隐含于这些数据中,针对某种特定的目的,可由数据解释其含义。例如卫星获得的地物遥感影像数据,经数字图像处理、识别与分析后,输出仍是数据。对于同一幅遥感影像数据,通过不同方法处理可以得到不同的地物目标分类,农业、矿业、军事等不同的应用部门由输出数据或影像可解译

出不同的结果,获取不同的信息,如农作物面积、矿藏分布或军事设施。在我们的专业学习中,通常遇到的是这种狭义的信息概念。

1.1.2 信息的性质

信息作为客观世界的第三要素,与物质、能量相比具有一些特殊的性质。

(1) 信息是无形的。

信息不同于物质和能量,它是客观世界中的一种看不见、摸不着、没有重量的基本要素。新闻、报纸、信号、密码等只不过是信息的载体。

(2) 信息是可以共享的。

在客观世界中,物质和能量所遵循的基本规律之一是守恒定律,即物质和能量不能创造也不能消灭,只能转换。然而,信息不受守恒定律的制约,没有重量,易于复制,能以极快的速度传播,是一种可以共享的重要的社会资源。信息的交流不但不会使信息的持有者失去原有信息,而且可以获得新的信息。

在现代社会中,飞速发展的通信手段和信息处理技术为信息资源的充分共享提供了优越的条件,同时国家之间的军事对抗、商业活动中的市场争夺、多媒体数字产品的版权归属等,也对信息的安全和保密提出了更高的要求。

(3) 信息是无限的。

客观世界的运动是永恒的。作为描述客观事物的运动状态和运动方式的信息,与客观事物及它们的运动一样,也是永恒的。

在组成客观世界的三大要素中,人类可以使用的物质和能量资源只能供有限的人使用,总有一天会出现短缺危机,而信息则永远在产生、更新和演变,可以多人共享使用,并且使用的人越多,其价值越高。信息已经成为人类社会中的一个取之不尽、用之不竭的知识源泉。

信息的这一无限性在时空上表现为可扩展性。例如,失去了现实应用时效的历史资料可以反映社会发展变化的统计规律,先进地区的科学技术可以带动落后地区的经济发展。

(4) 信息是可开发的。

信息的开发是指信息的表示、存储、传输、处理和利用。显然,信息的开发和利用历来是客观世界发展、人类文明史进化的一个基本条件。在信息社会的今天,信息技术产业已成为推动社会进步,拉动经济、科技、教育等各个领域发展的重要部分。

(5) 信息是可度量的。

信息反映事物的运动状态和方式。通过研究客观世界所遵循的自然规律,人类将不断地认识和掌握事物变化、发展的客观规律,并且找出适当的方法描述事物的运动状态和方式,于是反映客观事物的运动状态和方式的信息也可以按某种方式加以度量。

例如,在香农的信息定义中,信息量与事件发生的不确定程度及信源发出符号的随机性有关,信息是关于事件随机性的一种描述。因此,我们可以用概率统计的方法来度量信息。

设发信者发出的符号 a_i 出现的概率为 $P(a_i)$ 。 $P(a_i)$ 愈小,则 a_i 的随机性即不确定性愈大, a_i 含有的信息量也就愈大。由此可知, a_i 具有的信息量应当与 a_i 发生的概率成反比,即

$$I(a_i) = \log \frac{1}{P(a_i)} = -\log P(a_i) \quad (1.1)$$

在通信的过程中,信道中不可避免地存在着随机性的干扰。于是,在接收端收到符号 b_j 时,发信者发出符号为 a_i 的可能性可以用条件概率 $P(a_i|b_j)$ 来表示,那么在接收到符号 b_j 后对发信者发出的符号是否是 a_i 仍然存在的不确定性便成为

$$\log \frac{1}{P(a_i|b_j)} = -\log P(a_i|b_j)$$

于是,通过信息的传递,接收者对于事件 a_i 的不确定性改变了,表明通过这样的信息传输系统我们由 b_j 得到了关于 a_i 的信息。显然,由这一通信过程所获得的信息量的大小应当与关于事件 a_i 的不确定性的改变量有关。于是,通过信息传输,接收者由 b_j 得到的关于 a_i 的信息量可以表示为

$$I(a_i; b_j) = \log \frac{1}{P(a_i)} - \log \frac{1}{P(a_i|b_j)} = \log \frac{P(a_i|b_j)}{P(a_i)}$$

可见,香农给出的信息度量确实是一种对通信过程中所消除的不确定性的度量。

1.2 信息论的主要研究内容

由上面的讨论我们知道,信息论的研究对象是传输消息(符号)的系统。由于这些消息载着信息,因此这种消息传输系统即为信息传输系统,通常简称为通信系统。信息论的创始人香农以狭义的通信系统为物理模型,研究信息的定量描述方法和编码理论,分析通信系统中的有效性和可靠性问题,奠定了信息论的理论体系。随着科学技术的发展,信息论的研究范围、应用领域和指导意义已远远超出了原来的范围,成为研究广义信息系统中一般规律的工程学科,它的主要目的是提高信息系统的可靠性和有效性,实现系统的最优化。

客观世界中存在着各种各样的信息传输、存储和处理系统,如电报、电话、雷达、遥感、计算机系统等工程意义上的各类狭义的通信系统,以及人类社会的管理系统、生物有机体的神经系统、生物遗传系统等。这些系统的形式、用途各不相同,但从信息传输的角度分析,在本质上它们有许多共同之处,即在这些系统中都有信息的发送者和接收者,都存在着信息的传递、交换和处理。对于这些互不相同的信息系统,我们可抽象为一个广义的通信系统来描述,并概括为图 1-2 所示的模型。

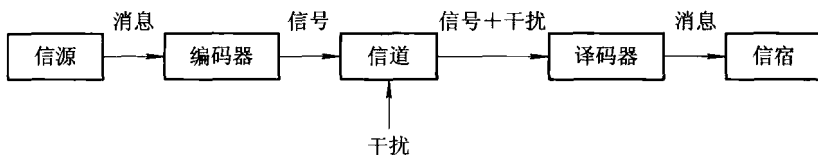


图 1-2 通信系统模型

广义的通信系统模型主要由信源、编码器、信道、译码器和信宿五个部分组成。利用这样的模型我们可以分析、探讨通信系统在传输消息的过程中的一般规律。

(1) 信源:发出信息的客观事物,可以是人,也可以是某种设备或物体。

由于消息是信息的载体,因此信源的输出是消息或消息序列,如电信号、文字、图像、

语音等。消息或消息序列可以是连续的，也可以是离散的。由前面的讨论我们已经知道，信息的基本属性之一是随机性，因此信源输出的消息、消息序列需要用随机过程加以描述。

信源研究的主要问题是其统计模型(统计特性描述)及信源所具有的信息量的定量表示。

(2) 信道：传输信号的物理媒介或通道。

在狭义的通信系统中，实际信道有明线、电缆、波导、光纤、无线电传播空间等。广义的通信系统的信道多种多样。除了传输信号，信道还具有存储信号的作用，如书信在邮递过程中不仅执行信息的传递任务，同时也起到了信号的存储作用。再如，计算机中的硬盘、移动存储设备不仅可以保存数据或文件，存储的数据、文件也可以与其他计算机进行交流，实现信息的传递和共享。

信道研究的主要问题是它能传输、存储多少信息，即它的信道容量有多大。

(3) 编码器：将信源输出的消息或消息序列转换成适合通信系统要求的信号的设备。

不同的通信系统中允许的消息或消息序列的表示形式可能不同。例如，面对面的交谈需将要表达的内容通过发声器官转换成听觉器官能够接收的声波，并在允许声波传播的空间中传输；使用邮政通信需将要传递的消息转换成文字并构成规范化的书信；电报通信则需将文字转换成由点、画构成的莫尔斯码；语音、图像、视频等数字媒体文件需使用二进制符号表示并按照一定的格式进行处理与存储。因此，对于任何通信系统而言，信源输出的信息都必须通过编码实现从消息到信号、数据的转换，才能够通过某种信道进行传输、存储和处理。由消息到信号、数据的转换一般要经过信源编码器和信道编码器。对于狭义通信系统，编码器还包括调制等各种处理。

编码器研究的主要问题是如何进行信源编码，使信源的消息被充分利用并可可靠地通信。

(4) 译码器：编码器的逆过程，它将信号转变为消息。

与编码器相对应，译码器分为信道译码器和信源译码器。对于狭义的通信系统，还包括信号的接收与解调。

(5) 信宿：消息的接收者，即接收消息的人或设备。

(6) 噪声源：信号在信道传播的过程中常常会受到噪声的干扰。噪声可分为系统内噪声和系统外噪声，如雷电、宇宙辐射、设备自身的电子噪声和人为电子干扰等。在广义通信系统模型中，这些干扰和噪声都等效地折合为信道干扰，可看做是由一个噪声源产生并作用于在信道中传输的信号。在通信系统中，噪声是影响可靠通信的主要原因之一，可通过各种信道编码技术提高系统的抗干扰能力。

通过对广义通信系统模型的分析可以看出，通信的基本目的是在接收端(信宿)准确地或近似地再现从另一端(信源)选择出来的消息，因而通信系统的基本问题是信源、信道及编码问题，信息论的基本任务则是为设计有效而且可靠的信息系统提供理论依据。

本教材主要涉及狭义的通信系统，即讨论香农的信息理论，在深入分析香农信息论的基本概念和编码定理的基础上，研究提高信息系统有效性的理论与工程手段，即讨论信源编码原理和数据压缩的一般方法。

1.3 信道编码的研究内容与发展简史

信道编码是20世纪40年代末提出、60年代发展起来的一门提高数据传输可靠性的理论与技术,至今已有60余年的历史。随着数字通信的发展,特别是20世纪70年代以来,卫星通信和高速数据网的飞速发展,对数据传输的可靠性提出了越来越高的要求,因此,如何提高数据传输的可靠性一直是通信发展过程中研究的重点之一。

自从1948年Shannon发表了《A Mathematical Theory of Communication》这篇论文后,就开创了两个现代研究领域——信息论和编码理论。他最杰出的贡献就是引入了概率论来分析和研究通信系统。在信道编码领域,他给出了“信息”的一个非常有用的定义,以及几个“信道编码定理”,描述了给定通信系统可靠传输的精确上界(称为信道容量)。

在这篇论文中,最令人感兴趣的结果是“noisy channel coding theorem for continuous channels with average power limitations”,这个定理采用带限加性高斯白噪声信道模型,这个信道模型可以近似描述许多实际的数字通信和存储系统。定理的证明表明,对于任何小于等于信道容量的传输速率,存在一个编码方案,可以达到任意小的错误概率;相反地,如果传输速率大于信道容量,则不存在任何编码方案可以达到可靠的性能。然而,这是一个存在性定理,对于如何寻找合适的编码方案,实现起来多么复杂,该定理并没有给出任何指导。

从1950年Hamming的工作开始,许多通信工程师和编码理论家已经开发了很多种不同的复杂度合理的方法,试图接近Shannon所预期的性能。在这里,我们将沿着过去60余年编码在通信和存储系统中的应用历程来看一下在缩小实际系统和信道容量之间的距离上已经取得的巨大进步。

在Shannon定义了可靠通信的理论极限的同时,Hamming和Golay正在着手开发第一个可实现的差错控制方案,他们的工作开辟了一个欣欣向荣的应用数学的分支——编码理论。通常认为Richard Hamming是发现第一个差错控制码的人。在1946年,Hamming在Bell实验室工作,从事弹性理论的研究,然而,他最终在计算机上花费了大量的精力。那时候,计算机的运行非常不稳定,虽然具备了检错能力,但是当发现错误的时候,程序只能中断执行。那时Hamming的程序很少不中断地从头到尾执行,他尝试了很多方法对输入进行编码,最终使得计算机能够纠正单个错误进而能连续运行。他的编码方法是在每4比特信息位后面插入3比特校验位,校验位是由信息比特线性组合得到的,被后人称做Hamming码(汉明码)。

虽然Hamming码取得了很大的进步,但也存在很多缺点:一是传输效率不高,二是在每个数据块中只能纠正一个错误。Marcel Golay指出了这些问题并将Hamming的工作进行了推广,这就是著名的Golay码。Golay码将数据中每12个比特组成一个数据块,然后插入11个比特的校验位,组成长度为23比特的码字,可以纠正3个比特错误。这类码字的一个共同特点是在每 k 个信息比特之后插入 r 个校验比特组成 n 个比特的码字,这就是众所周知的分组码。在引入信道编码的这60余年当中,已经找到了很多性能优良的分组码,并得到了大量的应用,比如Golay码就曾被应用到木星探测中。当然,现在它早已经被很多性能更好的编码方式代替了。

1957 年 Prange 提出了循环码的概念。这种码字可以用多项式来描述,有很严谨的数学结构。它有一个很大的优点是每个码字循环移位后仍然是一个码字,可以利用这种循环移位特性来降低编码器和译码器的复杂度,尤其是译码,采用一种 Meggitt 译码器的结构可以非常有效地对纠错能力较小的循环码进行译码,但是译码复杂度随着纠错能力的提高指数增加。

循环码的一个很重要的子类是 1959 年 Hocquenghem 以及 1960 年 Bose 和 Ray-Chaudhuri 组成的研究小组发现的,这就是著名的 BCH 码。Reed 和 Solomon 还在多进制上构造出 BCH 码,后人称之为 RS 码。RS 码的出现是编码历史上一个很重要的进步,因为它可以纠正突发错误。但是直到 1967 年 Berlekamp 才提出了一个有效的译码算法,RS 码才逐步得到广泛应用,如 CD、DVD。

虽然分组码得到了成功的应用,但是在使用过程中它也有几个缺点:第一,由于分组码是分帧的,因此在译码之前必须要接收到整个码字才可以进行,这会对系统引入一个不可接收的延迟,尤其是对于码长较长的分组码;第二,分组码需要精确的帧同步;第三,大部分基于代数的译码器输入的是硬判决比特,而不是解调器输出的没有量化的“软”值。如果分组码使用硬判决比特,则信道被假定为二进制信道;如果是软判决比特,则信道的输出是连续取值的。然而,为了达到 Shannon 预测的性能限,需要采用连续取值的信道输出。因此,虽然在相对较好的信道上分组码可以取得卓越的性能,但是当信噪比较低时,它具有相当差的性能。

注意,在低信噪比的情况下,分组码较差的性能并不是码本身的特性,而是由于硬判决译码具有次最优特性,因此分组码也可以用软判决来译码。但在不久以前,人们还认为软判决译码太复杂,目前这种想法正在发生改变,主要是因为最近几年的一些研究工作,如 RS 码的纠错删译码算法和 1998 年 S. Lin 等人提出的基于网格软判决译码算法。

1955 年, Elias 提出了卷积码的概念。卷积码可以克服分组码的缺点,卷积编码器采用移位寄存器对连续的比特流增加冗余。第一个有价值的译码算法是 1961 年 Wozencraft 和 Reiffen 提出的序列译码算法。之后,1963 年 Fano 和 1969 年 Jelinek 分别对其做了改进。虽然 Fano 和 Jelinek 的工作对译码算法进行了改进,但是直到 1967 年引入了 Viterbi 算法以后,最佳的译码方案(在最大似然的意义上)才可实际操作。

卷积码最致命的弱点是对突发错误非常敏感。

卷积码抗突发错误能力较差的问题可以通过交织器来减轻。通过打乱发送端的比特的顺序,并在接收端恢复比特的顺序,突发错误可以被展开,对译码器来说,就可以看成随机错误。

这种串行级联的形式是 David Forney 于 1966 年首先提出来的,并用于 NASA 和 ESA 在 1987 年制定的深空网络标准中。在这个标准中($q=8, n=255, k=223, t=16$)RS 码同 Odenwalder 卷积码级联使用。

1993 年 7 月在 Geneva Switzerland 召开的 International Conference on Communications (ICC)会议上,实际编码系统与 Shannon 理论极限之间的距离更加接近了。在这次会议上,有两篇论文讨论了一种新的编码方式和相关的译码技术,作者 Berrou、Glavieux 和 Thitimajshima 造了个新词“Turbo Codes”来描述这类新的码字,他们的这个发现产生了很大的影响,并获得了很高赞誉。