



普通高等教育“十二五”规划教材

信息理论与编码

齐 华 主 编

陈 红 张艳玲 副主编



中国电力出版社
CHINA ELECTRIC POWER PRESS



普通高等教育“十二五”规划教材

信息理论与编码

主 编 齐 华

副主编 陈 红 张艳玲

编 写 刘 军 姚红革 杨 超

主 审 廉保旺



中国电力出版社
CHINA ELECTRIC POWER PRESS

内 容 提 要

本书为普通高等教育“十二五”规划教材。

本书重点介绍经典信息论的基本理论,基本覆盖了信息论基本理论的主要内容。全书共9章,主要内容包括信息论概述、信息的度量、离散信源及其度量、连续信源及其度量、信道与信道容量、信源编码、信道编码、密码学基础、信息理论与编码的应用等。为了便于教学和读者自学,每章后都有习题。本书用丰富的例题和图示深入浅出地阐述基本概念、基本理论及实现原理;注重理论与工程实际相联系,给出了教材中有关问题的分析思路、方法、MATLAB源代码和处理结果,给出了一些可供学生自学和研讨的MATLAB习题。

本书可作为普通高等院校信息科学与信息技术等专业的教材用书,也可作为从事通信、雷达、导航、计算机、系统工程、生物工程、管理工程等相关领域的科研和工程技术人员的参考用书。

图书在版编目(CIP)数据

信息理论与编码/齐华主编. —北京:中国电力出版社, 2014.8

普通高等教育“十二五”规划教材

ISBN 978-7-5123-5843-0

I. ①信… II. ①齐… 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(2014)第083167号

中国电力出版社出版、发行

(北京市东城区北京站西街19号 100005 <http://www.cepp.sgcc.com.cn>)

北京丰源印刷厂印刷

各地新华书店经售

*

2014年8月第一版 2014年8月北京第一次印刷

787毫米×1092毫米 16开本 18.25印张 446千字

定价 36.00元

敬告读者

本书封底贴有防伪标签,刮开涂层可查询真伪

本书如有印装质量问题,我社发行部负责退换

版权专有 翻印必究



前言

美国科学家香农 (C. E. Shannon) 在 1948 年发表了“通信的数学理论”的学术论文, 信息论随之而诞生。它是一门应用概率论与随机过程等方法研究信息的获取、传输、存储、处理、再生、控制和利用等一般规律的科学。随着信息论的不断发展和完善, 它的研究已经冲破了香农狭义信息论的范畴, 几乎渗透到自然科学与社会科学的所有领域, 向多学科结合的广义信息论方向发展, 从而形成了涉及面极广的新的学科——信息科学。在现代科学技术高速发展的过程中, 人们已经普遍意识到, 学习和掌握信息论的相关知识已经成为一种必不可少的需求。

本书是编者根据“信息理论与编码”课程的特点, 在总结多年的教学经验和科研实践积累的基础上编写而成的。由于信息论的理论性较强, 同时对数学基础有一定的要求, 因此最初接触这门课程的学生难免有枯燥之感, 且在繁杂的数学公式面前望而却步。针对这种情况, 本书在编写方式上采用通俗易懂的文字, 强化对物理概念的理解, 用丰富的例题和图示深入浅出地阐述基本概念、基本理论及实现原理, 帮助读者更好地理解 and 掌握信息理论与编码技术的精髓要义。并将计算机技术和仿真技术相结合, 采用 MATLAB 作为虚拟实验室, 对重要的知识点通过仿真技术来增强读者对相关知识的理解。同时为了适应不同层次及不同专业的需求, 本书中对重要的定理还引入了一些较深的严谨证明, 作为提高部分并加“*”以示区别, 读者可根据自身需要加以选择。

本书注重理论与工程实际的联系, 给出了教材中有关问题的分析思路、方法、MATLAB 源代码和处理结果, 并附有可供学生自学和研讨的 MATLAB 习题。书中汇集信息理论在热力学、统计学、生物学、经济学以及医学等其他学科交叉结合的应用内容, 以拓展读者的知识视野, 激发读者对该课程的兴趣。对信息论中新发展的若干重要课题 (如信息失真理论的发展及在数据压缩和图像处理中的应用、信息安全等), 本书也做了专题介绍。

本书遵照由浅入深、循序渐进的教学规律, 系统介绍和论述信息论的基本理论、基本技术、基本方法。其内容包括理论基础篇、基础应用篇和专题应用篇。第 1~5 章为理论基础篇, 主要介绍信息论的基本理论和基本概念, 包括信息度量、信源熵、互信息、信道容量等概念、性质与计算; 第 6~8 章为基础应用篇, 主要介绍优化信息系统的手段和方法, 包括信源编码、率失真函数、信道编码及保密通信的基本理论与方法; 第 9 章为专题应用篇, 主要介绍信息理论在语音、图像、信息传输与安全及其他学科上的应用示例。

本书由西安工业大学的老师编写, 齐华担任主编, 陈红、张艳玲担任副主编。第 1、2 章由齐华编写, 第 3、4 章由刘军编写, 第 5、6 章由陈红编写, 第 7、8 章由张艳玲编写, 第 9 章由杨超编写, 书中仿真实验由姚红革制作。

西北工业大学电子信息学院廉保旺教授担任本书主审，并提出了许多宝贵意见。在本书的编写过程中，引用和参考了大量国内外专家学者的著作和文献，编者所在学院的研究生也协助做了许多工作。在此一并致谢。

限于作者水平及时间紧张，书中难免有疏漏之处，希望广大读者批评指正。

编 者

2013 年 12 月

目 录

前言

1 信息论概述	1
1.1 信息的基本概念与特征	1
1.2 信息论的产生与发展	4
1.3 信息论研究的主要内容及方法	8
1.4 香农信息论	9
习题	12
2 信息的度量	13
2.1 离散变量的自信息量	13
2.2 离散变量的互信息量	17
2.3 离散变量集的平均自信息量	21
2.4 离散变量集的平均互信息量	33
2.5 连续随机变量的信息度量	39
习题	42
3 离散信源及其度量	45
3.1 离散信源的描述与分类	45
3.2 离散无记忆信源	46
3.3 离散无记忆扩展信源	49
3.4 离散有记忆平稳信源	52
* 3.5 马尔科夫信源	55
3.6 信源的剩余度	59
习题	61
4 连续信源及其度量	64
4.1 连续信源的描述与分类	64
4.2 单维连续信源	65
4.3 连续信源的最大熵定理	74
4.4 熵功率	78
习题	79
5 信道与信道容量	81
5.1 信道的描述及分类	81
5.2 离散无记忆单符号信道及其容量	83
5.3 离散无记忆多符号信道及其容量	95
5.4 组合信道及其容量	97

5.5	多用户信道	101
5.6	连续信道及其容量	106
5.7	波形信道及其容量	112
5.8	信源与信道匹配	115
	习题.....	115
6	信源编码	118
6.1	信源编码的基本概念	119
6.2	信源的编码性能	122
6.3	无失真信源编码定理	123
6.4	无失真信源编码基本方法	133
6.5	限失真信源编码	160
	习题.....	183
7	信道编码	187
7.1	信道编码的基本概念	187
7.2	信道编码的基本思想	190
7.3	信道编码定理	194
7.4	常用检错码	201
7.5	几种重要的纠错码	203
	习题.....	240
8	密码学基础	242
8.1	密码学的基本概念	242
8.2	保密通信系统的数学模型	243
8.3	古典密码体制的基本类型	244
8.4	现代密码体制	249
8.5	密码体制的安全性	259
8.6	密码技术的应用	260
	习题.....	264
9	信息理论与编码的应用	266
9.1	信息论在多媒体通信中的应用	266
9.2	信息熵在热力学中的应用	272
9.3	信息论在生命科学中的应用	275
9.4	信息论在经济学中的应用	278
9.5	信息论在哲学中的应用	279
	参考文献	283

1 信息论概述



本章重点

- (1) 理解信息的概念和性质。
- (2) 了解信息理论的发展概况。
- (3) 理解和掌握通信系统模型。
- (4) 了解信息理论与编码的主要研究内容。

在当今高度信息化的社会,信息几乎渗透到人类活动的各个环节中,信息概念在自然、社会和思维等不同学科领域中被广泛应用,并与物质、能量一起构成了现代文明的三大支柱,对信息的产生、处理、储存、传输和显示成为重要的产业,研究这方面的科学就是信息科学。而信息理论(也称信息论)与编码是信息科学的主要理论基础之一,它研究信息的存在性和可能性问题,为具体实现提供理论依据。与之相对应的是信息技术,主要研究如何实现,怎样实现的问题。

随着信息和信息科学对现代社会生活各方面影响的不断加大和深化,人们对信息理论的认识和价值的估计也在不断深入。

本章首先阐述了信息的定义、特征及性质,简要回顾了信息理论的形成和发展历程,然后结合通信系统模型介绍模型中各部分的作用,最后阐述了信息与编码理论的主要研究内容。

1.1 信息的基本概念与特征

1.1.1 信息的一般概念

自从1928年美国学者哈特莱(Hartley)提出信息的概念以来,信息一词就与社会生活和经济发展产生了解之缘,很多学者从不同的角度和侧面给“信息”下过定义,流行的说法不下百种,他们都试图从不同的侧面和不同的层次来揭示信息的本质。例如:“信息是事物的变异度”,“信息是系统结构的有序性”,“信息是被反映的事物属性”,“信息是负熵”,“信息是谈论的事情、新闻和知识”,“信息是在观察研究过程中获得的数据情报、新闻和知识”,“信息是使概率分布发生改变的东西”……这些定义都或多或少地从某种程度上描述了信息的一些特性,但是都不够全面、系统和准确。美国数学家、控制论奠基人,维纳(Wiener)在其著作《控制论:动物与机器中的通信与控制问题》指出:“信息就是信息,不是物质,也不是能量。”维纳利用排他法告诉人们:信息不是物质和能量。这是对信息本质的最有原则性和最深刻的宣示,是把信息、物质和能量放在同样地位上的最早科学论断。

正因为信息一词定义形式繁多,所以当前还没有一个公认的关于信息的定义,但人人都能感觉到它的存在,也并不影响我们对信息基本特征的认识。我们暂时可以把这种目前尚难明确定义的信息称为广义理解的信息。下面采用一种比较普遍的说法来描述广义信息。

信息是认识主体（人、生物、机器）所感受的和所表达的事物运动的状态和运动状态变化的方式。以这种定义为基础，借用语言学中的术语，我们把广义信息分成 3 个基本层次，即语法（Syntactic）信息、语义（Semantic）信息、语用（Pragmatic）信息，并把语法信息、语义信息和语用信息的有机整体称为全信息，它们分别反映事物运动状态及其变化方式的外在形式、内在含义和效用价值。

语法信息是“事物运动状态和状态改变方式”本身。语言学领域，研究“词与词的结合方式”的学科称为语法学。

语法信息是信息的最基本层次，又称句法信息，是认识主体感知或表述的事物运动状态和特征的形式化关系，它只涉及事物运动的结构，即只考虑状态和状态之间的关系，也就是说，只表述客观事物运动状态而不考虑其意义。语法信息不是对某一类信息的称谓，而是按照信息的性质划分信息的最基本、最抽象的一个层次，也是理论上探讨最多的一个层次。按照事物运动状态和特征的不同，语法信息包括有限状态语法信息和无限状态语法信息，连续状态语法信息和离散状态语法信息。

语义信息是“事物运动状态和状态改变方式的含义”。在语言学里，研究“词与词的结合方式含义”的学科称为语义学。语义信息是信息认识过程的第二个层次。它是指认识主体所感知或所表述的事物的存在方式和运动状态的含义；换言之，语义信息不仅反映事物运动变化的状态，而且还要揭示事物运动变化的意义，涉及信息本身的含义及其逻辑上的真实性和精确性，但不考虑信息使用者个人的主观因素。人们常说某个信息是“真实的”、“确切的”，这就是一种语义评判。

语用信息是“事物运动状态和状态改变方式的效用”。语用信息是指信息内容对信宿的有用性，是信息最复杂、最实用的层次。信息的有用性取决于信宿对信息的需求状况，也就是信宿的信息状态与信源发出的信息间的相关性所决定的。任何信息的语用特性都与发信者和收信者个人过去的经验、现在的环境、他们的思想状态以及其他个人的因素有关。人们说某个信息是“有用的”、“无用的”、“有价值的”，则是语用性的判断。

因此，广义信息是把信息的形式、内容等全都包含在内的最广泛意义上的信息。

信息作为技术术语使用最初是源于计算机技术的出现和发展，人们为了把计算机处理的对象，如数据、记录、报表、文字等，用一个统一的、全面的、高层次的术语表达，而选择使用“信息”这一名称。作为技术术语的信息实际上是指一切符号、记号、信号等表达信息所用的形式或载体，其意义要比前面广义信息的含义具体得多，但仍然是比较笼统和含混不清的。

信息作为一个可以用严格的数学公式定义的科学名词最先出现在统计数学中，之后又出现在通信技术中。无论是在统计数学中还是在通信技术中定义的信息，都是一种统计意义上的信息，简称为统计信息。统计信息是一种有明确定义的科学名词，它与内容无关，且不随信息具体表达形式的变化（如把文字转换成二进制码）而变化，因此也独立于形式。它反映了信息表达形式中统计方面的性质，是一个统计学上的抽象概念，同时其适用范围要比广义信息狭隘得多，我们在本书中讨论的信息论正是关于这种统计信息的理论，即狭义信息论。

下面通过对“信息”、“消息”与“信号”这三个概念的对比进一步阐述信息的定义。

1.1.2 信息、消息与信号

日常生活中，人们往往对消息和信息不加区别，消息被认为就是信息。例如，当人们收

到一封电报,或者听了天气预报,人们就说得到了信息。实际上信息和消息是有区别的。信息是一个抽象的概念,它往往不能直接被感知,而要通过某种具体形式(如语言、文字、图像等)才能被感知。而这些具体形式就是消息,所以我们说,消息是表达信息的工具。消息是用文字、符号、数据、语言、图片、图像等能够被人们感觉器官所感知的形式,来表述客观物质世界的各种不同运动状态和主观思维活动。消息是相对具体的概念,而信息是抽象化的消息。换句话说,消息是信息的携带者,信息包含于消息之中。例如,人们看到一则标题为“上海成功主办了2010年世博会”的新闻消息,就得知了上海主办2010年世博会的具体情况,内容“上海成功主办了2010年世博会”是对上海主办2010年世博会的状况的一种表述。再例如,电视中转播世界杯,人们从电视图像中看到了足球赛进展情况,而电视的活动图像则是对足球赛运动状态的表述。当然,消息也可用来表述人们头脑里的思维活动。例如,朋友给你打电话说:“我刚做了个噩梦,现在好紧张。”此时,这则语言消息反映了人的主观世界——大脑物质的思维运动所表现出来的思维状态。由于主、客观事物运动状态或存在状态是千变万化的、不规则的、随机的。所以在收到消息以前,收信者存在“疑问”和“不确定”。因此,当我们得到一个消息后,可能会得到一定数量的信息,而我们所得到的信息,显然与我们在得到消息前对某一事件怀有的疑问或不确定性程度有关。获得消息后,原先的不确定性消除得越多,获得的信息就越多;如果原先的不确定性全部消除了,就获得了全部的信息;若消除了部分不确定性,就获得了部分信息;若原先不确定性没有任何消除,就没有获得任何信息。由此可见,信息是事物运动状态或它的存在方式的不确定性的描述。

需要指出的是,同一个消息可以含有不同的信息量,而同一信息可以使用不同形式的消息来载荷。例如:“阿根廷以3:0完胜巴西”这个关于球赛结果的信息,可用报纸文字、广播语言、电视图像等不同形式的消息来表述。当你第一次听到这个消息,你就获得了关于足球赛结果的信息,而如果在你已经得知了这个结果的情况下又有人再告诉你这个消息,则你没有获得任何信息量。可见,信息与消息是既有区别又有联系的。

为了克服时间或空间的限制而进行通信,就必须对消息进行加工处理,把消息变换成适合消息传输的物理量,这种物理量称为信号,如电信号、光信号、声信号、生物信号等。信号是消息的载体,是消息的表现形式,消息则是信号的具体内容。由于消息携带着信息,因此信号是带有信息的某种物理量,这些物理量的变化包含着信息,因此信号可以是随时间变化或随空间变化的物理量。在数学上,信号可以用一个或几个独立变量的函数表示,也可以用曲线图形等表示。同一信息可以用不同的信号来表示,同一信号也可以表示不同的信息。例如,红、绿灯信号,若在十字路口,红、绿灯信号表示能否通行的信息。若在电子仪器面板上,红、绿灯信号表示仪器是否正常工作或者表示电压高低等信息。信号与信息在本质上是根本区别的,信号仅仅是外壳,信息则是内核,两者互相依存,但属于不同的层次。

应当指出,信息与消息是两个不同属性的概念,而消息和信号则具有相同的属性,并且它们之间存在着确定的对应关系。但信息和消息之间却不存在这种关系,同一消息在不同场合可以表达不同的信息,而同一信息又可以用不同的消息来表达。

1.1.3 信息的特征

信息的特征是信息所特有的征象,是信息区别于其他事物的本质属性。信息作为客观世界存在的第三要素,与物质、能量相比,具有一些特殊的性质。

1. 信息具有存在的普遍性

客观世界充满着各种信息,如上下课的铃声,书报杂志上的文章、消息,电台播放的新闻、乐曲,五颜六色的图画,色香味俱全的水果等,其中都包含着信息。信息是人们对客观事物运动规律及其存在状态的认识结果,只要有事物的存在,就会有事物的运动和变化,就会产生信息。信息含义之广可以涵盖整个宇宙,如果没有信息的话,宇宙就会变得杂乱无章、不可理喻。

2. 信息具有时效性

信息的时效性是指信息从发生、接受到利用的时间间隔及效率。信息是有寿命、有时效的。信息的使用价值与其所提供的时间成反比,时间的延误会使信息的使用价值衰竭,甚至完全消失。

3. 信息具有可共享性

信息是人们适应外部世界,并与外部世界互相交换的内容,与此同时,人们在与外部世界的相互作用中还同时交换着物质和能量,但信息的交流与实物的交流有着本质的区别。实物交流,一方得到的正是另一方所丢失的;而信息的交流,不会使交流者失去原有的信息,双方或多方可共享信息。信息的共享性使信息资源易于扩散,使信息得到比物质资源更广泛的开发利用,也将对人类社会的发展起到积极的推动作用。

4. 信息具有可加工性

客观世界存在的信息是大量的、多种多样的,人们对信息的需求往往具有一定的选择性。在不同的应用场合,为了达到不同的目的,需要对大量的信息用科学的方法进行筛选、分类、整理、概括、归纳,排除无用信息,选取自己所需要的信息。为了更有效地传输,信息可以被压缩;为了更安全地传输,信息可以被加密;为了更可靠地传输,信息可以采用各种方法被编码、被调制,从而实现对信息的加工处理。

5. 信息可以产生动作

这说明信息能够发挥作用,获得信息后可能产生结果。例如,花朵盛开后产生的气味和色彩是信息,它可以引来蜜蜂采蜜。信息既具有能量的某些属性,又不同于能量。能量产生的动作是客观的,而信息的影响含有主观和客观的双重因素。

6. 信息具有依附性

信息依附于载体而存在,它自身不能独立存在和交流,而载体可以因不同需求而变换。各种信息必须借助于文字、图像、胶片、磁带、声波、光波、电磁波等物质形态的载体才能够表现,才能为人们听、视、味、嗅、触觉所感知,人们才能够识别信息和利用信息。

1.2 信息论的产生与发展

科学来源于实践,信息论作为一门学科,其形成当然也不例外。人类在生产实践中创造了语言,早期的人类直接面对面进行口头语言的通信,交流劳动中获得的信息,语言是信息的最早载体。后来又出现了图形、文字等存储、传输信息的载体。为了更有效地利用信息,还发明了除语言、文字、图形以外的传输手段。中国殷商时期的创举“烽火告警”就是利用火作为信号,进行较长距离的通信,是光通信的一种原始方式。在此后的一段漫长的时间里,人们并未对信息问题进行认真的关注。似乎只依靠人体本身的感觉器官与思维器官来传

输和处理信息,就足以应付人类生存和发展的需要了。然而到了近代,由于生产力的发展水平达到了一个更高的阶段,人们要观察遥远的天体、更深层次的微观世界、迅速准确地传递大量的数据……。这时,扩展人类接收和处理信息的能力的问题才逐渐引起人们的注意,对信息的研究逐渐被人们重视,人们对传送信息的通信系统要求也越来越高。如何提高通信系统的可靠性和有效性,如何设计出最优化的通信系统,是科学工作者面临的重大课题。通信系统的可靠性也就是信息传输的“好坏问题”。提高通信系统的可靠性,就是在通信过程中尽可能地减少或者消除噪声的干扰,提高信息传输的“质量”。通信系统的有效性也就是通信系统传输信息的“快慢问题”,提高通信系统的有效性,就是用最窄的频带,尽可能快地传输信息,提高信息传输的“速率”。在通信的实践中,人们发现在一定条件下,同时达到以上两个要求会出现矛盾。为此,有人想到,在限定的条件下,同时提高通信的可靠性和有效性的要求,可能存在一种理论上的界限,这就需要应用数学理论,这样,从通信的实践中提出了应用数学理论指导实践的要求。

1.2.1 信息论的产生

20 世纪 20 年代,奈奎斯特(H. Nyquist)和哈特莱(R. V. Hartley)提出了关于通信系统的传输效率问题的讨论。奈奎斯特将传输速率和带宽联系起来,他指出,如果以一个确定的速率来传输电信号,就需要一定的带宽。哈特莱提出,用消息出现的概率的对数作为消息中包含的信息量的测度,这样,就可以用数学的方法从数量上对信息进行测度。就是在这种情况下,美国数学家香农(C. EShannon, 1916—2001 年)在 1941~1944 年用概率论的方法对通信系统进行了深入研究,于 1948 年在《贝尔系统技术杂志》公开发表了题为“通信的数学理论”(Mathematical Theory of Communication)的里程碑性的论文。这篇论文中把通信的数学理论建立在概率论的基础上,把通信的基本问题归结为通信的一方能以一定的概率复现另一方发出的消息,并针对这一基本问题对信息作了定量描述。香农在这篇论文中还精确地定义了信源、信道、信宿、编码、译码等概念,建立了通信系统的数学模型,并提出了信源编码定理和信道编码定理等重要而带有普遍意义的结论。这篇论文的发表标志着仅用于通信系统的信息论的正式诞生,这就是香农信息论,或称狭义信息论,而香农本人也成为信息论的奠基人。

香农理论是通信发展史上的一个转折点,它使通信问题的研究从经验转变为科学。其核心是他指出了通信系统实现高效率和高可靠性地传输信息的方法,就是采用适当的编码。从数学的观点看,香农的编码定理是最优编码的存在定理,从工程角度出发,这些定理不是结构性的,并没有给出实现最优编码的具体方法。但是,定理给出了编码的极限性能,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。

20 世纪 40 年代,维纳从控制和通信的角度研究了信息问题。维纳研究的重点是在接收端,就是怎样从收到的信号中把各种噪声滤除。在有关“在控制火炮射击的随动系统中如何跟踪一个具有机动性的活动目标”的研究中,各种噪声的瞬时值或火炮的跟踪目标的位置的有关信息都是随机的,这就要求用概率和统计方法对它进行研究,用统计模型进行处理。在研究这些问题的基础上,维纳于 1948 年和 1949 年先后发表了两本专著《控制论》和《平稳时间序列的外推、内插和平滑化》。维纳把随机过程和数理统计的观点引入通信和控制系统中,揭示了信息传输和处理过程的统计本质,建立了信息最佳滤波理论,成为信息论的一个

重要分支。

1959年,香农发表了“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和率失真信源编码定理,后来发展成为“信息率失真理论”。这一理论是频带压缩、数据压缩的理论基础,是信息论领域中的重要研究课题,今天它仍然保持着蓬勃的发展势头,并在各个方面得到了广泛应用。有关数据压缩、多媒体数据压缩已发展成为一个独立的分支——数据压缩理论与技术。

与此同时,纠错与检错码的研究也取得了很大的进展,并成为信息论的又一重要分支——纠错码理论。信道编码技术把代数方法引入到纠错码的研究,利用群、环、域与线性子空间理论赋予码的代数结构,可以使通信信号具有检错和纠错的能力,但是代数编码的渐近性能较差,无法实现香农定理所给出的结果。因此,1960年左右,卷积码的概率译码被提出,并逐步形成了一系列概率译码理论。这一时期,信道编码已开始进入实用化的通信技术领域,以维特比译码为代表的译码方法被美国卫星通信所采用,至此香农理论已成为真正具有实用意义的科学理论。

1961年,香农发表的重要论文“双路通信信道”开拓了多用户信息理论的研究。多用户信息理论到20世纪70、80年代得到了迅速发展,1972年T. M. Cover发表了有关广播信道的研究,多用户信息理论成为这一时期信息论研究的一个主流课题。“双路通信”本身体现了网络化的思想,随着通信系统网络化思想的发展,对于各种类型的多用户信源、信道模型的研究也取得了众多成果。近30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。信息论的这些研究进展是与计算机网络、卫星通信、系统工程的实际需要息息相关的。

关于保密理论问题,香农在1949年发表了“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。在这篇论文中,香农精辟地阐明了关于密码系统的分析、评价和设计的科学思想,提出了保密系统的数学模型、随机密码、理想保密系统、理论保密性和实际保密性等重要概念,并提出了评价保密系统的5项标准。这篇论文不仅是分析古典密码的重要工具,而且是探索现代密码理论的有力武器。

总之,在1948年以后的十余年中,香农对信息论的发展做出了巨大的贡献。在1973年出版的信息论经典论文集中(总数为49篇),香农是12篇论文的作者。迄今为止,经典信息论的主要概念除通用编码外几乎都是香农首先提出的。除一系列基本的概念外,香农的贡献还在于证明了一系列编码定理,这些定理不但给出了某些性能的理论极限,而且实际上也是对香农所给基本概念的重大价值的证明。由于香农的这一系列贡献,香农被认为是信息论的创始人。香农是科学家的一个卓越的典范,他的学术风格是理工融合于一身,他把深奥而抽象的数学思想和一个概括的同时又很具体的对关键技术问题的理解结合起来,被认为是近几十年最伟大的工程师之一,同样也被认为是最伟大的数学家之一。

1.2.2 信息论的发展

信息论在过去的几十年中取得了巨大、丰富的理论和技术成果,把它总结一下,其发展大致经历了三个时期。

1. 20世纪50年代向各门学科冲击的时期

信息论的成就给许多学科带来了意外的希望。人们试图把信息概念和方法用来解决本学科所面临的许多未能解决的问题;试图把信息论用于解决语义学、听觉、神经、生理学及心

理学等问题。例如 1955 年在伦敦举行的第三届信息论会议, 涉及内容非常广泛, 包括解剖学、动物保健学、人类学、计算机、经济学、电子学、语言学、数学、神经生理学、神经精神学、哲学、语音学、物理学, 政治理论、心理学和统计学等。但由于狭义信息论存在不考虑信息发送者与接收者双方关于信息的意义(如信息是否真实)和信息的价值以及不能用来描述模糊信息等局限性, 因而在这些方面取得的成就不大。

2. 20 世纪 60 年代消化、理解的时期

这个时期是信息论在已有的基础上进行重大建设的时期。研究的重点集中在通信问题, 包括信息和信源编码问题, 噪声理论问题、信号滤波与预测问题、调制与信息处理问题等, 可归为一般信息论范畴。

3. 20 世纪 70 年代向广义信息论或信息科学发展的时期

这个时期信息论的发展是与世界范围的新技术革命相联系的。人们认识到信息可以当作与材料和能源一样的资源而加以利用和共享。信息论的概念和方法已广泛渗透到各个科学领域, 它迫切要求突破狭义信息论的狭隘范围, 以便使它能成为各种人类活动中所涉及的信息问题的基础理论, 出现了“有效信息”、“广义有效信息”、“语义信息”、“无概率信息”及“模糊信息”等概念, 从而使信息论呈现出多学科结合发展的态势。其理论与技术不仅直接应用于通信、自动控制、电子学、光学与光电子学、计算机科学、材料科学等工程技术学科, 而且广泛渗透到了管理学、医学、仿生学、经济学、语言学、哲学、生物学、心理学、社会学等人文学科。正是在这种多学科的互相渗透、互相结合的背景下, 诞生了一门综合性的新兴学科——信息科学。信息科学是研究信息获取、传输、交换、处理、检测、识别、存储、显示等功能的科学, 它已经成为世界各国最优先发展的科学之一。信息科学对这些学科的发展起着指导作用, 而这些学科的发展又丰富了信息科学并促使其迅速发展, 将人类推向信息时代, 使信息化成为时代的标志。我们可以借助钱学森关于人类知识结构的框图(见图 1.1)理解信息论与信息科学之间的关系, 以及它们在人类知识结构中的地位。

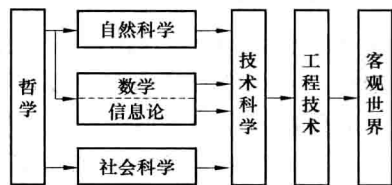


图 1.1 人类知识结构框图

直接作用于客观世界的是工程技术, 工程技术依赖于技术科学, 支撑技术科学的是基础学科, 基础学科包括自然科学、数学、社会科学, 它们又受哲学的指导。信息论可看作基础科学中的一个内容。

前面已提到, 本书中讨论的信息论是关于统计信息的理论。从技术本质的意义上看, 信息技术就是能够扩展人的信息器官(感觉器官、传导神经网络、思维器官、效应器官)功能的一类技术。

近代信息技术的基本内容包括感测技术、通信技术、智能技术及控制技术。感测技术包括传感技术和测量技术, 它们是感觉器官功能的延伸。通信技术的功能是传递信息, 它是传导神经网络功能的延长。智能技术包括计算机硬件、软件技术、人工智能技术和人工神经网络等, 它们是思维器官功能的延长。控制技术的功能是根据输入的指令信息(决策信息)对外部事物的运动状态和方式实施干预, 是效应器官功能的扩展和延长。

在信息技术中, 通信技术和智能技术处于核心地位, 而感测技术和控制技术则是核心与外部世界之间的接口, 构成信息技术内部结构的这四种技术关系是一个有机的整体, 它们共

同完成扩展人的智力功能的任务。

1.3 信息论研究的主要内容及方法

1.3.1 信息论的主要研究内容

信息论是一门应用概率论、随机过程、数理统计和近代代数的方法,来研究信息的基本性质及度量方法,研究信息的获取、传输、处理和利用的一般规律的科学。它的成果将为人们广泛而有效地利用信息提供基本的技术方法和必要的理论基础。它的主要目的是提高信息系统的可靠性、有效性、保密性和认证性,以便达到系统最优化;它的主要内容(或分支)包括香农理论、编码理论、维纳理论、检测和估计理论、信号设计和处理理论、调制理论、随机噪声理论和密码学理论等。根据这种情形,可以把信息论的研究划分为三个不同的范畴。

1. 狭义信息论

主要是总结了香农的研究成果,因此又称为香农信息论。主要通过数学描述与定量分析,研究的对象通信系统从信源到信宿的全过程,包括信息的测度、信道容量以及信源和信道编码理论等。强调通过编码使收、发端联合最优化,并且以定理的形式证明极限的存在。这部分内容是信息论的基础理论,它解决了信息论中的一部分问题。

2. 一般信息论

主要通过数学描述与定量分析,研究信息传输和处理问题,也称工程信息论。除了香农理论外,还包括噪声理论、信号滤波和预测、统计检测和估计理论、调制理论以及信息处理理论等。后一部分的内容主要以美国科学家维纳的微弱信号检测理论为代表的最佳接收问题。最佳接收是为了保证信息传输的可靠性,研究如何从噪声和干扰中接收信道传输的信号的理论,主要解决两个方面的问题:一是从噪声中判决有用信号是否出现,二是从噪声中测量有用信号的参数。他应用近代数理统计的方法来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。

3. 广义信息论

广义信息论是一门综合性的新兴学科,至今并没有严格的定义。概括说来,不仅包括狭义信息论、一般信息论的所有研究内容,还包括如医学、生物学、心理学、遗传学、神经生理学、语言学、社会学和经济学中等一切与信息问题有关的领域。反过来,所有研究信息的识别、控制、提取、变换、传输、处理、存储、显示、价值、作用和信息量的大小的一般规律以及实现这些原理的技术手段的工程学科,也都属于广义信息论的范畴。这个范畴的共同基础——控制论、系统论、仿生学、人工智能等内容,就是前面所说的信息科学。

由于信息论研究的内容极为广泛,又具有一定的相对独立性。故本书主要讨论信息论的基础理论,即香农信息论。

1.3.2 信息论的基本应用方法

我们有理由相信,信息论具有一般方法论的意义和价值,是从事信息产业研究与开发的必备知识。狭义信息论是帮助工程师从全局的观点观察和设计通信系统的理论方法,其提供的是一系列支持通信实践的指导原则,并使通信系统达到最佳的设计,如果不掌握信息论的基本原理,就不能从全局着眼处理具体的技术问题。

随着人们对信息论的研究日益广泛和深入,信息论的基本思想已渗透到许多学科。在人类社会已经走过农业时代和工业时代,进入信息时代的今天,信息理论的应用将不可避免地超出通信领域,而向其他自然科学和社会科学领域延伸和发展。人们可以运用系统论及信息的观点,把客观事物视为一个系统,并将客观事物的运动认为一个系统的过程,然后将这个过程抽象为信息传递和信息转换的过程,通过对信息流程的分析和处理达到对复杂的系统运动过程的规律性的认识。因此,信息论的基本方法是一种直接从整体出发,用联系的、转化的观点综合系统过程的研究方法,其应用的关键步骤如下。

第一步,根据研究对象与该对象发的信息之间某种响应的对应关系,撇开研究对象的物质和能量的具体形态,把研究对象抽象为信息及其变换过程。

第二步,对抽象出来的信息过程中的信息做出定性和定量的研究,从质和量的两方面对信息进行分析,达到对研究对象的客观认识。

第三步,在上一步分析过程所取得的第一手材料的基础上,综合整理这些材料,建立各种模型,对信息及(或)信源进行模拟。

第四步,根据对模型的研究,来评判被模拟的信息过程的功能,探明其机理,做出预测,并根据新获得的信息来改善模型,使其趋于完善。

值得注意的是,香农信息论定义的范围就是帮助工程师传送信息,而不是帮助人理解信息的含义。因此,不能认为信息论能适用所有的领域。

1.4 香农信息论

1.4.1 香农关于信息的定义

“信息是事物运动状态或存在方式的不确定性的描述”。这就是香农信息的定义。用数学的语言来讲,不确定性就是随机性,具有不确定性的事件就是随机事件。因此,可运用研究随机事件的数学工具——概率——来测度不确定性的大小,香农关于信息的定义,通常也称为概率信息,非常便于用数学工具进行研究,这是香农信息论取得成功的关键。

香农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。这种建立在概率模型上的信息概念排除了日常生活中“信息”一词主观上的含义和作用,而只是对消息的统计特性的定量描述,所以信息可以度量,而且与日常生活中信息的概念并不矛盾。例如向空中抛一颗石头,石头必然会落到地上,这是个预料之中的必然事件,若此必然事件果真发生了,则收信人不会得到任何信息,因为他早知道这个事件会发生,不存在任何不确定性。因此,香农的定义排除了对信息一词某些主观上的含义,根据这种定义,同一个消息对任何收信者而言,得到的信息的多少都是同样大,使得信息的概念是纯粹的形式化的概念。即香农信息只研究符号以及符号之间的统计关系,因此属语法学的层次。但也正是这种撇开信息的具体含义、重要程度,不考虑收信者的主观意志的定义方法,使香农信息的定义与实际情况不完全相符。事实上,信息有很强的主观性和实用性,同样一个消息对不同的人常常有不同的主观价值或主观意义。例如,老师给学生上一门专业课,甲同学准备考取本专业的研究生,乙同学则对本专业没有丝毫兴趣,正准备做一名歌手。按照香农的定义,老师所讲授的内容,对于甲、乙两位同学而言,得到的信息的多少是一样的,但是对于甲同学而言,非常有实用价值,会引起他足够的重视,而对于乙同学则没有什么作用。这种情况下,同一消息

对不同收信者引起了不同的关心程度和价值,实际上是获得了不同信息的,而香农对信息的定义是无法描述这种不同的。

综上所述,香农对信息的定义是科学的,能够反映信息的某些本质,但同时也有其局限性。其主要特征如下。

- (1) 信息是新知识、新内容。
- (2) 信息是能使客观主体对某一事物的不确定性减少的有用知识。
- (3) 信息是可以量度的。
- (4) 信息可以被携带、存储及处理。

1.4.2 通信系统一般模型

一般地说,通信系统是指从一个地方向另一个地方传送信息的系统。通信科学所面临的基本问题是如何迅速准确地传输(包括存储)信息。所谓“迅速”,就是信息传输的速度问题,即通信的有效性。所谓“准确”,也就是信息传输的质量问题及通信的可靠性。美国数学家香农(CE. Shannon)在1948年发表的文章的序言中有一句话:“通信的基本问题就是要在某一端准确地或近似地再现从另一端选择出来的消息。”正是沿着这一思路他应用数理统计的方法来研究通信系统,为解决通信理论中的一些基本问题找到了正确的方法,建立了仅用于通信系统的信息论。在信息理论的进一步研究中,大量的研究成果对通信理论和技术成熟发展起到了极为重要的推动作用。从最初形成时提供性能极限和进行概念方法性指导,发展到今天具体指导通信系统的结构组织和部件的设计,这种趋势势必还要进行下去,而信息论也在与通信理论、通信系统设计的理论日益融合的过程中逐步丰富和发展起来。可以说,自从有了人类,就有了伴随着人类的通信,而通信的目的就是传送信息,其方法和手段繁多。例如,手势、语言、烽火、击鼓传令、书信、电话、电视、因特网、数据和计算机通信等,都是信息传递的方式和信息交流的手段,都可看作通信。虽然通信系统形式各异,

但在本质上有许多共同之处。为了定量地研究信息在通信系统中的传输过程,香农在深入研究了各种复杂的通信系统后,将通信系统的形式抽象成一个统一的模型,如图1.2所示。



图 1.2 通信系统一般模型

香农对这一系统的各个基本部分都作了数学描述,我们将在本书的后面章节中详细讨论。

1. 信源

信源(Information Source)的功能是产生消息。消息中包含信息,有待于传输给接收端。信源是多方面的,它可以是人、生物、机器或其他事物,由于信源本身十分复杂,在信息论中我们仅对信源的输出进行研究。信源输出的消息有着各种不同的形式,可归为两类:离散消息,如符号、文字、数字等组成的符号或符号序列;连续消息,如话音、图像和在时间上连续变化的电参数等。由于信源的输出是随机的、不确定的,但却有着一定的规律,可以用随机变量或者随机过程来描述。信源研究的核心问题是:信源消息中所包含的信息量到底有多少,怎样将信息定量地表示出来,即如何量度信息。

2. 编码器

编码器(Coder)的功能是对信号进行变换和处理。编码问题可分为信源编码、信道编