研究生教材

信息论

孟庆生 著

西安交通大学出版社

研究生教材

信息论

孟庆生 著

西安交通大学出版社

内 容 提 要

本书介绍近代信息论的基本理论，包括信息理论、编译码技术及密码学三部分。全书分八章，前三章分别叙述信息量、信源编码理论及信道编码理论，四到七章为编译码技术，包括线性码、循环码、Goppa码及卷积码等。第八章是密码学。每章末都有若干问题与补充。最后两个附录补充Galois域及凸函数的知识。

本书适于作为自动控制、无线电技术、计算机科学、管理科学、信息与系统科学等专业研究生的教科书，也可作为数学系高年级学生的教材，并可供广大通讯工程技术人员自学参考。

信 息 论

孟庆生著

责任编辑 蒋 涛 杨 玲

西安交通大学出版社出版

（西安市咸宁路28号）

西安七二二六厂印装

陕西省新华书店发行　　各地新华书店经售

开本850×1168　1/32　印张：17　字数：430千字

1988年12月第1版　　1987年11月第1次印刷

印数：1——6,000册

统一书号：13340·105　定价：3.00元

《研究生教材》总序

研究生教育是我国高等教育的最高层次，是为国家培养高层次的人才。他们必须在本门学科中掌握坚实的基础理论和系统的专门知识，以及从事科学研究工作或担负专门技术工作的能力。这些要求具体体现在研究生的学位课程和学位论文中。

认真建设好研究生学位课程是研究生培养中的重要环节。为此，我们组织出版这套《研究生教材》，以满足当前研究生教学，主要是公共课和一批新型的学位课程的教学需要。教材作者都是多年从事研究生教学工作，有着丰富教学和科学研究经验的教师。

这套教材首先着眼于研究生未来工作和高技术发展的需要，充分反映国内外的最新学术动态，使研究生学习之后，能迅速接近当代科技发展的前沿，以适应“四化”建设的要求；其次，也注意到研究生公共课程和学位课程应有它最稳定、最基本的内容，是研究生掌握坚实的基础理论和系统的专门知识所必要的，因此在研究生教材中仍应强调突出重点，突出基本原理和基本内容，以保持学位课程的相对稳定性和系统性，内容有足够的深度，而且对本门课程有较大的覆盖面。

这套《研究生教材》虽然从选题、大纲、组织编写到编辑出版，都经过了认真的调查论证和细致的定稿工作，但毕竟是第一次编辑这样的高层次教材系列，水平和经验都感不足，缺点与错误在所难免。希望通过反复的教学实践，广泛听取校内外专家学者和使用者的意见，使其不断改进和完善。

西安交通大学研究生院

西安交通大学出版社

1986年12月

序

(一)

信息论是由Shannon奠基的一门崭新的数学学科，它产生于有效而可靠的通讯问题中，并获得了广泛的应用。

三十多年来，信息论在理论上更加完善，内容上更加丰富，应用上更为普遍。随着计算机科学的发展和新技术革命的需要，信息论与系统论、控制论一起受到普遍重视，并在心理学、语言学、生物学、经济学、美学、历史学以及物理学等方面开始了初步应用。由于信息论的思想、原理和方法具有广泛性，所以它必将得到更为迅速的发展。信息论为研究各种系统提供了广泛的数学工具，而计算机又为信息论的应用提供了强有力的武器。

(二)

信息论的基本问题是研究有效而可靠地传递信息的可能性与方法。

在日常生活中“信息”一词被广泛地使用着。从电视广告，报纸新闻，到来往信件，相互之间的谈话，人们总是在不断地获取信息。但是，只有给出信息的度量，才能使信息的研究成为一门数学学科。

1948年，美国工程师C·E·Shannon 在贝尔电器研究所出版的专门杂志上，发表了“通信的数学理论”，在这一开创性文章中，给出了信息度量的数学公式，为信息论的创立做出了独特的贡献。

信息反映观察事物所获得的知识，而知识总是和被观察事件发生的不肯定性相联系的。但是不肯定性不仅与事件发生的所有

可能状态有关，而且还与每个状态的发生有多大的可能性有关。Shannon定义的信息量，撇开了事件发生的时间、地点、内容以及事件与人们的情感及人们对事件的反应，而只顾及事件发生的状态数目及每种状态发生的可能性大小，这就使信息度量具有普遍意义和广泛的适应性。

有了信息度量，才能研究信息传递。由于信息传递过程伴随着物质与能量的传递，因此传递的信息可能被歪曲。为了尽可能地保证信息传递的可靠性，必须将所传递的消息进行编码并对接收到的消息进行译码。因此，信息论的基本问题即是在给定消息源及传递信道的条件下，选择适当的翻码与译码，使接收消息与发送消息不一致的概率尽可能地小。Shannon的开创性文章，对无记忆信道给出了这种翻码与译码存在的条件，这就是Shannon基本定理。

为了使Shannon信息论付诸实践，还必须研究翻码与译码的构造。这就构成了编译码技术。

由于军事、政治、外交、贸易等方面的需要，密码学作为通信理论的一部分也得到了发展。

信息论基本理论、编译码技术、密码学构成了信息论的三个重要的相互联系的组成部分。

（三）

“信息论”一书，博采众长，精心选材，自成体系，吸取了苏联与美国两大学派的优点，颇具特色。

自从Shannon的开创性文章发表以后，苏联与美国的科学家就采取了不同的研究途径。在苏联，是以Хинчин，Колмогоров，Добрушин为首的一批著名的数学家，致力于信息论的公理化体系与更一般更抽象的数学模型，他们对信息论的基本定理给出了更为普遍的结采，为信息论真正成为一门数学分支做出了贡献。

而在美国则相反，主要是由一批数学修养很高的工程技术人员，致力于信息可靠传递的可实现性。本书的作者，根据苏联与美国两大学派的特点，既考虑到数学的严格性，又考虑到工程实际的适用性，将严格的数学与有效的应用紧密结合起来，使信息论的背景、实质得到充分体现，使本书别具一格，引人入胜。

我们相信，本书对从事信息论理论研究的数学家与从事信息编译码技术的人员都会有所裨益。数学家会在坚实的基础上得到更有用的理论，工程技术人员则能在严格的数学指导下得到更有效的方法。因此，本书将促进数学家与工程技术人员在信息论这一学科中的紧密配合。这是本书作者的心愿，也是我的愿望。

胡国定

于南开大学　1986.3

前　言

本书介绍了近代信息论的基本理论，包括信息理论、编译码技术及密码学三部分。

近代信息论，也称狭义信息论，是自1948年美国工程师C·E·Shannon 的开创性文章〔注〕发表以后发展起来的，至今已将近四十年。这期间它经历了理论的确立、发展与逐步完善的过程；目前已被广泛应用于通信技术以及其他领域。四十年来，这方面的理论性文章及各种应用性技术报告浩如烟海，有关专著也已更新过几代。但为了帮助有志于信息科学的读者，在较短的时间内，以较少的预备知识，从信息论的入门开始，直达它的前沿，并且在掌握理论的同时，又学到一定的通信技术知识，这就是编写此书的动机和意愿。

首先，本书精心选材，具有适当的广度和深度；其次在内容安排上采用块状结构，以便各取所需；第三在叙述上持严谨的态度，所有定理均有详细证明。此外，每章末都有若干问题与补充，有些题目可作为初学的练习；有些是重要结果；有些则是难度较大的一些问题，需要读者发挥创造性来完成。

本书共分八章。前面三章是理论部分，分别叙述了信息量、信源编码理论及信道编码理论。其中除第一章必读外，另外两章的内容都是独立的专题，可供任意选用。由于信源与信道理论成对偶形，所以有些概念、结果及方法若在一章中已详述过，则在另一章便作省略。比如，信道容量的迭代算法，实质上也适用于信源的率失真函数的计算，我们只在一处作了详细介绍。此外，

〔注〕 C·E·Shannon : A Mathematical Theory of Communication, *Bell system Tech. J.*, 27, 379—423, 623—656, 1948.

这两章有些定理的证明过长，只关心应用技术的读者，可以一瞥而过，这并不影响后面内容的学习。第四章到第七章是本书的第二部分，即编译码技术。其中第四章线性码是基础，第五章循环码及第六章Goppa码等都是特殊的线性码，属代数码类，其重点是BCH码。第七章概述卷积码，主要介绍Viterbi 译法及Fano译法，后者是典型的概率译码法。第三部分为密码学，限于篇幅，在第八章中只介绍最基本的内容——密码的基本概念、加密及破译的基本方法等。最后两个附录，分别补充Galois域及凸函数的知识，这些内容是本书必需的数学基础。

本书大部分内容作为教材曾先后在南开大学及西安交通大学信息论方向高年级学生、研究生及助教进修班中讲授过。这次编撰成书，又增补了若干内容，由孙志盈同志校正并清理了原稿。

胡国定教授对本书的写作一直非常关心，给予极大的鼓励和支持。沈世镒同志详细审阅了原稿，提出了许多宝贵的意见。张文修同志对原稿作了部分校订。此外，西安交通大学出版社对本书的编辑出版大力支持。谨此一并致谢。

孟庆生

1986年春节于西安交通大学

目　录

第一章　信息量

§1.1　熵

1.1.1　信息的定性描述

当我们收到一封信或电报时，便能获得一定的信息，因为在此以前我们并不能肯定其中的一些内容。就是说，信息蕴含于不肯定性中，而不肯定性在概率论中是用随机事件或随机变量来描述的。

那么自然要问，哪些随机事件（或随机变量）含有较多的信息？

按常识一般认为，就单个事件比较，小概率事件者信息量大。百年不遇的事件，一旦发生，必定令人震惊（通常所谓"爆冷门"，即小概率事件发生）。就诸随机场比较，基本事件个数相同者，以等概分布场平均信息量大。比如，预测两个势均力敌者谁取胜，比判定两个实力悬殊的对手不肯定性大。就等概随机场而论，基本事件个数多者，平均信息量大，就是说，三择一比两择一不肯定性大。

1.1.2　信息的定量表征

由上述可见，信息伴随着不肯定性。信息的定量表征必然联系着不肯定性的度量。为定量测度随机事件的不肯定性，在前述分析的基础上进一步考虑下述问题。

设有 n 个互不相容的事件 $A_1, A_2, \cdots, A_n$，试验后，它们中有一个且仅有一个发生，但试验前，不能预知究竟哪一个事件将要发生（不肯定性）。为此将各事件按某一记数制（例如，二进制或十进制）依下述规则编号：

Ⅰ　凡等概事件按同样多个符号位数表示；

Ⅱ　凡大概率事件用较少的符号位数表示。

这种规则无疑暗示把每个事件的符号位数作为它的信息测度，而把每个概率场的平均符号位数作为其平均信息量。这种作法一举两得，一方面它符合前述信息作为不肯定性测度的直观印象，另一方面也便于信息的传输。因为大概率事件出现的机会总是多，而对它用较少的符号位来标记，必然会提高传输效率。

例 1.1.1　试将下述试验结果按上述规则编成二进制符号。

事　件	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	B_1	B_2	…	B_8
概　率	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{8}$	$\frac{1}{8}$	…	$\frac{1}{8}$

1.　依上述规则，将诸事件$\{A_i\}$分成两组，使它们的概率各为$\frac{1}{2}$：

$$E_0=\{A_1,A_2\},\quad E_1=\{A_3,A_4,A_5,A_6,A_7,A_8\}$$

$$P(E_0)=\frac{1}{2}=P(E_1)$$

将这两组中的事件按二进制数编号，使其首位数字各为0与1，即E_i中事件的首位数字为$i(i=0,1)$。

2.　将E_0与E_1各分为等概的两小组：

$$E_0=E_{00}+E_{01},\quad E_1=E_{10}+E_{11}$$

$$E_{00}=\{A_1\},\quad E_{01}=\{A_2\}$$

$$E_{10}=\{A_3,A_4\},E_{11}=\{A_5,A_6,A_7,A_8\}$$

$$P(E_{ij})=\frac{1}{4}=\frac{1}{2^2}\ (i,j=0,1)$$

由此确定各事件第二位数字的号码，即E_{ij}中事件的第二位数字