

计 算 机 科 学 丛 书

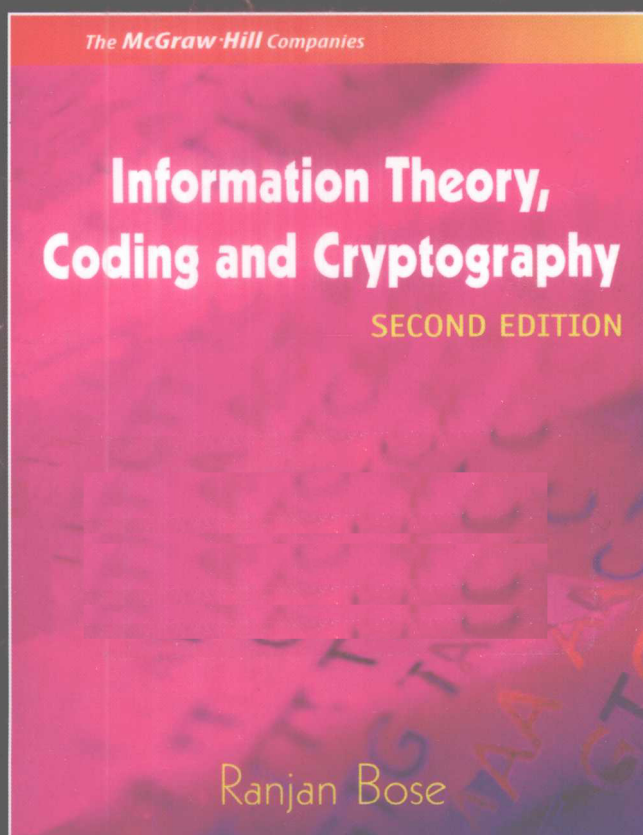
第2版

HZ BOOKS
华章教育

Mc
Graw
Hill Education

信息论、编码与密码学

(印) Ranjan Bose 著 武传坤 李徽 译



Information Theory, Coding and Cryptography
Second Edition



机械工业出版社
China Machine Press

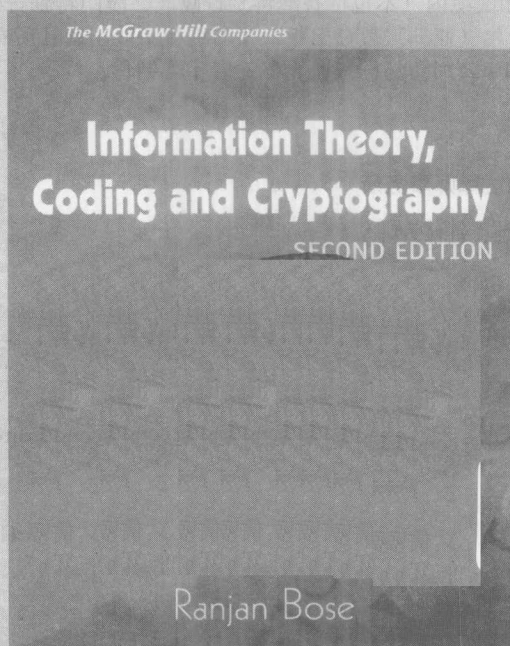


计 算 机 科 学 丛 书

第2版

信息论、编码与密码学

(印) Ranjan Bose 著 武传坤 李徽 译



Information Theory, Coding and Cryptography

Second Edition



机械工业出版社
China Machine Press

信息论、错误控制编码和密码学是现代数字通信系统中的三大支柱,本书用有限的篇幅将三者中所有重要的概念有机地结合起来,涉及信息论、信源编码、信道编码和密码学等方面的知识,不仅内容丰富,而且技术深度适当。

本书适合作为高等院校信息安全、电子工程及相关专业信息论和编码课程的教材,从事相关工作的专业技术人员也能从中受益。

Ranjan Bose: Information Theory, Coding and Cryptography, Second Edition (ISBN 0-07-066901-5).
Copyright © 2008 by McGraw-Hill Publishing Company Limited.

All Rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including without limitation photocopying, recording, taping, or any database, information or retrieval system, without the prior written permission of the publisher.

This authorized Chinese translation edition is jointly published by McGraw-Hill Education (Asia) and China Machine Press. This edition is authorized for sale in the People's Republic of China only, excluding Hong Kong, Macao SAR and Taiwan.

Copyright © 2010 by McGraw-Hill Education (Asia), a division of the Singapore Branch of The McGraw-Hill Companies, Inc. and China Machine Press.

版权所有。未经出版人事先书面许可,对本出版物的任何部分不得以任何方式或途径复制或传播,包括但不限于复印、录制、录音,或通过任何数据库、信息或可检索的系统。

本授权中文简体字翻译版由麦格劳-希尔(亚洲)教育出版公司和机械工业出版社合作出版。此版本经授权仅限在中华人民共和国境内(不包括香港特别行政区、澳门特别行政区和台湾)销售。

版权©2010由麦格劳-希尔(亚洲)教育出版公司与机械工业出版社所有。

本书封面贴有McGraw-Hill公司防伪标签,无标签者不得销售。

封底无防伪标均为盗版

版权所有,侵权必究

本书法律顾问 北京市展达律师事务所

本书版权登记号:图字:01-2010-1514

图书在版编目(CIP)数据

信息论、编码与密码学 第2版 / (印)博斯(Bose, R.)著;武传坤,李徽译. —北京:机械工业出版社, 2010.7

(计算机科学丛书)

书名原文:Information Theory, Coding and Cryptography, Second Edition

ISBN 978-7-111-30888-1

I. 信… II. ①博… ②武… ③李… III. ①信息论 ②信源编码-编码理论 ③密码-理论
IV. ①TN911.2 ②TN918.1

中国版本图书馆CIP数据核字(2010)第102762号

机械工业出版社(北京市西城区百万庄大街22号 邮政编码 100037)

责任编辑:秦健

北京市荣盛彩色印刷有限公司印刷

2010年9月第2版第1次印刷

184mm × 260mm · 15.25印张

标准书号:ISBN 978-7-111-30888-1

定价:39.00元

凡购本书,如有缺页、倒页、脱页,由本社发行部调换

客服热线:(010) 88378991; 88361066

购书热线:(010) 68326294; 88379649; 68995259

投稿热线:(010) 88379604

读者信箱:hzsj@hzbook.com

出版者的话

文艺复兴以降，源远流长的科学精神和逐步形成的学术规范，使西方国家在自然科学的各个领域中取得了垄断性的优势；也正是这样的传统，使美国在信息技术发展的六十多年间名家辈出、独领风骚。在商业化的进程中，美国的产业界与教育界越来越紧密地结合，计算机学科中的许多泰山北斗同时身处科研和教学的最前线，由此而产生的经典科学著作，不仅肇划了研究的范畴，还揭示了学术的源变，既遵循学术规范，又自有学者个性，其价值并不会因年月的流逝而减退。

近年，在全球信息化大潮的推动下，我国的计算机产业发展迅猛，对专业人才的需求日益迫切。这对计算机教育界和出版界都既是机遇，也是挑战；而专业教材的建设在教育战略上显得举足轻重。在我国信息技术发展时间较短的现状下，美国等发达国家在其计算机科学发展的几十年间积淀和发展的经典教材仍有许多值得借鉴之处。因此，引进一批国外优秀计算机教材将对我国计算机教育事业的发展起到积极的推动作用，也是与世界接轨、建设真正的世界一流大学的必由之路。

机械工业出版社华章公司较早意识到“出版要为教育服务”。自1998年开始，我们就将工作重点放在了遴选、移译国外优秀教材上。经过多年的不懈努力，我们与Pearson, McGraw-Hill, Elsevier, MIT, John Wiley & Sons, Cengage等世界著名出版公司建立了良好的合作关系，从他们现有的数百种教材中甄选出Andrew S. Tanenbaum, Bjarne Stroustrup, Brain W. Kernighan, Dennis Ritchie, Jim Gray, Alfred V. Aho, John E. Hopcroft, Jeffrey D. Ullman, Abraham Silberschatz, William Stallings, Donald E. Knuth, John L. Hennessy, Larry L. Peterson等大师名家的一批经典作品，以“计算机科学丛书”为总称出版，供读者学习、研究及珍藏。大理石纹理的封面，也正体现了这套丛书的品位和格调。

“计算机科学丛书”的出版工作得到了国内外学者的鼎力襄助，国内的专家不仅提供了中肯的选题指导，还不辞劳苦地担任了翻译和审校的工作；而原书的作者也相当关注其作品在中国的传播，有的还专程为其书的中译本作序。迄今，“计算机科学丛书”已经出版了近两百个品种，这些书籍在读者中树立了良好的口碑，并被许多高校采用为正式教材和参考书籍。其影印版“经典原版书库”作为姊妹篇也被越来越多实施双语教学的学校所采用。

权威的作者、经典的教材、一流的译者、严格的审校、精细的编辑，这些因素使我们的图书有了质量的保证。随着计算机科学与技术专业学科建设的不断完善和教材改革的逐渐深化，教育界对国外计算机教材的需求和应用都将步入一个新的阶段，我们的目标是尽善尽美，而反馈的意见正是我们达到这一终极目标的重要帮助。华章公司欢迎老师和读者对我们的工作提出建议或给予指正，我们的联系方式如下：

华章网站：www.hzbook.com

电子邮件：hzjsj@hzbook.com

联系电话：(010) 88379604

联系地址：北京市西城区百万庄南街1号

邮政编码：100037



华章科技图书出版中心

译者序

自从Shannon在1948年发表了一篇关于通信的数学理论的论文之后，人们开始了对信息理论的系统研究。Shannon在第二年（即1949年）又发表了一篇关于安全系统的通信理论的论文，于是又引发了对信息安全的系统研究。现代信息论除了一般的信息理论部分外，它的重要组成部分还包括信源编码、信道编码和密码学。这些部分既有信息理论上的描述，又有它们自己独特的设计技术和方法。在研究上，信源编码、信道编码和密码学都相对较独立，但又有不少将它们相结合的研究。因此，有必要对这些内容进行全面了解。

目前在市场上可以见到大量关于信息论和编码方面的书，也有许多专门研究密码和信息安全的书，但将它们融为一体的书却不多见。有些书的内容过于庞杂，对需要了解这方面知识的读者来说不够简洁易懂。Bose的这本书用较短的篇幅覆盖了信息论、信源编码、信道编码和密码学部分，不仅覆盖面超出了许多大部头的书，而且也有一定的技术深度，即使这方面的专家读起来也不乏味。这种精湛的概括和有机结合是本书的主要特色，使它成为一本很好的简明参考书。因此我们组织翻译出版了本书的第1版。

随着信息科学持续高速的发展，作为信息科学领域的一些专著文献也很快表现出与最新科技发展的差距。一本负责任的科技著作应该随所涉及领域的科学技术发展而及时更新其内容。本书作者本着对读者负责的态度，及时对本书内容进行了更新，因此出版了第2版。为了让读者阅读到最新的内容，我们也相应地对新版进行了翻译。

新版的翻译工作是在第1版翻译工作的基础上进行的。新版新添加内容和更新内容的翻译工作主要由李徽完成，武传坤做了一些校对工作。武传坤将校对时发现的问题反馈给李徽，李徽进行修改后再传给武传坤，这样的校对工作反复进行了4次，其中第5章更是进行了多次修改。即便如此，我们对翻译的准确性仍没有完全的把握，欢迎读者批评指正。

最后感谢机械工业出版社对我们工作的信任，希望读者喜欢本书。

译者



机械工业出版社

北京市西城区百万庄大街24号

www.dzbook.com 国内网站

电子邮箱: dzbook@163.com 电子邮箱

010-88379604 联系电话

北京市西城区百万庄大街24号 机械工业出版社

100037 邮政编码

第2版前言

从2002年本书英文第1版问世以及随后的9次重印中，我收到了许多热情读者的来信以及在各种会议上的信息反馈。他们给了我很大的鼓励和很多的赞美之词。信息论、编码和密码学领域正在不断扩张，并且在过去的六年里，有很多新的思想产生、成熟，然后在行业标准和应用中采用。在第2版中，我们收录了许多新的知识，这能帮助那些从工科学院毕业的学生们和一些工程师们更快更有效地学习这些知识。

新版共添加了14个小节、23个新例子以及48个新练习问题。增加这些内容的目的有两个：

(1) 可以更加完整地介绍知识。这样的内容有：Shannon-Fano-Elias编码、算术编码、随机过程的熵率、马尔可夫链的熵率、最小距离的界、截短循环码、Reed-Solomon编码器详细的硬件实现、Diffie-Hellman密钥协商协议等。

(2) 可以向读者介绍当前研究趋势——那些在实际系统中应用的理论。这样的内容有：多输入多输出(MIMO)信道、MIMO系统的信道容量、低密度奇偶校验(LDPC)码、空时码、Turbo码的交织器设计、量子密码学、生物加密等。

本书的读者是电机工程系和计算机科学系的低年级研究生和高年级本科生。同样，本书也可以为那些希望开阔知识面并且掌握新技术的工程师们提供便利。

本书的结构非常适合作为研究生阶段的一门完整课。如果针对高年级本科生，下面一些章节可以跳过：1.11, 1.13, 2.7, 2.8, 3.14, 3.15, 4.11, 5.8, 5.9, 5.10, 6.13, 7.7, 7.8, 7.9, 8.13, 8.14, 8.15, 8.16和8.17。上面所选择的章节同样可以作为研究机构为业界人士提供短期培训的内容。

下面是新版中增加的内容：

第1章：Shannon-Fano-Elias编码、算术编码、随机过程的熵率和马尔可夫链的熵率。

第2章：多输入多输出(MIMO)信道、MIMO系统的信道容量。

第3章：低密度奇偶校验(LDPC)码、最小距离的界、空时分组码。

第4章：准循环码和截短循环码。

第5章：Reed-Solomon编码器详细的硬件实现，实信道上RS码性能。

第6章：Turbo码的交织器设计。

第7章：空时格码。

第8章：素数、复杂性类、椭圆曲线密码学、Diffie-Hellman密钥协商协议、量子密码学、生物加密。

所有建议、意见和问题都欢迎发信给作者，E-mail地址是rbose@ee.iitd.ac.in。

祝阅读愉快！

第1版前言

信息论、错误控制编码和密码学是现代数字通信系统中的三大支柱。这三个课题都很大，而且针对其中的任何一个课题，都有很多好书加以讨论。本书试图用有限的篇幅将信息论、错误控制编码和密码学中所有重要的概念有机地结合起来，而不需要将书写得很厚。本书的意图就是使之成为一本简洁而生动的书。

本书是我在印度理工学院 (Indian Institute of Technology, IIT) 教授有关信息论和编码的不同课题的成果。在写本书的时候，我必须决定数学在本书中应占的分量。引用Richard W. Hamming的话：“数学就是一种有趣的智力运动，但它不应该挡住获取物理过程中合理信息的路。”一本书若是太数学化就有吓倒缺乏强大数学功底的学生的危险。另一方面，如果需要把信息论和错误控制编码中的概念学到一定深度，那么数学的应用也不能无限度地减少。这样一来，就要掌握好分寸。我在本书中努力达到极好的折中：只有在非用不可的时候才用到数学。在可能的情况下都用直观的解释。我也相信借助实例来教学是很有效的方法，因此，当引入一个新概念时，我总试图给出至少一个例子。

如何阅读本书

本书不但是对信息论、编码和密码学这一令人着迷的领域的生动介绍，而且还涉及相当有深度的详细内容。全书共分三个逻辑部分：

第一部分：信息论和信源编码

第二部分：错误控制编码（信道编码）

第三部分：安全通信编码

第一部分包括两章——第1章讨论信息的概念及其有效的表示方式。信息的有效表示引起数据压缩。本章还介绍了游程编码的概念、率失真函数和优化量化器的设计。本章最后简单介绍了图像压缩。

第2章讨论通信信道和信道容量的概念。本章试图回答这样的问题：给定一个已知带宽和信噪比的信道，该信道每秒可传递多少比特的信息呢？这同时也提出了错误控制编码的必要性。

第二部分包括五章内容，都是关于错误控制编码的——第3章介绍线性分组码。线性分组码是很有实用价值、指导性强而且简单的一类码。我们将讨论这类码的编码和译码策略，同时还将介绍完备码、最优线性码和最大距离可分 (MDS) 码的概念。

第4章讨论的是循环码，这是线性分组码的子类。循环码对纠正突发性错误特别有用。Fire码、Golay码和循环冗余校验 (CRC) 码都是特殊类型的循环码，本章对它们也进行了讨论。本章以循环码的电路实现结束。

第5章将读者带到BCH (Bose-Chaudhuri Hocquenghem) 码的世界，这是一类可纠正多个错误的功能极强的码。本章还讨论了Reed-Solomon码——BCH码的子类。

第6章讨论的是卷积码，这是一类本质上带记忆的码。本章将介绍网格码的概念并详细讨论维特比译码技术。还探讨了一些已知的好卷积码。最后介绍的是Turbo码，这是一类还不太旧的码。

第7章讨论网格编码调制 (TCM)，这是一种将编码和调制相结合的方案。本章将讨论TCM的编码和译码方法。读者将学到如何为加性高斯白噪声信道 (additive white Gaussian noise channel) 及衰退信道设计TCM方案。

第三部分仅包含关于密码学的一章——第8章，将介绍编码的另一种用法，即在安全通信方面的编码。本章将通过实例分别讨论保密密钥和公钥加密技术。还将讨论单向散列和应用混沌函数进行加密等其他技术。本章在结尾时给出了关于密码学政治因素的一个注解。

我试图在所有需要的地方引入实例。每章在结束时都有一个结论性的评论，包含描述重要结果和贡献来源的简单历史性评注。每章最后还有一个简单总结，可作为概括性参考或对某一特殊公式或定义的快速查找工具，也可直接为读者考试前的准备增加信心。每章后面的练习题能帮助读者将文中讨论的概念具体化。每章后面还加进了基于计算机的练习题，建议将这些练习题变成学习本课程的一部分。

我尽了最大努力使书中没有错误，遗憾的是没有一种简单易行的错误控制技术。我试图包括所有与本领域有关的重要的、实际的和有趣的概念。欢迎读者将发现的错误、遗漏及其他建设性建议发送到 rbose@ee.iitd.ac.in。

最后，我引用Blaise Pascal的话作结，他说：“一个人在写书过程中了解到的最后一件事是把什么内容作为开始。”

致谢

我想感谢印度理工学院电机工程系提供的令人振奋的学术环境，特别感谢S. C. Dutta Roy教授、Surendra Prasad教授、H. M. Gupta教授、V. K. Jain教授、Vinod Chandra教授、Santanu Chaudhury教授、S. D. Joshi教授、Sheel Aditya教授、Devi Chadha教授、D. Nagchoudri教授、G. S. Visweswaran教授、R. K. Patney教授、V. C. Prasad教授、S. S. Jamuar教授和R. K. P. Bhatt教授。对与Subrat Kar博士、Ranjan K. Mallik博士和Shankar Prakriya博士的友好讨论也很感激。我很庆幸有几批杰出的学生，他们的反馈对改善本书内容很有帮助。每章后面的许多练习题都曾作为学生作业或考试题使用过。

我从内心感激宾夕法尼亚大学的Bernard D. Steinberg教授，他一直引领着我，是我的良师益友，也是我博士论文的指导教师。对每当我请求帮助时总是给予支持和建议的Tel Aviv大学的Avraham Freedman教授我也心存感激。感谢德国Darmstadt理工大学的Rolf Jakoby教授就各种主题所做的令人鼓舞的讨论。我想感谢印度科学学院 (Indian Institute of Science) 电子通信工程小组的B. Sundar Rajan教授，我们曾就撰写此书做了初步的讨论。

K. Vasudevan	IIT电机工程系, Kanpur
Pankaj Joshi	Jodhpur工程学院及研究中心电子与通信工程系, Jodhpur
Tanveer Hassan	阿里格尔穆斯林大学工学院, Aligarh
S. L. Maskara	Jaypee科技信息研究所, Noida
Azizar Rahaman	未来信息职业技术学院计算机工程与科学系, Kolkata
Indrajit Das	梅格纳德萨哈技术学院计算机工程与科学系, Kolkata
Anindya Jyoti Pal	Heritage技术研究所, Kolkata
B. P. Pati	ETCE部门马哈拉施特拉邦工程院院士, Pune
M. Murugan	VIIT ETCE部门, Pune
J. N. Sarvaiya	SVNIT电机工程系, Surat

- Vikram Gadre IIT电机工程系, Mumbai
 M. Padmini MVJ工程学院, Bangalore
 Suresh Kuri Gogte技术研究所, Belgaum
 Mandi V. Mahalinga 安贝德卡技术研究所, Bangalore
 Prakasa Rao 政府工程学院ECE部门, Warangal
 C. R. Nataraj Sri Jayachamarajendra技术学院 (VTU), Mysore

我深深感激我的父母,因为他们给了我一生的爱和精神支持。我也感谢我的祖父母给我的祝福,和我弟弟Shantanu关于某些题目的无尽的讨论。

最后,我想感谢我的妻子也是最好的朋友, Aloka,她在我写本书的每一阶段都给予鼓励。她那建设性的意见和恰当的批评使本书更具有可读性。是她那无限的耐心、永久的支持、理解、爱、牺牲精神和幽默感才使我写这本书的梦想得以实现。

作者简介

Ranjan Bose 印度理工学院 (IIT) 电机工程系的教授。他在IIT (Kanpur分校) 的电机工程系获得工学学士学位,在美国宾夕法尼亚大学电机工程系获得硕士和博士学位。之后在Alliance半导体公司任高级设计工程师。自1997年11月,他成为印度理工学院的教员。他在1999年获得URSI青年科学家奖,在2000年7月获得Humboldt研究奖金,在2003年获得印度国家科学院青年工程师奖,在2004年获得青年教师AICTE事业奖和2005年由印度科技部颁发的BOYSCAST奖金。

目 录

出版者的话

译者序

第2版前言

第1版前言

第一部分 信息论和信源编码

第1章 信源编码 1

1.1 信息论简介 1

1.2 不确定性和信息 2

1.3 平均互信息和熵 6

1.4 连续随机变量的信息度量 9

1.5 信源编码定理 10

1.6 霍夫曼编码 15

1.7 Shannon-Fano-Elias编码 21

1.8 算术编码 22

1.9 Lempel-Ziv算法 23

1.10 游程编码和PCX格式 25

1.11 率失真函数 26

1.12 优化量化器的设计 29

1.13 随机过程的熵率 30

1.14 图像压缩简介 31

1.15 无损压缩的JPEG标准 32

1.16 有损压缩的JPEG标准 33

1.17 评注 34

1.18 小结 35

习题 37

上机习题 39

第2章 信道容量和编码 41

2.1 引言 41

2.2 信道模型 42

2.3 信道容量 43

2.4 信道编码 45

2.5 信息容量定理 48

2.6 Shannon限 50

2.7 MIMO系统的信道容量 51

2.8 码的随机选取 52

2.9 评注 57

2.10 小结 57

习题 58

上机习题 60

第二部分 错误控制编码 (信道编码)

第3章 纠错线性分组码 61

3.1 纠错码简介 61

3.2 基本定义 62

3.3 线性分组码的矩阵描述 65

3.4 等价码 66

3.5 奇偶校验矩阵 68

3.6 线性分组码的译码 70

3.7 伴随式译码 75

3.8 译码后的错误概率 (纠错概率) 75

3.9 完备码 78

3.10 汉明码 80

3.11 低密度奇偶校验 (LDPC) 码 81

3.12 最优线性码 83

3.13 最大距离可分 (MDS) 码 84

3.14 最小距离的界 84

3.15 空时分组码 85

3.16 评注 87

3.17 小结 87

习题 88

上机习题 90

第4章 循环码 91

4.1 循环码简介 91

4.2 多项式 91

4.3 多项式的除法算法 92

4.4 一种循环码的生成方法 96

4.5 循环码的矩阵描述 98

4.6 准循环码和截短循环码	101	6.10 著名的好卷积码	158
4.7 突发错误纠错	101	6.11 Turbo码	160
4.8 Fire码	103	6.12 Turbo译码	162
4.9 Golay码	103	6.12.1 改进的Bahl、Cocke、Jelinek和 Raviv (BCJR) 算法	162
4.9.1 二元Golay码	103	6.12.2 迭代MAP译码	163
4.9.2 三元Golay码	104	6.13 Turbo码的交织器设计	166
4.10 循环冗余校验 (CRC) 码	104	6.14 评注	167
4.11 循环码的电路实现	106	6.15 小结	167
4.12 评注	110	习题	169
4.13 小结	110	上机习题	171
习题	112	第7章 网格编码调制	173
上机习题	113	7.1 网格编码调制(TCM)简介	173
第5章 BCH码	114	7.2 编码调制的概念	173
5.1 BCH码简介	114	7.3 通过集合分割的映射	177
5.2 基本引理	114	7.4 Ungerboeck的TCM设计准则	180
5.3 极小多项式	115	7.5 TCM译码器	183
5.4 极小多项式作为生成多项式	118	7.6 AWGN信道性能评估	184
5.5 一些BCH码实例	118	7.7 d_{free} 的计算	189
5.6 BCH码的译码	122	7.8 衰退信道的TCM	190
5.7 Reed-Solomon码	125	7.9 空时网格码	193
5.8 Reed-Solomon码编码器和译码器 的实现	127	7.9.1 缓慢雷利衰退	194
5.8.1 硬件实现	127	7.9.2 快速雷利衰退	195
5.8.2 软件实现	128	7.10 评注	195
5.9 实信道上RS码性能	129	7.11 小结	195
5.10 嵌套码	131	习题	197
5.11 评注	132	上机习题	200
5.12 小结	133		
习题	134	第三部分 安全通信编码	
上机习题	135	第8章 密码学	203
第6章 卷积码	136	8.1 密码学简介	203
6.1 卷积码简介	136	8.2 加密技术概述	204
6.2 树码和网格码	136	8.3 加密算法所用到的运算	206
6.3 卷积码的多项式描述 (解析表示)	140	8.4 对称 (保密密钥) 密码学	206
6.4 卷积码的距离概念	144	8.5 数据加密标准 (DES)	208
6.5 生成函数	146	8.6 国际数据加密算法 (IDEA)	210
6.6 卷积码的矩阵描述	148	8.7 RC密码	211
6.7 卷积码的维特比译码	150	8.8 非对称 (公钥) 算法	212
6.8 卷积码的距离界	155	8.9 RSA算法	212
6.9 性能界	157	8.10 全球电子邮件加密标准	215

8.11 单向散列变换	216	8.18 密码分析	223
8.12 其他技术	217	8.19 密码学中的政治因素	224
8.13 椭圆曲线密码学	218	8.20 评注	225
8.14 Diffie-Hellman密钥协商协议	219	8.21 小结	227
8.15 利用混沌理论实现安全通信	221	习题	228
8.16 量子密码学	221	上机习题	231
8.17 生物加密	222		

第一部分 信息论和信源编码

第1章 信源编码

并不是我们注意到的每一件事都重要，也不是每一件重要的事我们都注意到了。

爱因斯坦 (1879—1955)

1.1 信息论简介

今天，我们生活在信息时代。因特网 (Internet) 已经成为我们生活中不可缺少的一部分，这使得太阳系第三大行星成为一个地球村。人们通过手机交谈已经是一件很平常的事。电影可以以DVD碟片的形式租回家欣赏。名片上印上电子邮箱和网址也很正常。许多人宁愿给朋友发送电子邮件和电子贺卡而不去发普通信件。股票行情也可以通过手机来查看。

信息已成为成功的关键 (它一直是成功的关键之一，但在今天的世界上它是最关键的)。在所有这些信息的背后，信息的交换却依靠小小的1和0 (即无所不在的比特)，通过它们一个接一个地排在一起来表达信息。我们今天所生活的信息时代的存在主要归功于发表于1948年的一篇精辟的论文，这篇论文为奇妙的信息论奠定了基础。信息论的创始人是美国电子工程师Claude E. Shannon，他在发表于*Bell System Technical Journal* (1948) 的论文“The Mathematical Theory of Communication” (通信的数学理论) 中阐述了自己的思想。广义地说，信息包括一切标准通信媒体的内容，如电报、电话、无线电、电视以及来自电子计算机、伺服机械装置系统和其他数据处理器件的信号。该理论甚至可应用于人体和其他动物神经网络的信号。

信息论最关注的是发现能描述为通信和处理信息而设计的控制系统的数学定律。它建立量化指标来度量信息以及不同系统在传输、储存和处理信息时的容量。有些要解决的问题与发现最好的使用各种已有通信系统的方法相关，也和最好的将有用的信息或信号同无用的信息或噪声分开的方法有关。另一个问题就是对给定的信息载体 (通常称为信道) 给出容量上界。尽管主要是通信工程师对那些结果感兴趣，但有些概念已被诸如心理学和语言学等领域采用并发现它们很有用。

信息论的界限非常模糊。这种理论与通信理论有很大的重叠部分，但它主要面向信息处理和通信方面的基本限制，而较少涉及所用元器件的详细运作情况。

本章，我们将首先阐述对信息的直观理解。然后用数学模型来描述信息源以及对信息源所发出的信息的量化度量。然后我们将陈述并证明信源编码定理。有了基本的数学框架之后，我们将介绍四种信源编码技术，即Huffman编码、Shannon-Fano-Elias编码、算术 (Arithmetic) 编码和Lempel-Ziv编码。本章还将讨论游程编码 (Run Length Encoding)、率失真函数 (Rate Distortion Function) 和优化量化器 (Optimum Quantizer)。为了说明相关的随机变量，我们将学习随机过程的熵率。本章后面介绍图像压缩，它是信源编码的一个重要应用领域。特别是，我们将简单讨论JPEG (Joint Photographic Experts Group) 标准。

1.2 不确定性和信息

任何信源,不管是模拟的还是数字的,都产生本质上随机的输出。假若不是随机,即我们能准确地知道其输出,那么就没必要传输它!信源存在模拟信源和离散信源两种。我们生活在一个模拟世界里,多数信源都是模拟信源,例如语音、温度波动等。离散信源都是人造的信源,例如从有限字母集中产生一连串字母(如,写电子邮件)的信源(如,人)。

在进一步介绍信息的数学度量之前,让我们先找一下直观感觉。请阅读下面的句子:

(1) 明天太阳将从东边升起。

(2) 在一小时后电话会响。

(3) 今年冬天德里将下雪。

这三个句子带有不同量的信息。事实上,第一个句子几乎带不来任何信息,因为每个人都知道太阳从东边升起,也就是说这件事再次发生的概率几乎为1(N. Bohr说道:“作预言是有风险的,特别是在涉及将来的时候。”)。第二个句子看来比第一个句子带来更多的信息,因为电话可能响,也可能不响。电话在一小时后响的概率是有限的(除非维修人员又在工作!)。最后一个句子你可能要读两遍,因为德里从来没下过雪,因此德里下雪的概率非常低。有趣的是,上述句子所携带的信息量与句子中所陈述的事件发生的概率有关,而且我们也观察到相反的关系。第一个句子讲的是发生概率几乎为1的事件,它几乎没带什么信息。第三个句子发生的概率很低,看来带来了不少的信息。(我们应读上两遍以确定没看错!)另外可以注意到句子的长度与所携带的信息量无关。事实上,第一个句子最长但所携带的信息量最少。

现在我们将建立信息的数学度量。

定义1.1 考虑可能输出为 $x_i, i=1, 2, \dots, n$ 的离散随机变量 X 。则事件 $X=x_i$ 的自信息(self-information)定义为

$$I(x_i) = \log \left(\frac{1}{P(x_i)} \right) = -\log P(x_i) \quad (1-1)$$

我们注意到高概率事件没有低概率事件所携带的信息多。对于 $P(x_i)=1$ 的事件,有 $I(x_i)=0$ 。因为低概率事件意味着高度的不确定性(反之亦然),具有高度不确定性的随机变量带来更多的信息。我们在本章中将一直用不确定性和信息量的这种相关性作自然解释。

$I(x_i)$ 的单位取决于取对数的底数,通常取为2或e。当以2为底数时,单位为比特(bit),而当以e为底数时,单位为奈特(nat, 自然单位)。由于 $0 \leq P(x_i) \leq 1$,故 $I(x_i) \geq 0$,即自信息是非负的。下面的两个例子说明为什么用对数来度量信息是合适的。

例1.1 考虑一个掷硬币的二元信源:若正面(H)出现则输出1,若反面(T)出现则输出0。对于该信源,有 $P(1)=P(0)=0.5$ 。来自该信源的每一个输出所含的信息量为

$$\begin{aligned} I(x_i) &= -\log_2 P(x_i) \\ &= -\log_2 P(0.5) = 1 \text{ (bit)} \end{aligned} \quad (1-2)$$

事实上,我们只能用1比特来表示来自这个二元信源的输出(例如,我们用1代表H,用0代表T)。

现在假定从该二元信源连续输出是统计独立的,即信源是无记忆的。考虑一个 m bit的数组,则共有 2^m 个可能的 m 比特组,每一个都等可能地具有概率 2^{-m} 。

一个 m 比特组的自信息为

$$I(x_i) = -\log_2 P(x_i) = -\log_2 2^{-m} = m \text{ (bit)} \quad (1-3)$$

同时,我们也注意到确实需要 m 个比特来表示可能的 m 比特组。

因此,当信源的一些输出被看做一个组的时候,这种信息的对数度量具有所期望的可加性。

例1.2 考虑一个离散无记忆信源(DMS)(信源C),它的输出为每次两个比特。该信源由例1.1中提到的两个二元信源(信源A和B)构成,每个信源贡献一个比特。信源C中的这两个二元信源是独立的。从直觉上看,组合信源(信源C)的信息量应该是组成该信源的两个独立信源的输出所含信息之和。让我们分析一下信源C的输出所含的信息量。有四种可能的情况{00, 01, 10, 11},每种情况都具有概率 $P(C) = P(A)P(B) = (0.5) \times (0.5) = 0.25$,这是因为信源A和B是独立的。信源C的每个输出所含的信息量为:

$$I(C) = -\log_2 P(x_i) = -\log_2 P(0.25) = 2 \text{ (bit)} \quad (1-4)$$

我们不得不用两比特来表示这个组合二元信源的输出。

因此,信息的对数度量对独立事件具有可加性。

下面考虑两个离散随机变量 X 和 Y ,其可能的输出分别为 $x_i, i=1, 2, \dots, n$ 和 $y_j, j=1, 2, \dots, m$ 。假设我们观察到输出 $Y=y_j$,想由此确定该事件所提供的关于事件 $X=x_i, i=1, 2, \dots, n$ 的信息量,也就是说我们想用数学方式表示出它们的互信息。我们注意到两种极端的情况:

- (1) X 和 Y 独立,在此情况下, $Y=y_j$ 的出现不提供任何 $X=x_i$ 的信息。
- (2) X 和 Y 为完全依赖的事件,在此情况下, $Y=y_j$ 的出现决定了 $X=x_i$ 的出现。

满足此条件的一种合适的度量是对条件概率

$$P(X=x_i|Y=y_j) = P(x_i|y_j) \quad (1-5)$$

除以概率

$$P(X=x_i) = P(x_i) \quad (1-6)$$

所得的商取对数。

定义1.2 定义 x_i, y_j 之间的互信息 $I(x_i; y_j)$ 为

$$I(x_i; y_j) = \log \left(\frac{P(x_i|y_j)}{P(x_i)} \right) \quad (1-7)$$

同前面一样, $I(x)$ 的单位取决于取对数的底数,通常为2或e。当底数为2时,单位为比特。

注意

$$\frac{P(x_i|y_j)}{P(x_i)} = \frac{P(x_i|y_j)P(y_j)}{P(x_i)P(y_j)} = \frac{P(x_i, y_j)}{P(x_i)P(y_j)} = \frac{P(y_j|x_i)}{P(y_j)} \quad (1-8)$$

因此

$$I(x_i; y_j) = \log \left(\frac{P(x_i|y_j)}{P(x_i)} \right) = \log \left(\frac{P(y_j|x_i)}{P(y_j)} \right) = I(y_j; x_i) \quad (1-9)$$

对 $I(x_i; y_j) = I(y_j; x_i)$ 的自然解释如下:事件 $Y=y_j$ 的出现所提供的关于 $X=x_i$ 的信息完全等同于事件 $X=x_i$ 的出现所提供的关于 $Y=y_j$ 的信息。

现在让我们查看两种极端情况:

(1) 当随机变量 X 与 Y 统计独立时, 有 $P(x_i|y_j) = P(x_i)$, 它导致 $I(x_i; y_j) = 0$ 。

(2) 当事件 $Y = y_j$ 的出现惟一决定事件 $X = x_i$ 的出现时, 有 $P(x_i|y_j) = 1$, 从而互信息为

$$I(x_i; y_j) = \log \left(\frac{1}{P(x_i)} \right) = -\log P(x_i) \quad (1-10)$$

这就是事件 $X = x_i$ 的自信息。

因此, 互信息的对数定义确认了我们的直觉。

例1.3 考虑图1-1所示的二元对称信道 (BSC)。这是一种从发射端 (Tx) 到接收端 (Rx) 传递许多1和0的信道。它偶尔以概率 p 发生错误。一个BSC会把1变为0, 也以同样概率把0变为1。令随机变量 X 和 Y 分别表示该BSC的输入和输出, 并设输入符号等可能地出现, 而且输出符号根据下面的信道转移概率依赖于输入:

$$P(Y=0|X=0) = 1-p$$

$$P(Y=0|X=1) = p$$

$$P(Y=1|X=1) = 1-p$$

$$P(Y=1|X=0) = p$$

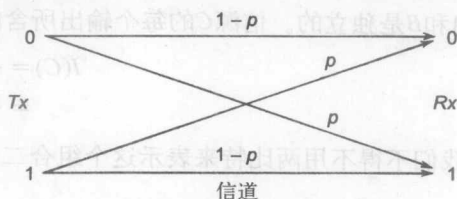


图1-1 一个二元对称信道

这说明在该BSC中传输时, 数字发生转变 (即出错) 的概率为 p 。从这些信道转移概率中我们得到

$$\begin{aligned} P(Y=0) &= P(X=0) \times P(Y=0|X=0) + P(X=1) \times P(Y=0|X=1) \\ &= 0.5(1-p) + 0.5(p) = 0.5 \end{aligned}$$

$$\begin{aligned} P(Y=1) &= P(X=0) \times P(Y=1|X=0) + P(X=1) \times P(Y=1|X=1) \\ &= 0.5(p) + 0.5(1-p) = 0.5 \end{aligned}$$

假定我们在接收端根据接收到的信号想确定从发送端发送的是什么。在给定 $Y=0$ 的情况下, 关于事件 $X=0$ 发生的互信息为

$$I(x_0; y_0) = I(0; 0) = \log_2 \left(\frac{P(Y=0|X=0)}{P(Y=0)} \right) = \log_2 \left(\frac{1-p}{0.5} \right) = \log_2 2(1-p)$$

类似地,

$$I(x_1; y_0) = I(1; 0) = \log_2 \left(\frac{P(Y=0|X=1)}{P(Y=0)} \right) = \log_2 \left(\frac{p}{0.5} \right) = \log_2 2p$$

下面我们考虑一些特殊情况。

假定 $p=0$, 即为理想信道 (无噪声), 则

$$I(x_0; y_0) = I(0; 0) = \log_2 2(1-p) = 1 \text{ (bit)}$$

因此, 从输出我们可以确定所传送的是什么。回想一下事件 $X = x_0$ 的自信息也是1bit。

但是, 若 $p=0.5$, 我们得到

$$I(x_0; y_0) = I(0; 0) = \log_2 2(1-p) = \log_2 2(0.5) = 0$$

很明显, 从输出我们得不到关于发送的是什么的任何信息。因此, 这是个无用信道。对于

这样的—个信道，我们可以在接收端用掷硬币的方法来确定发送的是什么。

假设我们有一个 $p=0.1$ 的信道，则

$$I(x_0; y_0) = I(0; 0) = \log_2 2(1-p) = \log_2 2(0.9) = 0.848 \text{ (bit)}$$

例1.4 令 X 和 Y 为表示图1-2所示的二元信道的输入和输出的二元随机变量。假定输入的符号等可能地选取，而且输出符号根据下面的信道转移概率依赖于输出：

$$P(Y=0|X=0) = 1-p_0$$

$$P(Y=0|X=1) = p_1$$

$$P(Y=1|X=1) = 1-p_1$$

$$P(Y=1|X=0) = p_0$$

由信道转移概率我们得到

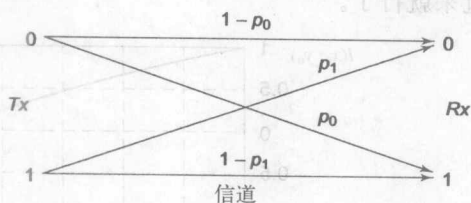


图1-2 一个非对称概率的二元信道

$$\begin{aligned} P(Y=0) &= P(X=0).P(Y=0|X=0) + P(X=1).P(Y=0|X=1) \\ &= 0.5(1-p_0) + 0.5(p_1) = 0.5(1-p_0+p_1) \end{aligned}$$

$$\begin{aligned} P(Y=1) &= P(X=0).P(Y=1|X=0) + P(X=1).P(Y=1|X=1) \\ &= 0.5(p_0) + 0.5(1-p_1) = 0.5(1-p_1+p_0) \end{aligned}$$

假设我们在接收端想根据所收到的信号来确定在发送端发送的是什么。在给定 $Y=0$ 的情况下，关于事件 $X=0$ 发生的互信息为

$$I(x_0; y_0) = I(0; 0) = \log_2 \left(\frac{P(Y=0|X=0)}{P(Y=0)} \right) = \log_2 \left(\frac{1-p_0}{0.5(1-p_0+p_1)} \right) = \log_2 \left(\frac{2(1-p_0)}{1-p_0+p_1} \right)$$

类似地，

$$I(x_1; y_0) = I(1; 0) = \log_2 \left(\frac{P(Y=0|X=1)}{P(Y=0)} \right) = \log_2 \left(\frac{2p_1}{1-p_0+p_1} \right)$$

定义1.3 定义在给定 $Y=y_j$ 的情况下，事件 $X=x_i$ 的条件自信息 (conditional self information) 为

$$I(x_i | y_j) = \log \left(\frac{1}{P(x_i | y_j)} \right) = -\log P(x_i | y_j) \quad (1-11)$$

由此，我们可以写为

$$I(x_i; y_j) = I(x_i) - I(x_i | y_j) \quad (1-12)$$

条件自信息可解释为在事件 $Y=y_j$ 的基础上关于事件 $X=x_i$ 的自信息。回顾上述结论 $I(x_i) \geq 0$ 及 $I(x_i | y_j) \geq 0$ ，因此，当 $I(x_i) < I(x_i | y_j)$ 时，有 $I(x_i; y_j) < 0$ ，而当 $I(x_i) > I(x_i | y_j)$ 时，有 $I(x_i; y_j) > 0$ 。因此，互信息可为正、负或0。

例1.5 考虑例1.3中的BSC。互信息 $I(x_0; y_0)$ 关于错误概率 p 的对应平面图如图1-3所示。

从图1-3可以看出，当 $p > 0.5$ 时， $I(x_0; y_0)$ 为负值。对此的自然解释为：一个负值互信息表明我们在观察到 $Y=y_0$ 时，应避免选取 $X=x_0$ 作为发送的比特。

对 $p=0.1$ ，

$$I(x_0; y_1) = I(0; 1) = \log_2 2(p) = \log_2 2(0.1) = -2.322 \text{ (bit)}$$