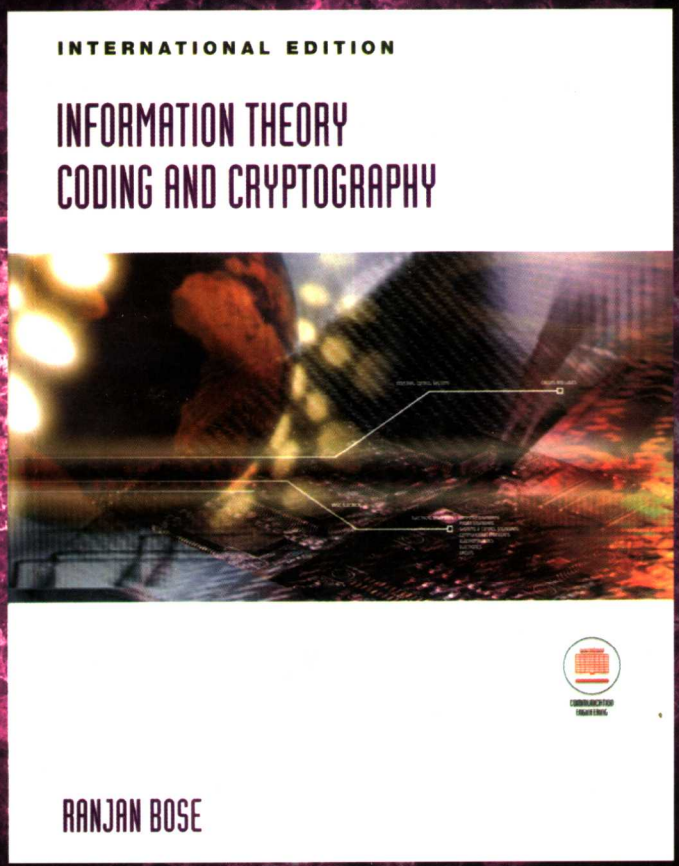
计 算 机 科 学 丛 书

信息论、编码与密码学

Ranjan Bose 著 武传坤 译



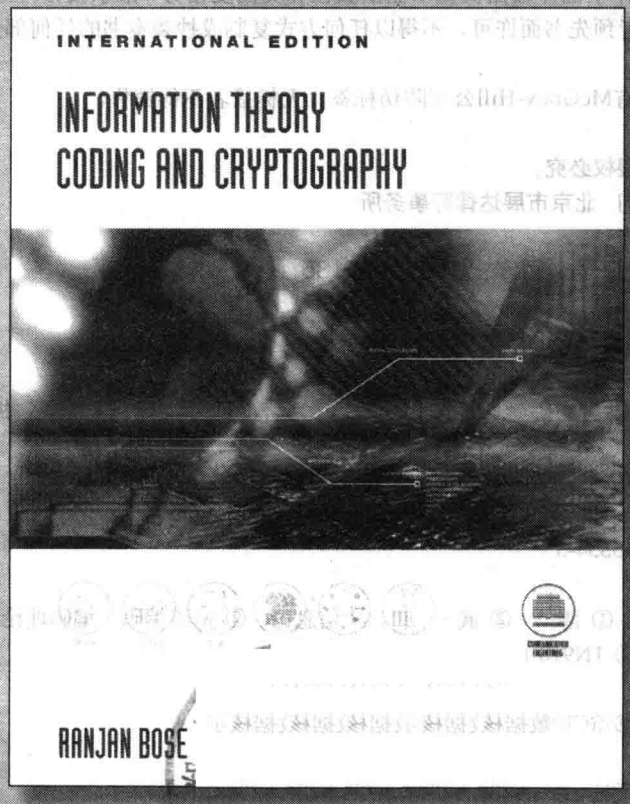
Information Theory, Coding and Cryptography

机械工业出版社
China Machine Press

计 算 机 科 学 丛 书

信息论：编码与密码学

Ranjan Bose 著 武传坤 译



Information Theory, Coding and Cryptography

机械工业出版社
China Machine Press

本书集中介绍了信息论、信源编码、信道编码和密码等方面的知识，不仅内容丰富，而且技术深度适当。适合作为高等学校信息安全、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。

本书版权登记号：图字：01-2003-5135

图书在版编目（CIP）数据

信息论、编码与密码学 /博斯（Bose, R.）著；武传坤译. -北京：机械工业出版社，2005.1
（计算机科学丛书）
书名原文：Information Theory, Coding and Cryptography
ISBN 7-111-15534-3

Ⅰ.信… Ⅱ.① 博… ② 武… Ⅲ.① 信息论 ② 信道编码－编码理论 ③ 密码－理论
Ⅳ.① TN911.2 ② TN918.1

中国版本图书馆CIP数据核字（2004）第112313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：王镇元
北京瑞德印刷有限公司印刷 · 新华书店北京发行所发行
2005年1月第1版第1次印刷
787mm × 1092mm 1/16 · 13.75印张
印数：0 001 - 4 000册
定价：29.00元

凡购本书，如有倒页、脱页、缺页，由本社发行部调换
本社购书热线：（010）68326294

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，不仅擘划了研究的范畴，还揭橥了学术的源变，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、从业人员较少的现状下，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图文信息有限公司较早意识到“出版要为教育服务”。自1998年开始，华章公司就将工作重点放在了遴选、移译国外优秀教材上。经过几年的不懈努力，我们与Prentice Hall，Addison-Wesley，McGraw-Hill，Morgan Kaufmann等世界著名出版公司建立了良好的合作关系，从它们现有的数百种教材中甄选出Tanenbaum，Stroustrup，Kernighan，Jim Gray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、研究及庋藏。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，有的还专诚为其书的中译本作序。迄今，“计算机科学丛书”已经出版了近百个品种，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，为进一步推广与发展打下了坚实的基础。

随着学科建设的初步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步入一个新的阶段。为此，华章公司将加大引进教材的力度，在“华章教育”的总规划之下出版三个系列的计算机教材：除“计算机科学丛书”之外，对影印版的教材，则单独开辟出“经典原版书库”；同时，引进全美通行的教学辅导书“Schaum's Outlines”系列组成“全美经典学习指导系列”。为了保证这三套丛书的权威性，同时也为了更好地为学校和老师们服务，华章公司聘请了中国科学院、北京大学、清华大学、国防科技大学、复旦大学、上海交通大学、南京大学、浙江大学、中国科技大学、哈尔滨工业大学、西安交通大学、中国人民大学、北京航空航天大学、北京邮电大学、中山大学、解放军理工大学、郑州大学、湖北工学院、中国国家信息安全测评认证中心等国内重点大学和科研机构在计算机的各个领域的著名学者组成“专家指导委员会”，为我们提供选题意见和出版监督。

这三套丛书是响应教育部提出的使用外版教材的号召，为国内高校的计算机及相关专业

的教学度身订造的。其中许多教材均已为M. I. T.，Stanford，U.C. Berkeley，C. M. U. 等世界名牌大学所采用。不仅涵盖了程序设计、数据结构、操作系统、计算机体系结构、数据库、编译原理、软件工程、图形学、通信与网络、离散数学等国内大学计算机专业普遍开设的核心课程，而且各具特色——有的出自语言设计者之手、有的历经三十年而不衰、有的已被全世界的几百所高校采用。在这些圆熟通博的名师大作的指引之下，读者必将在计算机科学的宫殿中由登堂而入室。

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，但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。教材的出版只是我们的后续服务的起点。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，我们的联系方法如下：

电子邮件：hzedu@hzbook.com
联系电话：（010）68995264
联系地址：北京市西城区百万庄南街1号
邮政编码：100037

专家指导委员会

（按姓氏笔画顺序）

尤晋元	王　珊	冯博琴	史忠植	史美林
石教英	吕　建	孙玉芳	吴世忠	吴时霖
张立昂	李伟琴	李师贤	李建中	杨冬青
邵维忠	陆丽娜	陆鑫达	陈向群	周伯生
周立柱	周克定	周傲英	孟小峰	岳丽华
范　明	郑国梁	施伯乐	钟玉琢	唐世渭
袁崇义	高传善	梅　宏	程　旭	程时端
谢希仁	裘宗燕	戴　葵		

秘　书　组

武卫东	温莉芳	刘　江	杨海玲

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。这些部分既有信息理论上的描述，也有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，因此它是一本很好的简明的参考书。

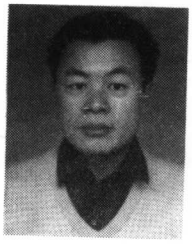
在翻译过程中对个别术语的译法我们请教了不同的专家。有些术语本身就有不同的中文译法，我们无法确定哪一种更流行，因此就选取其中的一种，但在全书中保持前后一致。我们在翻译中力求忠于原著，但由于翻译水平有限，个别地方翻译尚欠流畅。同时在翻译过程中针对原著中的一些错误，绝大部分都已改正过来，但碍于我们知识面和理解方面的不足，难免挂一漏万。所有这些都敬请读者批评指正。

希望这本书能对充实读者的知识，加深对理论的理解有所帮助。

译 者

2004年6月

译者简介



武传坤　中国科学院软件所信息安全国家重点实验室研究员。他在曲阜师范学院获理学学士学位，在西安电子科技大学获理学硕士和工学博士学位。1988年起任教于西安电子科技大学，先后被评为讲师、副教授和教授。1995年9月到澳大利亚昆士兰理工大学做博士后，之后在西悉尼大学做研究员，在澳大利亚国立大学任教。于2003年被选为中科院“百人计划”资助的研究员。

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简洁而生动的一本书。

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的话，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衷：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，而且还涉及到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：保密通信中的编码。

第一部分包括两章——第1章讨论信息及其有效表示方式的概念。信息的有效表示导致数据压缩。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。本章结束时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，该信道每秒中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、最优码和最大距离可分码（MDS）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码和循环冗余度校验码（CRC）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来结束。

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。将介绍Trellis码的概念及Viterbi详细译码技术。还探讨了一些已知的好的卷积码。最后介绍的是Trubo码，这是一类还不太旧的码。

第7章讨论Trellis编码调制（TCM），这是一种将编码和调制相结合的方案。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，即在保密通信方面的编码。本章将通过实例分别讨论保密密钥和公钥加密技术。还将讨论单向杂凑和应用浑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

Ranjan Bose

于新德里

致　谢

我想感谢印度理工学院（Indian Institute of Technology, IIT）电子工程系提供的令人振奋的学术环境，特别地想感谢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被使用过。

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。对于每当我请求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。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。

我想对为本书初稿给出有价值的反馈意见的下列人员表示感谢，他们是IIT Kanpur 的Ravi Motwani教授、IIT Kanpur 的A.K.Chaturvedi教授、Anna大学的N.Kumaravel教授、GITAM工程学院的V.Maleswara Rao教授、政府工程学院的M.Chandrasekaran教授和IIT Mumbai的Vikram Gadre教授。

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

最后，我想感谢我的妻子也是最好的朋友，Aloka，她在我写这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对使本书更具有可读性起了很大的帮助。是她那无限的耐心、永久的支持、理解和幽默感才使我写这本书的梦想得以实现。

Ranjan Bose

于新德里

作者简介

Ranjan Bose 印度理工学院（IIT）电力工程系的副教授。他在IIT（Kanpur分校）的电力工程系获得工学学士学位，美国宾夕法尼亚大学电力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，他成为印度技术学院的教员。Bose博士经常做编码和密码学方面的演讲。他在1999年获得URSI青年科学家奖，在2000年7月获得Humboldt研究金。

目　录

第三部分 安全通信编码

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。许多人宁愿给朋友送去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、电视以及来自于电子计算机、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，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，我们将介绍两种信源编码技术，即**Huffman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）。本章结束时介绍图像压缩，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。假若不是随机的话，即我们能准确地知道其输出，那么就没必要传输它！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。离散的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）。

4 在我们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：

（a）明天太阳将从东边升起。

（b）在一小时后电话会响。

（c）今年冬天德里将有雪。

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，也就是说这事再次发生的概率几乎为1。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！）。最后一个句子可能你要读两遍，因为德里从来没下过雪，因此德里下雪的概率非常低。有趣的是注意到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（使我们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，$i=1, 2, \ldots, n$的离散随机变量X。则事件$X=x_i$的自信息*（self-information）*定义为*

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

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$P(x)=1$的事件，有$I(x)=0$。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有更多的信息。我们在本章中将一直用不确定性和信息量的这种相关性做自然解释。

$I(x)$ 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$0 \leqslant P(x_i) \leqslant 1$，故$I(x_i) \geqslant 0$，即自信息是

5 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

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

事实上，我们只能用1比特来表示从这个二元信源的输出（例如我们用1来代表H，用0来代表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

$$\begin{aligned} I(x_i) &= -\log_2 P(x_i) \\ &= -\log_2 2^{-m} = m \text{ (bit)} \end{aligned} \tag{1-3}$$

同时，我们也注意到确实需要m比特来表示可能的m-比特组。

因此，当信源的一些输出被看作一个组的时候，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，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$P(C)=P(A)P(B)=(0.5)(0.5)=0.25$，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:

$$\begin{aligned} I(C) &= -\log_2 P(x_i) \\ &= -\log_2 P(0.25) = 2 \text{ (bit)} \end{aligned} \tag{1-4}$$

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，$i=1, 2, \ldots, n$和y_j，$j=1, 2, \ldots, m$。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$X=x_i$，$i=1, 2, \ldots, n$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

$$P(X=x_i|Y=y_j)=P(x_i|y_j) \tag{1-5}$$

除以概率

$$P(X=x_i)=P(x_i) \tag{1-6}$$

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

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

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

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

因此

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

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

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

6
~
7

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：

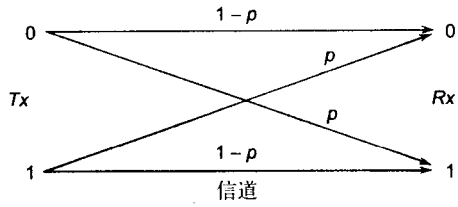


图1-1　一个二元对称信道

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

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

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

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

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

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

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

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

类似地，

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

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。对于这样的一个信道，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

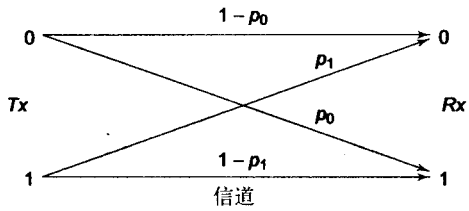


图1-2 一个非对称概率的二元信道

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

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

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

由此，我们可以写为

$$I(x_i; y_j)=I(x_i)-I(x_i\mid y_j) \tag{1-12}$$

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$I(x_i)\geqslant 0$及$I(x_i|y_j)\geqslant 0$，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、负或零。

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。