

信息电子类专业
研究生教学用书

信息论与网络编码

(翻译版)

*Information Theory and
Network Coding*

[加拿大] Raymond W. Yeung 著

蔡 宁 等译



高等教育出版社
HIGHER EDUCATION PRESS

信息电子类专业
研究生教学用书

信息论与网络编码

XINXILUN YU WANGLUO BIANMA

(翻译版)

Information Theory and Network Coding

[加拿大] Raymond W. Yeung 著
蔡 宁 等译



高等教育出版社·北京
HIGHER EDUCATION PRESS BEIJING

内容提要

本书内容由信息论和网络编码两部分组成。第一部分严密地论述了有关离散和连续系统的信息理论。在传统的信息论基础以外,又增加了 I -度量、Shannon型与非Shannon型不等式、嫡函数与群论的基本关系等内容。在第二部分,作者在信息论的基础上综合了网络编码的基本理论,包括对线性网络编码、卷积网络编码和多信源网络编码的详细讨论。

此外本书具有以下重要特色:①理论推导的严密性为本书的首要原则;②全书包含了大量的例子;③大量的原创性的习题;④每章后附有本章小结;⑤作为一本综合性教材,本书的两部分既可分别使用也可统一使用。

本书可以作为电气工程、计算机科学和应用数学等专业的本科高年级和研究生的教材,也可作为通信工程的专业人员的参考书。

Translation from the English language edition:

Information Theory and Network Coding by Raymond W. Yeung

Copyright © 2008 Springer Science + Business Media, LLC

All Rights Reserved

图书在版编目(CIP)数据

信息论与网络编码/(加)杨伟豪著;蔡宁等译. —北京:高等教育出版社, 2011.7

书名原文: Information Theory and Network Coding

ISBN 978-7-04-031470-0

I. ①信… II. ①杨…②蔡… 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(2011)第084238号

策划编辑 许怀镨

责任编辑 许怀镨

封面设计 李卫青

版式设计 范晓红

插图绘制 尹莉

责任校对 杨凤玲

责任印制 张福涛

出版发行 高等教育出版社

社址 北京市西城区德外大街4号

邮政编码 100120

印刷 北京天来印务有限公司

开本 787 mm × 960 mm 1/16

印张 36.5

字数 670千字

购书热线 010-58581118

咨询电话 400-810-0598

网址 <http://www.hep.edu.cn>

<http://www.hep.com.cn>

网上订购 <http://www.landaco.com>

<http://www.landaco.com.cn>

版次 2011年7月第1版

印次 2011年7月第1次印刷

定价 76.00元

本书如有缺页、倒页、脱页等质量问题,请到所购图书销售部门联系调换

版权所有 侵权必究

物料号 31470-00

译者序

“Information Theory and Network Coding” 是香港中文大学 Raymond W. Yeung(杨伟豪)教授在他的“A First Course in Information Theory”(以下简称原书)一书的基础上修订扩充而写成的。原书由 Kluwer Academic/Plenum Publishers 于 2002 年出版。出版后被加州大学 San Diego 分校、康奈尔(Cornell)大学等多所著名大学用作信息论的教材或教学参考书。信息论学界的泰斗——匈牙利科学院院士 Imre Csiszar 教授在 IEEE Transactions on Information Theory 为它写了书评,认为这是一部优秀的教科书。

作者在原书的基础上加入了网络编码理论作为本书的第二部分。原书的重点是离散随机变量的信息论。考虑到最近无线网络通信的蓬勃发展和广大工程人员对理论的迫切需求,为加强连续部分,作者又增加了两章有关连续随机变量的内容,这与原书原有的内容共同构成了本书的第一部分。

将信息论和网络编码的理论同时包括在一本书中是本书的一个特点。网络编码理论根植于信息论,它的基本思想也来自于信息论,因此它可以看成 Shannon 信息理论的延伸或一部分,这二者又是当前网络通信工程的理论基础。国际上很多学者又把这两方面同时列入自己的研究领域。这种做法可以使我国应用数学、通信理论和工程及计算机理论的青年学子更加方便地了解和学习这两个理论并融会贯通,也为我国广大的学者和工程技术人员提供了一本方便的参考书。

与其他同类的书籍相比,用相对较大的篇幅深入地讨论了 Shannon 型不等式和非 Shannon 型不等式的性质,这是本书另一个特点。Shannon 型不等式不仅是信息论的最重要的工具之一,而且被广泛用到了统计学、计算机科学直至经济学等重要科学领域之中。约半个世纪以来,Shannon 型不等式一直被认为是唯一的一类信息不等式,直到张箴教授和本书的作者杨伟豪教授在上世纪末发现了第一个非 Shannon 型不等式。到目前为止,已有无限个非 Shannon 型不等式被发现,而非 Shannon 型不等式也被 R. Dougherty 等人首次应用到

II 译者序

多信源网络编码的研究中。当前信息不等式的研究已成为信息论领域中的一个重要课题。本书可作为学习和研究信息不等式的一个重要参考书。

本书的两部分可以分别作为高校应用数学、通信和计算机科学专业的信息论和网络编码基础课程的研究生教材或教学参考书。数学基础较好的高等院校也可以考虑试用本书作为本科高年级的教学参考书。本书对有志于网络编码理论和信息论研究的人员是一本不错的入门书。

本书的翻译由西安电子科技大学、复旦大学、清华大学(深圳分校)和上海交通大学八位老师合力完成,这是一个集体劳动成果。分工如下:第1章,蔡宁;第2章,夏树涛;第3章,蔡宁、谢敏;第4章,肖嵩;第5章,白宝明;第6章,夏树涛;第7章,阚海滨;第8、9章,肖嵩;第10、11章,白宝明;第12章,阚海滨;第13、14、15章,李晖;第16章,谢敏;第17章,夏树涛;第18章,阚海滨;第19、20、21章,骆源。校对工作由骆源、谢敏和蔡宁完成。在此对以上全体老师深表感谢,尤其感谢骆源教授和谢敏教授,他们在百忙中为本书的翻译工作付出了大量的时间和辛勤的劳动。特别感谢我的学生蔡峰和骆源教授的学生庄卓俊从始至终为本书的翻译所做的大量的繁重工作。此外还要感谢参加最终统稿的学生,在专业术语、文字和打印符号的统一和校订及电脑工作等方面所付出的劳动和时间,他们是:王斌、王骁、肖鹤龄、周航、刘光军、郭网媚、杨颜博(以上为博士生)、冯桂国、潘昊、帅文静、毛凯、秦纪实(以上为硕士生),以及其他许多未提及的学生和工作人员,没有他们的辛勤劳动和团队精神,本书的翻译工作是不可能这么短的时间内完成的。

高等教育出版社的编辑为本书的翻译出版做了大量的工作,本书的作者杨伟豪教授自始至终关心着本书的翻译。在此衷心地感谢他们。

全书的翻译在国家自然科学基金重点项目“网络编码中的几个关键问题研究”(项目批准号:60832001)支持下完成,特此致谢。

最后,由于我们学识水平有限和时间仓促,书中不妥之处在所难免,恳请各位读者原谅并通过出版社反馈给我们。再好的翻译也无法原汁原味的反映原文的精妙之处,何况我们的有限水平,因此从个人的观点看,鼓励有条件的读者阅读本书的原文。

蔡 宁

2011年4月于西安

前言

本书是在 2002 年出版的我所著的《A First Course in Information Theory》一书的基础上发展而来的。当时,网络编码正处于初级发展阶段。近些年来,网络编码的研究进展迅速使其自成一个研究领域。根植于信息论的网络编码不但带来了网络通信研究的巨大变化,同时也对其他一些领域产生了重大影响,比如编码理论、网络、交换理论、无线通信、分布式数据存储、密码以及优化理论等。随着网络编码中新的应用不断涌现,此领域的一些基础性的结论多少有点不完整。因此,本书的主要目的之一就是系统地描述这些结论。

前一版书仅仅研究离散随机变量的信息论,本书增加了两章关于连续随机变量的信息论的内容,其中一章是微分熵,另一章是连续信道。由于增加了这些内容,本书综合性较强,更适合作为电子工程系的教科书。

本书的内容

本书共二十一章,第 1 章为信息科学的概述,第 2~16 章为第一部分,是信息论基础,后五章为第二部分,是网络编码理论。第一部分涵盖了信息论中的基本内容,为读者提供了阅读第二部分的基础。下面给出的每一章的摘要勾勒出了本书的主要内容。

第 1 章高度概括了本书的主要内容。首先,讨论了信息论的基本特征以及 Shannon 在 1948 年发表的奠基性论文的主要内容。其次,也简要介绍了 Shannon 的著作以及他的工作。

第 2 章介绍了 Shannon 关于离散随机变量的信息度量及其基本性质。此外,推导并解释了信息论中一些有用的等式和不等式。特别需要留意的是对具有零概率联合分布的处理。本章还讨论了最大熵分布。最后,以平稳信息源的熵率结束。

第 3 章引入了 I -度量理论,此理论建立了 Shannon 信息度量与集合论的一一对应关系。接着,列举一些实例说明信息图表可以简化信息论中很多结论。

II 前言

这些图表正发展成为解决信息论问题的基本工具。

第4章以前缀码为例,讨论利用唯一可译码的编码对数据进行无错误压缩。此外,给出了前缀码熵界的证明,此证明没有使用 Kraft 不等式以及基本不等式。另外,本证明有利于对前缀编码冗余度的讨论。

第5章对弱典型性进行了详尽的研究。弱渐近等分性以及信源编码定理在此也进行了讨论。此外,对于一个好的数据压缩设计能够产生近似独立同分布的比特,本章也给了解释。并且,本章也对 Shannon-McMillan-Breiman 定理做了初步讨论。弱典型性的概念将在第10章中结合连续随机变量做进一步讨论。

第6章对用于有限取值的随机变量的强典型性进行了详尽的分析。本章推导的结论将会用于接下来的两章中关于信道编码定理以及率失真定理的证明。

第7章在前一版书的基础上对离散无记忆信道做了更为详尽的分析。特别地,关于离散无记忆信道的定义使得有或无反馈的此类信道的编码设计的分析以及严格描述成为可能。信道编码定理的证明使用了图表方法,此方法有助于解释随机变量的条件独立性。

第8章简单介绍了率失真理论。用强典型性的证明得到了比 Shannon 原始的定理更强的结论。

第9章讨论了应用 Blahut-Arimoto 算法计算信道容量以及率失真函数,并且简化了收敛性的证明。本章特别强调了具有零概率点的分布的处理。

第10、11章讨论了连续随机变量的信息论。第10章介绍了微分熵以及相对信息度量的概念,并且讨论它们的一些性质。对于连续随机变量的渐近等分性,本章也给出了证明。呼应第2章关于最大熵分布的内容,本章最后研究了最大微分熵。

第11章讨论一类连续信道,在此类信道中,连续无记忆信道是作为基本元素存在的。在推导无记忆高斯信道的容量过程中,给出了输出端随机变量微分熵存在的理由。在此结论基础上,得到了并行/相关高斯信道的容量。此外,富有启发式的讨论也给出了关于有限带宽的白/有色高斯信道的容量。最后,证明了零均值高斯噪声是最坏的加性噪声。

第12章探讨了关于 Markov 结构的 I -度量的框架。此外,本章也讨论了全条件独立的集理论的性质以及 Markov 随机场。这里关于 Markov 随机场的讨论对于一般读者可能太过专业,然而,Markov 链的 I -度量的结构和简单的信息图表可以很好地解释其为 Markov 随机场的一个特例。

由于信息不等式控制着信息论中的可能性,有时也被称为信息论中的定律。因此,第13章对信息不等式的几何意义以及信息不等式与条件独立性的关

系做了详尽的解释。本章讨论的信息不等式框架是下两章的基础。

对于信息不等式的证明可以看做一个线性规划问题,第14章给出了解释。此解释给出了传统方法证明的所有信息不等式的全部特性。这些被称为 Shannon 型的不等式可用互联网上得到的软件包 ITIP 证明。这也说明 Shannon 型不等式可用来解决概率论中的条件独立性的推断问题。

自信息论诞生后,近半个世纪,所有已知的 Shannon 型不等式都是信息不等式。然而,在20世纪90年代后半期,一些非 Shannon 型不等式被发现。这些不等式暗示了信息论中超越 Shannon 所设定的定律的存在。第15章中,我们讨论了这些不等式及其应用。

第16章解释了信息论和群论之间的微妙关系。详细来讲,对于每一个所有联合分布都满足的信息不等式,都存在一个对应所有的有限群和它的子群都满足的群不等式,反之亦然。群不等式决定了任何有限群以及它的子群的序。关于 Shannon 型信息不等式的群论的证明也在本章给出。最后,从第15章中讨论的非 Shannon 型不等式,本章得到了对应的群不等式,但是这类不等式的意义以及内涵还需要进一步探讨。

从第17章开始,本书进入第二部分,首先讨论了蝶形网络,这是网络编码中的一个基本实例。接着,本章对蝶形网络的各种变形也进行了深入的分析。并且,通过一个简单的例子说明网络编码在无线以及卫星通信中相对于存储转发的优势。最后,我们还举例说明了多信源网络编码为什么本质上不同于单信源网络编码。

单信源网络编码的基本界,即最大流界,在第18章给予了详尽的解释。此界适用于所有的网络编码。

在第19章,我们讨论了无圈网络上的具有各类不同性质的达到最大流界的线性网络编码。本章还讨论了静态网络编码——一类在某些链路中断时可达最大流界的线性网络编码。最后,本章给出了在多项式时间内构造这些编码的算法。

在第20章,我们描述并分析了有圈网络上的卷积网络编码,并证明达到最大流界的编码的存在性。

第21章对网络编码理论进行了更为深入的分析。我们对多信源在点对点无圈网络中的多播情况进行了分析。并且,本章证明了一个通过信息不等式框架所表述的网络可达信息率区域的难以计算的刻画。

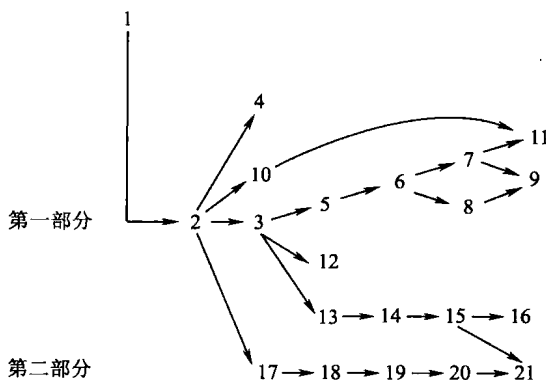
如何使用本书

本书的第一部分可以作为信息论的综合性教程。本书的内容之所以如此安排是因为如果没有第一部分,第二部分中的网络编码的讨论将是不完整的。不

IV 前言

过,除了第 21 章关于多信源网络编码的内容,第二部分完全可以作为单信源网络编码教材。

本书的第一、二部分分别需要有关于概率论以及线性代数的基础知识。了解一些数字通信的知识,有助于学习第 11 章。在学习第 20 章之前,应该先了解一些离散时间线性系统的相关知识。推荐读者根据下图去学习相关的章节。然而,由于有足够的相关章节可供参考,读者跳读本书也不会有太大的困难。



本书延续了前一版著作的写作风格,即所有推导都力求严格详尽。本书包含了大量的例子,这些例子经常用以提示重点。为了方便使用本书,在每一章的结尾都做了总结。

本书可作为教科书或参考书。作为教科书,本书可分两个学期来讲授,分别讲授第一、二部分。为此已准备了一个综合性的教学指南,如有需要,可与作者联系, whyung@ie.cuhk.edu.hk。

与其他大篇幅的文字一样,本书难免会有错误和遗漏。为了减少问题,错误校勘表将会在本书主页上登出, http://www.ie.cuhk.edu.hk/IT_book2/。

杨伟豪
中国香港
2007 年 12 月

致谢

本书是在我所著的《A First Course in Information Theory》的基础上于 2007 年扩充而成的。感谢来自德国洪堡基金会的 Bessel 研究奖的慷慨支持, 使我从 1 月到 4 月, 在对慕尼黑理工大学访问期间, 能够全身心地进行研究工作。感谢 Joachim Hagenauer 和 Ralf Koetter 对我的提名以及邀请, 同时还要感谢香港中文大学信息工程系对此行的安排, 使得此次访问顺利进行。

许多个人直接或间接地对本书的完成做出了贡献。首先我非常感激教授了我信息论以及写作的 Toby Berger, 同时对张箴, 蔡宁与 Bob Li 给予我的友谊与灵感致以最真诚的谢意。本书的完成与多年来支持与鼓励我的同事们密不可分, 他们是: Venkat Anantharam, Vijay Bhargava, Dick Blahut, Agnes 和 Vincent Chan, Tom Cover, Imre Csiszár, Tony Ephremides, Bob Gallager, Bruce Hajek, Te Sun Han, Jim Massey, Prakash Narayan, Alon Orlitsky, Shlomo Shamai, Sergio Verdú, Victor Wei, Frans Willems 和 Jack Wolf, 感谢他们多年来对我的支持和鼓励。同时还要感谢那些在此书的完成中做出贡献的所有参与者, 以及为此书提出宝贵意见的默默无闻的人们。

特别要感谢以下几位: 在关于微分熵与连续信道的讨论中 David Tse 使我获益匪浅; Terence Chan, Ka Wo Cheung, Bruce Hajek, Siu-Wai Ho, Siu Ting Ho, Tat Ming Lok, Prakash Narayan, Will Ng, Sagar Shenvi, Xiang Gen Xia, Shaohua Yang 和 Ken Zeger, 在完成本书的不同阶段, 都提出了非常有价值的意见; 我的研究生 Silas Fong, Min Tan 和 Shenghao Yang 仔细校对了对有关网络编码章节的内容; Silas Fong 帮助完成了整本书的插图工作。

在家庭方面, 我十分感激我的妻子 Rebecca 对我的关爱。在慕尼黑期间, 她细心照料了整个家庭, 让我能够全身心地投入到写作之中。我们十分感谢我们家庭的好朋友 Pui Yee Wong 女士, 在本书的最后阶段, 她照料了生病的 Rebecca,

II 致谢

以及感谢真诚地支持我们的我的姐姐 Georgiana。同时我们十分感激 Yu Lap Yip 医生对病情的及时诊断。非常感谢周末前来照顾我女儿 Shannon 的我妻子的姐姐 Ophelia, 以及女儿在她母亲生病期间无私的体贴给我们的家庭带来的极大的温暖与支持。

目录

1 信息的科学	1
---------------	---

I 信息论部分

2 信息度量	7
2.1 独立性和 Markov 链	7
2.2 Shannon 信息度量	13
2.3 固定有限字母表上 Shannon 信息度量的连续性	18
2.4 链式法则	20
2.5 信息散度	23
2.6 基本不等式	26
2.7 一些常用信息不等式	28
2.8 Fano 不等式	32
2.9 最大熵分布	36
2.10 平稳信源的熵率	39
附录 2.A: 可数无限字母表上随机变量的截断逼近	42
本章小结	44
习题	46
历史注记	51
3 I -度量	52
3.1 基本概念	53
3.2 两个随机变量的 I -度量	54
3.3 I -度量 μ^* 的构造	56
3.4 μ^* 可能是负数	59

II 目录

3.5 信息图	62
3.6 应用实例	68
附录 3.A: 容斥公式的一个变形	74
本章小结	76
习题	77
历史注记	80
4 无错误数据压缩	81
4.1 熵界	81
4.2 前缀码	86
4.2.1 定义和存在性	86
4.2.2 Huffman 码	88
4.3 前缀码的冗余	93
本章小结	97
习题	98
历史注记	99
5 弱典型性	100
5.1 弱渐近等分性	100
5.2 信源编码定理	103
5.3 高效信源编码	105
5.4 Shannon-McMillan-Breiman 定理	107
本章小结	109
习题	109
历史注记	111
6 强典型性	112
6.1 强渐近等分性	112
6.2 强典型性与弱典型性	121
6.3 联合典型性	121
6.4 基本不等式的解释	130
本章小结	131
习题	132
历史注记	134

7 离散无记忆信道	135
7.1 定义和容量	138
7.2 信道编码定理	146
7.3 信道编码定理中的逆命题	148
7.4 可达性	154
7.5 讨论	160
7.6 反馈容量	163
7.7 信源信道分离编码	168
本章小结	171
习题	172
历史注记	176
8 率失真理论	177
8.1 单字母失真度量	177
8.2 率失真函数 $R(D)$	181
8.3 率失真定理	187
8.4 逆定理	194
8.5 $R_I(D)$ 的可达性	197
本章小结	202
习题	203
历史注记	205
9 Blahut-Arimoto 算法	206
9.1 交替优化	207
9.2 算法	209
9.2.1 信道容量	209
9.2.2 率失真函数	214
9.3 收敛性	217
9.3.1 充分条件	217
9.3.2 信道容量的收敛性	221
本章小结	221
习题	222
历史注记	223

IV 目录

10 微分熵	224
10.1 预备知识	227
10.2 定义	230
10.3 联合微分熵, 条件 (微分) 熵及互信息	234
10.4 连续随机变量的 AEP	241
10.5 信息散度	243
10.6 最大微分熵分布	245
本章小结	247
习题	250
历史注记	252
11 连续信道	253
11.1 离散时间信道	253
11.2 信道编码定理	256
11.3 信道编码定理的证明	258
11.3.1 逆定理	258
11.3.2 可达性	261
11.4 无记忆 Gauss 信道	266
11.5 并行 Gauss 信道	269
11.6 相关 Gauss 信道	274
11.7 带限白 Gauss 信道	276
11.8 带限色 Gauss 信道	284
11.9 零均值 Gauss 噪声是最坏的加性噪声	286
本章小结	291
习题	293
历史注记	295
12 Markov 结构	296
12.1 条件相互独立	297
12.2 全条件相互独立	307
12.3 Markov 随机场	311
12.4 Markov 链	314
本章小结	317
习题	318

历史注记	318
13 信息不等式	320
13.1 区域 Γ_n^*	322
13.2 标准形信息表达式	323
13.3 几何框架	326
13.3.1 无约束不等式	326
13.3.2 有约束不等式	327
13.3.3 有约束恒等式	329
13.4 有约束不等式的等价性	329
13.5 条件独立的隐含问题	332
本章小结	333
习题	334
历史注记	335
14 Shannon 型不等式	336
14.1 元不等式	336
14.2 线性规划方法	338
14.2.1 无约束不等式	340
14.2.2 有约束的不等式和等式	341
14.3 对偶性	342
14.4 机器证明——ITIP	344
14.5 隐含问题的处理	348
14.6 元不等式的最小性	350
附录 14.A: 基本不等式和多项拟阵公理	354
本章小结	355
习题	356
历史注记	358
15 非 Shannon 型不等式	359
15.1 Γ_2^*, Γ_3^* 和 $\bar{\Gamma}_n^*$ 的特性	359
15.2 一个非 Shannon 型无约束不等式	368
15.3 一个非 Shannon 型有约束不等式	373
15.4 应用	380
本章小结	382

VI 目录

习题	382
历史注记	384
16 熵与群	386
16.1 群论基础	387
16.2 可群特征化的熵函数	392
16.3 $\bar{I}_n^*$ 的一个群特征	397
16.4 信息不等式和群不等式	400
本章小结	405
习题	405
历史注记	408
 II 网络编码基础	
17 引言	411
17.1 蝶形网络	412
17.2 无线通信和卫星通信	414
17.3 信源分离	416
本章小结	417
习题	417
历史注记	419
18 最大流界	420
18.1 点对点通信网络	420
18.2 达到最大流界的一些例子	423
18.3 一类网络编码	425
18.4 最大流界的证明	427
本章小结	430
习题	430
历史注记	432
19 单信源线性网络编码: 无圈网络	434
19.1 无圈网络	435
19.2 线性网络编码	436