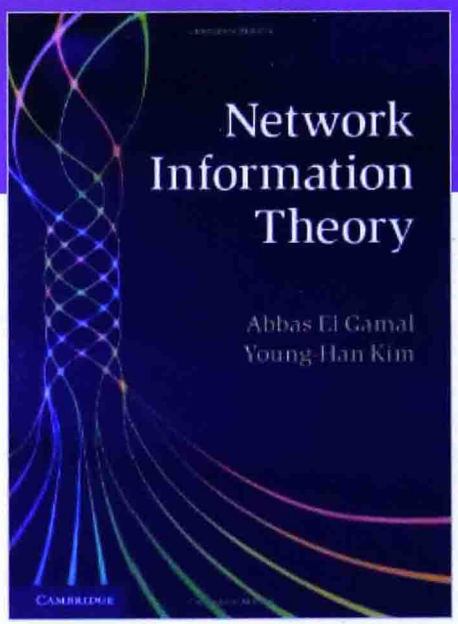
信息技术和电气工程学科国际知名教材中译本系列

Network Information Theory

网络信息论



Abbas El Gamal
Young-Han Kim 著

张林 译

清华大学出版社

CAMBRIDGE

信息技术和电气工程学科国际知名教材中译本系列

Network Information Theory

网络信息论

Abbas El Gamal
Young-Han Kim 著

张林 译

清华大学出版社

图书在版编目（CIP）数据

网络信息论 /(美) 盖莫尔 (Gamal, A.E.), (韩)金荣汉著; 张林译. --北京: 清华大学出版社, 2014
书名原文: Network information theory
信息技术和电气工程学科国际知名教材中译本系列
ISBN 978-7-302-34858-0
Ⅰ. ①网… Ⅱ. ①盖… ②金… ③张… Ⅲ. ①计算机网络－信息论 Ⅳ. ①G20 ②TP393.07
中国版本图书馆 CIP 数据核字(2014)第 234888 号

责任编辑：文 怡
封面设计：张海玉
责任校对：焦丽丽
责任印制：杨 艳

出版发行：清华大学出版社
网 址：http://www.tup.com.cn，http://www.wqbook.com
地 址：北京清华大学学研大厦 A 座 邮 编：100084
社 总 机：010-62770175 邮 购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn,010-62795954
印 装 者：三河市春园印刷有限公司
经 销：全国新华书店
开 本：185mm×260mm **印 张**：43.75 **字 数**：1038 千字
版 次：2015 年 1 月第 1 版 **印 次**：2015 年 1 月第1 次印刷
印 数：1～3000
定 价：99.00 元

产品编号：045254-01

献给我们的家人，
是他们的爱和支持，
促成了本书的诞生。

序 言

网络信息论旨在建立网络中信息流的根本极限，并探索获得这些极限的编码方法。它拓展了香农（Shannon）的点到点通信基础理论以及针对单播图网络的最大流-最小割定理，适用于多信源、多信宿共享资源的一般网络模型。虽然这个理论还远未成熟，但在过去的四十年中，研究者还是取得了很多优美的结果，并且在现实网络中展现出很大的潜力。本书采用简洁和有内在逻辑的结构，把这些结果呈现给读者，为电气工程、计算机科学、统计学以及其他相关学科的研究生和科研人员服务，并将这些结果普及到工业界的研究人员中。

网络信息论的第一篇论文是Shannon (1961)发表的关于双向信道的研究结果。直到十年之后，这项工作才得到一系列开创性论文的跟进，包括Cover (1972)关于广播信道的论文，Ahlswede (1971, 1974)以及Liao (1972) 关于多址接入信道的论文，Slepian, Wolf (1973a)关于无损分布式压缩的论文。这些研究成果在 1970 年代中期到 1980 年代前期引发了网络信息论研究的热潮，产生了很多新的成果和方法，有兴趣的读者可以阅读van der Meulen (1977)和El Gamal, Cover (1980)发表的两篇综述论文，也可以阅读Csiszár, Körner (1981b)影响深远的专著。然而，时至今日，包括香农双向信道在内的很多问题依然没有得到解答，1980 年代中期到 1990 年代中期，随着通信理论专家和实践者对这些问题兴趣的降低，网络信息论经历了“失去的十年”。在这期间，学术论文的发表数量很少，很多研究者转移了研究兴趣。1990 年代中期以来，由半导体技术、压缩和纠错编码、信号处理和计算机科学所引发的互联网和无线通信技术的发展重新点燃了学者们对于网络信息论的研究兴趣。除了旧有的开放问题，近期的工作针对新的网络模型、新的网络编码方法、容量的近似、尺度定律以及网络与信息论交叉等领域展开研究，一系列的新技术，诸如：连续抵消解码、多重描述编码、连续信息修正、网络编码等，已经开始在实际的网络中应用。

本书的由来

撰写本书的想法由来已久，早在 1980 年 Tom Cover 和本书的第一作者撰写前述综述论文的时候就已经产生。本书第一作者随后编写了一份手写的讲义，于 1982 年到 1984 年间在斯坦福大学开设了多用户信息论课程。为了满足研究生对于通信与信息理论学习的需求，他在 2002 年恢复了这门课，并在讲义中增补了最新的研究结果。2003 年暑期，更新后的讲义在 EPFL 开课。2007 年，本书的第二作者（也是 2002 年选课的学生），开始在加州大学圣地亚哥分校教授类似的课程。两个作者决定合作将讲义拓展为一本正式的教科书。自那以后，不同版本的讲义在很多大学经过了试用，包括斯坦福大学、加州大学圣地亚哥分校、香港中文大学、加州伯克利分校、清华大学、首尔国立大学、Notre Dame大学、 McGill 大学等。2010 年 1 月，讲义被上载到了 arXiv 在线数据库。本书就是基于这些

讲义撰写的。虽然我们尽力提供对于本领域研究成果最广泛的覆盖，但却无法做到毫无遗漏，近年来本领域论文数目爆炸式的增长使得几乎不可能仅用一本教材就覆盖全部内容。

本书的结构

我们尝试了几种内容组织的框架结构，包括沿着信源编码到信道编码的顺序（或逆序）来组织，或者沿着从图网络到一般网络的逻辑来组织，或者按照历史的线索来组织。最终，我们决定采用面向教学的需求来组织内容，这样可以较好地平衡对于新网络模型和新编码技术的介绍。我们首先讨论单跳网络，然后拓展到多跳网络。在每一类网络中，我们首先研究信道编码，然后介绍对应的信源编码，之后是联合信源-信道编码。对于无法顺利安放到这个框架下的几个重要内容，我们在拓展部分中加以介绍。本书主要采纳了离散无记忆网络和高斯网络模型，对于更加复杂模型中的信息流的极限，我们几乎一无所知。集中使用上述的模型也可以帮助我们用最简单的形式给出编码定理和证明。

在第 1 章中，我们通过简述书中一些例子，描画了网络信息论的全景。接下来的内容划分为四大部分和一组附录。

第一部分，基础知识（第 2、3 章）。 我们给出了信息论的必备基础知识，介绍了典型性的定义以及书中反复使用的几个引理，并回顾了香农的点到点信息编码定理。

第二部分，单跳网络（第 4 章至第 14 章）。 这部分讨论单轮、单向的通信。其中的每个节点或者是发送者、或者是接收者。本部分的内容分属三类通信场景。

- **独立消息通过有噪信道传输（第 4 章至第 9 章）。** 讨论有噪单跳网络的基本单元，第 4 章先由多址接入信道开始（多对一通信），随后第 5 章与第 8 章介绍广播信道（一对多通信），第 6 章介绍干扰信道（多个一对一信道）。我们把对广播信道的介绍分开进行，是出于教学上的考虑：第 8 章对于一般广播信道的研究需要用到第 7 章中有状态信道的基础。在第 9 章中，我们研究高斯矢量信道，它刻画了多天线（多入多出/MIMO）通信系统。
- **相关信源通过无噪信道传输（第 10 章至第 13 章）。** 讨论与有噪单跳网络对应的信源编码问题。第 10 章由分布式无损信源编码开始，随后在第 11 章中介绍有边信息的有损信源编码，在第 12 章中介绍分布式有损信源编码，在第 13 章中介绍多重描述编码。我们在这三章中逐步展开对分布式编码的讨论，帮助读者建立知识体系。
- **相关信源经由有噪信道传输（第 14 章）。** 讨论经由单跳有噪网络发送未经压缩的信源消息的一般问题。

第三部分，多跳网络（第 15 章至第 20 章）。 我们讨论有中继的网络或者存在多轮通

信的网络。在这个模型中，某些节点可以同时充当发送者和接收者。与第二部分的组织一样，本章的内容也分为三类场景。

- **独立消息经由图网络传输（第 15 章）。** 本章超越简单路由方法，讨论了网络图模型上的编码。
- **独立消息经由有噪网络传输（第 16 章至第 19 章）。**在第 16 章中，我们讨论中继信道。它是一个简单的两跳网络，包括一个发送者、一个接收者和一个中继。随后的第 17 章讨论反馈信道和双向信道。在第 18 章中，我们将中继信道和双向信道的结论推广到一般的有噪网络中。第 19 章进一步讨论大规模无线网络容量的近似和尺度定律。
- **相关信源经由图网络传输（第 20 章）。** 这一部分讨论与第 15 章至第 18 章中描述的信道编码对应的信源编码问题。

第四部分，拓展内容（第 21 章至第 24 章）。 本部分介绍了前三部分理论的拓展。第 21 章介绍了面向计算的通信，第 22 章介绍通信中的保密问题，第 23 章介绍了衰落信道，第 24 章介绍了网络和信息论的交叉问题。

附录。 为了尽量做到内容完备，我们在附录 A、B、E 中给出了关于凸集、凸函数、概率与估计、凸优化的背景知识。附录 C 介绍了对随机变量的势进行定界的方法，在本书的很多章中，该方法用于容量和速率区域的刻画。附录 D 介绍了 Fourier–Motzkin消去过程。

材料的组织

本书的每一章基本都包含了教学材料和高级技术专题。加星号的小节则属于细节或与主线无关的内容。每一章的结尾都列出了本章的核心内容、开放问题、文献说明等内容，正文中略去的证明会以习题的形式给出，一些过于技术或非核心的证明则会放在章尾的附录中，以便读者的精力能够集中在核心的观点和逻辑线条上。

本书遵循“一图胜千言”的原则，使用了大量图例来形象地说明模型和概念，证明则遵循尽可能简单的原则，所需的基本工具只须读者掌握基础概率论和一定程度的数学即可——读者如果修过基础信息论课程，那么其数学水平就足以应付本书的要求。书中可达性的证明基于联合典型性，这个性质由香农在其 1948 年的论文中给出，由 Forney 和 Cover 在 1970 年代进一步发展。在本书中，我们进一步引入一组更为简化的引理，以使证明步骤更加简明。我们展示了如何通过离散化过程和取恰当的极限，把离散无记忆网络的证明拓展到对应的高斯网络中去。本书中的一部分证明是全新的，其余的大多数证明则是论文中证明的简化版本，有一部分还更加严格。

在课程中使用本书

前面提到，本书多年来已经在多所大学用于网络信息论的教学。我们希望本书的出版

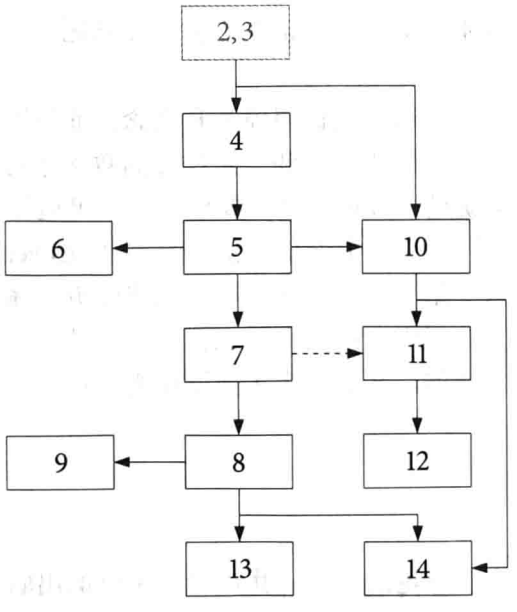
可以促进这门课程的推广。当然，我们撰写本书最主要的动机之一还是吸引更多的网络信息论爱好者。当前的通信与网络工程教育中主要包含的是点到点通信和有线网络的内容，而很多现代通信和网络系统中的创新则更加重视共享资源的有效使用，而这恰是网络信息论所关注的问题。我们相信，在掌握了实用的网络信息论知识后，下一代通信和网络工程师可以获得很多好处。我们尽一切的可能，面对这类读者简明地阐述相关的研究成果。特别地，本书中关于高斯信道、无线衰落信道、高斯网络的内容可以直接整合进无线通信的高级课程中去。

本书可以用作为时长为一学期、强调通信技术的基础信息论课程的主教材使用，也可以作为时长一学期的高等信息论课程的主教材，对通信、网络、计算机科学、统计等课程加以补充。书中的大部分教学内容可以通过一个时长为两学期的课程全面覆盖，课程的幻灯片可以参考：http://arxiv.org/abs /1001.3404/。

相关图

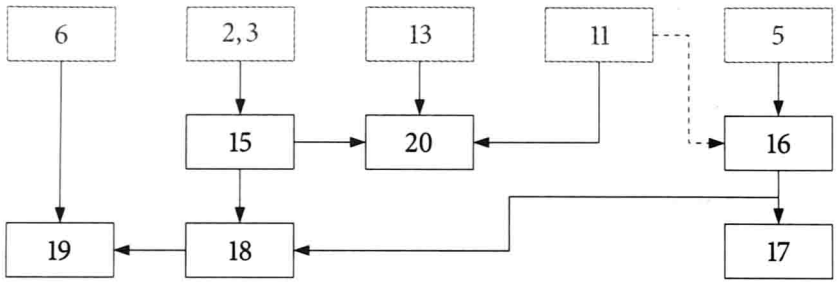
下面的图描述了各章之间的关联。每个方块表示一个章节，虚线框表明了先修章节。实线箭头表明了必要的阅读顺序，虚线箭头则表示建议阅读。

第二部分



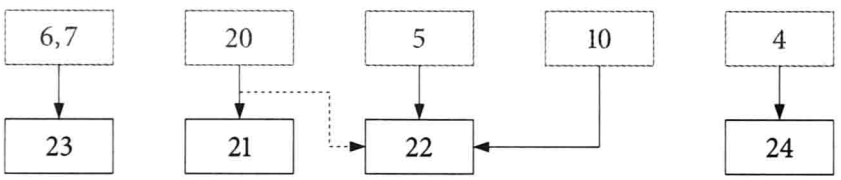
2 信息度量和典型性
3 点到点信息论
4 多址接入信道
5 退化的广播信道
6 干扰信道
7 有状态的信道
8 一般广播信道
9 高斯矢量信道
10 分布式无损压缩
11 有边信息的有损压缩
12 分布式有损压缩
13 多描述编码
14 联合信源-信道编码

第三部分



15 图网络
16 中继信道
17 交互式信道编码
18 离散无记忆网络
19 高斯网络
20 图网络上的压缩

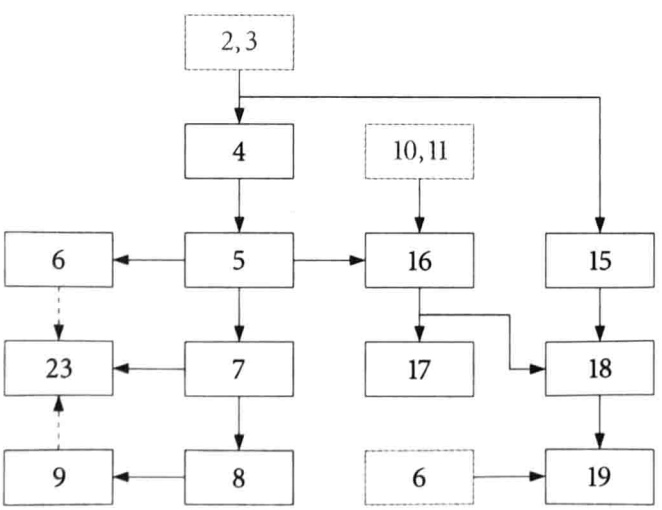
第四部分



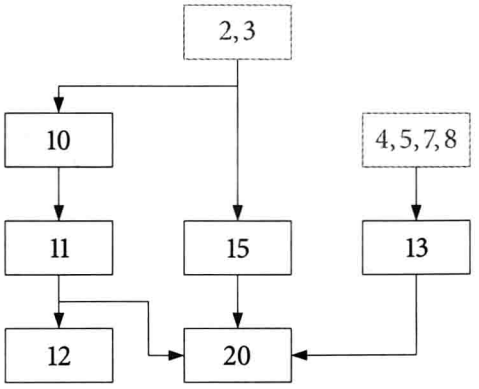
21 面向计算的通信
22 信息论保密学
23 无线衰落信道
24 网络与信息论

除了上面的分部相关图外，我们还提供下述按照研究内容组织的相关图。

通信



数据压缩



Abbas El Gamal
Young-Han Kim

于加利福尼亚州 Palo Alto 市
于加利福尼亚州 La Jolla 市
2011年7月

致 谢

本书是集体努力的成果。很多同事、课程助教、博士后和博士生都对本书的内容、组织、表述提供了极有价值的建议，并审阅了早期的初稿。

首先，也是最重要的，我们对 Tom Cover 怀有深深的感恩之情，他教会了我们所知关于信息论的一切，鼓励我们撰写此书，提供了许多深刻的建议。我们还特别感谢我们的助教 Ehsan Ardestanizadeh，Chiao-Yi Chen，Yeow-Khiang Chia，Shirin Jalali，Paolo Minero，Haim Permuter，Han-I Su，Sina Zahedi，Lei Zhao，他们为本书的撰写提供了巨大的帮助。特别地，我们要感谢 Sina Zahedi，他帮助完成了本书最初的讲义版本。我们感谢 Han-I Su 对于二次高斯信源编码和分布式计算两部分内容的贡献，也感谢他对于初稿的全面审读。Yeow-Khiang Chia 为信息论保密性和图网络中的压缩两章做出了重要的贡献，还提供了一些习题的解答，他还审读了本书的很多部分。Paolo Minero 在信息论和网络的章节中也有贡献。

我们还很感激我们的博士生。Bernd Bandemer 对于干扰信道一章有贡献，并阅读了书中的若干部分。Sung Hoon Lim 对于离散无记忆高斯网络一章做出了贡献。James Mammen 帮助完成了尺度定律的第一稿讲义，Lele Wang 和 Yu ü iang 也对于书中很多部分提供了有益的建议。

我们还从与同事的讨论中获益良多。Chandra Nair 贡献了广播信道一章中的很多结果和习题。David Tse 帮助梳理了衰落信道和干扰信道的内容组织。Mehdi Mohseni 帮助完成了高斯矢量信道的关键证明。Amin Gohari 帮助完成了信息论中的保密性一章的组织并给出了几个结论的证明。Olivier Lévêque 帮助完成了高斯网络的几个证明。我们还从 John Gill 处获得了很多排版风格和编辑方面的建议。Jun Chen，Sae-Young Chung，Amos Lapidoth，Prakash Narayan，Bobak Nazer，Alon Orlitsky，Ofer Shayevitz，Yossi Steinberg，Aslan Tchamkerten，Dimitris Toumpakaris，Sergio Verdú，Mai Vu，Michèle Wigger，Ram Zamir和 Ken Zeger 在本书的撰写过程中提供了有益的建议。我们还要感谢Venkat Anantharam，François Baccelli，Stephen Boyd，Max Costa，Paul Cuff，Suhas Diggavi，Massimo Franceschetti，Michael Gastpar，Andrea Goldsmith，Bob Gray，Te Sun Han，Tara Javidi，Ashish Khisti，Gerhard Kramer，Mohammad Maddah-Ali，Andrea Montanari，Balaji Prabhakar，Bixio Rimoldi，Anant Sahai,，Anand Sarwate，Devavrat Shah，Shlomo Shamai，Emre Telatar，Alex Vardy，Tsachy Weissman 和张林。

如果没有选修我们课程的无数热情好学的学生和他们的贡献，本书不可能诞生。他们中的一些人前面已经提及，此外，我们还想感谢Ekine Akuiyibo，Lorenzo Coviello，Chan-Soo Hwang，Yashodhan Kanoria，Tae Min Kim，Gowtham Kumar，Moshe Malkin，他们对于本书的部分内容做出了贡献。Himanshu Asnani，Yuxin Chen，Aakanksha Chowdhery，Mohammad Naghshvar，Ryan Peng，Nish Sinha 和 Hao Zou 为本书的初稿做了校对。加州大

学伯克利分校、麻省理工大学、清华大学、马里兰大学、特拉维夫大学、韩国高等技术研究院的一些研究生也提供了有价值的反馈。

我们想感谢本书的编辑 Phil Meyler 和其他剑桥大学出版社的职员，他们在本书的出版过程中提供了良好的支持。我们还要感谢行政助理 Kelly Yilmaz。最后，我们要感谢为本书提供了部分支持的 DARPA ITMANET 和美国国家自然科学基金。

致中国读者

非常高兴我们的著作《网络信息论》能够在中国出版，我们要感谢张林教授为翻译本书所付出的努力，我们还要感谢王乐乐提供的中文排版方面的帮助，清华大学出版社编辑文怡、剑桥大学出版社编辑菲尔·梅勒和双方出版社的工作人员也为这本书的出版付出了巨大的努力。

网络信息论研究的是网络中信息流的基本极限，以及达到这些极限的最优编码方法。除了研究本身的优雅和美感之外，网络信息论还给现有的通信技术带来了巨大的性能提升。对于这个领域关键成果的了解有助于下一代通信网络的研发。网络信息论研究中用到的数学工具和方法还可能用于其他的领域，例如计算机科学、经济学和生物学。本书采用高度结构化和浓缩的方法将网络信息论领域中令人兴奋的结果呈现给读者。

在 2010 年春季，本书的第一作者访问了清华大学，并教授了一个长达五个星期的网络信息论课程，吸引了超过 100 名学生参加，他们大多是清华和其他北京高校通信和网络领域的研究生。在这次中国之行中，作者还在复旦大学进行了一天的授课，在西安交通大学做了学术讲座。课程和讲座中学生体现出来的热情展示了信息论在中国的光明未来。我们希望这本《网络信息论》的中文版能够使得更多的中国学生受益于本领域的知识，并在中国建立一个活跃的信息论社区。

译者序

2011年至2013年，我承蒙清华大学和国家留学基金委支持，受 Abbas El Gamal教授邀请，在斯坦福的信息系统实验室（Information Systems Lab）从事了两年的访问研究，与很多信息论领域的知名学者有过密切的接触与合作。

那时候 Tom Cover 老先生还在世，常常午饭的时候在 Packard 一楼的 Bytes 咖啡厅看到他高高瘦瘦、颤颤巍巍的身影。有几次从中午一直聊到下午，从餐厅聊到他的办公室。老先生年轻的时候吸烟，年老后虽然戒掉了，但是胸前衬衣的口袋里面还总装着一包骆驼牌香烟，谈到兴奋的时候说话带着气喘，还不时地拿手去摸烟盒。我们讨论过很多话题：汉字的信息密度、热力学和信息论的关系、人类决策中非理性因素的起源等等，从这些有趣的谈话中能看到老先生心中一直保持着的好奇心。2012 年在南加州大学做短暂访问期间，很意外地听说 Cover 教授去世了，后来听说他早已得知自己罹患绝症，但却决意不扩散消息，而把一个快乐健康的形象留在大家的记忆中。半年后在斯坦福校友俱乐部为他举行的追思会上，他的侄子讲起的一个故事尤其让我印象深刻：有一次，Cover 要从拉斯维加斯的酒店出发赶飞机，在经过大堂牌桌的时候，把身上剩下的几个筹码全部押上。在赢了一局、筹码增倍后，他走到下一张牌桌前，又全押上，然后又赢翻倍。如此几次之后，他手上已经有了几百美元的筹码了。此时距离飞机起飞已经很近了，他必须做一个决定，要么把筹码换成现金之后离开，要么改变行程留下来继续玩下去。但 Cover 却做了一件谁也想不到的事，他用最后剩下的一丁点时间又连赢了几局，随后把手中大把的筹码往空中一抛，施施然地走出酒店赶飞机去了。Cover 曾经担任加州博彩业委员会的成员，对博彩游戏的原理了解甚详。对他来说，赌博可能压根儿就是个比赛聪明和记忆力的游戏，完全没有获利这一层目的。据说香农晚年对于股票投资的研究很感兴趣，但却并不热衷于靠这个发财。Cover 确实是有香农遗风的一位学者。

之所以由 Cover 老先生说起，是因为本书的第一作者 Abbas El Gamal 就是 Cover 早期的弟子。2010 年春季他在清华完整地讲授了网络信息论课程。当时本书的英文版还没有出版，但幻灯片和讲义大纲还是让许多学生获益，更闪光的则是他在授课过程中分享的对于信息论中主要结论的观点和看法，以一个亲历者和创造者的视角去讲授一门经典的课程，立意确实不凡。特别要感谢樊帅博士将课程全程的录像整理了出来供感兴趣的读者下载（http://sensor.ee.tsinghua.edu.cn/）。Abbas 是三十几年来信息论领域中的重量级人物。他早年和 Cover 的一系列合作工作是多用户信息论的经典之作，1980 年代初期他离开学校去创办企业，被认为是信息论进入低潮的标志之一，而经过多年后他重新回归教职，发现当年自己的许多工作仍然没有被超越。由一位世界顶级的理论研究者到务实进取的公司创始人，Abbas 在两个身份之间的转换令人叹服，而这可能恰恰是信息论这门学问的特点。

信息论是一门很安静的学问。自1948年香农发表划时代的论文“通信的数学原理”以来，他开创的以信息度量体系、信源和信道模型、典型性作为基础的研究范式就一直统治着这个理论研究的王国。虽然历经了 60 余年，信息论的研究由经典的点到点场景拓展到

多用户场景，并产生了诸多问题上的演进，但是基本的数学方法却一直保持了良好的一致性。从这个意义上来说，信息论的圈子有着自己的研究范式和方法论，相比于通信、网络等贴近实用工程的领域，信息论圈子更强调数学的逻辑和严谨，学者们在证明的精妙细节中体验着学院派研究的乐趣。

但信息论同时也是一门非常“入世”的学问。在 60 多年的历史中，产生了非常多意义非凡的实用技术。这些贡献大多数来自于信息论经典范式中“可达性”（Achievability）证明的构造性过程，例如LDPC码、连续干扰抵消、叠加编码、污纸书写编码等等，都是来自于证明中的“巧思”。一门数学理论能够产生如此多深远而重大的实际影响绝非幸致，香农建立的对信息系统抽象模型是成功的基础，而典型性则提供了对通信信息系统性能边界的强大分析能力。

在我国电子信息类的本科和研究生课程体系中，“信息论”一般是作为专业基础课开出的，帮助绝大多数毕业生储备了相关的基础知识。但与之形成对照的是，我国在国际信息论研究的领域却并不是特别活跃，信息论课程与通信、网络等应用技术类课程的脱节还比较明显。随着我国由信息技术的制造大国迈向信息技术的强国，需要更多高层次的工程和研究人才。他们不仅应该了解系统和技术是如何实现的（Know-how），更需要知道为什么应当如此实现（Know-why），从而具备原始创新的能力。信息论相关内容在工程教育中就显得非常的重要，值得加强。本书完整、结构化地梳理了自经典信息论以来本领域最主要的研究结论，并在方法层面上做了简洁优雅的统一，是一本难能可贵的“删削述正”的教科书，可以作为本科生高年级和研究生基础信息论的辅助教材，或者研究生高等信息论的教材使用。

在本书的翻译过程中，得到了来自同事和学生的大量帮助。本书的第二作者 Young-Han Kim 教授与学生王乐乐提供了非常及时的 Latex 排版方面的技术支持。我的学生余潇潇、刘铁铭、付乔、朱冰、顾明、焦剑涛提供了早期版本的翻译帮助，在此对他们表示感谢。由于译者水平所限，难免有不足之处，欢迎批评指正!

张林

2014年8月于清华园

数学符号

以下是本书用到的数学符号和术语。（译者注：本书涉及的数学符号与英文原版书保持一致）

集合、标量和矢量

用小写字母 $x, y, \ldots$ 表示常量和随机变量的取值。用 $x_i^j = (x_i, x_{i+1}, \ldots, x_j)$ 来表示一个长度为 $(j-i+1)$ 的序列或列矢量，其中 $1 \le i \le j$。当 $i = 1$时，我们一般省略下标，即 $x^j = (x_1, x_2, \ldots, x_j)$。有时，把确定维度的常矢量写作 $\mathbf{x}, \mathbf{y}, \ldots$，以 x_j表示 $\mathbf{x}$ 的第 j 个元素。令 $\mathbf{x}(i)$ 表示一个随时间 i 变化的矢量，$x_j(i)$ 为 $\mathbf{x}(i)$ 的第 j 个元素。这个矢量的序列表示为 $\mathbf{x}^n = (\mathbf{x}(1), \mathbf{x}(2), \ldots, \mathbf{x}(n))$。一个维度确定的全一的列矢量 $(1, \ldots, 1)$ 记为 $\mathbf{1}$。

令 $\alpha, \beta \in [0,1]$，$\bar{\alpha} = (1-\alpha)$，$\alpha * \beta = \alpha\bar{\beta} + \beta\bar{\alpha}$。

令 $x^n, y^n \in \{0,1\}^n$ 为 n 维二进制矢量。$x^n \oplus y^n$ 为两个矢量的元素模二和。

用手写体字母 $\mathcal{X}, \mathcal{Y}, \ldots$ 表示有限集合，$|\mathcal{X}|$ 表示集合 $\mathcal{X}$ 的势。下面是一些常见集合的记号：

- $\mathbb{R}$ 为实数轴，$\mathbb{R}^d$ 是 d 维实欧几里得空间。
- $\mathbb{F}_q$ 是有限域 GF(q)，$\mathbb{F}_q^d$ 是 GF(q)上的 d 维矢量空间。

花体字母 $\mathscr{C}$，$\mathscr{R}, \mathscr{P}, \ldots$ 表示 $\mathbb{R}^d$ 的子集。

对于一对整数 $i \le j$，定义离散区间 $[i:j] = \{i, i+1, \ldots, j\}$。更加一般地，对于 $a \ge 0$ 和整数 $i \le 2^a$，定义

- $[i:2^a) = \{i, i+1, \ldots, 2^{\lfloor a \rfloor}\}$，其中 $\lfloor a \rfloor$ 表示 a 的整数部分。
- $[i:2^a] = \{i, i+1, \ldots, 2^{\lceil a \rceil}\}$，其中 $\lceil a \rceil$ 表示 $\ge a$ 的最小整数。

概率和随机变量

事件 $\mathcal{A}$ 的概率用 $\mathsf{P}(\mathcal{A})$ 表示，已知 $\mathcal{B}$ 条件下，$\mathcal{A}$ 的条件概率表示为 $\mathsf{P}(\mathcal{A}|\mathcal{B})$。用大写字母 $X, Y, \ldots$ 表示随机变量。随机变量可以从有限集合 $\mathcal{X}, \mathcal{Y}, \ldots$ 中取值，也可以从实数轴 $\mathbb{R}$ 上取值。习惯上，用 $X = \emptyset$ 表示 X 是一个退化的随机变量（即一个未指明的常数）。事件 $\{X \in \mathcal{A}\}$ 的概率记为 $\mathsf{P}\{X \in \mathcal{A}\}$。

为与常数矢量的记号一致，用 $X_i^j = (X_i, \ldots, X_j)$ 表示长度为 $(j-i+1)$ 的随机序列或 $(j-i+1)$ 维随机列矢量，其中 $1 \le i \le j$。当 $i = 1$ 时，一般省略下标，记为 $X^j = (X_1, \ldots, X_j)$。

令 $(X_1, \ldots, X_k)$ 为一个 k 元随机变量组，$\mathcal{J} \subseteq [1:k]$。下标属于 $\mathcal{J}$ 的随机变量组表示为 $X(\mathcal{J}) = (X_j : j \in \mathcal{J})$。类似地，给定 k 个随机矢量 $(X_1^n, \ldots, X_k^n)$，

$$X^n(\mathcal{J}) = (X_j^n : j \in \mathcal{J}) = (X_1(\mathcal{J}), \ldots, X_n(\mathcal{J})).$$

有时候，我们用 $\mathbf{X}, \mathbf{Y}, \ldots$ 表示指定维度的随机（列）矢量，用 X_j 表示 $\mathbf{X}$ 的第 j 个元素。令 $\mathbf{X}(i)$ 为一个随时间 i 变化的随机矢量，$X_j(i)$ 表示 $\mathbf{X}(i)$ 的第 j 个元素。这个矢量的序列表示为 $\mathbf{X}^n = (\mathbf{X}(1), \ldots, \mathbf{X}(n))$。

下面的符号用于表示随机变量和随机矢量。

- $X^n \sim p(x^n)$ 表示 $p(x^n)$ 是离散随机矢量 X^n 的概率分布函数（probability mass function，pmf）。用 $p_{X^n}(\tilde{x}^n)$ 表示 X^n 的带参数 $\tilde{x}^n$ 的分布，即 $p_{X^n}(\tilde{x}^n) = \mathsf{P}\{X^n = \tilde{x}^n\}$，对所有 $\tilde{x}^n \in \mathcal{X}^n$。没有下标的函数 $p(x^n)$ 可以理解为定义在 $\mathcal{X}_1 \times \cdots \times \mathcal{X}_n$ 上的随机矢量 X^n 的分布。
- $X^n \sim f(x^n)$ 表示 $f(x^n)$ 是连续随机矢量 X^n 的概率密度函数（probability density function，pdf）。
- $X^n \sim F(x^n)$ 表示$F(x^n)$ 是 X^n 的累积分布函数（cumulative distribution function，cdf）。
- $(X^n, Y^n) \sim p(x^n, y^n)$ 表示 $p(x^n, y^n)$ 是 X^n 和 Y^n 的联合分布函数。
- $Y^n | \{X^n \in \mathcal{A}\} \sim p(y^n | X^n \in \mathcal{A})$ 表示 $p(y^n | X^n \in \mathcal{A})$ 是 Y^n 在已知 $\{X^n \in \mathcal{A}\}$ 时的条件概率分布函数。
- $Y^n | \{X^n = x^n\} \sim p(y^n | x^n)$ 表示 $p(y^n | x^n)$ 是 Y^n 在已知 $\{X^n = x^n\}$时的条件概率分布函数。
- $p(y^n | x^n)$ 是一组 $\mathcal{Y}^n$上的（条件）概率分布函数的集合，针对每一个 $x^n \in \mathcal{X}^n$ 定义。$f(y^n | x^n)$ 和 $F(y^n | x^n)$ 的定义与之类似。
- $Y^n \sim p_{X^n}(y^n)$ 表示 Y^n 与 X^n有同样的概率分布函数，即 $p(y^n) = p_{X^n}(y^n)$。对于条件概率分布，使用类似的记法。

已知随机变量 X，其函数 $g(X)$ 的期望记为 $\mathsf{E}_X(g(X))$，简记为 $\mathsf{E}(g(X))$。已知 Y 时，X 的条件期望记为 $\mathsf{E}(X|Y)$。用 $\mathrm{Var}(X) = \mathsf{E}[(X - \mathsf{E}(X))^2]$ 表示 X 的方差，用 $\mathrm{Var}(X|Y) = \mathsf{E}[(X - \mathsf{E}(X|Y))^2 | Y]$ 表示已知 Y时 X 的条件方差。

对于随机矢量 $\mathbf{X} = X^n$ 和 $\mathbf{Y} = Y^k$，$K_{\mathbf{X}} = \mathsf{E}[(\mathbf{X} - \mathsf{E}(\mathbf{X}))(\mathbf{X} - \mathsf{E}(\mathbf{X}))^T]$ 表示 $\mathbf{X}$ 的协方差矩阵，$K_{\mathbf{XY}} = \mathsf{E}[(\mathbf{X} - \mathsf{E}(\mathbf{X}))(\mathbf{Y} - \mathsf{E}(\mathbf{Y}))^T]$ 表示 $(\mathbf{X}, \mathbf{Y})$ 的互协方差矩阵，$K_{\mathbf{X}|\mathbf{Y}} = \mathsf{E}[(\mathbf{X} - \mathsf{E}(\mathbf{X}|\mathbf{Y}))(\mathbf{X} - \mathsf{E}(\mathbf{X}|\mathbf{Y}))^T] = K_{\mathbf{X}-\mathsf{E}(\mathbf{X}|\mathbf{Y})}$ 表示已知 $\mathbf{Y}$ 时 $\mathbf{X}$ 的条件协方差矩阵，即根据 $\mathbf{Y}$ 得到的 $\mathbf{X}$ 的最小均方误差估计（MMSE）的协方差矩阵。

对于标准随机变量和随机矢量，使用如下的记号：

- $X \sim \mathrm{Bern}(p)$：X 为伯努利随机变量，参数为$p \in [0, 1]$，即

$$X = \begin{cases} 1 & \text{以概率} p \\ 0 & \text{以概率} 1 - p \end{cases}$$

- $X \sim \mathrm{Binom}(n, p)$：$X$ 为二项分布随机变量，参数为$n \geq 1$ 和$p \in [0, 1]$，即

$$p_X(k) = \binom{n}{k} p^k (1 - p)^{n-k}, \quad k \in [0 : n]$$