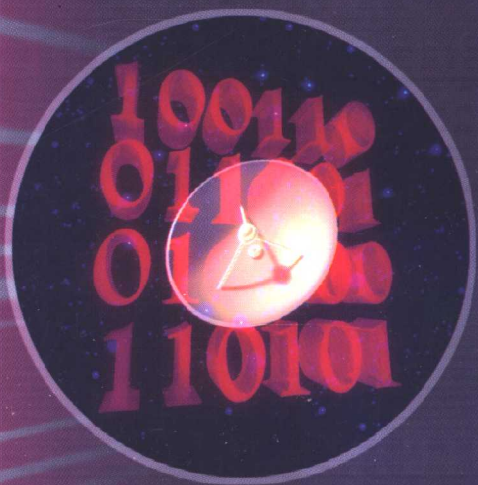




普通高等教育“十五”国家级规划教材

信息论与编码



仇佩亮 编著

高等教育出版社

普通高等教育“十五”国家级规划教材

信息论与编码

仇佩亮 编著

高等教育出版社

内容提要

本书是“十五”国家级规划教材。信息论和编码是研究信息传输和信息处理过程中一般规律和具体实现的一门应用科学,是现代信息科学和技术工程的基础理论。本书是在吸取了国内外经典教材的优点,结合作者教学经验的基础上编写而成。本书写得深入浅出,既保持理论的完整性、系统性,又概念清楚、易读易懂,同时介绍了信息论的新发展。教材主要介绍 Shannon 信息理论和相关的编码技术。内容包括如下 11 章:绪论、熵和互信息、离散无记忆信源的无损编码、信道、信道容量及信道编码定理、率失真理论和保真度准则下的信源编码、受限系统和受限系统编码、线性分组纠错编码、循环码、卷积码、Turbo 码与迭代译码、多用户信息论与多用户编码。

本书适合作为高等院校电子信息类专业的高年级本科生和研究生教材,对于从事信息科学和技术领域工作和研究的人员也极具参考价值。

图书在版编目(CIP)数据

信息论与编码/仇佩亮编著. —北京:高等教育出版社,
2003.12

ISBN 7-04-013047-5

I.信... II.仇... III.①信息论—高等学校—教材
②编码理论—高等学校—教材 IV.O157.4

中国版本图书馆 CIP 数据核字(2003)第 095841 号

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 100011
总 机 010-82028899

购书热线 010-64054588
免费咨询 800-810-0598
网 址 <http://www.hep.edu.cn>
<http://www.hep.com.cn>

经 销 新华书店北京发行所
印 刷 高等教育出版社印刷厂

开 本 787×960 1/16
印 张 32.5
字 数 610 000

版 次 2003 年 12 月第 1 版
印 次 2003 年 12 月第 1 次印刷
定 价 40.10 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

前 言

信息论与编码理论是 50 多年前由美国科学家 C.E. Shannon、R.W. Hamming 等人创立的。它以 Shannon 的不朽名著《通信的数学理论》为里程碑。几十年来许多优秀的学者、工程师共同努力推动了信息论与编码的理论和实践的发展,现在信息论与编码理论已成为信息科学的基础理论,也成为 20 世纪后半叶数字化革命的主要理论和技术支柱。

国外的一流学校在 20 世纪 50 年代末就开始设立信息论与编码课程,目前国内各高等院校的电子信息类专业本科生、研究生也都已把信息论与编码作为一门重要的专业基础理论课。由于信息论与编码的许多思想和方法已广泛地渗透到许多领域,它的许多研究成果也具有普遍意义,因此信息论与编码在许多领域,如在计算机、系统科学、统计学、物理学、生物学、经济学甚至社会学中都获得了成功的应用。信息论与编码理论对于从事这些相关领域工作和学习的人员来说也极具参考价值。

本书在作者多年教学经验和研究实践的基础上编写而成,由于信息论与编码本身既是一门工程科学,同时又是一门应用数学,因此作为教材必须既保持论述的科学性、严谨性,又要求深入浅出、通俗易懂,能为工程师所理解。本书中对于抽象的概念辅以必要的例子予以说明,对于复杂的证明则着重讲清证明思路而忽略繁琐的细节。本书所要求的数学基础是初等的,只要具有概率论、随机过程、线性代数和离散数学中的初等知识就足够了,但也要求读者具有一定的抽象思维能力。对于像 Shannon 理论中的精华——典型列理论和随机编码方法必须要慢慢地咀嚼、细细地品味才能体会它的真谛。

信息论与编码是一门应用科学,它最基本的应用背景是通信。著名的通信理论家 Viterbi 说过,如果把现代通信技术比喻成飞船,则晶体管是它的引擎而信息论是它的方向盘。在本书中突出了信息论和编码的应用,特别强调在通信中的应用。这样理论与应用结合,有助于读者了解产生理论和解决问题的实际背景,也提高了工科学生的学习兴趣。

信息论与编码是一门不断发展的学科,虽然信息论与编码中许多新理论、新概念可以追溯到 Shannon 原著,但是对它们深刻的理解、生动的应用和美妙的理论化则是后来许多学者发展的,许多成果也是 Shannon 本人始料不及的。因此

II 前言

本书除了对于信息论与编码的基本内容进行全面的介绍外,还对目前信息论与编码中某些研究热点进行了介绍,如关于受限系统和受限系统编码、多用户信息论与多用户编码、Turbo 码与迭代译码算法等。

本书分为 11 章,除第 1 章绪论外,第 2 章介绍信息量的定义和性质,第 3 章介绍离散信源的无损压缩编码,第 4 章介绍信道、信道容量和信道编码定理,第 5 章介绍失真受到限制的信源压缩编码问题,第 6 章介绍受限系统和受限系统编码,第 7 章介绍线性分组纠错编码,第 8 章介绍循环码,第 9 章介绍卷积码,第 10 章介绍 Turbo 码与迭代译码算法,第 11 章介绍多用户信息论与多用户编码。除了第 6、第 10、第 11 章以外的绝大多数内容适合于本科教学,其中带有 * 号的章节适合于研究生或具有一定基础的读者进一步深入学习。

几十年来国内外有不少信息论与编码方面的优秀教科书和专著,作者在编写本书过程中得益于以前对于这些著作的学习,此外,在编写本书过程中还参阅了许多文献、资料,在此作者对于这些著作的作者深表谢意。

作者要特别感谢清华大学朱雪龙教授,他非常仔细地审阅了本书全部内容并提出许多宝贵意见,对提高本书的质量起了重要的作用。作者也要感谢浙江大学朱华飞博士、张朝阳博士和谢磊博士,他们在信息论与编码课程教学中试用了本书的部分内容,为本书提出很好的改进意见。最后要感谢作者的妻子陈邦媛教授,她不仅关心作者的生活,承担起全部家务,为作者创造了一个安宁的写作环境,而且对于本书内容的组织安排、深浅分寸的掌握提出许多建设性意见,没有她的支持本书是不可能完成的。

限于作者的水平,本书中不妥和谬误之处难免,恳请读者批评指正。

仇佩亮

2003 年 7 月于杭州浙江大学求是村

策划编辑	张培东
责任编辑	关旭
封面设计	李卫青
版式设计	王艳红
责任校对	胡晓琪
责任印制	韩刚

郑 重 声 明

高等教育出版社依法对本书享有专有出版权。任何未经许可的复制、销售行为均违反《中华人民共和国著作权法》，其行为人将承担相应的民事责任和行政责任，构成犯罪的，将被依法追究刑事责任。为了维护市场秩序，保护读者的合法权益，避免读者误用盗版书造成不良后果，我社将配合行政执法部门和司法机关对违法犯罪的单位和个人给予严厉打击。社会各界人士如发现上述侵权行为，希望及时举报，本社将奖励举报有功人员。

反盗版举报电话：(010) 58581897/58581698/58581879/58581877

传 真：(010) 82086060

E - mail：dd@hep.com.cn 或 chenrong@hep.com.cn

通信地址：北京市西城区德外大街 4 号

高等教育出版社法律事务部

邮 编：100011

购书请拨打电话：(010)64014089 64054601 64054588

目 录

第1章 绪论	(1)
第2章 熵和互信息	(6)
2.1 随机变量的熵和互信息	(6)
2.1.1 事件的自信息和互信息	(8)
2.1.2 条件事件的互信息与联合事件的互信息	(10)
2.1.3 随机变量的平均自信息——熵	(11)
2.1.4 熵的性质	(14)
2.1.5 凸函数	(18)
2.1.6 随机变量间的平均互信息	(22)
2.1.7 概率分布的散度(相对熵)	(26)
2.1.8 关于疑义度的 Fano 不等式	(27)
2.1.9 马尔可夫链和数据处理定理	(28)
* 2.1.10 Shannon 信息度量与集合论之间的联系	(32)
* 2.1.11 信息论与博弈之间的关系	(38)
2.2 连续随机变量的互信息和微分熵	(40)
2.2.1 连续随机变量的互信息	(40)
2.2.2 连续随机变量的熵——微分熵	(42)
2.2.3 微分熵的极大化	(45)
2.3 平稳离散信源的熵	(48)
2.3.1 平稳离散信源的一般概念	(48)
2.3.2 平稳信源的熵	(49)
2.3.3 马尔可夫信源	(52)
2.4 平稳随机过程的信息量与熵	(55)
习题	(59)
第3章 离散无记忆信源(DMS)的无损编码	(64)
3.1 离散无记忆信源的等长编码	(64)

3.1.1 等长编码	(64)
3.1.2 Shannon 编码定理和典型列解释	(65)
3.1.3 渐近等分性质(AEP)与 Shannon 定理的证明	(67)
3.2 离散无记忆源(DMS)的不等长编码	(71)
3.2.1 不等长编码的惟一可译性和译码延时	(71)
3.2.2 Kraft 不等式	(75)
3.2.3 不等长编码定理	(77)
3.3 几种不等长编码算法	(79)
3.3.1 最佳不等长编码(Huffman 编码)	(79)
3.3.2 Shannon 编码法	(82)
3.3.3 Fano 编码	(84)
3.3.4 Shannon-Fano-Elias 编码	(87)
3.3.5 算术编码	(89)
* 3.3.6 通用信源编码算法	(95)
* 3.3.7 压缩编码与离散随机数发生	(100)
3.4 平稳信源和马尔可夫信源的编码定理	(104)
3.4.1 平稳信源的编码	(104)
3.4.2 马尔可夫信源的编码	(107)
习题	(111)
 第 4 章 信道、信道容量及信道编码定理	 (114)
4.1 信道、信道模型和分类	(114)
4.2 离散无记忆信道(DMC)及其容量	(115)
4.2.1 信道容量定义及例子	(116)
4.2.2 离散无记忆信道(DMC)的容量定理	(121)
4.2.3 对称离散无记忆信道容量的计算	(122)
4.2.4 转移概率矩阵可逆信道的容量计算	(126)
* 4.2.5 离散无记忆信道(DMC)容量的迭代计算	(127)
4.3 信道的组合	(132)
4.3.1 积信道(平行组合信道)	(133)
4.3.2 和信道	(134)
4.3.3 级联信道	(136)
4.4 离散无记忆信道(DMC)的编码定理	(138)
4.4.1 几个有关定义	(139)
4.4.2 二元对称信道编码定理的证明	(140)

* 4.4.3 一般离散无记忆信道编码定理的证明(典型列方法)	(144)
* 4.4.4 信道编码定理之逆	(149)
* 4.4.5 具有理想反馈的离散无记忆信道的容量	(150)
* 4.4.6 信源、信道编码分离定理和信源、信道联合编码	(151)
4.5 加性高斯噪声(AWGN)信道	(153)
4.5.1 高斯信道的容量	(155)
* 4.5.2 高斯信道编码定理	(156)
* 4.5.3 高斯信道编码定理之逆	(158)
* 4.5.4 带有独立高斯噪声的平行信道	(159)
* 4.5.5 带有相关高斯噪声的平行信道	(162)
* 4.5.6 MIMO 高斯信道的容量	(164)
4.6 模拟信道的信道容量	(171)
4.6.1 带限、加性白高斯噪声信道	(171)
* 4.6.2 带限、有色高斯噪声信道	(174)
习题	(175)

第5章 率失真理论和保真度准则下的信源编码	(180)
5.1 率失真函数的定义	(182)
5.2 简单信源的率失真函数计算	(186)
5.2.1 Hamming 失真度量下的贝努利信源	(186)
5.2.2 高斯信源	(188)
5.2.3 高斯矢量信源	(190)
5.3 率失真函数的性质	(193)
5.3.1 $R(D)$ 的非零区域($D_{\min}, D_{\max}$)	(193)
5.3.2 $R(D)$ 的向下凸性	(194)
5.3.3 $R(D)$ 为单调递减的连续函数	(195)
5.3.4 利用信源的对称性来计算率失真函数	(196)
* 5.4 率失真函数解的充要条件和参数方程	(199)
* 5.5 率失真函数的交替迭代计算	(205)
* 5.6 保真度准则下离散无记忆信源编码定理	(209)
5.6.1 可达性证明	(209)
5.6.2 逆定理证明	(213)
5.6.3 信道编码定理与限失真信源编码定理之间的对偶	(214)
5.7 无记忆连续信源的率失真函数	(215)
5.7.1 无记忆连续信源的率失真函数定义	(215)

* 5.7.2 平方误差失真度量下连续随机变量的率失真函数的上、下限	(217)
* 5.8 平方误差失真度量下有记忆高斯信源的率失真函数	(221)
5.8.1 有记忆信源的率失真函数定义	(221)
5.8.2 高斯信源的特征	(222)
5.8.3 离散时间平稳高斯信源的率失真函数	(223)
5.8.4 连续时间平稳高斯信源的率失真函数	(227)
习题	(228)
* 第6章 受限系统和受限系统编码	(231)
6.1 受限系统概述	(231)
6.1.1 受限信道	(231)
6.1.2 序列的自相关函数和功率谱	(234)
6.2 受限系统的表示和容量计算	(237)
6.2.1 受限系统的概念	(237)
6.2.2 $RLL(d, k)$ 序列	(238)
6.2.3 受限系统的有限状态转移图表示	(238)
6.2.4 受限系统的容量	(241)
6.2.5 受限系统容量的计算	(242)
6.2.6 最大熵游程受限序列的功率谱	(248)
6.3 受限系统编码方法	(250)
6.3.1 定长分组编码	(250)
6.3.2 码长最短的定长分组码	(253)
6.3.3 可变长度固定速率编码	(255)
6.3.4 向前看(LA)编码技术	(257)
6.4 基于 ACH 状态分裂算法的有限状态编码器	(259)
6.4.1 状态分裂	(260)
6.4.2 近似本征矢量	(261)
6.4.3 u -一致分裂	(264)
6.4.4 ACH 状态分裂算法	(266)
第7章 线性分组纠错编码	(269)
7.1 分组纠错编码的一般概念	(269)
7.1.1 用于纠错和检错的信道编码	(269)
7.1.2 二元对称信道的差错概率和差错分布	(270)
7.1.3 检错和纠错	(271)

7.1.4 自动重发请求 (ARQ) 编码	(273)
7.1.5 最大似然译码和最小 Hamming 距离译码	(275)
7.1.6 最小 Hamming 距离与检错、纠错能力的关系	(277)
7.2 线性分组纠错编码	(279)
7.2.1 线性分组编码的生成矩阵和校验矩阵	(279)
7.2.2 对偶码	(282)
7.2.3 线性分组码的最小 Hamming 距离和最小 Hamming 重量	(283)
7.3 线性分组码的纠错能力	(285)
7.4 线性分组码的译码	(288)
7.4.1 标准阵列译码法	(289)
7.4.2 伴随式译码	(291)
7.5 译码错误概率计算	(292)
7.5.1 码字错误概率	(292)
7.5.2 误比特率	(293)
7.6 二元 Hamming 码	(293)
7.6.1 Hamming 码的定义	(293)
7.6.2 Hamming 码的完备性	(295)
7.6.3 Hamming 码的对偶码	(295)
7.7 从一个已知线性分组码来构造一个新的线性分组码	(296)
习题	(298)
 第 8 章 循环码	 (301)
8.1 有限域代数的基本知识	(301)
8.1.1 有限域的定义	(301)
8.1.2 $GF(2^m)$ 的构成	(303)
8.1.3 有限域的特征和元素的阶数	(305)
8.1.4 最小多项式	(308)
8.2 循环码的定义和它的多项式表示	(309)
8.3 系统循环码的编码及其实现	(314)
8.3.1 系统循环码的编码	(314)
8.3.2 多项式运算的电路实现	(315)
8.3.3 循环码编码的电路实现	(320)
8.4 循环码的矩阵表示	(322)
8.5 循环码的译码及其实现	(325)
8.5.1 伴随式的计算	(325)

8.5.2 循环码的通用译码算法	(328)
8.5.3 梅吉特(Meggitt)译码器	(329)
8.6 几个重要的循环码	(331)
8.6.1 Hamming 循环码	(332)
8.6.2 BCH 码	(334)
8.6.3 Reed-Solomon(RS)码	(337)
习题	(339)
第9章 卷积码	(340)
9.1 卷积码的代数结构	(340)
9.1.1 卷积码的构成	(340)
9.1.2 卷积码编码器的冲击响应和生成矩阵	(341)
9.1.3 卷积码编码器的多项式描述	(346)
9.2 卷积码的图描述和重量计数	(347)
9.2.1 卷积码的树图描述	(347)
9.2.2 卷积码的网格图描述	(349)
9.2.3 卷积码的状态图描述	(349)
9.2.4 卷积码的重量计数	(351)
9.2.5 恶性码	(353)
9.3 卷积码的 Viterbi 译码算法	(354)
9.3.1 分支度量、路径度量和最大似然译码	(355)
9.3.2 Viterbi 译码算法	(357)
9.3.3 作为前向动态规划解的 Viterbi 算法	(359)
9.3.4 实现 Viterbi 译码算法的一些具体考虑	(363)
9.4 卷积码 Viterbi 译码算法的性能界	(365)
9.4.1 节点错误概率	(365)
9.4.2 比特错误概率	(368)
9.4.3 卷积码在 BSC 和 AWGN 信道的性能	(369)
9.5 凿孔卷积码	(372)
习题	(375)
*第10章 Turbo 编码与迭代译码算法	(377)
10.1 Turbo 码概述	(377)
10.2 Turbo 码编码器	(379)
10.2.1 递归系统卷积码(RSC)	(380)

10.2.2 网格终止问题	(382)
10.2.3 Turbo 码中的交织器	(383)
10.3 Turbo 码的性能分析	(388)
10.4 Turbo 码的迭代译码算法	(391)
10.4.1 Turbo 译码方式	(391)
10.4.2 SISO 译码算法(MAP 算法)	(393)
10.4.3 修正的 MAP 算法	(396)
10.5 迭代译码的信息论解释	(398)
10.5.1 最小交叉熵(MCE)原理	(398)
10.5.2 交叉熵与迭代译码的关系	(401)
* 第 11 章 多用户信息论与多用户编码	(405)
11.1 多用户信息传输模型和信源编码模型	(405)
11.1.1 多用户信息传输模型	(405)
11.1.2 多用户信源编码模型	(408)
11.2 多变量联合典型列及强典型列概念	(409)
11.2.1 多变量联合典型列及联合 AEP 性质	(409)
11.2.2 强典型列集合与强 AEP	(412)
11.3 多接入信道	(413)
11.4 广播信道	(418)
11.4.1 广播信道的定义	(419)
11.4.2 退化的广播信道	(420)
11.5 干扰信道	(425)
11.5.1 强干扰信道	(426)
11.5.2 高斯干扰信道	(428)
11.6 中继信道	(431)
11.6.1 退化中继信道	(433)
11.6.2 高斯中继信道	(436)
11.7 具有反馈的多用户信道	(438)
11.7.1 具有无噪反馈的无记忆多接入信道	(438)
11.7.2 具有无噪反馈的广播信道	(443)
11.7.3 双向信道	(446)
11.8 具有状态边信息的信道编码	(452)
11.8.1 具有缺损的硬盘存储器信道	(455)
11.8.2 仅发送端具有信道状态信息时的信道容量	(457)

11.8.3 脏纸上写字	(458)
11.9 相关信源的无损编码及在多接入信道上传输	(460)
11.9.1 相关信源的无损编码	(460)
11.9.2 相关信源在多接入信道上传输	(465)
11.10 具有边信息的信源编码	(469)
11.10.1 译码器具有边信息的无损信源编码	(469)
11.10.2 具有边信息的率失真问题	(471)
11.10.3 仅在译码器具有高斯边信息的高斯信源的率失真函数	(474)
11.10.4 DISCUS 算法	(476)
11.11 多描述信源编码	(480)
11.11.1 具有 2 个信道和 3 个接收机的多描述信源编码模型	(481)
11.11.2 可达性的证明	(488)
11.11.3 信息描述的相继细化	(490)
参考文献	(496)

第 1 章

绪论

信息论是应用近代概率统计方法来研究信息传输、交换、存储和处理的一门学科,也是源于通信实践发展起来的一门新兴应用科学。

信息是系统传输、交换、存储和处理的对象,信息载荷在语言、文字、数据、图像等消息之中。在信息论中,信息和消息是紧密相联的两个不同概念。同样一个消息,比如一张当日的报纸,对于不同的人从中可获得的信息是不一样的;同样的天气预报“明天有雨”,对于干旱地区和雨量充沛地区来说其信息含量也不一样。一张纸写上几个字成为一封家信,对于收信者是家书抵万金,但对旁人可能是废纸一张。因此信息是一种奇妙的东西,它是有别于物质和能量的一种存在。信息的本质和它的科学定义是当前科学界,乃至哲学界热衷研究的课题。信息的重要性是毋庸置疑的。控制论创始人维纳说过:“要有效地生活,就要有足够多的信息”。目前社会上流行一些提法,如“信息、材料、能源是现代科学的三大支柱”、“信息、物质、能量是构成一切系统的三大要素”……这些提法充分说明了人们对信息重要性的认识。

信息的度量是信息论研究的基本问题。从目前的研究来看,要对通常意义下的信息给出一个统一的度量是困难的。存在许多种关于信息度量的定义,但至今最为成功,也是最为普及的信息度量是由信息论创始人香农(Shannon)在他的光辉著作《通信的数学理论》^[17]中提出的,是建立在概率模型上的信息度量。他把信息定义为“用来消除不确定性的东西”。既然信息与不确定性相联系,因此用概率的某种函数来描述不确定性是自然的,所以香农用

$$I(A) = -\log P(A)$$

来度量事件 A 的发生所提供的信息,其中 $P(A)$ 为事件 A 的概率。这个定义与人们的直觉经验相吻合。如果一个随机试验有 N 个可能结果或者说一个随机消息有 N 个可能值,若它们出现的概率分别为 $p_1, p_2, \dots, p_N$,则这些事件的自信息的平均值

$$H = - \sum_{i=1}^N p_i \log p_i$$

作为这个随机试验或随机消息所提供的平均信息也是合理的。 H 也称为熵,这是借助于统计物理学中的一个名词。事实上熵作为信息的代名词也是由 20 世纪伟大的数学家、物理学家冯·诺依曼向香农建议的。在物理学中熵是描述系统的不规则性或不确定性程度的一个物理量。

信息论所研究的通信系统基本模型如图 1.1.1 所示。

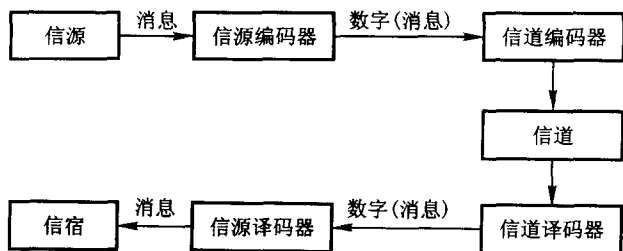


图 1.1.1 通信系统的基本模型

信源是产生消息(或消息序列)的源。消息通常由符号序列或时间函数组成。消息取值服从一定的统计规律,所以信源的数学模型可以是一个离散的随机序列或连续的随机过程。

信源编码器把信源产生的消息变换成数字序列。对无损信源编码来说,信源编码器的目的是在保证能从其输出数字序列中无错误地恢复出输入消息序列的前提下,减少输出数字序列的速率,也就是保证在不失真的条件下对输入消息序列进行压缩。在允许失真的情况下,信源编码的目的是对给定信源,在保证消息平均失真不超过某给定允许值 D 的条件下,尽量减少输出数字序列的速率。

信道在实际通信系统中是指传输信号的媒介或通道,如架空明线、电缆、电离层、人造卫星等。在信息论的模型中也把发送端和接收端的调制、解调器等归入信道,并把系统中各部分的噪声和干扰都归入信道中。在信道的输入、输出模型中,根据噪声和干扰的统计特性,用输入、输出的条件概率(或称转移概率)来描述信道特性。

信道编码器把信源编码输出的数字序列变换成适合于信道传输的,由信道入口符号组成的序列。信道编码器的最主要作用是要对其输出序列提供保护,以抵抗信道噪声和干扰。

信道译码器和信源译码器分别是信道编码和信源编码的反变换,信宿是消息的接收者,即消息的归宿。

信息论解决了通信中的两个基本问题。首先对于信源编码,信息论回答了“达到不失真信源压缩编码的极限(最低)编码速率是多少?”这一问题。香农的答复是这个极限速率等于该信源的熵 H 。事实上香农认为每个随机过程,不管是音乐、语言、图像,都有一个固有的复杂性,该随机过程不能被无失真地压缩到