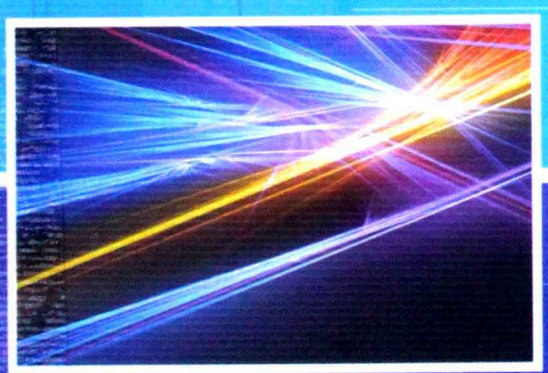
普通高等教育“十二五”规划教材

◎ 电子信息科学与工程类专业 规划教材

信息论与编码

◎ 孙丽华　陈荣伶　编著



電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

普通高等教育“十二五”规划教材
电子信息科学与工程类专业规划教材

信息论与编码

孙丽华　陈荣伶　编著

电子工业出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

本书重点介绍信息论与纠错编码的基础内容，全文共9章，主要内容包括信息及信息的度量、离散信源及信源熵、离散信道及信道容量、信源编码定理和信道编码定理、平均失真测度和信息率失真函数、率失真编码定理、线性分组码、循环码和卷积码，对一些较难理解的概念，辅有较多的例题，并配套免费电子课件、习题解答等教辅资料。

本书可作为高等学校理工类本科电子技术、信息工程、通信工程、雷达、计算机、信息安全、自动化、仪器仪表等相关专业学生的教材，也可作为信息科学及系统工程等领域科研和技术人员的参考书。

图书在版编目（CIP）数据

信息论与编码 / 孙丽华，陈荣伶编著. —北京：电子工业出版社，2012.9
电子信息科学与工程类专业规划教材
ISBN 978-7-121-17992-1

Ⅰ. ①信… Ⅱ. ①孙… ②陈… 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（2012）第 194570 号

策划编辑：王羽佳
责任编辑：王羽佳　　特约编辑：曹剑峰
印　　刷：涿州市京南印刷厂
装　　订：
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：787×1092　1/16　印张：13.75　字数：409 千字
印　　次：2012 年 9 月第 1 次印刷
印　　数：4 000 册　　定价：29.90 元

凡所购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

20 世纪以来，我们正处在一个信息时代，计算机技术、微电子技术、激光技术、多媒体技术、卫星通信和移动通信技术、计算机网络技术等各种新技术的兴起、发展及广泛应用，使得人们的空间距离、时间距离大大缩短，快速、强力地推动着人类社会的经济、科学的高速发展，将人类社会推入到一个高度化的信息时代。无论是在办公室，还是置身于社会，或者是足不出户在家，我们都受到各种信息的包围。尤其是计算机网络的迅猛发展，使得综合语音、视频和数据等多媒体应用已经从精巧的技术概念变成市场现实。

信息论是应用近代概率统计方法研究信息传输、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。当前人类已步入信息社会，随着信息处理技术的不断深入应用，信息在科学技术上的重要性早已超越了狭义的通信工程的范畴，渗透到自然科学与社会科学的所有领域，与电子技术、计算机网络、信息安全、自动控制、生物医学工程、遗传工程、人工智能等学科密切结合，受到各领域越来越多的关注，显示出它的勃勃生机和不可估量的发展前景。

在高等学校中，信息工程类专业是最热门的专业之一，信息技术已经改变了很多传统学科的知识结构。在这种形式下，许多高校都在相关专业开设了信息论课程，一方面，这门课是信息类专业的核心课程，很多学校都把它作为必修课或必选课；但另一方面，这门课程涉及多门工程数学理论，如概率统计论、线性代数、近世代数等，一直有教师难教、学生难学的说法。本书力求在内容筛选及编排上以读者最易接受的方式介绍信息理论的知识。

本书的内容分为两部分：一部分为信息论基础，以香农（Claude E. Shannon）信息论为基础，论述近代信息理论的基本概念和主要结论；另一部分为编码部分，介绍几种常用的信道编码方法。

第 1 章为“信息论基础”，介绍信息论的基本概念，最新发展，以及本书的研究对象——各种信源和信道。

第 2～6 章为信息论部分，介绍信息的度量，内容主要围绕香农三大定理展开，研究在不允许失真的情况下信息传输率的极限值，以及给定信源且允许一定失真的条件下信息速率的极限值，并研究在误码率小于给定值的条件下如何最有效地利用信道的传输能力。

第 7～9 章为编码部分，编码是后人沿着香农指明的可行方向，为寻求有效而可靠的编译码方法而发展起来的一门学科，主要研究在有噪信道条件下各种可行的编码方案及实施技术。

与现有的各种“信息论与编码”教材相比，本教材特色如下：

（1）本书力图在编排上由浅入深，循序渐进，希望读者以易于掌握的方式接受信息论与编码的基本理论。

（2）对于部分具有结论性、指导性的定理，教材省去了冗长烦琐的定理证明，注重物理概念的阐述以及对工作和实际应用的指导意义。

（3）增加了编码部分的内容。教材第 7～9 章分别论述纠错码中最基本的线性分组码、循环码和卷积码的编译码理论，并列举了几种常用的码，如汉明码、BCH 码和卷积码，介绍了它们主要的编译码方法。

（4）对一些难以理解的概念，本书配有较多例题，以帮助读者理解抽象定理。各章后面配有较多难易程度不等的思考题和习题，以供选用。

（5）本书依据编者数十年一线教学和科研经验，在《信息论与纠错编码》第 1 版和第 2 版的基础上编著而成。7 年间，我们使用本教材进行了数十个班的教学，通过切身体会的总结，并广泛收集了广大读者的反馈意见，我们对内容进行了增删、调整，使之更趋合理。

本书全部内容的教学约需 60 学时，不同专业可根据需要进行调整。

本书配有**教学课件和配套辅助文件**，需要者可登录华信教育资源网 http://www.hxedu.com.cn **免费注册下载**。

本书第 1 章、第 9 章、附录 A 和附录 B 由陈荣伶编写，第 2～8 章由孙丽华编写，由孙丽华负责全书的策划、修改和统编。王磊劼、简琪瑶、孙庆如也参与了本书的编写工作。

本书在编写过程中参阅了一些国内外相关著作，这些著作已在参考文献中一一列出，在此谨向有关作者表示深深的谢意！本书在编写过程中得到电子工业出版社的大力支持，王羽佳编辑做了大量的工作，使本书得以顺利出版，在此一并表示衷心的感谢！

本书涉及知识领域广泛，而今科技发展日新月异，由于时间和水平有限，书中难免有差错和不足之处，敬请读者批评、指正！

孙丽华

2012 年 7 月

目　录

第 1 章
信息论基础

内容提要

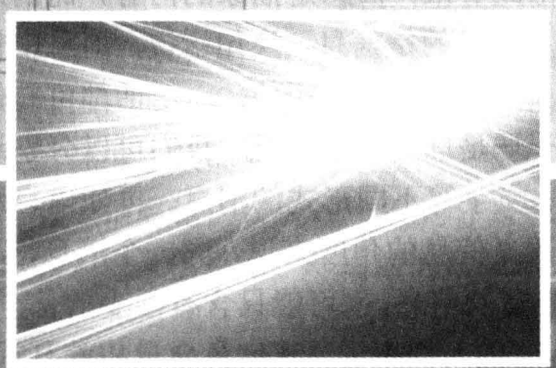
信息论是人们在长期的通信实践中发展起来的一门新兴应用科学，它应用近代概率统计方法来研究信息的传输、交换、存储和处理。自香农（Claude E.Shannon）发表《通信的数学理论》开始，随着信息概念的不断深化，信息理论在科学技术上的应用早已超越了狭义的通信工程范畴，受到越来越多的关注。本章首先引出信息、消息的概念，讨论信息论的研究范畴；然后简述数字通信系统的结构和特点，讨论离散信源、波形信源和离散信道的数学模型和特点；最后介绍几种常见的离散无记忆信源和离散无记忆信道。

知识要点

信息的定义、信息论的研究范畴、数字通信系统的组成、离散信源和离散信道的数学模型。

教学建议

本章是信息论的基本概念，后续信息的度量、信源编码及信道编码都是围绕本章的概念而展开的，建议学时数为 2 学时。



1.1 信息的概念

人们认为，物质、能量和信息是构成客观世界的三大要素。信息是物质和能量在空间和时间上分布的不均匀程度，或者说信息是关于事物运动的状态和规律。物质、能量和信息三者相辅相成，缺一不可。没有物质和能量就不存在事物的运动，也就没有运动状态和规律，当然也就没有信息；反过来，事物在运动，这种运动的状态和规律就成为信息。

因此可以说，没有了信息也就没有了一切！

那么，到底什么是信息呢？

信息有以下三种不同层次的定义。

- 语法信息：它是事物运动状态和规律的本身。它只研究事物运动可能出现的各种状态以及这些状态之间的关系，不涉及状态的含义和效用。
- 语义信息：它是事物运动状态和规律的具体含义。它研究各种状态和实体间的关系，即研究信息的具体含义。
- 语用信息：它是事物运动状态和规律及其含义对观察者的效用。它研究事物运动状态和规律与使用者的关系，即研究信息的使用价值。

可以看出，研究语用信息要以语义信息和语法信息为基础，研究语义信息要以语法信息为基础。语法信息是最抽象最基本的层次，通信工程中的信息传递问题正是基于语法信息。

我们知道，通信系统中形式上传输的是消息，消息与信息有何区别呢？

消息是能被人们的感觉器官感知的客观物质和主观思维的运动状态（或存在状态）。消息传递过程的基本特点是：收信者在收到消息以前是不知道消息的具体内容的。在通信之前，收信者无法判断发信者将发送何种状态的消息。即使收到消息，由于干扰的存在也不能断定所得到的消息是否正确和可靠。总之，收信者存在着“不确定性”。通过消息的传递，收信者知道了消息的具体内容，原先的“不确定”部分或全部消除了，我们说收信者获得了信息。因此，对收信者来说，消息的传递过程是一种消除或部分消除不确定性的过程。消除了不确定性就获得了信息，不确定性消除得越多，获得的信息就越多。由此看来，信息是抽象的内容，而消息是具体的形式。通信系统中形式上传输的是消息，实质上传输的是信息。换句话说，消息中包含信息，消息是信息的载体，信息是消息中包含的有意义的内容。一个短信，一句话都可看作一个消息。不同形式的消息可以包含相同的信息。例如一场足球赛事的状况，我们可以分别通过电视、广播和报纸来了解，这其中就涉及图像、语言、文字等不同形式的消息。再如语言和文字发送同一天的天气预报，信息内容是相同的。而从语义信息的角度来说，同一个消息，不同的人从中可以获得的信息是不同的，它可能包含非常丰富的信息，也可能只含有很少的信息。例如气象广播“明日有雨”，对于干旱地区和雨量充沛地区的人们来说，其信息含量相差甚远。

信息不同于消息，同时也不同于信号。

通信系统中为了克服时间和空间的限制，必须对发信者输出的消息进行加工处理，变换成适合传输和存储的物理量，这种物理量称为信号，如电信号、声信号、光信号等。信号是消息的另一种表现形式，信号携带着信息。例如发短信这一通信过程，手持移动电话系统的传输通道是无线电波，发信者发出的字母、图片或文字等消息是不能直接在无线电波中传输的。需要先将其变换成 7 位、8 位或 16 位的二进制代码，再转换成脉冲电信号。此时脉冲电信号可看

作是消息在无线电波中的表现形式，其载荷着信息。在通信系统的接收端，接收到的脉冲电信号被翻译成收信者能理解的字母、图片或文字，收信者就获得了信息。

信号携带信息，但不是信息本身。同一信息可用不同的信号来表示，同一信号也可表示不同的信息。信息、消息和信号是既有区别又有联系的三个不同的概念。

信息论是源于通信实践发展的一门新兴学科，从通信的角度讲，信息论是应用近代概率统计方法研究信息的基本性质及度量方法，研究信息的获取、传输、存储和处理的一般规律的科学。自 1948 年美国科学家香农（Claude E. Shannon）在 Bell 系统技术杂志上发表重要著作《通信的数学理论》开始，信息论就开启了迅猛发展的篇章。香农信息理论以概率论为工具，定量地描述了信息的含义，通过信源编码定理和信道编码定理指出，在通信系统中采用适当的编码后，能够在随机噪声干扰下有效而可靠地传送信息，并从理论上论证了信息传输的一些基本界限。随后这一理论引起了数学家和通信工作者的高度关注，陆续推出了 Fano 信源编码、Huffman 信源编码、Viterbi 信道译码、数据压缩、网络信息论等各种理论。

信息论是在长期的通信工程实践中发展起来的，但是由于信息问题本身具有极为广泛的意义，信息论很快就渗透到其他领域并相继取得了新的发展，如信息生物学、量子密码学、信息经济学等。

（1）熵估计：熵是信息不确定性的度量，熵估计是研究随机信号或序列特性的基本技术。熵的估计和压缩编码技术常应用于物种 DNA（脱氧核糖核酸）序列的存储、传送等处理中。

（2） 密码学：保密通信系统是一个应用了密码学技术的通信系统，与一般的通信系统相比，增加了保密性和认证性两大功能。保密通信能隐藏和保护传送的消息，只有被授权者才能接收和理解，并且接收者可验证消息的完整性，防止伪造和篡改。

（3）计算机科学：计算机的计算能力发展加快了通信的速度，而各种信源编码、信道编码、存储编码技术的发展也推动了计算机技术的发展。计算机科学与通信理论密不可分，比如计算机中的“最佳随机数发生”与最佳信源编码被证明是等价的。

（4）经济学：信息理论中的最大熵原理的基本思想是，在满足一定的约束条件下，选择使信息熵最大的概率分布。这一理论可以解决封闭经济体中货币量的分布和财富的分布问题。

（5）信息分类：分类问题可以用信息论的数学方法来解决。利用信息量来描述生命现象的离散性，借助信息理论对类群的离散性给出一个合适的数值度量，用它作为衡量分类是否合理的数值标准，从而可以构造新的分类运算方法。

对于信息论的研究，一般划分为以下三个不同的范畴。

（1）狭义信息论：即通信的数学理论，主要研究狭义信息的度量方法，研究各种信源、信道的描述和信源、信道的编码定理。

（2）实用信息论：研究信息传输和处理问题，也就是狭义信息论方法在调制解调、信息处理、检测与估计以及保密理论等领域的应用。

（3）广义信息论：包括信息论在自然和社会中的新应用，如模式识别、机器翻译、自学习自组织系统、心理学、生物学、经济学、社会学等一切与信息问题有关的领域。

在信息时代，人们对于信息的理解远远超出了狭义信息论的讨论范围，要求进一步认识和发展信息概念和信息理论。信息科学的很多问题还在探索之中，本书只限于讨论在通信学科中已建立了完整理论并取得重大技术成就的狭义信息论。

1.2 数字通信系统

通信的基本问题是在彼时彼地精确地或近似地再现此时此地发出的消息。

消息分为两类：离散消息和连续消息。离散消息也称为数字消息，其消息状态数是可数的或离散型的，如符号、文字等。连续消息又称为模拟消息，消息状态是连续变化的，如语音、图像等。通信中消息被转换成电信号，按信号特征的不同，通信系统分为数字通信系统和模拟通信系统。相比模拟通信系统，数字通信系统更能适应对通信技术的高要求，它具有以下优点：

（1）抗干扰能力强，中继时可再生，可消除噪声积累；

（2）差错可控制，可改善通信质量；

（3）便于加密和使用 DSP（Digital Signal Processing）技术处理；

（4）可综合传递各种消息，传送模拟消息时，只要在发送端增加模数转换器，在接收端增加数模转换器即可。

数字通信系统的主要性能指标如下。

（1）有效性

一般用码元传输速率或信息传输速率来衡量通信的有效性。码元传输速率是每秒钟传送的码元个数，单位为波特。信息传输速率是每秒钟传送的信息量，单位为比特/秒。在二元通信系统中，这两种速率在数值上是相等的。

（2）可靠性

用误码率或误信率表示。误码率是指错误接收码元在传送总码元数中所占的比例。误信率也称误比特率，指信息量被传错的概率。误码率和误比特率越低，可靠性越强。

各种数字通信系统，如电话、电视、遥控和雷达系统，虽然形式和用途各不相同，但从信息传输的角度来看，它们在本质上有许多共同之处。对有收、发两端的单向传输系统，一般可概括为图 1-1 所示的统计模型。

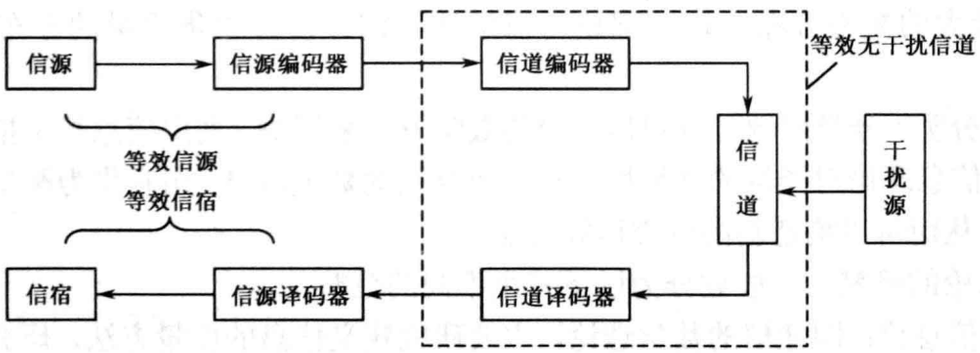


图 1-1 数字通信系统模型

这个模型包括以下五部分。

1. 信源

信源是产生消息的源。消息可以有多种形式，如语言、文字、图像等。消息可以是离散的，也可以是连续的。通信的结果是为了获得信息，信息包含在消息中，或者说消息是信息的载体。信源输出的消息是随机的，在没有收到这些消息之前，收信者所获得的信息的多少是不确定的。消息通常由符号序列或时间函数组成，其取值服从一定的统计规律，在信息论中用离散的随机

变量或连续的随机过程来描述消息。

2. 编码器

编码器是将消息变换成适合于传输的数字序列的设备。编码器分为两种：信源编码器和信道编码器。

信源编码器对信源输出的消息进行适当的变换和处理，来提高信息传输的效率。信源编码常采取消除冗余或根据需要的质量标准去掉一些次要信息等措施，达到压缩每个信源符号所需代码数目的目的，所以也叫压缩编码。例如，在发中文短信时，需将每个汉字编码为 16 位的 UCS2（Unicode Character Set）编码，为提高传输效率，可在不改变语意的情况下将词语或句子压缩。比如，“奥林匹克运动会”可压缩为“奥运会”，这样，原意不变，而冗余度大大减少。再如，电视信号只含 4%的有效信息，采用无失真压缩编码可达 30 倍的压缩率，而多媒体会议采用有损压缩则可压缩上百倍。

经过信源编码的码字序列均被认为是重要信息，如果在传输中受到干扰发生错误或误差超过给定标准，则不满足接收者的质量要求。信道编码是为了抵抗信道的干扰，提高通信的可靠性而对信源编码器的输出进行的变换和处理。为了提高可靠性，可以扩展带宽，降低传输速率，等等，而最常用、最有效的措施是采用差错控制编码，增加冗余码元来自动纠错或检错重发。具体来说就是，对信源编码器的输出符号增加一些冗余符号，并让这些冗余符号与信源编码器的输出符号满足一定的数学约束关系。当出现传输错误后，这种数学约束关系就会被破坏，因此在接收端就能发现错误。针对不同错误的数学运算结果不同，还可以判断出错误的具体位置，从而实现纠错。如奇偶检验码，通过增加一位奇/偶检验位可检验出奇数位错，该奇/偶检验位与信息的内容无关，是个冗余码元。

3. 信道

信道是信息传输和存储的媒介，如光纤、电缆、无线电波、磁盘、书籍等。信道上不可避免地存在各种干扰源，比如来源于无线发射机的无线电干扰、电气设备的工业干扰，以及宇宙射线的天电干扰及电子器件的内部干扰等。为了分析方便，我们将系统其他部分产生的各种干扰都等效地折合成信道干扰。信道的输出是信道输入信号和干扰的组合，由于干扰往往具有随机性，所以信道的特性也用一个随机过程来描述。

4. 译码器

译码是编码的逆变换，分为信道译码和信源译码。由于信道干扰的影响，信道输出的信号序列中可能已有错误，信道译码就是从受干扰的信号中尽可能地纠正其中的错误，再现信源编码器的输出。

信源译码就是将信道中传输的各种信号还原成收信者能感知的消息。

5. 信宿

信宿是消息的接收者。可以是人，也可以是机器。利用收信者的判别能力，采用合适的编码器可以显著提高通信效率。例如，人的视觉残留效应允许对图像采用不连续传输的方式达到连续的视觉效果。再如，人的听觉掩蔽效应允许压缩在大幅度频率分量附近的信号而不影响听觉效果。

通信的最终目的是有效地、可靠地传递消息。有效性和可靠性两者往往相互矛盾，要提高

有效性，就要减少信源的冗余度，缩短每个数据码元所占的时间，这样势必使波形变窄，能量减少，从而使受到干扰后产生错误的可能性增加，传送消息的可靠性降低；若要求可靠，就要增加纠错检错码元，这样增加了信道的冗余度，从而使传送消息的效率变慢。如上例中，若发短信“奥运会”，当接收到“X 运会”时，无法判断所发消息是“奥运会”、“亚运会”还是“农运会”等，可见，所发消息虽然冗余度很小，但容错能力较差；而如果发短信“奥林匹克运动会”，当收到“X 林匹克运动会”时，我们很容易纠正其中的错误，译为“奥林匹克运动会”，说明信源的冗余度对于抵抗信道的干扰是有益的。那么怎样将矛盾的可靠性和有效性统筹兼顾？香农的信息理论指出，在一定的准则下，可以实现有效而可靠的通信。

数字通信系统的模型不是一成不变的，它根据实际情况而定。例如，在研究信息传输的有效性时，可将信道编码器、信道译码器和信道组合起来，等效为一个无干扰信道，这样信源编码器的研究只和信源、信宿有关。而在研究信息传输的可靠性时，可将信源译码器和信宿等效为信宿，将信源和信源编码器等效为一个对于信道编码器而言的信源，这样信道编码的研究只和信道有关，与信源、信宿无关。理论表明，这种简化方法对大多数理论结果没有太大限制。

1.3 信源及其数学模型

信源是产生消息的源，消息中含有信息。信息是抽象的，而消息是具体的，所以可通过消息来研究信源，研究信源各种可能的输出及输出各种可能消息的不确定性。虽然消息是随机的，但其取值服从一定的统计规律，因此信息论中用随机变量或随机过程来描述消息，或者说，用一个样本空间及其概率测度$\{X, q(X)\}$来描述信源。

根据样本空间 X 取值分布的不同情况，信源可分为以下三种类型。

（1）离散信源：消息集 X 为离散集合。即时间和幅度取值都离散的信源，如投硬币、掷骰子、书信、计算机代码等。

（2）连续信源：时间离散而幅度取值连续的信源，如温度、压力等。

（3）波形信源：时间连续的信源，如语音、图像信源等。

连续信源和波形信源输出的消息可以经过抽样和量化分别处理成时间离散和幅度取值离散的消息，因此本书中主要讨论离散信源的情况。

根据信源的统计特性，信源又分为以下两种类型。

（1）无记忆信源：先后不同时刻的消息，其取值相互独立。或者说，消息的概率分布与它发生的时刻毫无关联。

（2）有记忆信源：某一时刻消息的取值与前面若干时刻消息的取值有关联。如中文句子中前后文字的出现是有依赖性的。为了描述这种关联性，有记忆信源的数学模型通常采用联合概率空间来描述。

1.3.1 离散无记忆信源

1. 离散无记忆单符号信源

离散无记忆单符号信源（Discrete Memoryless Source，DMS）输出的是单个符号的消息。每个符号代表一个消息，不同时刻发出的符号之间彼此统计独立，而且符号集中的符号数目是

有限的或可数的。用离散随机变量表示信源发出的符号消息，用离散随机变量的概率分布表示信源发出该消息的可能性。离散无记忆单符号信源的数学模型可以表示为离散型的概率空间，即

$$\begin{bmatrix} X \\ q(X) \end{bmatrix} = \begin{bmatrix} x_1 & x_2 & \cdots & x_k \\ q(x_1) & q(x_2) & \cdots & q(x_k) \end{bmatrix}$$

式中，$q(x_i)$是信源输出符号消息 x_i 的先验概率，满足 $0 \leqslant q(x_i) \leqslant 1$，$1 \leqslant i \leqslant k$，且 $\sum_{i=1}^{k} q(x_i) = 1$。

信源每次输出的符号消息 $x_i \in \{a_1, a_2, \cdots, a_k\}$，即 x_i 的取值必定是 k 个符号$\{a_1, a_2, \cdots, a_k\}$中的某一个。

当信源给定，信源输出的消息及其概率分布也就给定，所以每一个信源都有唯一的概率空间。

【例 1.1】 二进制对称信源只能输出符号 0 或 1，输出 0 的概率为 p，输出 1 的概率为 $1-p$，用 0、1 表示信源的两个消息，概率空间可描述为

$$\begin{bmatrix} X \\ q(X) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ p & 1-p \end{bmatrix}$$

【例 1.2】 随机掷一个无偏骰子，每次朝上一面的点数是随机的，把可能出现的点数看作信源输出的消息，那么该信源可以描述为

$$\begin{bmatrix} X \\ q(X) \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1/6 & 1/6 & 1/6 & 1/6 & 1/6 & 1/6 \end{bmatrix}$$

2. 离散无记忆扩展信源

单符号信源的消息数很有限，尤其在数字通信中，通常采用二进制，只能有 2 个消息。为了扩展信源的消息数，在实际情况下，信源输出的消息往往不是单个符号，而是由先后许多不同时刻发出的符号所组成的符号序列。设序列由 N 个符号组成，若这 N 个符号取自同一符号集$\{a_1, a_2, \cdots, a_k\}$，并且先后发出的符号彼此间统计独立，则我们将这样的信源称为离散无记忆的 N 维扩展信源，其数学模型为 N 维概率空间，即

$$\begin{bmatrix} \boldsymbol{X} \\ q(\boldsymbol{X}) \end{bmatrix} = \begin{bmatrix} \boldsymbol{x}_1 & \boldsymbol{x}_2 & \cdots & \boldsymbol{x}_{k^N} \\ q(\boldsymbol{x}_1) & q(\boldsymbol{x}_2) & \cdots & q(\boldsymbol{x}_{k^N}) \end{bmatrix}$$

式中，$\boldsymbol{x}$ 为各种长为 N 的符号序列，$\boldsymbol{x} = x_1 x_2 \cdots x_N$，$x_i \in \{a_1, a_2, \cdots, a_k\}$，$1 \leqslant i \leqslant N$，序列集 $\boldsymbol{X} = \{a_1 a_1 \cdots a_1, a_1 a_1 \cdots a_2, \cdots, a_k a_k \cdots a_k\}$，共有 k^N 种序列，$\boldsymbol{x} \in \boldsymbol{X}$。由于序列中前后符号无关，故序列的概率 $q(\boldsymbol{x}) = q(x_1 x_2 \cdots x_N) = \prod_{i=1}^{N} q(x_i)$，说明符号序列的概率是序列中各个符号概率的乘积，满足 $0 \leqslant q(\boldsymbol{x}_i) \leqslant 1$，$1 \leqslant i \leqslant k^N$，且 $\sum_{X} q(\boldsymbol{x}) = 1$。

【例 1.3】 将二进制对称信源进行三维扩展，则信源的符号序列共有 2^3 种：000，001，010，011，100，101，110，111。由 $q(0) = p$，$q(1) = 1 - p$ 可得序列的概率依次为

$q(000) = q(0) \cdot q(0) \cdot q(0) = p^3$　　$q(001) = q(0) \cdot q(0) \cdot q(1) = p^2(1-p)$

$q(010) = q(0) \cdot q(1) \cdot q(0) = p^2(1-p)$　　$q(011) = q(0) \cdot q(1) \cdot q(1) = p(1-p)^2$

$q(100) = q(1) \cdot q(0) \cdot q(0) = p^2(1-p)$　　$q(101) = q(1) \cdot q(0) \cdot q(1) = p(1-p)^2$

$q(110) = q(1) \cdot q(1) \cdot q(0) = p(1-p)^2$　　$q(111) = q(1) \cdot q(1) \cdot q(1) = (1-p)^3$

将这 8 种序列看成 8 个消息，得到一个新的信源，即

$$\begin{bmatrix} \boldsymbol{X} \\ q(\boldsymbol{X}) \end{bmatrix} = \begin{bmatrix} 000 & 001 & 010 & 011 & 100 & 101 & 110 & 111 \\ p^3 & p^2(1-p) & p^2(1-p) & p(1-p)^2 & p^2(1-p) & p(1-p)^2 & p(1-p)^2 & (1-p)^3 \end{bmatrix}$$

1.3.2 离散有记忆信源

汉字或英文字母组合成中、英文句子时，往往要受到语法、习惯用语、修辞等的制约，因此中、英文句子中前后出现的汉字、字母往往是有依赖性的。例如，英文字母 T 后面最常出现 H 和 R，而根本不会出现 Q，F，X。这种依赖性我们称为有记忆。

离散有记忆信源的输出需要用联合概率空间$\{\boldsymbol{X}, q(\boldsymbol{X})\}$来描述，信源输出的消息可表示为符号序列$\boldsymbol{x} = x_1 x_2 \cdots x_i \cdots$，其中，$x_i$表示在 i 时刻信源所发出的符号，i 的数值越小，时间上越早。很明显，有记忆信源在 i 时刻发出的符号 x_i 与 i 时刻以前信源所发出的符号有关，因此 x_i 的分布概率应描述为条件概率 $p(x_i | \cdots x_{i-2}\, x_{i-1})$。

多数有记忆信源的记忆长度是有限的，即某一时刻信源发出的符号只与前面已发出的若干个符号有关。为了描述这种有限的记忆关系，常引入“状态”的概念。这样，信源发出的符号与信源所处状态有关。

下面以马尔可夫信源为例来介绍有记忆信源。

设信源在 r 时刻发出的符号 x_r 与前 m 个符号 x_{r-m}, $x_{r-m+1}, \cdots$, x_{r-1} 有关（称为 m 阶），这 m 个时间上依次相邻的符号组成一个状态 s，若 $x_i \in \{a_1, a_2, \cdots, a_k\}$，则可能的状态有 k^m 种，即 $s_1, s_2, \cdots, s_{k^m}$。用 e_r 表示 r 时刻信源发出符号 x_r 之前的状态，$e_r = x_{r-m}\, x_{r-m+1} \cdots x_{r-1} = s_i$，当符号 x_r 发出后，状态将发生改变，记为 $e_{r+1} = x_{r-m+1} x_{r-m+2} \cdots x_r = s_j$，用 $p(s_j | s_i)$表示 s_i 状态到 s_j 状态的转移概率。

当状态转移概率和已知状态下发出符号的概率与时刻无关，即 $p(e_{r+1} = s_j | e_r = s_i) = p(e_{t+1} = s_j | e_t = s_i) = p(s_j | s_i)$和 $p(x_r = a_l | e_r = s_i) = p(x_t = a_l | e_t = s_i) = p(a_l | s_i)$时，称为时齐的。

若信源输出的序列消息与信源的状态满足下列两个条件，则该信源就称为马尔可夫信源。

（1）某一时刻信源的输出符号只与当时的信源状态有关，而与以前的状态无关。有

$$p(x_r = a_l | e_r = s_i, e_{r-1} = s_t, e_{r-2} = s_n, \cdots) = p(x_r = a_l | e_r = s_i)$$

当具有时齐性时，满足

$$\sum_{l=1}^{k} p(x_r = a_l | e_r = s_i) = 1$$

（2）某一时刻信源所处的状态只由前一时刻的输出符号和前一时刻的状态唯一决定。

$$p(e_{r+1} = s_j | x_r = a_l, e_r = s_i) = \begin{cases} 0 \\ 1 \end{cases}$$

表明，若信源处于某一状态 s_i，当它发出一个符号后，一定转移到另一状态。状态的转移依赖于信源发出的符号 a_l，因此状态转移概率由条件概率 $p(a_l | s_i)$确定。

对于时齐马尔可夫信源，满足

$$\begin{cases} p(s_j) = \sum_i p(s_i) p(s_j | s_i) \geqslant 0 \\ \sum_j p(s_j) = 1 \end{cases}$$

【例 1.4】 某二阶时齐马尔可夫信源，设信源符号集为$\{a_1, a_2\}$，状态集为$\{s_1 = a_1\, a_1, s_2 = a_1\, a_2$或$a_2\, a_2, s_3 = a_2\, a_1\}$，各状态之间的转移情况如图 1-2 所示，求各状态的概率分布。

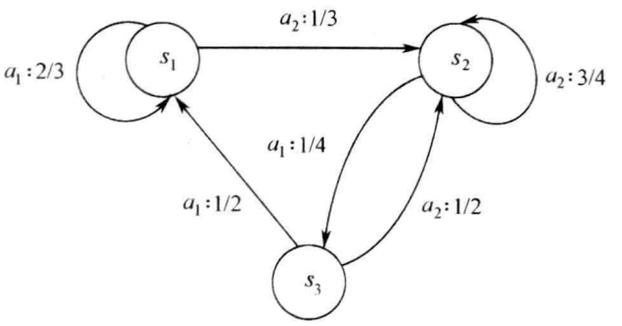


图 1-2　状态转移图

由图 1-2 可知，已知状态下发出符号的概率分别为

$$p(a_1 \mid s_1) = \frac{2}{3}, \qquad p(a_2 \mid s_1) = \frac{1}{3}$$

$$p(a_1 \mid s_2) = \frac{1}{4}, \qquad p(a_2 \mid s_2) = \frac{3}{4}$$

$$p(a_1 \mid s_3) = \frac{1}{2}, \qquad p(a_2 \mid s_3) = \frac{1}{2}$$

由以上条件概率，可得状态转移概率分别为

$$p(s_1 \mid s_1) = \frac{2}{3}, \quad p(s_2 \mid s_1) = \frac{1}{3}, \quad p(s_3 \mid s_1) = 0$$

$$p(s_1 \mid s_2) = 0, \quad p(s_2 \mid s_2) = \frac{3}{4}, \quad p(s_3 \mid s_2) = \frac{1}{4}$$

$$p(s_1 \mid s_3) = \frac{1}{2}, \quad p(s_2 \mid s_3) = \frac{1}{2}, \quad p(s_3 \mid s_3) = 0$$

由于系统是时齐的，由方程组

$$\begin{cases} p(s_1) = \dfrac{2}{3}p(s_1) + \dfrac{1}{2}p(s_3) \\ p(s_2) = \dfrac{1}{3}p(s_1) + \dfrac{3}{4}p(s_2) + \dfrac{1}{2}p(s_3) \\ p(s_3) = \dfrac{1}{4}p(s_2) \\ p(s_1) + p(s_2) + p(s_3) = 1 \end{cases}$$

可进一步求出各个状态的分布概率，得 $p(s_1) = \dfrac{3}{13}$，$p(s_2) = \dfrac{8}{13}$，$p(s_3) = \dfrac{2}{13}$。

1.3.3　波形信源

波形信源输出的消息在时间和幅度取值上都是连续的，如语音、图像信号。对于这种信源输出的消息，可用随机过程来描述。常见的波形信源输出的消息是时间上或频率上有限的随机过程，根据取样定理，它可以转换成时间上离散，而每个取样值都连续的随机变量，若对每个取样值再量化处理，就可将连续的取值转换成有限的或可数的离散值。这样波形信源就可转换成离散信源来处理。

连续信源的数学模型是连续型的概率空间，即

$$\begin{bmatrix} X \\ q(X) \end{bmatrix} = \begin{bmatrix} (a,b) \\ q(x) \end{bmatrix}$$

满足 $$\int_a^b q(x)\mathrm{d}x = 1$$

式中，$q(x)$为随机变量 x 在取值区间(a, b)的概率密度函数。

【例 1.5】 高斯分布信源，其概率统计模型为

$$\begin{bmatrix} X \\ q(X) \end{bmatrix} = \begin{bmatrix} (-\infty, +\infty) \\ \dfrac{1}{\sqrt{2\pi\sigma^2}} \mathrm{e}^{\frac{-(x-m)^2}{2\sigma^2}} \end{bmatrix}$$

1.4 信道及其数学模型

信源输出的是包含信息的消息，而消息在送入信道前必须转换成适合信道传输或存储的信号。信道是信息传输的通道，如图 1-3 所示，信道有输入端和输出端。信息论中仅关心信道输入、输出之间的关系，而不研究信号在信道中传输的物理过程。因此可以将信道模型看成一个黑匣子。由于干扰的存在，信道的输入和输出之间一般不是确定的函数关系。

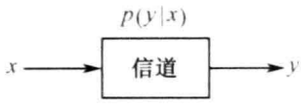


图 1-3 信道模型

数字通信系统中只讨论编码译码问题，可以将信道看成一个数字序列的变换器，它将输入信号 x 变换成输出信号 y，以信道转移概率 $p(y|x)$来描述信道的统计特性。

信道可以按不同的特性进行分类，根据输入和输出信号的特点可分为以下四类。

（1）离散信道：信道的输入和输出都是时间上离散、取值离散的随机序列。离散信道有时也称为数字信道。

（2）连续信道：信道的输入和输出都是时间上离散、取值连续的随机序列，又称为模拟信道。

（3）半连续信道：输入序列和输出序列中一个是离散的，而另一个是连续的。

（4）波形信道：信道的输入和输出都是时间上连续，并且取值也连续的随机序列。

与信源一样，其他信道都可以通过抽样或量化转化为离散信道。根据统计特性，即转移概率 $p(y|x)$的不同，信道又可分为以下两类。

（1）无记忆信道—信道的输出 y 只与当前时刻的输入 x 有关。

（2）有记忆信道—信道的输出不仅与当前时刻的输入有关，还与以前的若干个时刻的输入及输出信号有关。

实际上，卫星信道和深空信道可近似看成离散无记忆信道。在高频、散射和有线信道中，各种干扰所造成的错误往往不是单个地而是成群成串地出现，也就是一个错误的出现往往引起前后码元的错误，表现为错误之间的相关性，因此它是有记忆信道。

1.4.1 离散无记忆单符号信道

离散无记忆单符号信道（Discrete Memoryless Channel，DMC）的输入和输出信号都是离散无记忆的单个符号，设信道的输入符号 $x_i \in \{a_1, a_2, \cdots, a_k\}$，$1 \leqslant i \leqslant k$，输出符号 $y_j \in \{b_1, b_2, \cdots, b_D\}$，$1 \leqslant j \leqslant D$，离散无记忆单符号信道的特性可表示为转移概率矩阵，即