21世纪高等院校信息与通信工程规划教材
21st Century University Planned Textbooks of Information and Communication Engineering

信息理论与编码（第2版）

吕锋 王虹 刘皓春 编著

Information Theory and Coding ,Second Edition

人民邮电出版社
POSTS & TELECOM PRESS

精品系列

21世纪高等院校信息与通信工程规划教材
21st Century University Planned Textbooks of Information and Communication Engineering

信息理论与编码（第2版）

吕锋 王虹 刘皓春 编著

Information Theory and Coding ,Second Edition

人民邮电出版社
北京

精品系列

图书在版编目（CIP）数据

信息理论与编码 / 吕锋，王虹，刘皓春编著. -- 2版. -- 北京 : 人民邮电出版社，2010.9
21世纪高等院校信息与通信工程规划教材
ISBN 978-7-115-20660-2

Ⅰ. ①信… Ⅱ. ①吕… ②王… ③刘… Ⅲ. ①信息论－高等学校－教材②信源编码－编码理论－高等学校－教材③信道编码－编码理论－高等学校－教材 Ⅳ. ①TN911.2

中国版本图书馆CIP数据核字(2010)第058331号

内 容 提 要

本书系统地介绍香农信息论的基本内容及其应用。全书共8章。前3章是全书的理论基础，主要介绍信息论的基本理论知识；第4章讨论信源无失真编码，目的在于提高信源的信息含量效率；第5章讨论信道编码，借此可解决传送的可靠性问题；第6章介绍信源有失真编码方法；第7章介绍网络信息论的一些基本理论和新成果，论述多用户通信系统的信道容量、信道编码定理、实现编码定理的码的结构问题等理论、技术；第8章简要阐述用密码技术如何保证电子信息的有效性、保密性、完整性。

本书可作为高等院校通信、信息类专业和相关专业本科生教材或教学参考书，也可作为相关领域科研人员、工程技术人员的参考书。

21世纪高等院校信息与通信工程规划教材

信息理论与编码（第2版）

◆ 编　著　吕　锋　王　虹　刘皓春
责任编辑　贾　楠

◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街14号
邮编　100061　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京鑫正大印刷有限公司印刷

◆ 开本：787×1092　1/16
印张：16　2010年9月第2版
字数：390千字　2010年9月北京第1次印刷

ISBN 978-7-115-20660-2

定价：29.00元

读者服务热线：(010)67170985　印装质量热线：(010)67129223
反盗版热线：(010)67171154
广告经营许可证：京崇工商广字第0021号

第2版前言

应广大使用者和出版社的要求，根据编者使用该书教学的实际，编者对2004年2月出版的《信息理论与编码》进行了修订。本次修订主要包括以下3个方面。

（1）对教学中发现的编印错误进行了修订。

（2）增减、补充了部分内容，以便更适应教学实际的需要。

（3）修订了部分习题。

参加本书修订工作的主要有吕锋、王虹、刘皓春、刘雪冬，其中刘皓春承担了大部分工作，刘雪冬修订了习题，全书由吕锋统稿。

编　者

第1版前言

信息是事物运动的状态和方式，是关于事物运动的千差万别的状态和方式的知识。人类社会的生存、发展都离不开信息的获取、传递、处理、控制和利用。

信息论是整个信息科学发展的起源和基石。21世纪是高度信息化的时代，信息论不仅在通信领域中发挥越来越重要的作用，也是解决通信领域中相关问题的有力工具；而且由于信息理论蕴涵着独特的、有效的、新颖的解决问题的思路和方法，这一学科已渗透到其他相关的自然科学、社会科学领域，与计算机技术、电子技术、控制技术、网络技术、人工智能、生物工程、医学工程、管理科学等学科密切结合，显示了它的勃勃生机。因此，在现代科学技术高速发展的过程中，学习和掌握信息科学显得尤为重要。

信息论是一门利用概率论、随机过程和数理统计等数学方法来研究信息的存储、度量、编码、传输、处理中一般规律的重要学科，是数学知识与通信技术相结合的边缘学科。自从香农1948年发表奠定信息论基础的“通信的数学理论”一文以来，信息科学有了很大的发展并已经延伸到许多领域中。当今，它主要研究如何提高信息系统的可靠性、有效性、保密性和认证性，从而获取最优信息系统。

本书系统地介绍香农信息论的基本内容及其应用。全书注重基本概念、基本理论和基本分析方法的论述，并结合实例给出详细的数学推演过程和证明，力求概念清晰、结构严密、内容由浅入深、章节循序渐进。

全书共8章。其中前3章是全书的理论基础，主要介绍信息论的基本理论知识。第1章阐述了信息的概念、信息论的研究内容以及应用范围等，期望为读者展示一个信息论的轮廓；第2章详细地讨论了信息的度量方法，侧重于信息的数学建模；第3章讨论信道，描述和分析了各种不同类型信道的模型和特性；第4章讨论信源无失真编码，目的在于提高信源的信息含量效率；第5章讨论信道编码，借此可解决传送的可靠性问题；第6章介绍信源有失真编码方法，对连续信源只能进行有失真编码；第7章介绍网络信息论的一些基本理论和新成果，论述多用户通信系统的信道容量、信道编码定理、实现编码定理的码的结构问题等理论、技术。第8章简要地探讨了信息安全、密码学，阐述用密码技术如何保证电子信息的有效性、保密性、完整性。

信息论是一门既具有严密的逻辑演绎推理系统，又具有丰富生动的时代气息的科学理论。全书按照理论联系实际的原则，基于信息论中的重要结论、分析方法、解决思路的论述，并力求反映近年来国内外信息理论的新发展。

本书的第 1 章、第 2 章由吕锋教授编写，第 3 章、第 5 章和第 6 章的 1、2 节由刘皓春副教授编写，第 7 章、第 8 章和第 6 章的 3、4 节由王虹副教授编写，第 4 章由苏扬副教授编写。全书由吕锋教授统稿。

本书可作为高等院校通信、信息类专业和相关专业本科生教材或教学参考书，也可作为科研人员、工程技术人员的参考书。

限于编者水平，书中难免出现错误和缺憾，殷切期望广大读者批评指正。

编　者

目　录

第 1 章　绪论……1
1.1　信息的概念……1
1.1.1　信息概念的复杂性……1
1.1.2　信息的定义……3
1.2　信息论的主要研究内容……4
1.3　信息论的发展历程……7
习题……10
第 2 章　信息的度量……11
2.1　信源模型……11
2.2　（概率）信息的描述……13
2.3　不确定性与信息……14
2.3.1　自信息量……14
2.3.2　联合自信息量……15
2.3.3　条件自信息量……16
2.3.4　自信息量的性质和相互关系…17
2.3.5　互信息量及其性质……19
2.4　离散随机变量的（统计）平均不确定性——离散熵……22
2.4.1　离散熵……22
2.4.2　离散熵的性质……24
2.5　联合熵和条件熵……26
2.5.1　联合熵……27
2.5.2　条件熵……27
2.5.3　各类熵之间的关系……28
2.6　平均互信息量及其性质……29
2.7　离散无记忆信源的扩展……31
2.8　离散平稳信源的熵……32
2.9　马尔可夫信源的信息熵……33
2.9.1　马尔可夫链……33
2.9.2　马尔可夫信源……35
2.9.3　马尔可夫信源的信息熵……37
2.10　离散信源的信息（速）率和信息含量效率……38
2.11　连续随机变量下的熵和平均互信息量……39
2.11.1　连续随机变量的熵……39
2.11.2　连续随机变量下的联合熵、条件熵以及平均互信息量……42
2.11.3　微分熵的极大化问题……43
2.11.4　连续信源的熵功率……46
本章基本概念……46
习题……49
第 3 章　信道模型和信道容量……55
3.1　信道模型与信道分类……55
3.2　离散无记忆信道的数学模型……56
3.3　概率的计算问题……58
3.4　信道的疑义度、散布度和平均互信息……60
3.4.1　信道的疑义度……60
3.4.2　信道的散布度……61
3.4.3　信道的平均互信息……63
3.5　信道容量 C……66
3.5.1　信道容量的定义……66
3.5.2　离散无噪信道的信道容量……67
3.5.3　离散对称信道……71
3.5.4　一般 DMC 达到信道容量的充要条件……76
3.5.5　信道容量的迭代算法……80
3.6　扩展信道及其信道容量……81
3.6.1　扩展信道的数学模型……82
3.6.2　扩展信道的平均互信息量和信道容量……83
3.7　信道的组合……85
3.7.1　串联信道……85
3.7.2　独立并联信道……87
3.8　信源与信道的匹配……87
3.9　连续信道及其信道容量……88
3.9.1　连续信道的数学模型……88

3.9.2 加性高斯噪声信道的信道容量……89
3.9.3 一般加性噪声信道的信道容量的界……92
3.10 波形信道及其信道容量……93
本章基本概念……96
习题……100
第 4 章 离散无记忆信源无失真编码……104
4.1 信源编码概论……105
4.2 码的唯一可译性……107
4.2.1 常见码及其唯一可译性……107
4.2.2 码树和 Kraft 不等式……108
4.3 定长编码……110
4.3.1 离散无记忆信源的渐近均分性质……110
4.3.2 定长编码定理……113
4.4 变长编码定理……116
4.5 变长编码方法……117
4.5.1 霍夫曼编码……118
4.5.2 费诺编码……123
4.5.3 香农编码……124
4.6 几种实用的无失真信源编码……125
4.6.1 游程编码……125
4.6.2 算术编码……129
4.6.3 基于字典的编码……132
本章基本概念……134
习题……135
第 5 章 有噪信道编码……138
5.1 译码规则与错误概率……138
5.2 两种典型的译码规则……140
5.3 平均差错率与信道编码……143
5.3.1 “简单重复”编码……144
5.3.2 对符号串编码……145
5.4 汉明距离与最小距离译码规则……148
5.5 有噪信道编码定理……150
5.5.1 联合典型序列……150
5.5.2 有噪信道编码定理……152
5.6 Fano 不等式和有噪信道编码逆定理……153
5.7 线性分组码……155
5.7.1 线性分组码的生成矩阵和校验矩阵……156
5.7.2 汉明距离和码的纠错、检错能力……158
5.7.3 线性码的伴随式与伴随式译码……160
本章基本概念……161
习题……162
第 6 章 限失真信源编码……165
6.1 失真测度……165
6.2 信息率失真函数及其性质……167
6.2.1 信息率失真函数的定义……167
6.2.2 信息率失真函数的性质……168
6.3 限失真信源编码定理……171
6.4 信息率失真函数的计算……171
6.4.1 离散信源信息率失真函数的参量表示计算方法……171
6.4.2 离散信源信息率失真函数的迭代计算方法……179
本章基本概念……182
习题……183
第 7 章 网络信息论基础……185
7.1 概论……185
7.2 网络信道的分类……186
7.3 网络信源编码模型……188
7.4 多随机变量联合典型序列……190
7.5 相关信源编码定理……193
7.6 多址接入信道……196
7.7 高斯多址接入信道……200
7.8 广播信道……203
7.9 中继信道……207
7.10 具有边信息的信源编码定理……208
本章基本概念……211
习题……213
第 8 章 信息安全与密码学基础……214
8.1 信息安全概述……214
8.2 网络模型与安全服务功能……215
8.2.1 开放系统互连（OSI）参考

模型……215
8.2.2 安全分层原则……216
8.2.3 安全服务功能……216
8.2.4 网络安全对策……218
8.3 密码学基础知识……220
8.3.1 基本术语……220
8.3.2 代替密码……222
8.4 密码算法的数学背景……225
8.4.1 信息论……225
8.4.2 复杂性理论……227
8.4.3 数论基础……228
8.5 数据加密标准……231
8.5.1 数据加密标准的开发……231
8.5.2 DES 算法概要……231
8.5.3 初始置换……232
8.5.4 密码运算函数 $f(R,K)$……232
8.5.5 密钥置换……233
8.5.6 扩展置换……234
8.5.7 S 盒替代……234
8.5.8 P 盒置换……236
8.5.9 逆初始置换……236
8.5.10 DES 的安全性……236
8.6 公开密钥算法……237
8.6.1 公开密钥密码体制……237
8.6.2 背包公钥密码……238
8.6.3 RSA 公钥加密……240
8.6.4 数字签名……242
本章基本概念……244
习题……246
参考文献……248

第1章 绪论

信息论是研究信息及其运动规律的科学。科学的各个领域中都存在大量的信息问题，最早对信息问题进行系统理论研究的是通信工作者，这是因为通信的核心任务是传递信息，为了设计出有效的通信系统，必须对传输对象信息进行定量分析，由此发展起来了一套行之有效的通信的数学理论，即信息论。信息论的诞生，以美国学者香农（Shannon）1948 年发表题为“通信的数学理论”的著名论文为标志。香农在论文中利用概率论作为数学工具，对通信中的一系列基本理论问题进行深入研究，给出了信息和信道容量度量公式，得到了一组表征信息传递关系的编码定理。信息论自诞生以来，吸引了各领域的大量学者，经过几十年的发展，广泛地渗透到生物学、医学、管理学、经济学等其他各个领域，由此兴起了一门新学科——信息科学。

信息科学正处发展之中，但其经典理论已完善，并得到成功应用，这部分理论通常称为经典信息论或香农信息论。本书主要介绍经典信息论。

本章首先阐述信息的概念，然后讨论信息论的研究目的和研究内容，最后对信息论的发展历程和应用进行简单介绍。

1.1 信息的概念

任何一门科学都有它自己的基本概念，而理解和掌握这些基本概念是学习这门科学的基础。信息论最基本和最重要的概念就是信息。因此信息既是信息论的出发点，也是它的归宿。具体地说，信息论的出发点是认识信息的本质和它的运动规律；它的归宿则是利用信息来达到某种具体的目的。

1.1.1 信息概念的复杂性

当今社会，信息一词，在各种场合都被广泛采用，但如同数学中的“集合”一词一样，要给它下一个严格的定义却异常之难。即使是信息论的奠基人香农（C.E.Shannon），在其著名论文《通信的数学理论》中，也并没有给信息下一个明确的定义，留下一个悬案。香农论文发表之后，由于其方法新颖，引来许多专家学者对信息进行深入研究，研究中碰到的首要问题就是要给“信息”一词下一个明确的定义。很多学者都给“信息”下过定义，流行的说法不下百种，而且对此还展开了一些重要的哲学争论，到现在还没有一个定论。钟义信先生在《信息科学原理》一书中引述了三十多种比较典型和有代表性的说法，这些说法出发点不

同，所站角度不一，有些则带有较明显的学科倾向，但都在一定层面上对信息概念做了描述。以下为作者从中选取的一部分内容，按个人理解略作归类、分析，供读者参考。

1．用人们熟知的、与信息有某种联系的概念来定义信息

（1）信息是消息。

（2）信息是数据。

此类定义只接触到与信息相关的一些表象，未触及信息的实质。在日常交流中，信息常以消息的形式出现，消息中可能含有信息，但不是信息本身。数据则是记录信息的一种形式，并非是唯一形式。

2．用某些学科的专门术语和名词来定义信息

（1）信息是集合之间的变异度。

（2）信息是一种场。

（3）信息是信号。

“集合”和“场”分别是从数学和物理学中引入的概念，姑且不谈其自身在所属学科或领域存在的争议，就概念本身就很难懂，拿来定义信息使人更加难以理解。信号是电专业的专用名词，是表现信息的一种形式，或传输信息的一种载体，不是信息本身。

3．从广义的角度或者说从哲学意义上来定义信息

（1）信息就是信息，既不是物质也不是能量。

（2）信息是事物之间的差异。

（3）信息是事物相互作用的表现形式。

（4）信息是事物联系的普遍形式。

（5）信息是物质的普遍属性。

这类定义很多，它们的共性是力争从一般意义下来定义信息，哲学味道很浓，但难以从定义出发引出信息的度量方法。此类定义容易引起哲学争论，当然，争论的过程实际上也是认识深入的过程，工科学生了解这些定义，对开阔自己的视野非常有益。

4．从控制论和系统论的角度来定义信息

（1）信息是与控制系统相联系的一种功能现象。

（2）信息是控制的指令。

（3）信息是系统组织程度的度量。

（4）信息是有序性的度量。

（5）信息是负熵。

前两种是从控制论的角度给出定义，这两说法不能说没有道理，因为控制系统必须有信息与之相关联，才能实施有效的控制，而控制指令中必然含有信息，但根据这两种说法，我们还是不知信息到底是什么。后3种是从系统论角度下的定义，这3种说法意思差不多，因为系统的有组织程度与有序性意思相近，而熵代表无组织程度，负熵即为有组织程度。这3种定义与香农对信息的理解较为接近，香农虽未明说，但从其论文可看出，香农把信息理解为消除不确定性的东西。

5. 从随机不确定性的角度来定义信息

（1）信息是收信者事先不知道的报道。

（2）信息是用以消除不确定性的东西。

下此类定义者通常对通信有所了解，有些本来就是通信领域的专家学者。他们在定义信息时考虑到了通信的实际情况，即收信者在收到信息之前是心存疑问的，存在一定的不确定性，收到信息之后，不确定性会减少或消除，因此说，信息是用以消除不确定性的东西。例如，假设巴西足球队和阿根廷足球队将进行一场重要的国际比赛，你在未得到赛事结果的任何消息之前，你可能会根据两队以往的战绩判断，两队势均力敌、胜负参半，即比赛结果存在不确定性，而且这时不确定性是最大的。若从电视新闻中得到消息是“上半场巴西队 3:0 领先”，这时你会重新判断比赛结果，认为巴西队取胜的可能性大增加，这说明比赛结果的不确定性大大减少了，有部分不确定性消除了。若新闻中说“巴西队 3:0 取胜”，则比赛结果的不确定性完全消除了。无论是不确定性部分消除还是完全消除，都是因为收到了信息，因此将信息定义为消除不确定性的东西是有道理的。

1.1.2 信息的定义

信息概念众说纷纭，定义信息尽管困难，但却是不可回避的问题，本书采用钟义信先生提出的信息定义体系，即按适用面的不同来分层次地定义信息。层次愈高，适用面愈宽。适用面不同意味着给定义附加的约束条件不同，约束条件愈多，适用面愈窄。

钟先生将最高层次的信息称为**本体论层次信息**，定义为：某事物的（本体论层次）信息，就是事物运动的状态和方式，也就是事物内部结构和外部联系的状态和方式。

信息是事物运动的状态与方式，具体地讲，就是事物内部结构和外部的联系和运动的状态与方式。在此，“事物”泛指一切可能的研究对象，包括外部世界的物质客体，也包括主观世界的精神现象；“运动”泛指一切意义上的变化，包括机械运动、物理运动、化学运动、生物运动、思维运动和社会运动等；“运动方式”是指事物运动在时间上所呈现的过程和规律；“运动状态”则是事物运动在空间上所展示的性状与态势。

本体论层次的信息是最广意义下的信息，是无条件的信息，与是否有（认识或观察）主体无关。世上一切事物始终处于运动之中，有些是已知的，有些是未知的，因此都在产生信息。

本体论层次的信息定义适用面最广，但使用起来却不太方便，它与后面将要给出的信息度量方式难以产生直接的联系。鉴于此，可给定义附加一些约束条件，降低定义的层次，当然适用面会相应变窄。最具实际意义的约束条件是加入人类这个认识或观察的主体，从认识论的角度来定义信息，此层次的信息称为**认识论层次信息**，定义为：某主体关于某事物的（认识论层次）信息，是指该主体所感知的相应事物的运动状态及其变化方式，包括状态及其变化方式的形式、含义和效用。

认识论层次下的信息同时考虑了事物运动状态及其变化方式的外在形式、内在含义和效用价值 3 个因素，因此，较之本体论层次信息，尽管适用面变窄，但内涵却丰富得多。之所以如此，原因在于加入了人这个认识主体，人有感觉能力、理解能力以及判断能力，因此，对事物的运动状态及其变化方式，可感觉其外在形式、理解其内在含义以及判断其效用价值。

由于认识论层次信息内涵丰富，笼统地加以研究实属困难，为此，钟先生借用语言学中的术语，将认识论层次信息进行细分，将涉及形式因素的信息部分称为**语法信息**，涉及含义因素的信息部分称为**语义信息**，涉及效用因素的信息部分称为**语用信息**。这样，认识论层次的信息就是同时涉及语法信息、语义信息和语用信息的**全信息**。

全信息内涵丰富，是广义信息论研究的对象。由于全信息涉及语义和语用因素，两者都会牵扯到认识主体的主观意识，因此度量起来异常困难，到现在还没建立起成熟的理论与方法。

在全信息中，只涉及形式因素的语法信息是最基本的，至于其内在含义和效用价值都要根据外在形式来理解和判断。回到通信的实际情况中来看，通信工程师最关心的是什么呢？通信的主要任务是将信息的外在形式准确、快速地传送给收信者，至于信息的内在含义和效用价值就靠收信者自己去理解和判断了，因此通信工程师最关心的是语法信息。

经典信息论，或称香农信息论，就是以能用概率方法描述的语法信息为研究对象，这种概率型语法信息简称为**概率信息**。基于概率信息的信息理论，最初由香农提出，经过后来诸多学者的补充完善，发展已较为成熟，并且在通信领域得到成功应用，成为通信的数学基础理论。

根据香农的论述，可给出概率信息的定义：（概率）信息是消除随机不确定性的东西，认识主体通过观察获得的（概率）信息量在数值上等于随机不确定性的减少量，或者笼统地说，（概率）信息就是随机不确定性的减少。

本书主要讨论经典信息论，因此将以概率信息的定义为基础加以展开，此后若无特殊说明，所说的信息都特指概率信息。

1.2 信息论的主要研究内容

从上一节介绍的信息定义及其分类中，我们知道信息可分为语法信息、语义信息和语用信息。信息论是关于信息的本质和传输规律的科学的理论，是研究信息的计量、发送、传递、交换、接收和储存的一门新兴学科。信息是信息论研究的主要内容。根据研究内容范围的大小，可对信息论进行分类。

狭义信息论，也称经典信息论。它主要研究信息的测度、信道容量以及信源和信道编码理论等问题。这部分内容是信息论的基础理论，又称香农基本理论。

一般信息论，主要是研究信息传输和处理问题。除了香农理论以外，还包括噪声理论、信号滤波和预测、统计检测与估计理论、调制理论、信息处理理论以及保密理论等。后一部分内容是以美国科学家维纳（N.Wiener）为代表。

可以看出，狭义信息论和一般信息论研究的都是关于语法信息的问题。

广义信息论不仅包括上述两方面的内容，而且包括所有与信息有关的自然和社会领域。如模式识别、计算机翻译、心理学、遗传学、神经生理学、语言学、语义学甚至包括社会学中有关信息的问题，即广义信息论不但研究语法信息，还将研究领域延伸到语义信息和语用信息的范畴。

信息论最初是从狭义的通信系统基础上发展起来的，理论一旦从实践中抽象出来，其意义就远远超出了原来的研究范围。除了电报、电话等狭义的通信系统以外，生物有机体的遗

传系统、神经系统以及人类社会的管理系统等，都涉及信息传输问题，都可用信息论的方法加以研究。

信息论所讨论的问题可用如图 1.1 所示的信息传输基本模型加以说明。图 1.1 所示实际上是一个广义的点到点单向信息传输系统模型，实际的信息传输系统未必如此简单，但用图 1.1 所示的模型可解释各种信息传输系统中的一些共性问题，对这些共性问题进行分析总结，会得到一些重要的基本概念。

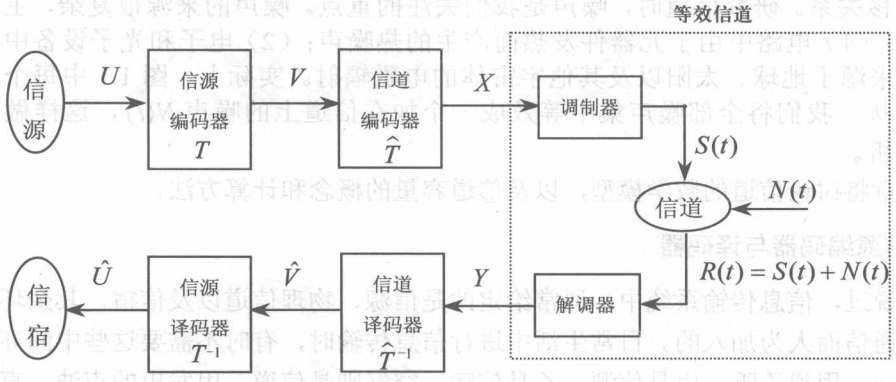

图 1.1 信息传输基本模型

通常，实际的信息传输系统中，事先给定的是图中椭圆框出的部分，即发出信息的信源，接收信息的信宿和传输信息的物理媒介信道，其余中间环节都是由人来设计的。信息传输性能的好坏，很大程度取决于这些中间环节设计的优劣。

1. 信源、信宿和信道

信源是发送消息的源，根据其输出的性质，有数字信源和模拟信源之分。离散信源输出离散的符号或数字消息序列，如电报机输出在时间上离散的符号序列；模拟信源输出连续波形信号，如麦克风输出连续语音信号。

信源是信息论的主要研究对象之一，但在信息论中并不探讨信源的内部结构和物理机理，而把注意力放在信源的输出上，重点讨论信源输出的描述方法及性质。在认识主体看来，信源的输出都是随机的（具有不确定性），因此，可将信源输出的消息视为某个随机实验的输出或某个随机变量的取值，这样可用随机数学方法予以处理。另外，从等效的观点来看，图 1.1 中每一个环节的输出，都可视为一个等效信源的输出。信源的数学模型、不确定性测度以及信息度量将在第 2 章集中介绍。

信宿取信息归宿之意，即收信者或用户，是信息传送的终点或目的地。语义信息和语用信息就是由信宿来理解和判断的。信息论只关心信息传输的方法与手段，信息传输的目的是将信源发出的消息准确及时地传送至信宿，而消息的含意（语意信息）和效用（语用信息）与信息传输方法或手段完全无关，因此本书后文内容对信宿不作过多探讨。

传输信息的物理媒介通常称为物理信道，如空气、双绞线、同轴电缆、光纤等。物理信道的输入信号是 $S(t)$，输出信号是 $R(t)$。$R(t)$ 通常是 $S(t)$ 的不完全复现，之所以不完全，是因为存在随机干扰信号，即噪声 $N(t)$，对于加性噪声，有 $R(t)=S(t)+N(t)$。

各种物理信道都有其固有的通过频带，为了使载荷信息的信号频谱结构与信道的通过频带相匹配，在信号送入物理信道之前，必须对信号进行调制，即进行信号频谱迁移，这就是调制器的作用，在信道输出端加解调器将信号复原。调制与解调技术，是“通信原理”重点讨论的问题之一。在“信息论”中，不专门讨论调制与解调技术，而是将二者与物理信道合并到一起，作为一个等效信道来处理。

其实，图1.1所示中任一输入至任一输出之间的通道，都可看做是一个等效信道。信息论中研究的信道都是等效信道，所关心的问题是：在噪声干扰下，信道输入至输出之间的状态转移关系。研究信道时，噪声是我们关注的重点。噪声的来源很复杂，主要有以下几种情况：（1）电路中由于元器件发热而产生的热噪声；（2）电子和光子设备中的发射噪声；（3）来源于地球、太阳以及其他宇宙体的电磁辐射。实际上，图1.1中每个环节都存在噪声干扰，我们将全部噪声集中等效成一个加在信道上的噪声$N(t)$，这样做主要是为了便于分析。

第3章将讨论信道的数学模型，以及信道容量的概念和计算方法。

2．信源编码器与译码器

前面说过，信息传输系统中，通常给定的是信源、物理信道以及信宿，其余环节都是为保证有效通信而人为加入的。日常生活中进行信息传输时，有时不需要这些中间环节。如两人当面讲话，甲说乙听，甲是信源，乙是信宿，空气则是信道；甲发出的声波，直接通过空气传到乙，中间环节全无。若两人相隔很远，甲费尽全力喊话，由于声波在空气中传播会逐渐衰减，所以乙还是不能听见。这种情况下，必须借用别的通信手段，其中电通信是较好的选择之一。

要进行电通信，首先要把实际信源发出的非电信号，如声音、图像、文字等，转换成电信号，这个过程称为换能。换能的方法和技术是“检测与转换”研究的内容，我们这里研究的信源，都是经过换能之后的等效信源，即图1.1中信源的输出已经是电信号。

以离散传输系统为例，信源发出一个离散符号序列$\bar{u}=u_1u_2\cdots u_N$，该序列携带一定量的信息，这些信息分散在各个符号u_i之中。从信息传输的角度看，总是希望信息传输的效率尽量高，即希望以最小的代价（如最短的时间、最小的能量等）传递尽可能多的信息。假定传送一个符号所耗的时间是固定的，那就希望各个符号所携带的信息尽量多，理想情况下，希望各个符号携带的信息同样多，并达到最大。但实际信源未必如此。一般，信源发出的符号序列中，各符号携带的信息量相差很大，即信息分布不均匀，因此有必要对这个符号序列加以变换，使得变换之后的序列信息分布均匀化。这种变换称为信源编码，信源编码器的输出序列，其信息分布大致均匀，且接近最大。因此，编码之后的序列较“紧凑”，而编码之前的序列较“松散”（有信息的冗余），这种由“松散”变为“紧凑”的过程也称数据压缩。总之，信源编码的实质就是为了去掉信源中的信息冗余。

对于自然性质较好的离散信源，如本书中重点研究的离散无记忆信源，可以实现无失真编码。离散信源无失真编码的理论与方法，是第4章讨论的主题。

有些信源不可能做到无失真编码。例如，为了进行数字通信，需对模拟信源的输出进行采样，将其变为离散序列，这样量化误差就不可避免，即存在编码失真。允许一定失真的编码称为限失真编码，其理论将在第6章介绍。

信源译码是信源编码的逆过程，如果把信源编码视为变换或映射T_1，信源译码通常就是T_1的简单求逆，即T_1^{-1}，因此不必多加讨论。

3. 信道编码器与译码器

信道编码也可以看做是一种变换 T_2，主要作用是提高信息传送的可靠性。因为有噪声干扰，等效离散信道在传送某个信息位（或序列）时，总有出错的可能，比如，信道的输入为“0”，但在输出端收到的可能是“1”。为了减小这种传送出错的可能性，最简单的办法是将这个“0”重复传送多次，如重复传送 2 次，即先将“0”变成“000”，再送入信道传送。把“0”变成“000”是由信道编码器来完成的。“000”中的第一个“0”载荷信息，称为信息位；后两位是为提高传送可靠性而加入的，不载荷信息，称为（信息）冗余位。信道编码通常是在信息序列中有目的地加入冗余，从而使原序列变“长”，这与信源编码的做法刚好相反。

由于噪声干扰，传送“000”或“111”时某些位可能出错，信道可能的输出是“000，001，…，111”，要将其恢复成“0”或“1”，需要进行信道译码——变换 $\hat{T}_2^{-1}$。信道译码（变换 $\hat{T}_2^{-1}$）规则要根据信道的噪声特性而定，因此，$\hat{T}_2^{-1}$ 不是 T_2 的简单反变换，通常还不是一一变换，而是多一变换，问题比信源译码复杂得多，需专门讨论。

信道编码与译码的有关问题，将在第 5 章介绍。

1.3 信息论的发展历程

实践是科学的源泉，信息论作为一门科学，其形成、产生和发展也不例外。生产实践是人类物质和精神文明发展的基础，而物质与文明的进步又依赖于人类获取、传递、处理、加工和利用信息的能力。人类在生产过程中建立了人与人之间的关系，而要维护这种关系就必须要有信息，要进行通信。通信是人与人之间交流信息的手段。

信息论作为真正意义上的一门科学，是从 19 世纪中叶开始的。19 世纪中叶到 20 世纪 40 年代可以看做是信息论产生前的准备阶段。公认 1948 年香农发表的著名论文《通信的数学原理》标志着现代信息论的诞生，解决了通信传输中的一系列问题。现在，人们对信息论进行了更深入和广泛的研究，从原来的语法信息深入到语义信息和语用信息，即所谓广义信息论。

17 世纪到 19 世纪，由于牛顿力学的巨大影响，机械唯物论在科学领域中占有统治地位，机械唯物论者否认客观世界存在着偶然因素。但是正当绝大多数科学家都用牛顿力学的方式思考时，美国物理学家吉布斯（Gibbs • Josiah Willard）和奥地利物理学家波尔兹曼（Boltzmann • Ludwig）首先把统计学引入物理领域，使物理学对客观世界中存在的不确定性和偶然性不得不加以考虑。把研究偶然性作为一种科学方法引入物理学，这是吉布斯的一大功绩，也为信息论的诞生作出了贡献。这种探究方法为信息理论的创立提供了方法论的前提。波尔兹曼指出熵是关于一个物理系统分子运动状态的物理量，表示分子运动的混乱程度，并且把熵和信息联系起来，提出“熵是一个系统失去了的‘信息’的度量”。将偶然性、熵函数引入物理学为信息论的产生提供了理论前提。

在这一期间，人们对传输理论也进行了一定程度的研究。如，1832 年莫尔斯电报系统中高效率编码方法对后来香农的编码理论是有启发的，1885 年凯尔文（L • Kelvin）曾经研究过一条电缆的极限传信串问题。

到 20 世纪 20 年代，随着电话和电报等电子通信手段的发明和投入使用，人们对信息传输的要求越来越高，因此怎样提高通信系统传输信息的能力和传输的可靠性，怎样对各种形

式信息中所包含的信息进行定量的描述，就成为当时迫切需要解决的问题。

1922 年卡松（J.R.Carson）提出边带理论，指明信号在调制（编码）与传送过程中与频谱宽度的关系。1924 年奈奎斯特（H.Nyquist）也提出，电信号的传输速率与信道频带宽度之间存在着比例关系。哈特莱（R.V.Hartley）在 1922 年发表《信息传输》的文章，首先提出消息是代码、符号而不是信息内容本身，使信息与消息区分开来，在 1928 年提出把消息考虑为代码或单语的序列，并用消息可能数目的对数来度量消息中所含有的信息量。他的工作对后来香农的思想有很大的影响，为信息论的创立提供了思路。1936 年阿姆斯特朗（E.H.Armstrong）提出增加信号带宽可以使抑制噪声干扰的能力增强，并给出了调制指数大的调频方式，使调频实用化，出现了调频通信装置。1936 年达德利（H.Dudley）发明了声码器。当时他提出的概念是：通信所需要的带宽至少应与所传送的带宽相同。

到了 20 世纪 40 年代，随着雷达、无线电通信和电子计算机、自动控制相继出现和发展以及防空系统的需要，许多科学技术工作者对信息问题进行了大量的研究。

维纳在研究防空火炮的控制问题时，把随机过程和数理统计的观看引入通信和控制系统中来，揭示了信息传输和处理过程的本质。他从直流电流或者至少可看做直流电流的电路出发来研究信息论，独立于香农，将统计方法引入通信工程，奠定了信息论的理论基础。维纳把消息看做可测事件的时间序列，把通信看作统计问题，在数学上作为平稳随机过程及其变换来研究。他阐明了信息定量化的原则和方法，类似地用“熵”定义了连续信号的信息量，提出了度量信息量的香农—维纳公式：单位信息量就是对具有相等概念的二中择一的事物作单一选择时所传递出去的信息。维纳的这些开创性工作有力地推动了信息论的创立，并为信息论的应用开辟了广阔的前景。

1948 年香农发表了著名的论文《通信的数学理论》，1949 年他又发表了另一篇论文《在噪声中的通信》，在这两篇论文中，香农用概率测度和数理统计的方法系统地讨论了通信的基本问题，得出了几个重要而带有普遍意义的结论，这两篇论文奠定了现代信息论的基础。香农也被公认为现代信息论的创始人。

这一理论揭示了在通信系统中采用适当的编码后能够实现高效率和高可靠性信息传输，并得出了信源编码定理和信道编码定理；认为通信就是信息传输、是将消息由发信者送给收信者的过程，因而给出了一般通信系统的模型；用统计数字的方法，正确处理信息的形式和内容的辩证关系，解决了信息量问题，给出了信息量的数学公式。

信息论出现之后，在科学界引起了极大的震动。随后，许多科学家在这方面做了大量的工作，取得了一大批成果，使信息论（通信理论）发展成为一个相当成熟和完备的科学体系，为现代通信系统、现代网络传输和信息科学的发展提供了强有力的支撑。

数学家哥尔莫戈洛夫、范恩斯坦（A.Feinstein）、沃尔夫维兹（J.Woltwitz）等人将香农得到的数学结论作了进一步的严格论证和推广，使得这一理论有了更为坚实的数学基础。

1952 年费诺（R.M.Fano）给出并证明了费诺不等式，并给出了关于香农信道编码逆定理的证明。1957 年沃尔夫维兹采用了类似典型序列方法证明了信道编码强逆定理。1961 年费诺又描述了分组码中码率、码长和错误概率的关系，并提供了香农信道编码定理的充要性证明。1965 年格拉戈尔（R.G.Gallager）发展了费诺的证明结论并提供了一种简明的证明方法。1975 年科弗尔（T.M.Cover）采用典型序列方法证明了这一结论。1972 年阿莫托（S.Arimoto）和布莱哈特（R.Blahut）分别提出了信道容量的迭代算法。