

高等院校电气信息类规划教材

# 信息论与编码

张 莲 周登义 余成波 编著



中国铁道出版社  
CHINA RAILWAY PUBLISHING HOUSE

TN911.2/35

2008

高等院校电气信息类规划教材

# 信息论与编码

张 莲 周登义 余成波 编著

中国铁道出版社  
CHINA RAILWAY PUBLISHING HOUSE

## 内 容 提 要

本书是一本 21 世纪教学的有关信息论与编码的教材。全书共分 6 章,即绪论、信息的量度及离散信源、信源编码、离散信道及信道容量、信道编码以及信息工程中的数据保密。

本书重点介绍信息处理的理论基础、实现原理与方法。内容分为两大部分,即理论基础(前四章)和应用(后两章)。理论基础部分主要介绍信息的基本理论与基本概念,包括:信息熵、互信息、信息率失真函数、信道容量以及它们的性质与计算等。应用部分主要介绍信息与通信系统中的优化及其实现手段与方法,包括:信源编码定理、无失真的统计匹配编码、解除相关性的预测编码与变换编码、实用性的文字传真编码、语音编码与图像编码等提高系统有效性的信源编码、信道编码定理、分组码的基本理论与方法、卷积码的基本理论与方法等提高系统可靠性的信道编码以及信息工程中的数据保密等。

本书适合作为高等理工科院校电子信息工程、通信工程、信号与信息处理学科的本科生教材,也可供研究生、夜大、自学考试及成人教育等有关专业选用,还可供有关科技人员学习参考。

### 图书在版编目(CIP)数据

信息论与编码/张莲,周登义,余成波编著. —北京:

中国铁道出版社,2008.1

高等院校电气信息类规划教材

ISBN 978-7-113-08619-0

I. 信… II. ①张…②周…③余… 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. TN911.2

中国版本图书馆 CIP 数据核字(2008)第 006551 号

书 名: 信息论与编码

作 者: 张 莲 周登义 余成波

出版发行: 中国铁道出版社(100054,北京市宣武区右安门西街 8 号)

策划编辑: 严晓舟 秦绪好

责任编辑: 杨 勇 徐盼欣

封面设计: 付 巍

封面制作: 白 雪

印 刷: 中国铁道出版社印刷厂

开 本: 787mm×1092mm 印张: 16 字数: 375 千

版 本: 2008 年 4 月第 1 版 2008 年 4 月第 1 次印刷

印 数: 1~5 000 册

书 号: ISBN 978-7-113-08619-0/TP·2707

定 价: 26.00 元

版权所有 侵权必究

本书封面贴有中国铁道出版社激光防伪标签,无标签者不得销售

凡购买铁道版的图书,如有缺页、倒页、脱页者,请与本社计算机图书批销部调换。

《信息论与编码》是信息、通信、电子工程类专业的基础，对理论研究和工程应用均有重要的指导作用，它的应用领域非常广泛，几乎遍及各个工程技术学科。随着传统的物质型经济在全世界范围内大规模地向信息型经济转变，人们在思想上也不断地接受着信息化的洗礼。特别是进入 20 世纪 90 年代以来，全球信息化的浪潮一浪高过一浪，“信息高速公路”、“国家信息基础结构”，一个又一个崭新的概念，一个又一个全新的事物，接踵而至，纷至沓来，令人眼花缭乱，应接不暇。于是，广大信息类专业的本科生及科技人员迫切需要掌握信息论与编码的基本知识。

为了适应高等学校教学改革和教材改革的需求，依据我国当前电子信息工程、通信工程学科课程设置与教学改革的实际情况，对传统的“信息论基础”、“信息处理与编码”、“数字图像处理与压缩编码技术”课程的教学内容，经适当选择和裁剪组合，以信息与通信系统的优化为主线，力求简明、扼要、实用，编写了此本以介绍信息工程中基本理论、基本技术、基本方法为主的教材。

全书共分 6 章，即绪论、信息的量度及离散信源、信源编码、离散信道及信道容量、信道编码、信息工程中的数据保密。内容包括理论基础（前四章）和应用（后两章）两个方面。理论基础部分主要介绍信息的基本理论与基本概念，包括：信息熵、互信息、信息率失真函数、信道容量以及它们的性质与计算等。应用部分主要介绍信息与通信系统中的优化及其实现手段与方法，包括：信源编码定理、无失真的统计匹配编码、解除相关性的预测编码与变换编码、实用性的文字传真编码、语音编码与图像编码等提高系统有效性的信源编码、信道编码定理、分组码的基本理论与方法、卷积码的基本理论与方法等提高系统可靠性的信道编码以及信息工程中的数据保密等。

本书由重庆工学院张莲、周登义、余成波编著。其中，周登义编写了第 1~3 章，张莲编写了第 4~6 章，余成波对全书进行了统稿。秦华锋、谢东坡、李泉、胡柏栋、龚智、许超明等同志参加了部分章节的编写与排版工作。本书在编写过程中得到了重庆工学院有关领导的大力支持和帮助。许多兄弟院校的同行为本书的编写提出了许多宝贵意见并提供了帮助。在此，一并表示衷心的感谢。

本书适合作为高等理工科院校电子信息工程、通信工程、信号与信息处理学科的本科生教材，也可供研究生、夜大、自学考试及成人教育有关专业选用，还可供有关科技人员学习参考。

鉴于我们的水平有限，书中难免有疏漏和不足之处，望广大同行与读者给予批评指正。

编 者

2008 年 1 月

|                            |    |
|----------------------------|----|
| 第 1 章 绪论 .....             | 1  |
| 1.1 信息的概念 .....            | 1  |
| 1.1.1 信息的定义、特征与性质 .....    | 1  |
| 1.1.2 信息的分类 .....          | 3  |
| 1.1.3 信息、消息和信号的区别与联系 ..... | 4  |
| 1.2 信息传输系统的组成及各部分的功能 ..... | 4  |
| 1.2.1 模拟信息传输系统 .....       | 4  |
| 1.2.2 数字信息传输系统 .....       | 5  |
| 1.3 信息论研究的对象和内容 .....      | 7  |
| 1.4 信息论发展的历史和趋势 .....      | 9  |
| 第 2 章 信息的量度及离散信源 .....     | 13 |
| 2.1 自信息量和条件自信息量 .....      | 13 |
| 2.1.1 自信息量 .....           | 13 |
| 2.1.2 条件自信息量 .....         | 16 |
| 2.2 互信息量和条件互信息量 .....      | 17 |
| 2.2.1 互信息量 .....           | 17 |
| 2.2.2 互信息量的性质 .....        | 18 |
| 2.2.3 条件互信息量 .....         | 19 |
| 2.3 离散信源的信息量 .....         | 19 |
| 2.3.1 信源的数学模型 .....        | 19 |
| 2.3.2 信源的分类 .....          | 20 |
| 2.3.3 平均信息量 .....          | 22 |
| 2.4 熵的基本性质 .....           | 33 |
| 2.5 消息序列的熵 .....           | 38 |
| 2.5.1 离散无记忆信源 .....        | 38 |
| 2.5.2 离散无记忆的扩展信源 .....     | 39 |
| 2.5.3 离散平稳信源 .....         | 42 |
| 2.5.4 马尔可夫信源 .....         | 46 |
| 2.6 信源的相关性和剩余度 .....       | 50 |
| 习题 .....                   | 53 |

|                           |     |
|---------------------------|-----|
| 第3章 信源编码 .....            | 57  |
| 3.1 无失真信源编码 .....         | 57  |
| 3.1.1 编码器 .....           | 57  |
| 3.1.2 分组码 .....           | 59  |
| 3.1.3 等长码和等长编码定理 .....    | 61  |
| 3.1.4 变长码和变长编码定理 .....    | 68  |
| 3.1.5 变长码的编码方法 .....      | 75  |
| 3.2 限失真信源编码 .....         | 85  |
| 3.2.1 失真测度 .....          | 86  |
| 3.2.2 信息率失真函数 .....       | 88  |
| 3.2.3 离散信源的信息率失真函数 .....  | 91  |
| 3.2.4 限失真信源编码定理 .....     | 98  |
| 3.2.5 连续信源的信息率失真函数 .....  | 100 |
| 3.3 常用信源编码 .....          | 102 |
| 3.3.1 矢量量化编码 .....        | 102 |
| 3.3.2 预测编码 .....          | 108 |
| 3.3.3 变换编码 .....          | 113 |
| 3.3.4 传真编码 .....          | 117 |
| 3.3.5 语音压缩编码 .....        | 121 |
| 3.3.6 图像编码 .....          | 126 |
| 习题 .....                  | 131 |
| 第4章 离散信道及信道容量 .....       | 133 |
| 4.1 信道分类与描述 .....         | 133 |
| 4.1.1 信道的分类 .....         | 133 |
| 4.1.2 信道的描述 .....         | 135 |
| 4.2 离散无记忆信道 .....         | 136 |
| 4.2.1 离散信道的数学模型 .....     | 136 |
| 4.2.2 单符号离散信道 .....       | 137 |
| 4.3 信道传输的平均互信息 .....      | 139 |
| 4.3.1 信道疑义度 .....         | 139 |
| 4.3.2 平均互信息 .....         | 140 |
| 4.4 平均互信息的特性 .....        | 140 |
| 4.5 信道容量的概念及其计算方法 .....   | 145 |
| 4.5.1 信道容量的定义 .....       | 145 |
| 4.5.2 几种典型离散信道的信道容量 ..... | 146 |
| 4.5.3 对称离散信道的信道容量 .....   | 147 |
| 4.5.4 一般离散信道的信道容量 .....   | 151 |

|                               |     |
|-------------------------------|-----|
| 4.5.5 离散无记忆的扩展信道及其信道容量 .....  | 154 |
| 4.5.6 串联信道和并联信道及其信道容量 .....   | 160 |
| 4.6 信源与信道的匹配 .....            | 165 |
| 习题 .....                      | 166 |
| <b>第 5 章 信道编码</b> .....       | 168 |
| 5.1 信道编码的基本概念 .....           | 168 |
| 5.1.1 信道编码在数字通信系统的地位和作用 ..... | 168 |
| 5.1.2 信道编码的基本思想和分类 .....      | 169 |
| 5.1.3 差错控制的基本方式 .....         | 172 |
| 5.1.4 信道编码基本数学知识 .....        | 174 |
| 5.2 有噪信道编码 .....              | 175 |
| 5.2.1 噪声信道的编码问题 .....         | 175 |
| 5.2.2 错误概率与编码方法 .....         | 180 |
| 5.2.3 有噪信道编码定理 .....          | 186 |
| 5.3 线性分组码 .....               | 191 |
| 5.3.1 分组码的性质 .....            | 191 |
| 5.3.2 生成矩阵与奇偶校验矩阵 .....       | 192 |
| 5.3.3 几种典型的分组码 .....          | 194 |
| 5.4 卷积码 .....                 | 204 |
| 5.4.1 卷积码的编码 .....            | 204 |
| 5.4.2 卷积码的译码 .....            | 210 |
| 5.5 纠正突发错误码 .....             | 214 |
| 5.5.1 突发差错与纠突发差错的基本概念 .....   | 214 |
| 5.5.2 法尔码 .....               | 215 |
| 5.6 交织码 .....                 | 218 |
| 习题 .....                      | 222 |
| <b>第 6 章 信息工程中的数据保密</b> ..... | 224 |
| 6.1 信息保密通信的模型 .....           | 224 |
| 6.2 传统密码体制 .....              | 225 |
| 6.2.1 单表代换密码 .....            | 225 |
| 6.2.2 多表代换密码 .....            | 227 |
| 6.2.3 多字母代换 .....             | 231 |
| 6.2.4 转置密码 .....              | 232 |
| 6.3 分组(块)密码 .....             | 234 |
| 6.3.1 分组加密的基本概念 .....         | 234 |
| 6.3.2 数据加密标准(DES) .....       | 236 |
| 6.4 公钥密码体制 .....              | 243 |

|                       |     |
|-----------------------|-----|
| 6.4.1 公钥密钥的一般原理 ..... | 243 |
| 6.4.2 RSA 体制 .....    | 244 |
| 习题 .....              | 245 |
| 参考文献 .....            | 247 |

# 第 1 章 绪 论

## 本章主要内容

- 信息的概念
- 信息传输系统的组成及各部分的功能
- 信息论研究的对象和内容
- 信息论发展的历史和趋势

众所周知,客观世界有三大基本要素:物质、能量和信息。在生产和生活中,人们对于物质和能量早有认识,两者早已成为自然科学的研究对象,并分别形成了专门的学科,如物理学、化学、天文学、地学、生物学等。20 世纪 40 年代末,人们终于认识到信息的客观存在,并建立了研究信息的学科——信息论。信息论是人们在长期通信工程的实践中,由通信技术与概率论、随机过程和数理统计等相结合而逐步发展起来的一门新兴交叉学科,是应用近代数理统计方法研究信息的传输、存储与处理的学科。随着信息科学的崛起,使以物质和能量二者为中心的传统自然科学观念让位于以信息、物质和能量三者为中心的现代科学观,使力量型的科学成为智慧与力量相结合的科学,使以解放人类体力劳动为目标的传统科学转变为以解放体力和智力劳动为目标的现代科学。总之,信息科学的兴起极大地改变了整个科学结构、内容和方向,改变了科学发展的前景和科学的思维方式。随着信息概念的不断深化,它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,在许多领域中日益受到科学工作者的重视。

本章首先引出信息的概念,进而讨论信息传输系统基本模型,给出信息论研究的主要对象、目的和内容,最后简述信息论学科发展的历史、现状和未来方向。

## 1.1 信息的概念

### 1.1.1 信息的定义、特征与性质

信息是信息论中最基本、最重要的概念,是一个既复杂又抽象的概念。生活在信息时代,信息对每个人都有着特殊重要的意义。那么何谓信息呢?

科学来源于实践。科学上许多术语往往来自日常生活,信息这个术语同样如此,它是在人类社会互通情报的实践中产生的。在日常生活中,信息是指“消息”、“情况”、“知识”、“情报”,等等。例如,当人们收到一封电报、接到一个电话,或从收音机里听到了天气预报,或看了电视里的新闻之后,人们就获得了“信息”。但到底获得了多少信息呢?对于这个问题,有时仅仅有一些模糊的概念而无法确切地回答。例如,当打电话的对方告诉的消息是早就知道的,就觉得这个电话没有什么意义,或者说没有带来什么信息;相反,

如果电话中传来的消息不但是原来所不知道的，而且是完全出乎意料的，就会觉得这个电话印象很深，给了很多信息。又如，甲乙两人同去听某一学者讲课，由于两人的业务基础不同，他们听到的虽然是同一内容，但听后所得到的新知识，或者说所得到的有用的信息往往是不一样的。科学上所说的信息正是从这个原始的、含糊不清的概念中加以概括、提炼、提高和开拓而得到的，它有严格、确切的含义，有一定的数学模式，并能定量地量度。

在日常生活中，收到一封电报、接到一个电话或听到天气预报后，所得到的具体内容是对某一事物状态的描述。例如，天气预报说“晴间多云”，这是对天气状态的具体描述。电报上的报文“母病愈”，这是对母亲身体健康情况的具体描述。这些都是人脑以外的客观物质世界表现出来的各种不同的运动状态。而电话中说“他想去上海”，这是存在于他头脑里的思维活动，反映了人的主观世界——大脑物质的思维运动所表现出来的思维状态。

在信息社会中，“信息”这个名词应用十分广泛（如报纸上和电视节目中的经济信息、商品信息、人才交流信息等），但由于信息科学比起其他学科，如物理学、化学、天文学、地学、生物学等还显得很年轻，人类对信息的认识还很不够，迄今为止，信息还没有形成一个完整的、确切的定义。不同的研究学派对信息的本质及其定义还没有形成统一的意见和认识。综合信息的各种定义，比较一致的定义是：信息是认识主体（人、生物、机器）所感受的或所表达的事物运动的状态和运动状态变化的方式。可以这样认为：

（1）信息是普遍存在的。它存在于自然界，存在于人类社会，也存在于思维领域。哪里有事物，哪里就有事物运动的状态和方式。

（2）信息与物质是既有联系又有区别的两个概念。物质是信息的载体，物质的运动是信息的源泉，但信息只是事物运动的状态和方式，不是事物的本身。信息与物质不能等同。

（3）信息与能量也是既有联系又有区别的两个概念。传递信息需要能量，驾驭能量则需要信息；然而，信息是事物运动的状态和方式，能量是物体做功的本领，两者之间有质的区别。

（4）既然信息是事物运动的状态和方式，那么人类要认识事物就必须取得信息，同样，要变革事物也必须要信息。

综上所述，信息作为客观世界存在的第三要素，具有以下特征：

（1）信息来源于物质，又不是物质本身；它从物质的运动中产生出来，又可以脱离源物质而相对独立地存在。

（2）信息也来源于精神世界，但又限于精神领域。

（3）信息与能量息息相关，但又与能量有本质的区别。

（4）信息具有知识的本性，但又比知识的内涵更广泛。

（5）信息是具体的，并且可以被（生物、机器等）所感知、提取、识别，可以被传递、存储、变换、处理、显示、检索和利用。

（6）信息可以被众多用户所共享。

（7）语法信息在传递和处理过程中永不增值；并且在封闭系统中，语法信息的最大可能值不变。

（8）信息是能使认识主体对某一事物的未知性或不确定性有所减少的有用的知识。

(9) 接收者在收到信息之前,对其内容是不知道的,所以信息是新知识、新内容。

(10) 信息可以产生,也可以消失,同时信息可以被携带、存储及处理。

(11) 信息是可以量度的,信息量有多、少的差别。

根据以上特征和信息的定义,可以得到信息的一些重要的性质。

(1) 普遍性:信息是普遍存在的。

(2) 无限性:在整个宇宙时空中,信息是无限的;即使是在有限的空间(时间有限或无限)中,信息也是无限的。

(3) 相对性:对于同一个事物,不同的观察者所能获得的信息量可能不同。

(4) 转换性:信息可以在时间上或空间中从一点转移到另一点。

(5) 变换性:信息是可变的,可以由不同的载体和不同的方法来载荷。

(6) 有序性:信息可以用来消除系统的不定性,增加系统的有序性。

(7) 动态性:信息具有动态性质,一切活的信息都随时间而变化。因此,信息也是有时效、有“寿命”的。

(8) 转化性:从潜在的意义上讲,信息是可以转化的。它在一定的条件下,可以转化为物质、能量、时间及其他。

(9) 共享性:即信息是可以共享的,信息的交流不会使交流者失去原有的信息,而且还可以获得新的信息。

(10) 可量度性:信息的数量与质量是可量度的,即信息量。

### 1.1.2 信息的分类

由前面可知,信息是一个十分复杂的研究对象。要找到一种通用的方法来恰如其分地描述各种各样的信息,即使不是不可能,至少也是很困难的。就算能够找到一种方法可以用来描述一切可能的信息,这种方法也必然是非常笼统、非常一般化,不可能具体细致地描述各种不同类型的信息。为了具体地描述信息,通常将信息进行分类,这样就可以分门别类地进行描述,也可以分门别类地建立描述方法。

同其他事物的分类一样,信息分类也有许多不同的原则和方法。

(1) 从信息的性质来分类,可以分为:语法信息、语义信息和语用信息。

(2) 从观察的过程来分类,可以分为:实在信息、先验信息和实得信息。

(3) 从信息的地位来分类,可以分为:客观信息(包括观察对象的初始信息,经过观察者干预之后的效果信息、环境信息等)和主观信息(包括决策信息、指令信息、控制信息、目标信息等)。

(4) 从信息的作用来分类,可以分为:有用信息、无用信息和干扰信息。

(5) 从信息的逻辑意义来分类,可以分为:真实信息、虚假信息 and 不定信息。

(6) 从信息的传递方向来分类,可以分为:前馈信息和反馈信息。

(7) 从信息的生成领域来分类,可以分为:宇宙信息、自然信息、社会信息和思维信息等。

(8) 从信息的应用部门来分类,可以分为:工业信息、农业信息、军事信息、政治信息、科技信息、文化信息、经济信息、市场信息和管理信息等。

(9) 从信息源的性质来分类,可以分为:语声信息、图像信息、文字信息、数据信息

和计算信息等。

(10) 从信息的载体性质来分类, 可以分为: 电子信息、光学信息和生物信息等。

(11) 从携带信息的信号形式来分类, 可以分为: 连续信息、离散信息和半连续信息(混合信息)等。

总之, 针对不同的信息, 找到不同的具体描述方法, 建立相应的度量方法, 这样才能最有效地把握信息。

### 1.1.3 信息、消息和信号的区别与联系

信息是认识主体所感受的或所表达的事物运动的状态和运动状态变化的方式, 是事物运动状态或存在方式的不确定性的描述。

把客观物质运动和主观思维活动的状态用文字、符号、数据、语言、图片等能够被人们感觉器官所感知的形式表达出来, 就构成了消息。从通信的观点出发, 构成消息的各种物理现象要具有两个条件: 一是能为通信双方所理解, 二是可以传递。因此, 从电报、电话或电视中得到的是一些具体的消息, 是描述主、客观各种事物运动状态的消息。而电报、电话、电视等则都是这些消息的传递系统。可以这样讲, 消息是信息的载荷者, 是描述信息的一种表现形式(如语言、文字等), 同一种信息可用不同的消息来载荷(如某一事件, 既可用语言来表达, 也可用文字来描述), 即是对某个事物的描述和反映, 是表示事物内涵的一种形式。信息包含在消息之中, 是通信系统中传送的对象。

把消息变换成适合信道传输的物理量, 这种物理量称为信号(如电信号、光信号、声信号和生物信号等)。目的是迅速有效地传送和交换信息。信号是一个物理量, 可测量、可描述、可显示, 它携带着消息, 是消息的运载工具。信号是承载信息的实体, 信号仅仅是外壳, 信息则是内核。目前, 在信息传输中主要使用的信号是电信号、光信号和无线电信号。

## 1.2 信息传输系统的组成及各部分的功能

信息论研究的主要问题是, 在通信系统设计中如何实现信息传输、存储和处理的有效性和可靠性。通常可以将通信系统称为信息传输系统, 例如电报、电话、图像、计算机和导航等系统。完成信息传输功能的所有技术设备总称为信息传输系统或通信系统。按照信道中传输的是模拟信号还是数字信号, 可将信息传输系统分为模拟信息传输系统与数字信息传输系统。下面概括性地就它们的组成及各部分的功能分别进行介绍。

### 1.2.1 模拟信息传输系统

模拟信息传输系统传输的是模拟信号, 这种模拟信号在任意时刻的取值是任意的, 它是时间的连续函数。任何消息传输系统(电报、电话、传真、电视、雷达、视觉神经等)都有一个发出消息的发送端(一般称为信源)和接收消息的接收端(一般称为收信者或信宿)以及连接两者的通道(一般称为信道), 其基本模型如图 1-1 所示。发送端输出信号送至信道(即信号传输媒介), 再传输给接收端。

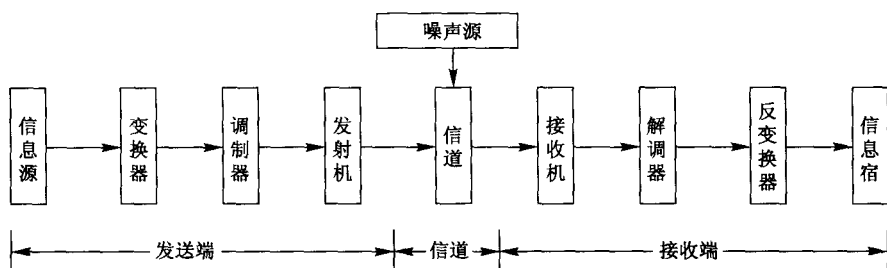


图 1-1 模拟信息传输系统的一般模型

发送端由信息源、变换器、调制器和发射机构成。信息源（简称信源）产生含有信息的信息，是被传输的对象。它可以是输出信息的人或机器设备，如打电话，说话人就是信息源，语音就是消息。像语音一样，大多数消息都是非电量，不宜于在信道中进行远距离传输，为此需要将它们变换成电信号。这种变换由变换器（亦称传感器）完成，变换关系应为单值函数，否则，在接收端就无法恢复成原消息。调制器的作用是将一种信号变换成另一种宜于在给定的信道上传输的信号。具体地说，就是利用调制器将频率较低的电信号调制（载荷）到频率更高的载波信号上，然后加到发射机。模拟信号的调制方式通常有：调幅（AM）、单边带调制（SSB）、调频（FM）、调相（PM）等。发射机主要包括倍频器（或变频器）和功率放大器，其作用是使已调载波信号的频率和功率达到实际应用所要求的数值。

信道是指消息的信号从发射端传到接收端的媒介或通道（即传递信息的通道）。它是包括收发设备在内的物理设施。按传输媒介的不同，可将信道分为有线信道和无线信道。在狭义的通信领域中，常用的有线信道有架空明线、同轴电缆、波导、光纤等；无线信道有无线电波及激光传播空间等。

接收端由接收机、解调器、反变换器和信息宿组成，用来完成与发送端相反的变换过程和作用。其中，接收机是一个低电平部件，主要包括低噪声高频放大器、混频器和中频放大器。它将信道传输来的微弱信号（一般为微伏量级）放大到解调器所需强度的信号（一般为伏的量级），并最大限度地降低信道噪声的影响。从信息传输的角度来看，接收机可用一个带通滤波器来等效，也不会影响问题讨论的实质。在讨论时，常假定该带通滤波器具有理想归一化的传输函数特性，即带宽内的传输函数等于1，带宽外的传输函数为零。解调器的功能与调制器相反，即从已调制的高频载波信号中解调出被传输的低频信息信号，再经反变换器将该信息信号恢复成原消息，并送至信息宿（简称信宿，是指信息传送的目的地，即原消息的归宿或接收者）。

噪声源是实际传输系统中客观存在的干扰源，有内部噪声和外部干扰两方面。为了研究这种影响，都折合成一个加到信道上的噪声源，并且认为是一种高斯白噪声。

### 1.2.2 数字信息传输系统

数字信息传输系统即数字通信系统的一般模型，如图 1-2 所示，同样也是由发送端、信道和接收端三大部分组成，但在信道中传输的是数字信号。该信号只能取有限个离散值，而且出现的时间也是离散的。与模拟信息传输系统相比可知，该系统除在发送端增加了两个编码器及在接收端相应地增加两个译码器之外，其余部分的组成和功能与模拟信息传输

系统基本相同。对于数字信号其调制方式通常有：幅度键控（ASK）、频移键控（FSK）、相移键控（PSK）以及一些新的数字调制方式（如参差正交相移键控（SQPSK）、连续相位频移键控（CPSK）及最小键控（MSK）等）。

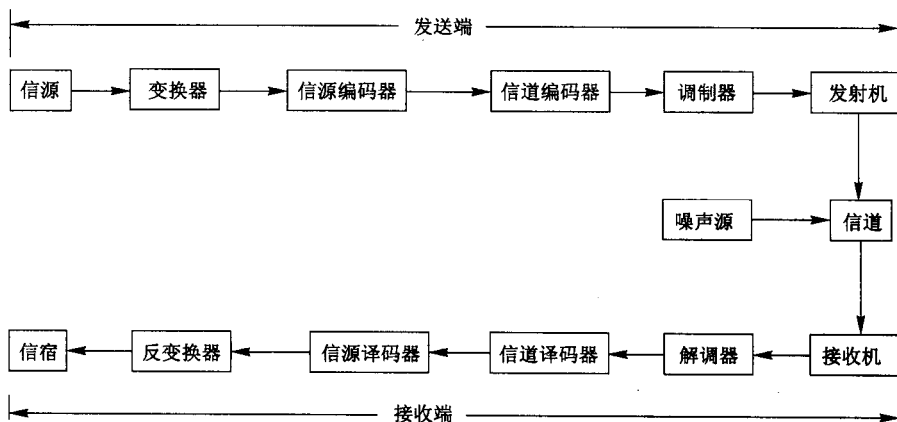


图 1-2 数字信息传输系统的一般模型

当变换器输出的信息信号是模拟信号时，信源编码器将其变换成数字信号，以便在数字信息传输系统中传输。因此，信源编码器又称为模/数（A/D）变换器或脉冲编码器。信源译码器的作用是将数字信号变换成模拟信号，故又被称为数/模（D/A）变换器或脉冲译码器。信道编码器、译码器的作用在于提高传输系统的抗干扰能力（这将在后面章节详细介绍）。

与模拟信息传输系统相比，数字信息传输系统的主要优点是：

- （1）抗干扰能力强，特别是在中继传输时更为明显。
- （2）可以进行差错控制，因而提高了信息传输的可靠性。
- （3）便于使用现代计算机技术，对信号进行处理、存储和变换，从而提高了信息传输的灵活性。

（4）便于加密，实现保密信息传输。

（5）易于与其他系统配合使用，构成一个灵活、通用、多功能的综合业务信息传输网。

（6）易于集成化和大规模生产，其性能一致性好，且成本低。

其主要缺点是：

（1）占用信道频带较宽。

（2）要有一个复杂的同步系统。

需要提醒的是：一个信息传输系统是模拟式的还是数字式的，不取决于被传输的信息信号，而是决定于信道中传输的载波信号是模拟的还是数字的。

通信系统的根本目的是传输消息。但消息传递过程的一个最基本、最普通却又不十分引人注意的特点是：收信者在收到消息以前是不知道消息的具体内容的。消息的传递过程对收信者来说是一个从不知到知的过程，或者说是一个从不确定到确定的过程。如果没有这样一个特点，那就根本不需要通信系统了。试想，如果收信者在收到

电报或电话之前就已经知道报文的内容或电话的内容，那还要电报系统、电话系统干什么呢？

由于消息是对客观和主观的各种事物运动状态的具体描述，所以从通信过程来看，收信者的所谓“不知”就是不知道发送端将发送描述何种运动状态的消息。例如发电报，报文“母病愈”是母亲身体健康状态的一种描述，而母亲身体健康情况会表现出不同的状态。可见收信者在看到报文以前存在一种“不确定性”，他不能确定母亲身体健康状态如何。一旦看到报文后，只要报文是清楚的，在传递过程中没有差错，那么原来的“不确定性”就没有了，他就获得了信息。所以，通信过程是一种从不确定到确定的过程，即是消除不确定性的过程。不确定性消除了，收信者也就获得了信息。

这里就有一个定量地测度信息的问题。为此需要对信息进行定量描述，此部分内容将在第2章进行研究。

### 1.3 信息论研究的对象和内容

与其他科学一样，信息论也是从生产实践中总结出来的，反过来又服务于实践。从前面关于信息概念的讨论中可知：信息论的研究对象是消息传输系统。由于消息中包含着信息，所以消息传输系统也是信息传输系统，简称通信系统。人们通过消息的传输和处理过程来研究信息传输和处理过程中的共同规律。

信息论最初是在狭义的通信系统基础上总结提高而发展起来的，但理论一旦从实践中抽象出来，它的意义就远远超越了原来的范围。这里所谈的通信系统是广义的，不只是指电报、电话等一类狭义的通信系统，而是指所有的信息流通系统。如生物有机体的遗传系统、神经系统等，甚至人类社会的管理系统都属于广义的通信系统。

研究一个概括性很强的通信系统，其目的就是要找到信息传输过程的共同规律。一旦总结出这种共同规律，就可以用来指导具体通信系统的设计，使设计出来的各种通信系统具有更高的可靠性和有效性。

所谓可靠性高，就是要使信源发出的消息经过信道传输以后，尽可能不失真地再现在接收端。而所谓有效性高，就是经济效果好，即用尽可能短的时间和尽可能少的设备来传送一定数量的信息。两者的结合就能使系统达到最优化。

提高可靠性和提高有效性常常会发生矛盾，这就需要统筹兼顾。例如，为了兼顾有效性（考虑经济效果），有时就不一定要求绝对准确地接收端再现原来的消息，而是可以允许一定的误差或一定的失真，或者说允许近似地再现原来的消息。

香农（C. E. Shannon）在1948年发表文章的序言中提出：“通信的基本问题是要在某一端准确地或近似地再现从另一端选择出来的消息。”这句话恰如其分地表达了信息论研究的目的是提高通信系统的可靠性和有效性。

关于信息论研究的具体内容，是一个有争议的问题。有人认为信息论只是概率论的一个分支，这是某些数学家的观点。当然，这种看法是有一定根据的，因为香农信息论确实为概率论开拓了一个新的分支。但如果把信息论限制在数学范围内，这就太狭隘了。也有人认为信息论只是熵的理论，这是某些物理学家的观点。他们对“熵”特别感兴趣，熵的概念确实是香农信息论的基本概念之一，但信息论的全部内容要比

熵的概念广泛得多。

归纳起来,信息论研究的内容大致包括以下几个方面。

(1) 通信的统计理论的研究

主要研究利用统计数学工具分析信息和信息传输的统计规律,其具体内容有:①信息的度量;②信息速率与熵;③信道传输能力——信道容量。

(2) 信源的统计特性

主要包括:①文字(如汉字)、字母(如英文)统计特性;②语声的参数分析和统计特性;③图片及活动图像(如电视)的统计特性;④其他信源的统计特性。

(3) 收信者接收器官的研究

主要包括:①人的听觉和视觉器官的特性;②人的大脑感受和记忆能力的模拟。这些问题的研究与生物学、生理学、心理学的研究密切相关。

(4) 编码理论与技术的研究

主要包括:①有效性编码,用来提高信息传输效率,主要针对信源的统计特性进行编码,所以有时也称为信源编码;②抗干扰编码,用来提高信息传输的可靠性,主要针对信道统计特性进行编码,所以也称为信道编码。

(5) 提高信息传输效率的研究

主要包括:①功率的节约;②频带的压缩;③传输时间的缩短,即快速传输问题。

(6) 抗干扰理论与技术的研究

主要包括:①各种调制制度的抗干扰性;②理想接收机的实践。

(7) 噪声中信号检测理论与技术的研究

主要包括:①信号检测的最佳准则;②信号最佳检测的实践。

由上面的讨论可以看出,信息论的研究内容极为广泛,是一门新兴的边缘学科,是当代信息科学基本而重要的理论基础。综上所述,信息论的研究范畴可以概括为以下三个方面的内容:

(1) 信息论基础(狭义信息论)。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。即为香农基本理论。

(2) 一般信息论。主要研究通信的一般理论,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、调制理论以及信息处理理论等。后一部分以美国科学家维纳(N. Wiener)为代表,其中最贡献的是维纳和苏联数学家柯尔莫哥洛夫(A. KOJIMOpOB)。

虽然维纳和香农等人都是运用概率和统计数学的方法来研究准确地或近似地再现消息的问题,都是为了使消息传送和接收最优化,但他们之间却有一个重要的区别。维纳研究的重点是在接收端。研究一个信号(消息)如果在传输过程中被某些因素(如噪声、非线性失真等)所干扰时,在接收端怎样把它恢复、再现,从干扰中提取出来。在此基础上,创立了最佳线性过滤理论(维纳滤波器)、统计检测与估计理论、噪声理论等。而香农研究的对象则是从信源到信宿之间的全过程,是收、发端联合最优的问题。其重点是放在编码。他指出,只要在传输前后对消息进行适当的编码,就能保证在干扰的存在下,最佳地传送和准确或近似地再现消息。为此发展了信息测度理论、信道容量理论和编码理论等。

(3) 广义信息论。广义信息论不仅包括上述两个方面的内容,而且包括所有与信息有

关的领域,如心理学、遗传学、神经生理学、语言学、语义学,甚至于包括社会学中有关信息的问题。

本书主要介绍狭义信息论和一般信息论的内容,把其他所有与信息有关的领域都看成是信息论的应用。

综上所述,信息论是一门应用概率论、随机过程、数理统计和近代代数的方法,来研究广义的信息传输、提取和处理系统中一般规律的工程科学;它的主要目的是提高信息系统的可靠性和有效性以便达到系统的最优化;它的主要内容(或分支)包括香农理论、编码理论、维纳理论、检测和估计理论、信号设计和处理理论、调制理论和随机噪声理论等。

由于信息论研究的内容极为广泛,而各分支又有一定的相对独立性,因此本书仅论述信息论的基础理论。

## 1.4 信息论发展的历史和趋势

信息论是信息科学的主要理论基础之一,它是在长期通信工程实践和理论基础之上发展起来的。信息论从诞生到今天,已有170多年历史,现已成为一门独立的理论科学。回顾其发展历史,可以知道理论是如何从实践中经过抽象、概括、提高而逐步形成的。在现代科学技术高度发展过程中,学习和掌握信息论日益成为一种必要。

我们知道,通信系统是人类社会的神经系统,日常生活、工农业生产、科学实践以及战争等,一切都离不开信息传递和流动,即使在原始社会也存在着最简单的通信工具和通信系统,这方面社会实践是悠久漫长的,对人类社会的发展有着十分重要的作用。

电的通信系统(电信系统)已有170多年的历史了。在其发展过程中,一个很有意义的历史事实是:当物理学中的电磁理论以及后来的电子学的电子学理论一旦有某些进展,很快就会促进电信系统的创造发明或改进。例如,当法拉第于1820~1830年期间发现电磁感应的基本规律后,不久莫尔斯就建立起电报系统(1823~1835年),1876年,贝尔又发明了电话系统。1864年麦克斯韦预言了电磁波的存在,1888年赫兹用实验证明了这一预言,接着,1895年英国的马可尼和俄国的波波夫就发明了无线电通信。20世纪初(1907年),根据电子运动的规律,福雷斯特发明了能把电磁波进行放大的电子管,之后很快出现了远距离无线电通信系统。大功率超高频电子管发明以后,电视系统就建立起来了(1925~1927年)。电子在电磁场运动过程中能量相互交换的规律被人们认识后,就出现了微波电子管(最初是磁控管,后来是速调管、行波管),接着,在20世纪30年代末和40年代初的二次世界大战初期,微波通信系统、微波雷达系统等迅速发展起来;50年代后期发明了量子放大器。60年代初发明的激光技术,使人类进入了光纤通信的时代。

信息论是在长期通信工程实践和理论研究的基础上发展起来的,其形成和发展的历史可以追溯到19世纪30年代。

1832年莫尔电报系统中高效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)对调幅信号的频谱结构进行了研究,并建立了信号频谱概念。1924年奈奎斯特(H. Nyquist)解释了信号带宽和信息率之间的关系。他指出,如果以一个确定的速率来传输电报信号,就需要一定的带宽。他将信息率与带宽联系起来了。