

普通高等教育“十三五”规划教材·电子信息与电气工程类专业规划教材

# 信息论 经典与现代

Information Theory  
Classical and Modern

刘宴涛 王雪冰 秦娜◎编著

 中国工信出版集团

 电子工业出版社  
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY  
<http://www.phei.com.cn>



普通高等教育“十三五”规划教材·电子信息与电气工程类专业规划教材

# 信息论 经典与现代

Information Theory Classical and Modern

刘宴涛 王雪冰 秦 娜◎编著

电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

## 内 容 简 介

本书主要包括两部分内容：经典香农信息论和现代网络信息论。经典香农信息论主要讨论信息的度量、表示和传输等问题，包括熵、信道容量、信源编码和信道编码等概念和理论，这部分内容分布在本书的前 11 章。第 12、13 章介绍现代网络信息论，主要讨论信息在网络中的有效传输问题，包括网络编码和网络容量域，这部分内容是近十几年来信息论研究的新课题。

本书内容自成体系，读者只需要具备高等数学、线性代数和概率论的数学基础即可，本书所使用的其他数学工具，如有限域、信息不等式等，均以附录的形式提供给读者，因此极大地提高了读者的学习效率。本书可作为高等学校电子信息工程、通信工程及相关专业的本科生、研究生教材，也可供工程技术人员参考使用。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。  
版权所有，侵权必究。

### 图书在版编目 (CIP) 数据

信息论：经典与现代/刘宴涛，王雪冰，秦娜编著. —北京：电子工业出版社，2019.8  
普通高等教育“十三五”规划教材. 电子信息与电气工程类专业规划教材  
ISBN 978-7-121-36110-4

I. ①信… II. ①刘… ②王… ③秦… III. ①信息论 IV. ①G201

中国版本图书馆 CIP 数据核字 (2019) 第 041346 号

责任编辑：李 敏 特约编辑：刘 炯 毛俊权 肖 姝

印 刷：北京七彩京通数码快印有限公司

装 订：北京七彩京通数码快印有限公司

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：787×1 092 1/16 印张：19.25 字数：517 千字

版 次：2019 年 8 月第 1 版

印 次：2019 年 8 月第 1 次印刷

定 价：88.00 元

凡所购买电子工业出版社图书有缺损问题，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, 88258888。

质量投诉请发邮件至 [zlt@phei.com.cn](mailto:zlt@phei.com.cn)，盗版侵权举报请发邮件至 [dbqq@phei.com.cn](mailto:dbqq@phei.com.cn)。

本书咨询联系方式：[limin@phei.com.cn](mailto:limin@phei.com.cn) 或 (010) 88254753。

# 前 言

## 一、“信息论”的课程特点

“信息论”是通信工程、电子信息工程等相关专业的专业基础课，其重要性可以跟“信号与系统”“通信原理”等课程相比。但是，从课程特点上看，信息论比这些课程更抽象，在“信号与系统”“通信原理”等课程中涉及的概念或技术往往非常具体，例如，波形和频谱都是可观测的，采样、量化、调制、解调等技术也都很直观、具象；从数学工具上看，微积分、线性代数和概率论中比较简单的数学运算对于学习和理解这些课程已经足够。然而，在“信息论”中的概念往往非常抽象。例如，至今尚无法给出信息完美的或公理化的定义，熵和互信息等都是看不见、摸不着的抽象的量。此外，渐近等分割性等定理的证明需要用到概率极限理论，信道编码和网络编码又需要具备有限域等近世代数的数学基础，这些都是本科生学得比较差，甚至没有学习过的内容，这对有效地学习“信息论”构成了巨大障碍。

尽管抽象难懂，但“信息论”对于信息技术相关学科专业知识体系的构建是至关重要的。“信息论”是信息科学的奠基石，熵和信道容量等概念从认识论的层面帮助我们透过现象看本质，揭示了信息的根本特征和通信的关键问题，信源编码和信道编码则从方法论的层面帮助我们提高通信的有效性和可靠性，直接服务于工程应用。因此，学习信息论，了解其基本概念和理论，建立信息论的思维和视角对于通信工程和电子信息工程等专业的学生和从业者是非常必要的。

## 二、本书的目的

本书的目的之一是为读者展示和解释经典香农（Shannon）信息理论，搭建一座扶梯，帮助读者克服概念抽象、定理晦涩、推导烦琐等困难，在不破坏科学性和严谨性的前提下，用朴素的语言阐释“信息论”相关定理和定义背后的含义，以及在哪里和如何应用这套理论，把信息论与工程应用联系起来。

本书的目的之二是打开一扇门，引导读者走进网络信息论这个较新的研究领域。网络信息论研究的是信息在网络中传输、处理、存储、控制和利用的规律。虽然有很多著作把 20 世纪 70 年代至 2000 年之前研究的多用户信息理论也称为网络信息论，但作者认为，真正意义上的网络信息论的诞生应该是以 2000 年提出的网络编码技术为标志和开端的。这段时间研究的网络通信问题在网络拓扑、传输机制和分析方法等方面更能体现网络信息论的内涵，因此，如果把多用户信息理论称为初等网络信息论的话，2000 年之后的网络信息论则可称为现代网络信息论。由于现代网络信息论从诞生至今还不到 20 年的时间，

其理论体系的成熟度远不如经典香农信息理论，因此本书旨在起导引而非综述的作用，点到为止地介绍网络编码的基本概念及网络容量域分析等问题，还有很多课题，如网络传输的安全性<sup>[24,37]</sup>、网络存储编码<sup>[42]</sup>、网络纠错码<sup>[31]</sup>、网络层析和拓扑推断<sup>[43]</sup>、网络卷积码等，没有包括进来。

### 三、本书的主要内容

本书共 13 章，第 1 章为绪论，第 2~11 章为经典信息论部分，第 12 章和第 13 章为现代网络信息论部分，对各章具体内容概括如下。

第 1 章为绪论，介绍信息论的发展简史、信息论的研究对象和研究内容、信息的概念等。

第 2 章讨论离散随机变量及其相关的离散熵、联合熵、条件熵、平均互信息、熵率等概念，还介绍了马尔可夫信源。

第 3 章介绍信源编码、等长码和变长码等概念，以及渐近等分割性定理，并基于该定理引出香农第一定理，还介绍了 4 种离散信源编码方法。

第 4 章讨论离散信道和信道容量，介绍离散信道的数学模型和平均互信息的两种凸性，以及信道容量的概念和计算。

第 5 章介绍有噪信道编码理论，包括译码规则的概念、译码规则和译码错误概率的关系、降低译码错误概率的可行思路、联合渐近等分割性和香农第二定理等。

第 6 章介绍波形信源和波形信道，包括随机过程基础、连续信源的微分熵的定义和性质、最大熵分布、连续信道和波形信道。最后，作为波形信道的重要实例，分析了高斯信道的信道容量，并引出著名的香农公式。

第 7 章介绍率失真理论，这也是香农信息论体系的重要组成部分，具体包括失真度、失真矩阵、试验信道、率失真函数的定义、性质和计算，以及香农第三定理。

第 8 章介绍最经典的信道编码方法——线性分组码，包括线性分组码的定义、生成矩阵和校验矩阵。国内很多教材在介绍这部分内容的时候，大多以汉明码或别的实例为切入点，把生成矩阵和校验矩阵直接提供给读者，让读者明白线性分组码的编译码过程，但这种编排方式不利于读者理解生成矩阵和校验矩阵的由来，无法抓住线性分组码的本质特征。本章紧密围绕生成矩阵和校验矩阵的正交性展开，标准阵译码、伴随式译码、译码错误概率等问题都立足于这个正交性。根据多年的教学经验，笔者认为这种编排方式有利于帮助读者透过现象看本质，深刻理解线性分组码的内涵。

第 9 章介绍线性分组码的一个子类——循环码，包括循环码的定义、多项式表示、应用除法求余电路搭建系统循环码的编译码电路，以及 Meggit 译码器的工作原理等。

第 10 章介绍卷积码，包括：卷积码与分组码的区别，卷积码的电路图表示、多项式表示、状态图表示、网格图表示，著名的 Viterbi（维特比）译码方法。

第 11 章介绍多用户信息理论，包括相关信源编码、具有边信息的信源编码、多址接入信道、广播信道和中继信道的容量域。这部分内容可以看作初等网络信息论，其中的概念（如容量域）有助于理解第 13 章关于网络容量域的问题。

第 12 章介绍网络编码的概念、思想，以及相对传统路由传输体制的优缺点，并介绍了几种网络编码方法。

第 13 章介绍网络容量域的概念和分析方法。网络容量域可以类比于信道容量，但两者的数学模型、分析方法和问题复杂度都大相径庭。本章还介绍了几种具体的分析路由容量域和编码容量域或容量限的方法。

需要说明的是，在经典香农信息论的理论体系中还包括保密通信理论。香农在 1949 年发表的 *Communication Theory of Secrecy Systems*<sup>[19]</sup>中建立了保密通信的信息论框架，为保密通信理论和密码学的发展奠定了理论基础，但后来密码学和通信系统安全逐渐发展为一门独立的学科，其研究内容和研究方法越来越自成体系，而且已经有大量专门介绍密码学的著作存在，所以本书没有把密码学理论包括进来。

除上面 13 章内容外，为了帮助读者掌握本书使用的数学工具，本书还补充了 4 个附录。

附录 A 介绍了近世代数的基础知识，包括集合、代数系统、群、环、域等概念，重点讨论了有限域的运算规则，以及扩域、扩域元素的多项式表示、幂表示和向量表示等。有限域是编码学的数学基础，不学习有限域虽然也能理解线性分组码的编译码过程，以及循环码和卷积码的多项式表示（这也正是国内大部分现行教材的编排方式），但这种理解流于表面，不够深刻，当进一步学习如有限几何码、网络编码等编码方法时就会遭遇实质性的困难，因此学习有限域对透彻地理解信息论和编码学是非常必要的。

附录 B 介绍了向量空间和矩阵的基础知识。这部分内容在线性代数中学习过。介绍这部分内容是为了帮助读者理解线性分组码生成矩阵和校验矩阵的正交性。

附录 C 介绍了博弈论中矩形博弈的相关概念，包括博弈值、鞍点、Nash 均衡等。这部分内容主要用于第 13 章网络容量域分析。博弈论最初诞生于经济学领域，但近年来逐渐和其他学科交叉融合。博弈论的方法可以帮助解决通信中资源的优化配置和某些性能极限等问题，了解一些博弈论的基础内容有助于拓展工科学生的视野。

附录 D 介绍了信息不等式。这部分内容是近代信息论的重点研究课题，完全可以作为一章独立存在，但其中的概念，如熵空间、可熵化、熵区域、香农不等式、基本不等式和元不等式，对于本科生而言抽象程度较高、难度较大，因此以附录的形式提供给读者，可以作为选学内容。另外，这部分内容有助于理解和分析网络的编码容量域。

为了巩固每章的学习内容，本书为各章提供了一些习题，而且在习题答案中为绝大部分习题提供了详细的求解过程。这一方面补充、丰富了各章的例题，另一方面极大地帮助读者理解学习内容，掌握解题方法。

本书第 1~6 章及附录 B、附录 C 由王雪冰（中国石油大学胜利学院）完成，第 7~10 章由秦娜（北京理工大学珠海学院）完成，第 11~13 章及附录 A、附录 D 由刘宴涛（北京理工大学珠海学院）完成，全书由刘宴涛统稿。

#### 四、本书的使用方法

本书的章节安排和学习顺序如下图所示。



由于各院校开设“信息论”课程的学时不同，所以学习内容也应该有所取舍。以 68 个学时为例，可以学习全部 13 章和 4 个附录的内容（本科生附录 D 从简）。对于 51 个学时的课程安排而言，可以免去第 13 章和附录 C、附录 D，对于附录 A，只需要了解  $GF(p)$ ，尤其是  $GF(2)$  上的四则运算规则和多项式运算规则即可，可免去对扩域的学习；对于第 12 章，简要介绍网络编码的基本思想即可。如果学时很紧张（如 34 个学时），则可以考虑免去第 7 章、第 11 章、第 12 章、第 13 章和全部附录，剩下的学习内容也可以帮助读者了解“信息论”课程的基本概念，建立信息论思维。

考虑到国内很多著作对国外科学家名字的音译不同，如 Shannon 被译成山农、仙农、香农等，这很容易造成读者的混淆，因此本书所涉及国外科学家的名字，除香农、马尔可夫外，大部分使用原名。

### 五、致谢

任何一本著作都不可能凭空产生，本书在编写过程中参阅了许多信息论方面的教材和专著，包括傅祖芸<sup>[2,3]</sup>、朱雪龙<sup>[4]</sup>、吴伟陵<sup>[5]</sup>、Cover<sup>[6]</sup>、Yeung<sup>[7]</sup>、田宝玉<sup>[8,9]</sup>、陈运<sup>[10]</sup>、冯桂<sup>[11]</sup>、曹雪虹<sup>[12]</sup>、王新梅<sup>[13]</sup>、冯克勤<sup>[15]</sup>等诸位老师的著作，这些著作作为本书提供了宝贵的素材和思想源泉。此外，作者还阅读了大量的 IEEE、ACM、IET、Elsevier、Springer 等数据库的期刊和会议论文，这些学术成果不仅开阔了作者的眼界，促进了作者的科研工作，而且极大地助力了本书的完成。本书把这些引用源列于书后的参考文献中，在此谨向引用源的作者致以最诚挚的敬意和感谢！

其次，我要向我的恩师，北京理工大学的安建平老师和杨杰老师致以最诚挚的谢意！是恩师把我引入学术和科研的道路上来，为我打开了信息论的大门，我的科研工作和包括本书在内的科研成果都和恩师的指导密不可分。我还要感谢北京理工大学的刘珩老师，当年在一起的学习和科研岁月，以及博士毕业后的多次科研合作极大地帮助了我研究能力和科学水平的提升，在此深表感谢！

本书的成书、出版受到国家自然科学基金面上项目（No. 61471045）和辽宁省自然科学基金面上项目（No. 20170540008）的资助，在此一并致谢！

最后，限于编著者的水平，书中可能会有疏漏甚至错误之处，敬请读者批评指正。

刘宴涛

2019 年 5 月

# 目 录

第 1 章 绪论	1
1.1 从通信谈起	1
1.2 模拟通信与数字通信	2
1.3 信息论的诞生——香农 1948 年发表的论文	3
1.4 什么是信息	4
1.5 信息论的研究内容	5
习题	7
第 2 章 离散信源和离散熵	8
2.1 信源的数学模型及分类	8
2.2 离散熵	9
2.3 离散熵的性质	12
2.4 二维信源的联合熵和条件熵	13
2.5 平均互信息	15
2.5.1 两个随机变量的平均互信息	15
2.5.2 多个随机变量的平均互信息	17
2.6 离散平稳信源的熵率	18
2.7 马尔可夫信源	21
2.7.1 马尔可夫链	21
2.7.2 马尔可夫信源概述	23
2.8 本章小结	25
习题	25
第 3 章 离散无失真信源编码	28
3.1 信源编码的基本概念	28
3.1.1 信源编码的两种策略	28
3.1.2 信源编码的分类	29
3.2 渐近等分割性定理	30
3.3 等长信源编码	33

3.4	变长信源编码	35
3.5	离散信源编码方法	39
3.5.1	Huffman 编码	39
3.5.2	Fano 编码	42
3.5.3	香农编码	43
3.5.4	算术编码	44
3.6	本章小结	46
	习题	46
<b>第 4 章</b>	<b>离散信道和信道容量</b>	<b>48</b>
4.1	信道的分类和数学模型	48
4.1.1	信道的分类	48
4.1.2	信道的数学模型	49
4.2	平均互信息的凸性	50
4.3	信道容量	52
4.3.1	一般离散信道的信道容量	55
4.3.2	对称信道的信道容量	60
4.4	多符号信道和并联信道	62
4.5	串联信道和数据处理定理	64
4.6	本章小结	65
	习题	66
<b>第 5 章</b>	<b>有噪信道编码</b>	<b>69</b>
5.1	单符号离散信道的译码规则	69
5.2	如何降低译码错误概率	73
5.3	译码错误概率和信息传输率的折中	76
5.4	信道编码	80
5.5	联合渐近等分割性定理和香农第二定理	82
5.6	信源信道分离编码	88
5.7	本章小结	89
	习题	90
<b>第 6 章</b>	<b>波形信源和波形信道</b>	<b>92</b>
6.1	随机过程基础	92
6.1.1	信号的分类	92
6.1.2	随机过程	93
6.1.3	随机波形信源	96

6.2	连续型随机变量的微分熵	96
6.2.1	连续型随机变量	96
6.2.2	微分熵	99
6.2.3	微分熵的性质	102
6.2.4	最大熵分布	103
6.3	连续信道和波形信道	104
6.3.1	连续信道和波形信道的分类	104
6.3.2	连续加性信道的转移概率密度函数	104
6.3.3	连续信道和波形信道的信道容量	106
6.4	高斯信道	106
6.4.1	高斯信道与离散信道	107
6.4.2	高斯信道的信道容量	109
6.4.3	限带 AWGN 信道的信道容量	111
6.5	香农公式	112
6.5.1	增加信道容量的两种方法	112
6.5.2	$E_b/N_0$ 和香农限	112
6.6	本章小结	114
	习题	115
<b>第 7 章</b>	<b>率失真理论</b>	<b>116</b>
7.1	量化失真	117
7.2	失真度与率失真函数	117
7.3	率失真函数的定义域	121
7.4	率失真函数的性质	125
7.5	率失真函数的计算	126
7.5.1	离散信源率失真函数的计算	126
7.5.2	连续信源率失真函数的计算	132
7.6	保真度准则下的信源编码定理	136
7.7	本章小结	136
	习题	137
<b>第 8 章</b>	<b>线性分组码</b>	<b>139</b>
8.1	线性分组码的一般理论	140
8.1.1	基本概念	140
8.1.2	$G$ 矩阵和 $H$ 矩阵	141
8.1.3	伴随式	144

8.1.4	检错和纠错	144
8.1.5	标准阵译码和伴随式译码	147
8.1.6	线性分组码的几何解释和检错、纠错能力	149
8.2	汉明码 (Hamming Code)	150
8.3	本章小结	152
	习题	153
<b>第 9 章</b>	<b>循环码</b>	<b>155</b>
9.1	基本概念	155
9.2	循环码的多项式表示法	155
9.3	循环码的 $G$ 矩阵和 $H$ 矩阵	159
9.4	系统循环码	160
9.5	循环码的编码	161
9.6	循环码的译码	162
9.6.1	梅吉特译码	163
9.6.2	捕错译码	165
9.6.3	大数逻辑译码	166
9.7	本章小结	167
	习题	167
<b>第 10 章</b>	<b>卷积码</b>	<b>168</b>
10.1	一般概念	168
10.2	卷积码的多项式表示	173
10.3	卷积码的状态图表示	174
10.4	卷积码的网格图表示	175
10.5	维特比译码	176
10.6	本章小结	178
	习题	179
<b>第 11 章</b>	<b>多用户信息论</b>	<b>180</b>
11.1	相关信源编码	180
11.2	具有边信息的信源编码	183
11.3	多址接入信道	183
11.4	广播信道	186
11.5	中继信道	187
11.6	本章小结	188
	习题	189

第 12 章 现代网络信息论 .....	190
12.1 网络编码基本思想 .....	191
12.2 网络编码的概念 .....	193
12.3 线性网络编码 .....	195
12.3.1 确定网络编码 .....	195
12.3.2 随机网络编码 .....	199
12.4 本章小结 .....	200
习题 .....	201
第 13 章 网络容量域 .....	202
13.1 网络流 .....	202
13.2 网络容量域 .....	203
13.3 均匀分数网络 .....	205
13.4 路由容量域 .....	206
13.4.1 多重单播路由网络容量域 .....	207
13.4.2 一重组播路由网络容量域 .....	210
13.4.3 二重混合路由网络容量域 .....	218
13.5 编码容量域 .....	221
13.5.1 编码容量域的理论解 .....	221
13.5.2 编码容量域的割集限 .....	223
13.6 本章小结 .....	226
习题 .....	226
附录 A 有限域 .....	227
A.1 集合 .....	227
A.1.1 集合的定义 .....	227
A.1.2 集合的运算 .....	228
A.1.3 映射 .....	230
A.1.4 代数系统 .....	231
A.2 群 .....	231
A.2.1 群的定义 .....	231
A.2.2 陪集和拉格朗日定理 .....	233
A.3 环 .....	233
A.3.1 环的定义 .....	233
A.3.2 整环 .....	235
A.3.3 多项式环 .....	236

A.4 域	237
A.4.1 域的定义	237
A.4.2 扩域	240
A.4.3 GF(2)	244
A.5 小结	246
附录 B 向量空间	247
附录 C 矩形博弈	249
附录 D 信息不等式	253
D.1 从集合论视角看待信息量	253
D.2 熵空间和原子空间	257
D.3 信息不等式	261
D.4 元形式香农信息度量	263
D.5 $\Gamma_2^*$ 和 $\phi_2^*$	266
D.6 $\Gamma_3^*$	267
习题答案	269
参考文献	295

## 绪 论

### 1.1 从通信谈起

自然界每时每刻都在进行各种各样的通信活动,蜜蜂以跳舞的方式通知同伴蜜源的方向,蝙蝠、海豚和鲸鱼以声呐的方式进行定位、测距、辨别障碍物,以及发现食物和危险,绝大多数兽类和禽类的种群采用的更为普遍的通信方式则通过叫声。人是高级动物,伴随着人类不断地征服自然、改造自然的活动中,人类发明了飞鸽传书、烽火示警、驿马传信、旗语、灯语等传递信息的方式,人类还创造了语言、文字,发明了造纸术和印刷术,极大地提高了通信的有效性、准确性和可靠性,使得大量的信息存储和大范围的信息流通成为可能。然而,在电通信方式出现之前,人类的通信活动依然是低效率、近距离的,无论是烽火示警,还是飞鸽传书,信息传递的时效性都是很低的。

狭义的现代通信方式是指近 200 年发展起来的电通信,即通过电磁波承载和传输信息的方式。电通信是伴随着电磁学理论和电子学理论的发展而发展起来的。1820—1830 年, Oersted 发现了电流的磁效应, Faraday 找到了电磁感应规律。1837 年, Morse 发明了电报,并于 1844 年在华盛顿和巴尔的摩之间成功实现了长途电报传输,虽然在 Morse 之前也有若干发明家致力于静电电报的研究,但 Morse 实现了电报技术的实用化。1876 年, Bell 发明了电话系统,开启了人类社会的话音通信时代。1855—1864 年, Maxwell 以 3 篇论文《论法拉第的力线》《论物理的力线》和《电磁场的动力学理论》建立了电磁场理论,他在 1865 年预言了电磁波的存在,并推导出电磁波的传播速度等于光速。1888 年,德国物理学家 Hertz 用实验验证了电磁波的存在;1899 年,意大利人 Marconi 完成了无线电通信实验,并在 1900 年让无线电信号穿过了英吉利海峡,从此人类社会进入无线通信时代。19 世纪的电通信主要解决的问题集中在如何把信息转换成电形式并把它们进行远距离传输,这个时期的技术发展缺乏理论支撑。进入 20 世纪后,电通信则从理论和技术两个层面向前推进。

一方面,电信技术和电信设备制造取得了突飞猛进的发展。1904 年,英国物理学家 Fleming 发明了真空电子二极管。1907 年, Forest 通过在二极管里加入栅极发明了能把电磁波进行放大的真空电子三极管,这不仅极大地推动了电台、雷达和收音机的技术进步,而且为计算机的诞生奠定了基础。在 20 世纪 20 年代大功率超高频电子管出现后,电视系统就建立起来了。紧接着,在第二次世界大战期间,微波通信和雷达系统被广泛使用。1937 年,英国人 Reeves 提出了脉冲编码调制 (PCM) 的概念,为数字通信的发展奠定了基础。1946 年,第一台计算机 ENIAC 在宾夕法尼亚大学诞生,把人类社会带入了智能时代。20 世纪 60 年代,伴随着激光和光纤技术的突破,光纤通信使人类社会驶入了通信的快车道。

20 世纪后半段到现在,伴随着集成电路突飞猛进的发展,计算机与通信技术、网络技术日趋融合,人类社会已经进入网络通信时代。

另一方面,伴随着通信技术的发展,许多理论问题逐渐被提出和解决。1924 年, Nyquist 在 *Certain Factors Affecting Telegraph Speed* 这篇文章中证明信号的传输速率和信道带宽成正比,该工作在 1928 年得到发展,提出了限带信号的采样定理。1928 年, Hartley 在 *The Transmission of Information* 一文中提出把消息看成等概的序列,并把消息数的对数定义为信息量,这是历史上首次对信息进行度量,但 Hartley 的工作没有考虑信源的统计特性,所以这种对信息的度量是有缺陷的。1936 年, Armstrang 在 *A Method of Reducing Disturbances in Radio Signaling by A System of Frequency Modulation* 一文中指出,可以用信号带宽换取信噪比增益。总之 20 世纪前 40 年,通信系统的设计目标是對抗信号失真,采用的分析方法是 Fourier 理论,信息等同于消息,被看作确定的过程或信号。20 世纪 40 年代之后,伴随着通信体制由模拟向数字的转变,通信系统的设计目标从對抗信号失真逐渐转变为對抗噪声和干扰,分析方法也从确定性分析转变为统计分析。这样一来,通信工程就和统计科学紧密结合起来了,信息的传递和恢复变成了  $n$  中选 1 的消息的选择、传递和判决。因此,需要发展一个关于信息量的统计理论,信息论正是在这样的背景下诞生的。下面通过比较模拟通信和数字通信来进一步阐释通信工程的统计特色。

## 1.2 模拟通信与数字通信

信息论及与之紧密相关的编码技术是在通信技术由模拟通信向数字通信转变的过程中诞生的。其实,最早的 Morse 电报系统就是一种数字通信系统,该系统采用持续时间不同的点、横线和空格为英文字母进行编码,并以电流脉冲的形式在电线中传输。但电报出现不久,采用模拟通信方式的电话系统为人们提供了更方便的话音通信,并逐步取代了电报系统成为主流通信方式。模拟通信以电话和广播为代表,模拟通信系统在概念和系统构成上很简单,其核心器件是调制解调器和放大器,系统设计的主要要求是线性性,即信宿收到的波形  $y(t)$  应该是信源发送波形  $x(t)$  的线性函数,即  $y(t) = kx(t)$ ,否则在信宿就会产生失真。然而,这种简单的系统设计要求在实现上却非常困难,由于放大器的线性范围有限,信号在传输过程中不可避免地会受到噪声干扰,再加上信源发送波形的不可预测性,在设计模拟通信系统时很难实现完美的线性性。

与模拟通信系统形成鲜明对比的是,数字通信系统在概念和系统构成上非常复杂,如图 1-1 所示,收发双方包括很多功能模块。尽管如此,数字通信系统的设计和实现却容易得多,系统性能也远远优于模拟通信。首先,数字通信系统在有限的时间间隔内发送有限波形集中的一个波形,而模拟通信系统则从无限个波形中选择一个进行发送。其次,与模拟通信系统不同,数字通信系统接收端的任务不是精确地再现被传输的波形,而是根据受到噪声干扰的接收信号判决发送端发送的是哪一个波形,因此,数字通信系统更关心判决差错概率,而不是信号波形的失真度,这极大地降低了对系统线性性的要求。再次,对于中继接力通信,模拟通信无法在中间节点纠正波形失真,因此具有失真累加效应;而在数

字通信系统中,中继节点只要能正确判决出上一级发送的是哪个波形,就可以重生该波形向下一级传送,因此消除了失真累加。最后,数字通信可以使用编码技术,如密码、纠错码,这极大地提高了通信的安全性和可靠性。

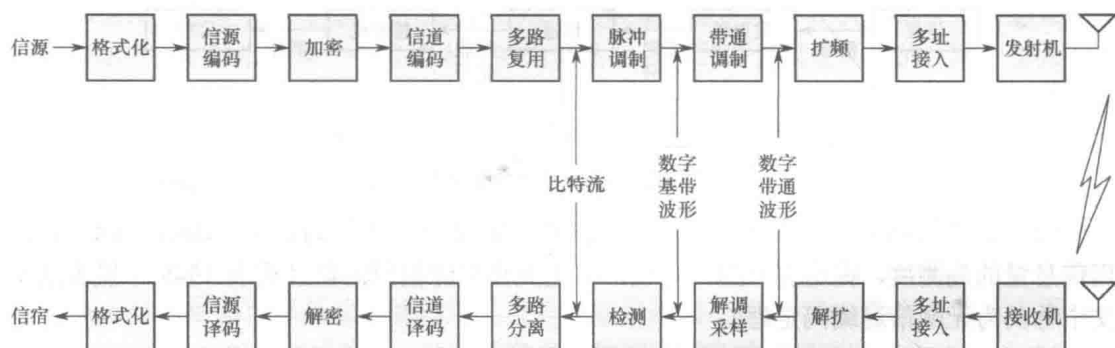


图 1-1 数字通信系统框架<sup>[44]</sup>

分析比较模拟通信和数字通信的技术特点可以发现,包括发送端、信道和接收端的数字通信系统呈现明显的统计特点。这就要求通信界研究者和工程师们既要对通信设备制造业做出重大的变革和更新换代,又要在理论层面,如信息的表示、传输、检测、估计、采样、量化和编译码等,建立一套能够反映通信系统统计特点的理论体系。信息论就诞生在这样的背景下。

### 1.3 信息论的诞生——香农 1948 年发表的论文

进入 20 世纪 40 年代后,随着人们越来越从统计科学的视角看待通信工程,以及越来越应用概率统计、随机过程的方法建模和分析通信问题,人们需要建立一套关于信息量的统计理论。然而,还有一些理论和概念问题亟待解决,包括:

- (1) 信息的本质是什么?
- (2) 对信息如何进行度量?
- (3) 信道的传输性能极限是什么?

在 Nyquist、Hartley 和 Reeves 等人工作的基础上,1948 年 7 月和 10 月,美国 Bell 实验室的香农在 *Bell System Technical Journal* 上分两次连载了一篇论文 *A Mathematical Theory of Communication*<sup>[18]</sup>。该文系统地解决了上述 3 个问题,搭建了信息理论框架,标志着信息论的诞生。1949 年,该文被伊利诺伊大学出版社汇编成书,为了突出香农的贡献,该书被改名为 *The Mathematical Theory of Communication*。以下通过回顾这篇论文,一方面了解香农的工作和贡献,另一方面理解信息论的研究内容和理论框架。这篇论文的内容可以简要概括如下。

(1) 建立了统一的香农通信系统框架,如图 1-2 所示。其中,信源发出的消息可以是像自然语言字母序列这样的离散信源,也可以是话音、图像、视频等形式的连续信源;发射机的作用是把信源发出的消息转变为适合信道传输的信号,例如,电报发射机把英文字

母编码为“.”“-”和空格组成的序列，电话发射机则把声压成比例地转换成电流，PCM系统则包括采样、量化、编码等操作；信道包括各种形式的物理信道；接收机执行发射机的逆操作；信宿是指接收消息的人或物。



图 1-2 香农通信系统框架

(2) 把离散信源建模为马尔可夫随机过程，定义信息为不确定性 (Uncertainty)，提出信息量的熵测度，提出香农第一定理，即无失真信源编码定理 (香农 1948 年发表的论文中称其为无噪信道编码定理)。

(3) 对于离散有噪信道，指出信息传输率  $R$  等于信源的熵减去信道疑义度，即

$$R=H(X)-H(X|Y)$$

定义信道容量等于  $\max(R)$ ，并提出香农第二定理，即有噪信道编码定理。

(4) 对于连续信源，提出微分熵的定义。

(5) 对于连续信道，给出峰值功率受限和平均功率受限两种情况的信道容量计算公式，后者即著名的香农 (Shannon) 公式。

(6) 提出信源保真度 (Fidelity) 的概念，香农 1959 年发表的论文 *Coding Theorems for A Discrete Source with A Fidelity Criterion*<sup>[20]</sup>对保真度进行了更系统的研究，建立了率失真理论，并提出了香农第三定理，即保真度准则下的信源编码定理。

香农于 1948 年发表的论文基本涵盖了信息论的全部内容，香农三大定理构建了信息论的理论框架，因此香农被称为信息论的奠基人。香农 1948 年发表的论文掀起了人们对信息论的研究热潮，包括香农本人在内的众多研究者一方面不断完善香农理论体系，另一方面在包括信源编码、信道编码、率失真理论和多用户信息理论等方面不断开拓，取得了一个又一个理论成果，提出了多种信源压缩编码和信道纠错编码方案，从而构建了较完备的信息论大厦。

## 1.4 什么是信息

信息的含义可以从广义和狭义两个范畴来理解，前者不限于通信领域。广义上，信息是与物质和能量并列的基本概念，是物质世界的三大支柱。1948 年 Wiener 在其著作 *Cybernetics or Control and Communication in the Animal and the Machine* 中指出，“信息就是信息，既不是物质，也不是能量。”美国学者 Oettinger 说：“没有物质什么都不存在，没有能量什么都不发生，没有信息什么都没有意义。”然而，信息并不像物质和能量那样具象，信息是物质的一种属性，需要依附于事物而存在，但信息可以被复制和存储，还可以在事物之间传递和交换。我国学者钟义信教授把信息定义为关于事物运动的、千差万别的状态和方式的知识。基于该定义，可以把信息分成 3 个层次：语法信息、语义信息和语用