应用信息与编码理论

主　编　包建荣
副主编　姜　斌　孙闽红　唐向宏

ZHEJIANG UNIVERSITY PRESS
浙江大学出版社

序　言

信息论是整个信息科学的基石，它利用概率论、随机过程和数理统计等数学方法来研究信息存储、度量、编码、传输、处理中的一般规律。自香农(C. E. Shannon)1948 年发表奠定信息论理论基础的“通信的数学理论”一文以来，信息理论有了较大发展，并已延伸到众多领域。由此，人们也逐渐认识到，在科技高度发展的现代信息社会中，学习和掌握信息理论日益成为相关专业人员的重要需求。

本教材系统地介绍了香农信息论的基本内容及其编码应用，即信息度量、容量以及信源信道编码理论等问题。全书共分七章。第一章介绍信息基本概念，信息论研究对象、目的和内容，及其起源和发展。第二章介绍信源度量，给出了信源的概念及其性质。第三章介绍信道模型和分类、信道平均互信息、信道容量概念及其计算。第四章介绍信息率失真理论，侧重讨论了离散无记忆信源，包括信源失真测度、信息率失真函数及其计算、限失真信源编码定理等。第五章介绍了信源输出信息的有效表示，即离散信源无失真编码。具体包括离散无记忆信源等长、变长编码定理、离散平稳信源编码定理及典型变长编码方法。第六章介绍有噪信道编码，包括译码规则、编码方法等对信息在信道传输的影响，及在有噪信道下实现可靠传输的有噪信道编码定理。第七章简介现代信息论的最新发展，如网络信息论的基本结论及信道分类、相关信源编码和多源接入信道等内容。通过上述七章内容，希望能为读者提供较全面和系统的信息论与编码基础知识。

全书注重应用信息及编码理论的基本概念、理论和分析方法进行阐述，力求物理意义清晰，数学结构简洁、完整，并结合具体实例给出较详尽的数学推导和证明。在内容编排上，力求由浅入深、循序渐进，以易接受的方式系统地介绍信息论及编码的基本内容及其应用系统。为了提高读者分析和解决信息论与编码问题的能力，除第一章和第七章外，其余各章均附有适量习题，可根据实际需要选用。

本教材主要由包建荣、姜斌、唐向宏、孙闽红等四位教师合作编写。姜斌撰写第三章信道模型及概念等，且负责整理大部分习题；孙闽红撰写第二章信源编码；唐向宏撰写第一章

绪论。其余部分由包建荣编撰完成。此外，聂建园、孙启超等多名研究生参与了文字校对、习题核对等工作，在此一并表示诚挚的感谢。

本书得到了杭州电子科技大学省重点学科“电路与系统”及杭州电子科技大学信息工程学院一流学科B建设“杭电信工学院电子科学与技术专业”的资助，特此感谢。此外，本书最后章节的通信信号处理模型方法应用等部分内容的编撰，还得到了浙江省自然科学基金（编号：LZ14F010003）、国家自然科学基金（编号：61471152）、东南大学移动通信国家重点实验室开放研究基金（编号：2014D02）、浙江省公益性技术应用研究计划项目（编号：2015C31103）、浙江省2016年度高等教育教学改革项目（编号：jg20160237）等课题的资助。

感谢国内外信息论与编码理论界的知名学者香农、格拉格、傅祖芸、朱雪龙、周荫清、仇佩亮等专家和教授们。编者之所以能编写此书，得益于对他们著作的学习和理解。

感谢浙江大学出版社樊晓燕编审，正是她的辛勤劳动，使得本书得以顺利出版发行。

由于编者水平有限，书中难免还存在一些缺点和错误，希望广大读者批评指正。

作　者

2017年9月

目　录

第 1 章

绪　论

信息论(Information Theory)是人们在长期的通信工程实践中,将通信电子技术与矩阵理论和线性代数、概率论、随机过程和数理统计等基础学科相结合,而逐步发展起来的一门新兴交叉学科。1948 年,香农(C. E. Shannon)发表了著名的论文《通信的数学理论》("A Mathematical Theory of Communication"),首次用概率测度和数理统计等方法系统研究了通信的本质问题,给出了信息的度量表示,得出了具有普遍意义的重要结论,由此奠定了信息论的理论基础,为信息的表达、传输、存储和处理等过程提供了坚实的理论依据。近几十年来,随着信息概念的不断深化和信息论的迅猛发展,信息论所涉及的内容也早已超出了狭义通信工程的范畴,它已逐渐渗透到许多学科,如属于经济学科的证券分析等,也日益得到众多领域工作者的重视。

本章首先简要阐述信息的基本概念,进而较深入地探讨信息论所研究的主要对象、目的和内容,最后简述信息论的形成和发展。

1.1　信息的基本概念

1.1.1　信息、消息及信号

在日常生活中,人们常错误地将信息混淆为消息,认为得到了消息,就得到了信息。如当人们收到一封邮件、接到一个电话、收看了电视节目等,就说得到了"信息"。确实,人们根据这些消息可获得各种信息,信息与消息联系密切。但信息与消息并非等同。以下根据通信的过程和实质来阐述信息与消息的联系,从而给出信息的基本定义。

通信系统被用来传输各类消息,而这些被传输的消息有不同形式,如文字、数字、语言、音符、图像等。所有这些不同形式的消息都能被人们感知,即人们通过通信,在接收到消息后,可得到所描述的某事物状态的具体内容。如听气象广播,气象预报为"晴",这就是对某地的气象状态的具体描述。又如,电视转播足球赛,人们从电视图像中看到足球赛的进展,而电视活动图像则是对足球赛运动状态的描述。可见,语言、图像等消息都是对客观物质世界的各种不同运动或存在状态的表述。此外,消息也可表述人类的思维活动。如朋友给你

打电话说“我想去旅游”，你就得知了朋友的想法。此时，该语言消息反映了人的主观思维运动所表现的思维状态。

定义 1.1 用文字、符号、数据、语言、图像等能被人们感知的形式，把客观物质运动和主观思维活动的状态表达出来的载体称为**消息**。

从通信观点出发，构成消息的各形式要有两个条件：一是能被通信双方理解；二是可传递。因此，人们从电话、电视等通信系统中得到的是一些描述各种主、客观事物运动或存在状态的消息。各种通信系统可概括成如图 1-1 所示的框图。

图 1-1 通信系统框图

由图 1-1 可知，在各种通信系统中，被传输的是消息。消息传递过程有以下特点：

(1)接收者在收到消息前，不知道消息的具体内容，即在收到消息以前，他无法判断发送者发来的具体消息；

(2)接收者在收到消息前，无法判断所描述的状态；

(3)接收者在收到消息后，因存在干扰，不能断定所得消息是否正确和可靠。

总之，接收者存在“不知”“不确定”或“疑问”。通过消息传递，接收者得知了消息的具体内容，原先的“不知”“不确定”和“疑问”得以消除或部分消除。因此，对于接收者来说，消息传递是一个从不知到已知，或从知之甚少到知之甚多，或从不确定到部分确定或全部确定的过程。如果一个通信系统不具备这些功能，它就失去了存在的意义。

因此，通信是一种消除不确定性的过程。消除了不确定性，就获得了信息。原先的不确定性消除得越多，获得的信息就越多。如果原先的不确定性全部消除了，就获得了全部信息；如果消除了部分不确定性，就获得了部分信息；如果原先的不确定性无任何消除，就没有获得任何信息。

定义 1.2 **信息**是对事物运动状态或存在方式的具有不确定性的描述。

例如，甲告诉乙“你买的股票涨了”，则乙就获得了信息。如果丙又告诉乙同样的话，则对乙来说，没有获得其他任何信息。在该事件中，“股票涨了”是对结果的描述。而结果不止一种，也可能是不变或跌了。可见乙在得到消息前存在不确定性。在得到消息之后，只要甲未说错，乙的不确定性就消除了，从而获得了信息。

由分析可知，在通信中形式上传输了消息，实质上传输了信息。同一信息可由不同形式的消息来承载，如前例中股票的涨跌情况可用报纸文字、广播语言、电视图像等不同消息来表述。而一则消息也可承载不同信息，它可能包含丰富的信息，也可能只包含极少的信息。因此，信息与消息既有区别，又有联系。消息包含信息，是信息的载体，得到消息即可获得信息。

所以，信息不同于消息，也不同于信号。在实际通信中，为了克服时间或空间上的限制而通信，需要对消息进行各种加工处理。

定义 1.3 在实际通信中，需要将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、光、声、生物等信号）。

信号是一个物理量，可测量、描述、显示。它携带了消息，是消息的载体。而信息与信号有本质上的区别：信号是承载信息的实体，它仅是外在，而信息则是内核。如文字消息不能直接在互联网的传输信道中传输，需先将文字变换成二进制码，再转换成适合信道传输的信号，才能在信道中传输。此时，这个称为信号的物理量承载了文字消息。在其接收端，通过各种反变换，若无干扰的话就可恢复出原文字消息。接收者收到电子邮件后，也消除了原有的不确定性，从而获得了信息。因此，信息、消息和信号是既区别又联系的三个不同概念。

1.1.2 信息的定义与度量

从信息、消息及信号的区别与联系的阐述中可以得到，信息是对事物运动状态或存在方式的不确定性的描述。那么根据香农信息的定义，信息该如何度量呢？

人们收到一封电子邮件，或是听了广播，看了电视，到底得到多少信息量呢？显然，信息量与不确定性的消除程度有关。消除多少不确定性，就获得多少信息量。那么，不确定性的大小能度量吗？

用数学语言来讲，不确定即为随机，具有不确定性的事件就是随机事件。因此，可应用研究随机事件的数学工具——概率论和随机过程来度量不确定性。即不确定性的大小可直观地看成事先猜测某随机事件是否发生的难易程度。

如设有甲、乙两个袋，各袋内装有大小均匀的 100 个球。甲袋内红、白球各 50 个，乙袋内有红、白、蓝、黄四种球，各 25 个。现随意从甲袋或乙袋中摸出 1 个球，并猜测取出的球是什么颜色。该事件具有不确定性。显然，从甲袋中摸出的是红球要比从乙袋中摸出的是红球容易。因为在甲袋中只是在“红”与“白”两种颜色中选择一种，而且“红”与“白”机会均等，即获取概率各为 1/2。但在乙袋中，红球只占 1/4，摸出的是红球可能性就小。自然，“从甲袋中摸出红球”比“从乙袋中摸出红球”的不确定性小。由此可见，不确定性大小与可能发生的消息数及各消息发生的概率有关。

由此可见，某一事物状态的不确定性大小，与该事物可能出现的不同状态数及各状态出现的概率大小有关。既然不确定性能度量，则信息也可度量。

针对信息度量，以下先给出三个基本概念：样本空间、概率测度和概率空间。

1. 样本空间

某事物各种可能出现的状态，即所有可选择消息的集合，称为**样本空间**。每个选择消息是该样本空间的元素。

2. 概率测度

对于离散消息集合，**概率测度**就是对每个可能选择的消息指定一个概率（非负，且总和为 1）。

3. 概率空间

定义 1.4 一个样本空间及其概率测度统称为一个**概率空间**。

概率空间一般用$[X,P]$表示。在离散情况下，X的样本空间可写成$[a_1,a_2,\cdots,a_q]$。样本空间中选择任意元素a_i的概率表示为$p_X(a_i)$，其下标X表示所考虑的是X的概率空间。一般如果不会引起混淆，下标可略去，写成$p(a_i)$。故在离散情况下，概率空间为

$$\begin{bmatrix} X \\ p(x) \end{bmatrix} = \begin{bmatrix} a_1 & a_2 & \cdots & a_q \\ p(a_1) & p(a_2) & \cdots & p(a_q) \end{bmatrix} \tag{1-1-1}$$

其中，$p(a_i)$是选择符号a_i作为消息的概率，称为**先验概率**。在接收端，对是否选择该消息(符号)a_i的不确定性与a_i的先验概率成反比，即对a_i的不确定性可表示为先验概率$p(a_i)$的倒数的函数。根据其特性，取该函数为对数函数。

定义 1.5 对随机变量X，消息(符号)a_i的**自信息**定义为

$$I(a_i) = \log_r \frac{1}{p(a_i)} = -\log_r p(a_i) \tag{1-1-2}$$

在接收端，收到的消息集合为Y。由于信道存在干扰，设接收端收到的消息(符号)为b_j。该b_j可能与a_i相同，也可能与a_i有差异。于是把条件概率$p(a_i/b_j)$称为**后验概率**。$p(a_i/b_j)$是接收端收到消息(符号)b_j后，发送端发的是a_i的概率。则在接收端收到b_j后，发送端发送符号是否是a_i尚存在的不确定性应是后验概率的函数，即$\log_r \frac{1}{p(a_i/b_j)}$。故接收者在收到消息(符号)$b_j$后，已消除的不确定性为先验不确定性减去尚存的不确定性，即为接收者获得的信息量。

定义 1.6 对随机变量X和Y，X的消息(符号)a_i和Y的消息(符号)b_j之间的**互信息**定义为

$$I(a_i;b_j) = \log_r \frac{1}{p(a_i)} - \log_r \frac{1}{p(a_i/b_j)} \tag{1-1-3}$$

如果信道无干扰，信道统计特性将使a_i以概率为1传送到接收端。此时，接收者接到消息后，尚存在的不确定性就等于零，即$p(a_i/b_j)=1$，$\log_r \frac{1}{p(a_i/b_j)} = 0$，不确定性被全部消除。此时，互信息等于自信息，即有

$$I(a_i;b_j) = I(a_i) \tag{1-1-4}$$

以上就是香农关于信息的定义和度量，通常也称为**概率信息**。香农定义的信息概念在现有的各种理解中较深刻。其优点如下：

(1)信息概念是一个科学定义，有明确的数学模型。

(2)信息概念与日常用语中信息的含意并不矛盾。

(3)信息概念排除了日常对信息一词的主观含义。同一个消息对任何接收者来说，所得信息量(互信息)都相同。

但香农定义的信息也有其局限性，存在一些缺陷。

(1)定义香农信息的出发点是假定事物状态可用一个以经典集合论为基础的概率模型来描述。而实际存在的某些事物运动状态要寻找一个合适的概率模型非常困难。

(2)香农信息的定义和度量未考虑接收者的主观特性和意义,也撇开了事物的本身含义、具体用途、重要程度和引起后果等因素。这与实际情况不一致。如当收到同一消息后,对不同接收者来说常引起不同的感情、关心程度、价值等。这些都应认为是获得了不同信息。故信息有很强的主观性和实用性。

因此,香农信息的定义和度量较为科学,能反映信息本质,但却有局限。目前,国内外有关信息的"定义"已不下百种。它们都从不同侧面和层次来揭示信息的本质。但因人们对信息本质的认识还不充分,故有关信息定义还处在争论阶段,尚未形成一个普遍公认的、完整的、确切的定义。为此,有关信息的定义及其数学模型的研究还在不断深入开展。随着人们对信息这一概念的深入研究,将会得出更合理、确切的信息定义和度量,达到彻底揭示信息本质、全面准确地把握信息的目标。

1.2 信息的基本概念

1.2.1 信息论的基本模型

由上性节关于信息概念的讨论可见,虽然各通信系统的形式和用途各不相同,但本质是相同的,即都是信息传输系统。为了便于研究信息传输和处理的共同规律,可将各通信系统中具有共同特性的部分抽取出来,概括成一个统一的理论模型,即通信系统模型,如图 1-2 所示。

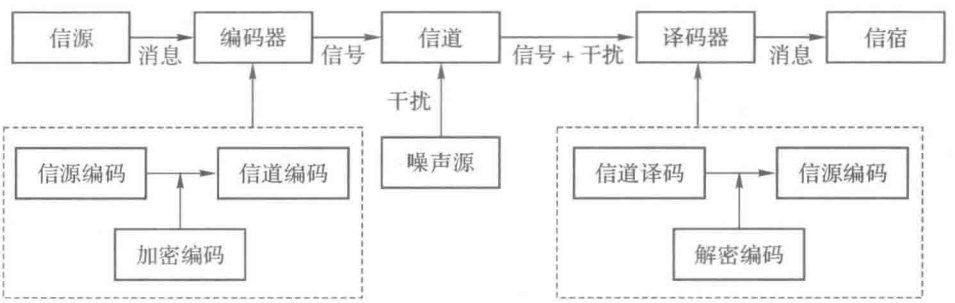

图 1-2 通信系统模型

信息论研究的对象正是统一的通信系统模型。人们通过系统中的消息传输和处理来研究信息传输和处理的共同规律。

通信系统模型主要包括以下五个部分。

1. 信源

信源是产生消息的来源,是信息运动的出发点。信源输出消息,但它不是信息本身。信源输出的消息有多种形式,可为离散的或连续的,也可为时间序列,它们分别可用离散型随机变量、连续型随机变量及随机过程等数学模型表示。

2. 编码器

编码把消息变换成信号，是对消息符号编码处理的过程；而译码为编码的反变换。编码器输出适合信道传输的信号，信号携带消息，是消息的载体。

编码器可分为两种，即信源和信道编码器。信源编码是对信源输出的消息做适当变换和处理，目的是提高信息传输效率。信道编码是为了提高信息传输的可靠性而对信号进行变换和处理。香农信息论分别用几个重要定理给出了编码理论的性能极限。

3. 信道

信道是指通信系统把携带消息的信号从甲地传输到乙地的媒介。在狭义通信系统中，实际信道有数据线、电缆、波导、光纤、无线电波传播空间等，这些都是属于传输电磁波能量的信道。当然，对广义通信系统，信道还可以是其他传输媒介。

信道除了传送信号以外，还能存储信号，如书写通信等。

信息传输不可避免地会引入噪声和干扰。为了分析方便，把在系统其他部分产生的干扰和噪声都等效折合成信道干扰，看成是由一个噪声源产生，并作用于所传输的信号上。因此，信道输出叠加了干扰的信号。由于干扰或噪声往往具有随机性，所以信道特性也可用概率空间描述。而噪声源的统计特性又是划分信道的依据。

4. 译码器

译码就是把信道输出的编码信号(已叠加了干扰)做反变换，以尽可能准确地恢复原始信源符号。译码器也可分成信源和信道译码器。

5. 信宿

信宿是消息传送的对象，即接收消息的人或机器。

图 1-2 给出的模型只适用于收、发两端为单向通信的情况。它只有一个信源和信宿，信息传输是单向的。在实际情况中，信源和信宿各有若干个，即信道有多个输入和输出。另外，信息传输方向也常常是双向的。如广播通信是单输入多输出的单向传输通信，而互联网通信则是多输入多输出的多向传输通信。要研究这些通信系统，只需对两端单向通信系统模型做适当改变，即可引出多用户通信系统模型。因此，图 1-2 所示的是最基本的通信系统模型，是信息论研究的对象。

1.2.2 信息论的研究目标

研究图 1-2 所示的通信系统，其目标就是要找到信息传输的共同规律，提高信息传输可靠性、有效性、保密性和认证性，从而使信息传输系统达到最优化。

可靠性高，指信源发出消息经信道传输后，尽可能准确、不失真地再现在接收端。

信息传输可靠性是所有通信系统努力追求的首要目标。要实现高可靠性传输，可采取诸如增大发射功率、增加信道带宽、提高天线增益等传统方法，但这些方法往往难度较大，有些场合甚至无法实现。而香农信息论指出：经适当信道编码后，同样可提高信道传输的可靠性。

有效性高，指在一定时间内传输尽量多的信息量，或在每个传送符号内携带尽可能多的信息量。

信息传输的有效性是通信系统追求的另一重要目标。这就需对信源进行高效率压缩编码，尽量去除冗余度。通常，提高可靠性和有效性常会发生矛盾，这就需要统筹兼顾。比如为了兼顾有效性，有时就不一定要求绝对准确地在接收端再现原消息，而是允许有一定误差或失真，或允许近似地再现原消息。

保密性就是要隐蔽和保护通信系统中传送的消息，使其只能被授权接收者获取，而不能被其他未授权者接收和理解。

认证性是指接收者能正确判断所接收消息的正确性，能验证消息的完整性，确定消息不是被伪造的或篡改过的。

有效性、可靠性、保密性和认证性四者构成了现代通信系统对信息传输的全面要求。

1.2.3 信息论的研究内容

目前，关于信息论的研究内容，主要有以下三种理解。

1. 狭义信息论

它是以客观概率信息为研究对象，从通信信息传输中总结和开拓的理论。它主要研究信息度量、信道容量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，又称香农基本理论。

2. 一般信息论

它主要研究信息传输和处理问题。除了香农理论外，一般信息论还包括噪声和信号的滤波与预测、统计检测与估计、调制以及信息处理等理论。后一部分内容是以美国科学家维纳研究的控制论等为代表的。

虽然维纳和香农等人都是运用概率和统计的数学方法来研究准确或近似再现消息的问题的，都是为了使消息传送和接收最优化，但他们的研究却有重要区别。维纳的研究重点在接收端。他研究当消息在传输过程中受到干扰后，在接收端将其恢复、再现，从干扰中提取出来。在此基础上，他创立了最佳线性滤波理论（维纳滤波器）、统计检测与估计理论、噪声理论等。而香农的研究对象则是从信源到信宿的全过程，是收、发端联合最优化问题，其重点是编码。香农定理指出，只要在传输前后对消息进行适当的编、译码，就能保证在有干扰的情形下，最佳地传送消息，并准确或近似地再现消息。为此，研究人员发展了信息度量理论、信道容量理论和编码理论等的情形。

3. 广义信息论

广义信息论是一门综合的新兴学科，它不仅包括上述两方面内容，还包括所有与信息有关的自然科学领域，如模式识别、计算机翻译、心理学、遗传学、神经生理学、语言学、语义学等有关信息问题，即凡是能够用广义通信系统模型描述的过程或系统，都能用信息基本理论来研究。

总之，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信息的传输、提取和处理系统中一般规律的科学，其主要研究目标是提高信息系统的可靠性、有效性、保密性和认证性，以便达到系统最优化，其主要内容包括香农理论、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。

信息论的研究内容极为广泛，本书主要结合电子通信等应用，介绍信息论的基本理论，即香农信息理论。

1.3 信息论的发展历程

了解信息论的发展对于深入了解信息论有很大帮助。信息论从诞生起，至今已有近七十年历史，现已成为一门独立的理论科学。回顾其发展历史，可知信息论是如何从实践中经抽象、概括、提高而逐步形成的。信息论是在长期的通信工程实践和理论基础上发展起来的，其形成的历史最早可上溯到19世纪30年代。

1832年，莫尔斯电报系统中高效率编码方法对后来香农编码理论有较大启发。

1885年，开尔文(L. Kelvin)曾研究过电缆的极限传信率问题。

1917年，坎贝尔(G. A. Campbell)申请了第一个滤波器专利，为频分复用信道提供了条件。

1922年，卡森(J. R. Carson)研究了振幅调制信号的频谱结构，开始明确上下边带概念。

1924年，奈奎斯特(H. Nyquist)开始分析电报信号传输中脉冲速率与信道带宽的关系，建立了限带信号采样定理。

1928年，哈特莱(R. V. Hartley)发展了奈奎斯特的工作，第一次从通信观点出发对信息量做了定义，提出把消息考虑为代码或单语序列。在s个代码中选N个代码，即构成s^N个可能消息，提出“定义信息量$H = N\log_r s$”，即定义信息量等于可能消息数的对数。其缺点是没有统计特性概念。哈特莱的工作对后来的香农思想有很大影响。

从上述进展可知，在20世纪30年代前，通信研究的主要目标还集中在如何使发送的信号无失真地送到接收端，所用的方法还是分析确定信号方法，具有较大的局限性。

1930年，维纳(N. Wiener)开始把傅里叶分析方法全面引入随机信号的分析研究中。

1936年，兰登(V. D. Landon)发表了第一篇有关噪声的论文。

1936年，阿姆斯特朗(E. H. Armstrong)提出了频率调制，指出增加信号带宽可增强抑制噪声干扰的能力，使调频实用化，出现了调频通信装置。

1939年，达德利(H. Dudley)发明了声码器，提出了通信所需带宽至少应与所传送消息的带宽相同。

1939年，里夫(H. Reeve)提出了具有强干扰能力的脉冲调制。

对噪声的研究到1945年由赖斯(S. O. Rice)做了全面总结。故20世纪40年代中期，通信理论已全面走上统计分析之路，抗干扰已取代抗失真成为通信研究的中心问题。

20世纪40年代初期，维纳在研究防空火炮控制问题时，发表了题为《平稳时间序列的外推、内插与平滑及其工程应用》的论文。他把随机过程和数理统计观点引入通信和控制系

统，揭示了信息传输和处理过程的统计本质。他还利用自己提出的“广义谐波分析理论”对信息系统中的随机过程做了谱分析，使通信系统理论研究上了一个新台阶。

1948年，香农在《贝尔系统技术杂志》上发表了两篇有关通信的数学理论的文章。在这两篇论文中，他利用概率测度和数理统计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，并由此奠定了现代信息论基础。

香农信息理论的核心是：揭示了在通信系统中采用适当编码后能实现高效率和高可靠地传输信息的现象，并得出了信源编码定理和信道编码定理。从数学上看，这些定理是最优编码存在定理。但从工程上看，这些定理是非结构性的，不能从定理结果直接得出实现最优编码的具体途径，但它们给出了编码的性能极限，在理论上阐明了通信系统中各种因素的相互关系，为人们寻找最佳通信提供了重要依据。

香农的论文《通信的数学理论》发表后，不仅引起了与信息有关的应用领域的兴趣，也引起了一些数学家的兴趣。如科尔莫戈罗夫(A. N. Kolmogorov)、范斯坦(A. Feinstein)等将香农基本概念和编码定理推广到更一般的信源模型、更一般的编码结构和性能度量，并给出严格证明，使该理论具有更坚实的数学基础。

另外，在通信技术界，研究也转到信源和信道编码的具体构造上，这方面取得了稳步发展。

1. 无失真信源编码

在香农编码方法提出后，许多科学家对无失真信源编码开展了大量研究。

1952年，费诺(Fano)提出了费诺编码；同年，霍夫曼(D. A. Huffman)提出了霍夫曼编码，并证明它是最佳码。

1963年，埃利斯(P. Elias)提出了算术编码。

1968年，科尔莫戈罗夫提出了通用编码。

这些编码经改进都先后实用化。如霍夫曼编码用于传真图像的压缩标准，算术编码用于二值图像压缩标准JBIG，通用编码用于计算机文件压缩等。

2. 有失真信源编码

将信息量化这一最古老的方法经发展已成为语音和图像压缩最重要的手段。如北美移动通信标准IS-95中语音压缩的标准算法就是矢量量化算法。

1955年，埃利斯(P. Elias)提出了预测编码。该码现已成为美国军用通信语音压缩的标准算法。

1959年，香农发表了《保真度准则下的离散信源编码定理》一文，其发展成为信息率失真理论。该理论是信源编码的核心问题，是频带压缩、数据压缩的理论基础。至今它仍是信息论研究的课题。

1969年，T. S. Huang提出了分组交换与量化方法。经发展，现在已在电视图像压缩的各种标准如H. 261、JPEG、MPEG中得到应用。

3. 面向数字信道的信道编码

另一部分科学家从事寻找最佳编码(纠错码)的工作，并已形成一门独立分支——纠错

码(BCH 码)理论。

20 世纪 40 年代末,戈莱(M. J. E. Golay)和汉明(C. W. Hamming)提出分组编码技术,把代数方法引入纠错码的研究,形成了代数编码理论,由此找到了大量可纠正多个错误的性能优异码,且提出了可实现的编译码方法。不少分组码,如汉明码、戈莱码、法尔(Fire)码、BCH 码等都在通信技术中获得广泛应用。

但是,代数编码的渐近性能很差,不能实现香农信道编码定理所指出的结果。因此,1960 年前后研究者提出了卷积码和概率译码,并逐步形成了一系列概率译码理论。其中,以维特比(Viterbi)译码为代表的译码方法被美国卫星通信系统所采用,使香农理论成为真正具有实用意义的科学理论。1993 年提出的 Turbo 码在性能上已非常接近理论极限。

4. 面向模拟信道的信道编码

1974 年,梅西(J. L. Massey)提出将编码与调制统一考虑的概念。1982 年,该想法在 G. Ungerboeck 等人的研究下终于取得突破,这就是网格编码调制。现在,网格编码调制正在向卫星通信、磁记录等领域扩展其应用范围。

在信息论的形成与发展过程中,多用户信息研究也取得了较大发展,使网络信息论理论日趋完善。

1961 年,香农的论文《双向通信信道》开拓了多用户信息研究。20 世纪 70 年代以来,随着卫星通信、计算机通信网的迅速发展,多用户信息理论的研究异常活跃,成为当时信息论中心研究的课题之一。

1971 年艾斯惠特(R. Ahlswede)和 1972 年廖(H. Liao)找出了多元接入信道的信道容量区。1973 年沃尔夫(J. K. Wolf)和斯莱平(D. Slepian)将它推广到公共信息的多元接入信道。伯格曼斯(P. Bergmans)、格拉格(R. G. Gallager)、科弗尔(T. M. Cover)、马登(K. Marton)和范·德·缪伦(E. C. Van der Meulen)等分别在网络信息论方面做了大量研究。

关于保密理论问题,香农在其 1949 年发表的题为《保密通信的信息理论》的论文中,首先用信息论的观点对信息保密问题做了全面的论述。由于保密问题的特殊性,直至 1976 年迪弗(Diffe)和海尔曼(Hellman)发表了题为《密码学的新方向》一文,提出了公开密钥密码体制后,保密通信才得到广泛研究。尤其在今天,信息安全和保密问题更加突出。人们把线性代数、初等数论、矩阵分析等引入保密问题研究,形成了密码学理论。

根据上述信息论形成及发展历程,信息论从最初形成时仅提供性能极限和概念方法性指导,发展到今天能具体指导通信系统结构组织和部件设计,这种趋势势必还将继续,而信息论也将在与通信理论、通信系统设计的理论日益融合的过程中得到进一步发展。

随着信息论的发展,它不仅在通信、计算机以及自动控制等电子学领域中得到直接应用,而且还广泛地渗透到社会学、生物学、医学、生理学、语言学和经济学等各领域,向多学科结合方向发展。在信息论与电子计算机、自动控制、系统工程、人工智能、仿生学等学科互相渗透、互相结合的基础上,形成了一门综合的新兴交叉学科——信息科学。信息科学是以信息为主要研究对象、以信息运动规律和利用信息原理为主要研究内容、以信息科学方法论为主要研究方法、以扩大人的信息功能(特别是智力功能)为主要研究目标的一门新兴交叉学