第 1 章　绪　　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相结合而逐步发展起来的一门学科。通常人们公认信息论的奠基人是当代伟大的数学家、美国贝尔实验室杰出的科学家香农(C. E. Shannon),他在 1948 年发表了著名的论文《通信的数学理论》,为信息论奠定了理论基础。近半个世纪以来,以通信理论为核心的经典信息论,正以信息技术为物化手段,向高精尖方向迅猛发展,并以神奇般的力量把人类社会推入了信息时代。随着信息理论的迅猛发展和信息概念的不断深化,信息论所涉及的内容早已超越了狭义的通信工程范畴,进入了信息科学这一更广阔、更新兴的领域。

本章首先引出信息的概念,进而讨论信息论这一学科的研究对象、目的和内容,并简述本学科的发展历史、现状和动向。

1.1　信息的概念

人类从产生那天起,就生活在信息的海洋之中。

人类社会的生存和发展,无时无刻都离不开接收信息、传递信息、处理信息和利用信息。

自古以来,人们就对信息的表达、存储、传送和处理等问题进行了许多研究。原始人的“结绳记事”也许是最初期的表达、存储和传送信息的方法。我国古代的“烽火告警”是一种最早的快速、远距离传递信息的方式。语言和文字则是人类社会用来表达和传递信息的最根本的工具。造纸术和印刷术的发明,使信息表示和存储方式产生了一次重大的变革,使文字成为信息记录、存储和传递的有效手段。特别是电报、电话和电视的发明,使信息传送快速、便利、远距离,再次出现了信息加工和传输的变革。近百年来,随着生产和科学技术的发展,使信息的处理、传输、存储、提取和利用的方式及手段达到了更新更高的水平。

近代,电子计算机的迅速发展和广泛应用,尤其个人微型计算机得以普及,大大提高了人们处理加工信息、存储信息及控制和管理信息的能力。

20 世纪 50 年代后期,随着计算机技术、微电子技术、传感技术,激光技术、卫星通信和移动通信技术、航空航天技术、广播电视技术、多媒体技术、新能源技术和新材料技术等新技术的发展和应用,尤其近年来以计算机为主体的互联网技术的兴起和发展,它们相互结合、相互促进,以前所未有的威力推动着人类经济和社会高速发展。正是这些现代新科学、新技术汇成了一股强大的时代潮流,将人类社会推入到高度信息化的时代。

在当今“信息社会”中,人们在各种生产、科学研究和社会活动中,无处不涉及信息的交换和利用。迅速获取信息,正确处理信息,充分利用信息,就能促进科学技术和国民经济的飞速发展。可见,信息的重要性是不言而喻的。

那么,什么是信息呢?

1. 信息、情报、知识、消息及信号间的区别与联系

信息是信息论中最基本、最重要的概念,它是一个既抽象又复杂的概念。这一概念和在实践中提出来的其他科学概念一样,是在人类社会互通情报的实践过程中产生的。在现代信息理论形成之前的漫长时期中,信息一直被看作是通信消息的同义词,没有赋予它严格的科学定义。到了 20 世纪 40 年代末,随着信息论这一学科的诞生,信息的含义才有了新的拓展。

在日常生活中,信息常常被认为就是“消息”、“情报”、“知识”、“情况”等。的确,信息与它们之间是有着密切联系的。但是,信息的含义更深刻、更广泛,它是不能等同于消息、情报、知识和情况的。

● 信息不等同于情报。

情报往往是军事学、文献学方面的习惯用词。如“对敌方情况的报告”,“文献资料中对于最新情况的报道或者进行资料整理的成果”等称为情报。在“情报学”这一新学科中,它们对于“情报”是这样定义的,“**情报**是人们对于某个特定对象所见、所闻、所理解而产生的知识”。可见,情报的含义要比“信息”窄得多。它只是一类特定的信息,不是信息的全体。

● 信息也不等同于知识。

知识是人们根据某种目的,从自然界收集得来的数据中,整理、概括、提取得到有价值的、人们所需的信息。知识是一种具有普遍和概括性质的高层次的信息。例如,如图 1.1 所示,有一堆 A、B 两所大学学生的考试成绩数据。为了了解 A、B 两所大学学生的学习成绩水平的差别,而进行统计处理,得到一张曲线图,从中获得了有关 A、B 两所大学学生学习水平的知识。当然,还可以从这堆数据中获得其他有关知识(两所大学男、女生成绩差别等)。又例如,获得大量的遥感图片数据,根据不同目的,处理后可以得到不同的知识(地质知识、地形知识、水源知识等)。由此可知,知识是以实践为基础,通过抽象思维,对客观事物规律性的概括。知识信息只是人类社会中客观存在的部分信息。所以知识是信息,但不等于信息的全体。

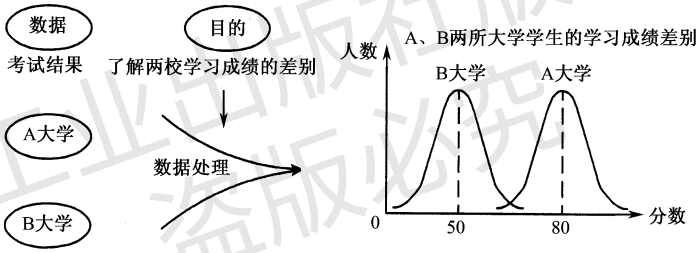


图 1.1　统计处理后的分布曲线

● 信息也不等同于消息。

人们也常常错误地把信息等同于消息,认为得到了消息,就是得到了信息。例如,当人们收到一封电报,接到一个电话,收听了广播或看了电视等以后,就说得到了“信息”。的确,人们从接收到的电报、电话、广播和电视的消息中能获得各种信息,信息与消息有着密切的联系。但是,信息与消息并不是一件事,不能等同。

我们知道,在电报、电话、广播、电视(也包括雷达、导航、遥测)等通信系统中传输的是各种各样的消息。这些被传送的消息有着各种不同的形式,如文字、符号、数据、语言、音符、图片、活动图像等。所有这些不同形式的消息都是能被人们感觉器官所感知的,人们通过通信,接收到消息后,得到的是关于描述某事物状态的具体内容。例如,听气象广播,气象预报为“晴间多云”,这就告诉了我们某地的气象状态,而“晴间多云”这广播语言则是对气象状态的具体表述。又如,我们收到一份电报为“母病愈”,则得知了母亲的身体健康状况,报文“母病愈”是对母亲身体健康状况的一种描述。再如电视中转播球赛,人们从电视图像中看到了球赛进展情况,而电视的活动图像则是对球赛运动状态的描述。可见,语言、报文、图像等消息都是对客观物质世界的各种不同运动状态或存在状态的表述。当然,消息也可用来表述人们头脑里的思维活动。例如,朋友给你打电话,电话中说:“我想去上海”,你就得知了你朋友的想法。这时,此语言消息则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。

因此,用文字、符号、数据、语言、音符、图片、图像等能够被人们感觉器官所感知的形式,把客观

物质运动和主观思维活动的状态表达出来就成为**消息**。

构成消息的各种形式必须具备两个条件:一是能被人们感知和理解的,二是可以进行传递和获取的。

可见,消息中包含信息,是信息的载体。得到消息,从而获得信息。同一则信息可用不同的消息形式来载荷。如前例中,球赛进展情况可用电视图像、广播语言、报纸文字等不同消息来表述。而一则消息也可载荷不同的信息,它可能包含非常丰富的信息,也可能只包含很少的信息。因此,信息与消息是既有区别又有联系的。

● 既然信息不同于消息,当然也不同于信号。

在各种实际通信系统中,往往为了克服时间或空间的限制而进行通信,必须对消息进行加工处理。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,生物信号等)。

信号携带着消息,它是消息的物理体现,是消息的运载工具。如前例中,“母病愈”这种关于母亲身体健康状况的信息,用汉文“母病愈”的消息来表述,然后通过电报系统传送到另一地的收信者。因为这个电报系统的传递信道是无线电电波信道,所以汉文消息不能直接在信道中传输。一般,需先将汉文(如“母病愈”)变换成四位码,然后变换成由点、划和空隔三种符号组成的莫尔斯码,再转换成脉冲电信号,然后经过调制变成高频调制电信号,才能在信道中传输。此时,脉冲电信号或高频调制电信号都载荷着汉文消息,表述了母亲身体健康的一种状态。在通信系统的接收端,通过解调,反变换,若无干扰的话就可恢复成原汉文消息——“母病愈”。收信者收到报文后,就得知了母亲病愈,身体健康,从而获得了信息。可见,信号携带信息,但不是信息本身。同样,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。例如,红、绿灯信号。若在十字路口,红、绿灯信号表示能否通行的信息。若在电子仪器面板上,红、绿灯信号却表示仪器是否正常工作或者表示高低电压等信息。所以,信息、消息和信号是既有区别又有联系的三个不同的概念。

2. 哈特莱、维纳、朗格等人对信息的定义

关于信息的科学定义,到目前为止,国内外已有不下百余种流行的说法。它们都是从不同的侧面和不同的层次来揭示信息的本质的。

哈特莱(R. V. L. Hartley)是最早对信息进行科学定义的。他在 1928 年发表的《信息传输》一文中,首先提出“信息”这一概念。他认为,发信者所发出的信息,就是他在通信符号表中选择符号的具体方式,并主张用所选择的自由度来度量信息。

哈特莱的这种理解在一定程度上能够解释通信工程中的一些信息问题,但它存在着严重的局限性。首先,他所定义的信息不涉及信息的价值和具体内容,只考虑选择的方式。其次,即使考虑选择的方式,但没有考虑各种可能选择方式的统计特性。正是这些缺陷严重地限制了它的适用范围。

1948 年,控制论的创始人之一,美国科学家维纳(N. Wiener)出版了《控制论——动物和机器中通信与控制问题》一书。维纳在该书中是这样来论述信息的,他指出:“信息是信息,不是物质,也不是能量”①。这就是说,信息就是信息自己,它不是其他什么东西的替代物,它是与“物质”、“能量”同等重要的基本概念。正是维纳,首先将“信息”上升到“最基本概念”的位置。

后来,维纳在《人有人的用处》②一书中,提出:“信息是人们适应外部世界并且使这种适应反作用于外部世界的过程中,同外部世界进行互相交换的内容的名称。”又说:“接收信息和使用信息的过程,就是我们适应外部世界环境的偶然性变化的过程,也是我们在这个环境中有效地生活的过

① N. Wiener,《控制论——动物和机器中的通信与控制问题》,科学出版社,1963 年

② N. Wiener,《人有人的用处》,商务印书馆,1978 年

程。”“要有效地生活,就必须有足够的信息。”的确,信息对人类的生存是很重要的,但是信息不仅仅与人类有关,不仅仅是人与外部世界交换的内容。在自然界中,一切生物体都在与外部世界进行着互相交换信息,一切生物体都有它们独自的接收信息和交换信息的方式。俗话说“禽有禽言,兽有兽语”,这是动物之间特别是群体动物之间传递信息的方式。人们发现动物之间可以利用气味、声音、不同的运动姿态,乃至超声波、电磁场等多种方式来传递信息。另外,信息的确是人们与外部世界互相交换的内容,但是,人们在与外部世界相互作用过程中,还进行着物质与能量的交换。这样就又把信息与物质、能量混同起来。所以,维纳关于信息的定义是不确切的。

关于信息的定义,有人提出用变异度、差异量来度量信息,认为“信息就是差异”。这种说法的典型代表是意大利学者朗格(G. Longe)。他在 1975 年出版的《信息论:新的趋势与未决问题》一书序言中,提出:“信息是反映事物的形式、关系和差别的东西。信息是包含于客体间的差别中,而不是在客体本身中。”“在通信中仅仅差别关系是重要的。”也就是说,他定义信息是客体之间的相互差异。的确,宇宙内到处存在着差异,差异的存在使人们存在着“疑问”和“不确定性”。从这个角度看,差异确是信息。但是,并不能说没有差异就没有信息。所以,这样定义的信息也是不全面的、不确切的。

3. 香农信息的定义

香农在 1948 年发表了一篇著名的论文——《通信的数学理论》。他从研究通信系统传输的实质出发,对信息做了科学的定义,并进行了定性和定量的描述。

如前所述,各类通信系统——电报、电话、广播、电视、雷达、遥测……等传送的是各种各样的消息。消息的形式可以不同,但它们都是能被传递的,能被人们感觉器官(眼、耳、触觉等)所感知的,而且消息表述的是客观物质和主观思维的运动状态或存在状态。

香农将各种通信系统概括成如图 1.2 所示的框图。在各种通信系统中,其传输的形式是消息。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。在收到消息以前,收信者无法判断发送者将会发来描述何种事物运动状态的具体消息;他更无法判断是描述这种状态还是那种状态。再者,即使收到消息,由于干扰的存在,他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“不知”、“不确定”或“疑问”。通过消息的传递,收信者知道了消息的具体内容,原先的“不知”、“不确定”和“疑问”消除或部分消除了。因此,对收信者来说,消息的传递过程是一个从不知到知的过程,或是从知之甚少到知之甚多的过程,或是从不确定到部分确定或全部确定的过程。如果不具备这样一个特点,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接听到电话之前就已经知道报文或电话的内容,那还要电报、电话系统干什么呢?

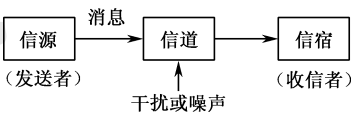


图 1.2　通信系统框图

由于主、客观事物的运动状态或存在状态是千变万化的、不规则的、随机的,因此在通信以前,收信者存在“疑义”和“不知”。例如,在电报通信中,收报人在收到报文前,首先他不知何人会给他发电报,而且也不知将要告诉他什么事情。只有当他收到报文是“母病愈”后,才能确定是他家人告诉他母亲的身体情况。其次,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,到底出现的是什么状态是随机的、变化的。收信者在看到报文以前,他不能确定母亲身体健康状态如何,也存在“不确定性”。只要报文是清楚的,在传递过程中没有差错,那么,他收到报文以后,他原来所有的“不确定性”都没有了,他就获得了所有的信息。如果在传递过程中存在着干扰,使报文完全模糊不清,收信者收到报文以后,原先所具有的不确定性一点也没有减少,他就没有获得任何信息。如果干扰使报文发生部分差错,使收信者原先的不确定性减少了一些,但没有全部消除,他就获得了一部分信息。所以,通信过程

是一种消除不确定性的过程。不确定性的消除,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,就获得了全部的信息;若消除了部分不确定性,就获得了部分信息;若原先不确定性没有任何消除,就没有获得任何信息。由此可见,**信息是事物运动状态或存在方式的不确定性的描述**。这就是**香农信息的定义**。

从以上分析可知,在通信系统中形式上传输的是消息,但实质上传输的是信息。消息只是表达信息的工具,载荷信息的客体。显然,在通信中被利用的(亦即携带信息的)实际客体是不重要的,而重要的是信息。信息较抽象,而消息是较具体的,但还不一定是物理性的。通信的结果是消除或部分消除不确定性从而获得信息。

4. 香农信息的度量

根据香农的有关信息的定义,信息如何测度呢?当人们收到一封电报,或听了广播,或看了电视,到底得到多少信息量呢?显然,信息量与不确定性消除的程度有关。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?

用数学的语言来讲,不确定性就是随机性,具有不确定性的事件就是随机事件。因此,可运用研究随机事件的数学工具——概率论和随机过程来测度不确定性的大小。若从直观概念来讲,不确定性的大小可以直观地看成是事先猜测某随机事件是否发生的难易程度。

例如,假设有甲、乙两个布袋,各袋内装有大小均匀,手感完全一样的球 100 个。甲袋内红、白球各 50 个,乙袋内有红、白、蓝、黑四种球,各 25 个。现随意从甲袋或乙袋中取出一球,并猜测取出的是什么颜色的球,这事件当然具有不确定性。显然,从甲袋中摸出是红球要比从乙袋中摸出是红球容易得多。这是因为,在甲袋中只在“红”与“白”两种颜色中选择一种,而且“红”与“白”机会均等,即摸取的概率各为 1/2。但在乙袋中,红球只占 1/4,摸出是红球的可能性就小。自然,“从甲袋中摸出的是红球”比“从乙袋中摸出的是红球”的不确定性来得小。从这个例子可以得出,不确定性的大小与可能发生的消息数目及各消息发生的概率有关。

再如气象预报,我们知道可能出现的气象状态有许多种。以十月份北京地区天气为例,经常出现的天气是“晴间多云”、“晴”或“多云”,其次是“多云转阴”、“阴”、“阴有小雨”等,而“小雪”这种天气状态出现的概率是极小的,“大雪”的可能性则更小更小。因此,在听气象预报前,我们大体上能猜测出天气的状况。由于出现“晴间多云”、“晴”或“多云”的可能性大,我们就比较能确定这些天气状况的出现。当预报明天白天“晴间多云”或“晴”,我们并不觉得稀奇,因为和我们猜测的是基本一致,所消除的不确定性要小,获得的信息量就不大。而出现“小雪”的概率很小,我们很难猜测它是否会出现,所以这事件的不确定性很大。如果预报是“阴有小雪”,我们就要大吃一惊,感到气候反常,这时就获得了很大的信息量。出现“大雪”的概率更小,几乎是不可能出现的现象,它的不确定性更大。如果一旦出现“大雪”的气象预报,我们将万分惊讶,这时将获得更大的信息量。由此可知,某一事物状态出现的概率越小,其不确定性越大;反之,某一事物状态出现的概率接近于 1,即预料中肯定会出现的事件,那它的不确定性就接近于零。

这两个例子告诉我们:某一事物状态的不确定性的大小,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。既然不确定性的大小能够度量,可见信息是可以测度的。

(1) 样本空间

我们把某事物各种可能出现的不同状态,即所有可能选择的消息的集合,称为**样本空间**。每个可能选择的消息是这个样本空间的一个元素。

(2) 概率测度

对于离散消息的集合,概率测度就是对每一个可能选择的消息指定一个概率(非负的,且总和为 1)。

(3) 概率空间

一个样本空间和它的概率测度称为一个**概率空间**。

一般概率空间用$[X,P]$来表示。在离散情况下,X的样本空间可写成$\{a_1,a_2,\cdots,a_q\}$。样本空间中选择任一元素a_i的概率表示为$P_X(a_i)$,其脚标X表示所考虑的概率空间是X。如果不会引起混淆,脚标可以略去,写成$P(a_i)$。所以在离散情况下,概率空间为

$$\begin{bmatrix} X \\ P(x) \end{bmatrix} = \begin{bmatrix} a_1, & a_2, & \cdots, & a_q \\ P(a_1), & P(a_2), & \cdots, & P(a_q) \end{bmatrix}$$

其中$P(a_i)$就是选择符号a_i作为消息的概率,称为**先验概率**。

(4) 自信息

在接收端,对是否选择这个消息(符号)a_i的不确定性是与a_i的先验概率成反比的,即对a_i的不确定性可表示为先验概率$P(a_i)$的倒数的某一函数。我们取该函数为对数函数,并把这样定义的不确定性称为该消息(符号)a_i的**自信息**,即

$$I(a_i) = \log \frac{1}{P(a_i)} \tag{1.1}$$

(5) 互信息

由于信道中存在干扰,假设接收端收到的消息(符号)为b_j,这个b_j可能与a_i相同,也可能与a_i有差异。我们把条件概率$P(a_i \mid b_j)$称为**后验概率**,它是接收端收到消息(符号)b_j后而发送端发的是a_i的概率。那么接收端收到b_j后,发送端发送的符号是否是a_i尚存在的不确定性,应是后验概率的函数,即是$\log \frac{1}{P(a_i \mid b_j)}$。于是,收信者在收到消息(符号)$b_j$后,已经消除的不确定性为:先验的不确定性减去尚存在的不确定性。这就是收信者获得的信息量,定义为**互信息**,即

$$I(a_i;b_j) = \log \frac{1}{P(a_i)} - \log \frac{1}{P(a_i \mid b_j)} \tag{1.2}$$

如果信道没有干扰,信道的统计特性使a_i以概率1传送到接收端。这时,收信者接到消息后,尚存在的不确定性就等于零,即$P(a_i \mid b_j)=1$,$\log \frac{1}{P(a_i \mid b_j)}=0$,不确定性全部消除。由此得互信息

$$I(a_i;b_j) = I(a_i) \tag{1.3}$$

收信者就获得了消息a_i所含有的全部信息量。

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**。

(6) 香农信息定义的优点

香农定义的信息概念在现有的各种理解中,它比较深刻,有许多优点。

- 首先,它是一个科学的定义,有明确的数学模型和定量计算。
- 其次,它与日常用语中的信息的含意是一致的。例如,设某一事件a_i发生的概率等于1,即a_i是预料中一定会发生的必然事件,如果事件a_i果然发生了,收信者将不会得到任何信息(日常含义),因为他早知道a_i必定发生,不存在任何不确定性。

根据式(1.1),因为$P(a_i)=1$,所以得 $I(a_i)=\log \frac{1}{P(a_i)}=0$

即自信息等于零。反之,如果a_i发生的概率很小,即猜测它是否发生的不确定性很大,一旦a_i果然发生了,收信者就会觉得很意外和惊讶,获得的信息量很大。根据式(1.1),因为$P(a_i) \ll 1$,故得

$$I(a_i) = \log \frac{1}{P(a_i)} \gg 1$$

- 再者,它排除了对信息一词某些主观上的含义。根据上述定义,同样一个消息对任何一个收信者来说,所得到的信息量(互信息)都是一样的。因此信息的概念是纯粹的形式化的概念。

(7) 香农信息定义的缺陷

香农定义的信息有其局限性,存在一些缺陷。

- 首先,我们已经看到,这个定义的出发点是假定事物状态可以用一个以经典集合论为基础的概率模型来描述。然而对实际某些事物运动状态或存在状态要寻找一个合适的概率模型往往是非常困难的。对某些情况来讲,是否存在这样一种模型还值得探讨。而且这个定义只考虑概率引发的不确定性,不考虑由于其他因素如模糊性等而造成的不确定性。
- 其次,这个定义和度量没有考虑收信者的主观特性和主观意义,也撇开了信息的具体含意、具体用途、重要程度和引起后果等因素。这就与实际情况不完全一致。例如,当得到同一消息后,对不同的收信者来说常会引起不同的感情、不同的关心程度、不同的价值,这些都应认为是获得了不同的信息。又例如,甲乙两人同去听一段音乐,若甲者缺乏欣赏音乐的起码知识和必要训练的话,这种信息就不能发生什么作用;若乙者是一位训练有素的音乐家,那么他将从这段音乐中获得大量信息。因此,信息有很强的主观性和实用性。

由此可见,香农信息的定义和度量是科学的,是能反映信息的某些本质的;但却是有缺陷的、有局限的。这样就使它的适用范围受到严重的限制。

5. 信息的广义概念

(1) 信息是物质世界的三大支柱之一

目前,哲学家和科学家普遍认为,物质、能量和信息是物质世界的三大支柱,是科学历史上三个最重要的基本概念。

世界是物质的。没有物质就没有世界,就没有一切,也就没有信息。可以说信息与物质同存,信息是物质的一种普遍属性。

在物质世界中任何事物都处于永恒的运动和普遍的相互作用之中。只要有运动和相互作用的事物,就需要有能量,也就会产生各种各样事物运动的状态和方式,就产生信息。信息是作为物质存在方式和状态的自身显示,同样也是相互作用的自身显示。可见,信息源于物质世界本身,源于物质世界的运动和相互作用之中,所以信息是普遍存在的。

信息是物质的属性,但不是物质自身,信息具有相对独立性。事物运动的状态和方式一旦体现出来,就可以脱离原来的事物而相对独立地载附于别的事物上,而被提取、变换、传递、存储、加工或处理。因此,信息不等于它的源事物,也不等于它的载体。信息虽不等于物质本身,但它也不可能脱离物质而独立存在,必须以物质为载体,以能量为动力。这三者是相辅相成,缺一不可的。这也正是信息的绝对性、普遍性和独立性。

正是信息的这种相对独立性,使得它可以被传递、复制、存储和扩散。这就是信息的可贵特性——共享性。信息的共享是无限的。只要是无干扰和全息传递,共享的信息就是完全等同的,并不因为信息被共享后而使原占有者丢失信息。所以,信息传播、扩散越快、越广,就越加速推动人类社会的发展和进步。可以说,信息的共享性对人类社会的发展有着特别重要的意义。

信息作为事物运动和相互作用的自身显示,与事物及它们的运动和相互作用一样是永恒的、无限的、动态的。事物每时每刻都在与其他事物的相互作用及自身的运动中改变着自身的信息,所以信息永远在产生、演变、更新。而且人类对信源信息的认识也是有时间性的。虽然认识的信息一旦形成被存储起来,在一般情况下绝不会自行发生变化,但是信源的信息却在不断地变化着,因此主观认识信息有个衰老的问题,从而失去本身的价值。所以,信息是有时效性的。

综上所述,信息具有以下主要特性:

① 信息、物质、能量统一于事物一身,信息和物质一起规定着事物的功能。

② 信息的存在具有普遍性、无限性、动态性、时效性和相对独立性。

③ 信息具有可传递性、可转换性、可扩散性、可复制性、可存储性和可分割性，因而具有可共享性。

④ 信息具有可度量性。信息量守恒是客观事物固有的特性。信息不因认识而消失，也不因传递、复制和扩散而增值。

(2) 语法、语义、语用信息

从这种观点出发，我国学者钟义信教授在本体论的层次(最高、最普遍的层次，也是无约束条件的层次)上，对信息做了定义。他认为：“**信息**就是事物运动的状态和方式，就是关于事物运动的千差万别的状态和方式的知识。”[14]

钟义信教授又在本体信息的基础上，引入认识主体的一些约束条件，从而又提出了语法信息、语义信息和语用信息三个不同的定义。

语法信息是事物运动状态和状态改变的方式的本身。所以它不涉及这些状态的含义和效用，是最抽象最基本的层次。它只研究事物运动各种可能出现的状态，以及状态之间的关系。香农的信息定义正是属于这个层次，是从概率统计角度来研究事物运动各种可能出现的状态及状态间的关系，因此是概率性的语法信息，它能较好地解决通信工程这样一类信息传递的问题。

语义信息是事物运动状态和方式的具体含义。这是研究各种状态和实体间的关系，即研究信息的具体含义。

语用信息是事物运动状态和方式及其含义对观察者的效用，或者是相对于某种目的的效用。这是研究事物运动状态和方式与使用者的关系，即研究信息的主观价值。

在这些信息定义的基础上，他提出了对语法信息的统一的度量形式，又建立了语义信息量、语用信息量和综合语用信息量等概念和度量。这综合语用信息量在特定条件下可以转换为其他信息度量，而且可以在特定条件下转化成目前国际上学术界认可的任一信息量公式。

显然，此处的信息概念已远远超出了原来通信领域的范畴。

由于人们对信息的本质认识还不够充分，因此国际上尚未形成一个普遍公认的、完整的、确切的定义。为此，有关信息的定义和其测度的研究还在不断地深入。我们深信，随着人们对信息这一概念的不断深入研究，将会得出更合理、更确切的信息的定义和测度，达到彻底揭示信息的本质，全面和准确地把握信息。

1.2 信息论研究的对象、目的和内容

1. 信息论研究的对象

从关于信息概念的讨论中，我们已经看到：各种通信系统如电报、电话、电视、广播、遥测、遥控、雷达和导航等，虽然它们的形式和用途各不相同，但本质是相同的，都是信息的传输系统。为了便于研究信息传输和处理的共同规律，我们将各种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，如图 1.3 所示。通常称它为通信系统模型。

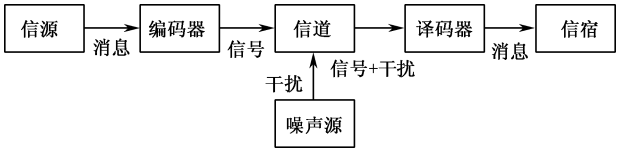


图 1.3 通信系统模型

这个通信系统模型也适用于其他的信息流通系统，如生物有机体的遗传系统、神经系统、视觉系统等。甚至人类社会的管理系统都可概括成这个模型。

信息论**研究的对象**正是这种统一的通信系统模型。人们通过系统中消息的传输和处理来研究

信息传输和处理的共同规律。

通信系统模型主要分成下列五部分。

(1) **信息源**(简称信源):顾名思义,**信源**是产生消息和消息序列的源。它可以是人、生物、机器或其他事物。它是事物各种运动状态或存在状态的集合。如前所述,“母亲的身体状况”,“各种气象状态”等客观存在是信源。人的大脑思维活动也是一种信源。信源的输出是消息,消息是具体的,但它不是信息本身。消息携带着信息,消息是信息的表达者。

另外,信源可能出现的状态(即信源输出的消息)是随机的、不确定的,但又有一定的规律性。

(2) **编码器:编码**是把消息变换成信号的措施,而**译码**就是编码的反变换。**编码器**输出的是适合信道传输的信号,信号携带着消息,它是消息的载荷者。

一般编码器可分为两种,即信源编码器和信道编码器。信源编码是对信源输出的消息进行适当的变换和处理,目的是为了提高信息传输的效率。所以又称为信源压缩编码。而信道编码是为了提高信息传输的可靠性而对消息进行的变换和处理,又称为信道纠错编码。当然对于各种实际的通信系统,编码器还应包括换能、调制、发射等各种变换处理。在保密通信系统中,还应该包括加密编码,目的是为了提高信息传输的安全性和证实性。

(3) **信道:信道**是指通信系统把载荷消息的信号从甲地传输到乙地的媒介或通道。在狭义的通信系统中实际信道有明线、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,对广义的通信系统来说,信道还可以是其他的传输媒介。

信道除了传送信号以外,还有存储信号的作用,如磁带、光盘或书写通信方式等。

在信道中引入噪声和干扰,这是一种简化的表达方式。为了分析方便起见,把在系统其他部分产生的干扰和噪声都等效地折合成信道干扰,看成是由一个噪声源产生的,它将作用于所传输的信号上。这样,信道输出的是已叠加了干扰的信号。由于干扰或噪声往往具有随机性,因此信道的特性也可以用概率空间来描述,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)进行反变换,一般认为这种变换是可逆的。**译码器**一般也可分成信源译码器和信道译码器。若在保密通信系统中,应还包括解密译码。

(5) **信宿:信宿**是消息传送的对象,即接收消息的人或机器。信源和信宿可处于不同地点和不同时刻。

图 1.3 给出的模型只适用于收发两端单向通信的情况。它只有一个信源和一个信宿,信息传输也是单向的。更一般的情况是:信源和信宿各有若干个,即信道有多个输入和多个输出,另外信息传输方向也可以双向进行。例如,广播通信是单个输入,多个输出的单向传输的通信;而卫星通信网则是多个输入,多个输出和多向传输的通信。要研究这些通信系统,我们只需对两端单向通信系统模型做些适当修正,就可引出网络通信系统模型。因此,图 1.3 的通信系统模型是最基本的。

近年来,以计算机为核心的大规模信息网络,尤其是互联网的建立和发展,对信息传输的质量要求更高了。不但要求既快速有效又能可靠地传递信息,而且还要求信息传递过程中保证信息的安全保密,不被伪造和窜改。因此,在编码器这一环节中还需加入加密编码。相应地,在译码器中加入解密译码。

为此,我们把图 1.3 的通信系统模型中编(译)码器分成信源编(译)码、信道编(译)码和加密(解密)编(译)码三个子部分。这样,信息传输系统的基本模型如图 1.4 所示。

2. 信息论研究的目的

研究如图 1.4 所示的这样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,以提高信息传输的可靠性、有效性、保密性和认证性,使信息传输系统达到最优化。

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,尽可能准确地、不失真地再现在接收端。

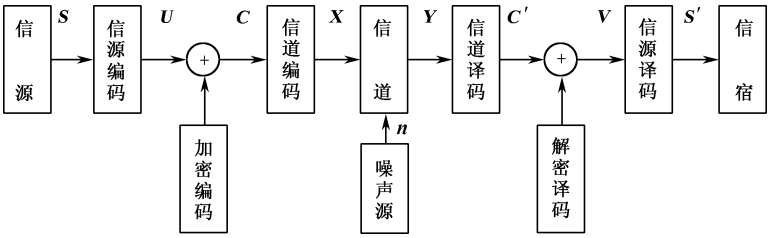


图 1.4　信息传输系统的模型

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。

以后我们会看到,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在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。

所谓**保密性**就是隐蔽和保护通信系统中传送的消息,使它只能被授权接收者获取,而不能被未授权者接收和理解。

所谓**认证性**是指接收者能正确判断所接收的消息的正确性,验证消息的完整性,而不是伪造的和被窜改的。

可靠性、有效性、保密性和认证性四者构成现代通信系统对信息传输的全面要求。

信息传输系统模型不是不变的,它可根据信息传输的要求而定。在研究信息传输可靠性时,将信源、信源编码和加密编码都等效成一个信源,而将信宿、信源译码和解密译码都等效成一信宿。在研究信息传输有效性时,可只考虑信源与信宿之间的信源编(译)码,将其他部分都看成一无干扰信道。在考虑信息传输的保密性和认证性时,将信源和信源编码等效成一信源;将信道编码、信道、噪声源和信道译码等效成一无干扰信道;而将信源译码和信宿等效于信宿。这样划分是否合理呢?通过全书的讨论,我们可以得出,这样划分是合理的。

3. 信息论研究的内容

关于信息论研究的具体内容是有过争议的。某些数学家认为信息论只是概率论的一个分支。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,这就太狭义了。也有些物理学家认为信息论只是熵的理论,他们对“熵”特别感兴趣。当然,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。

目前,对信息论研究的内容一般有以下三种理解。

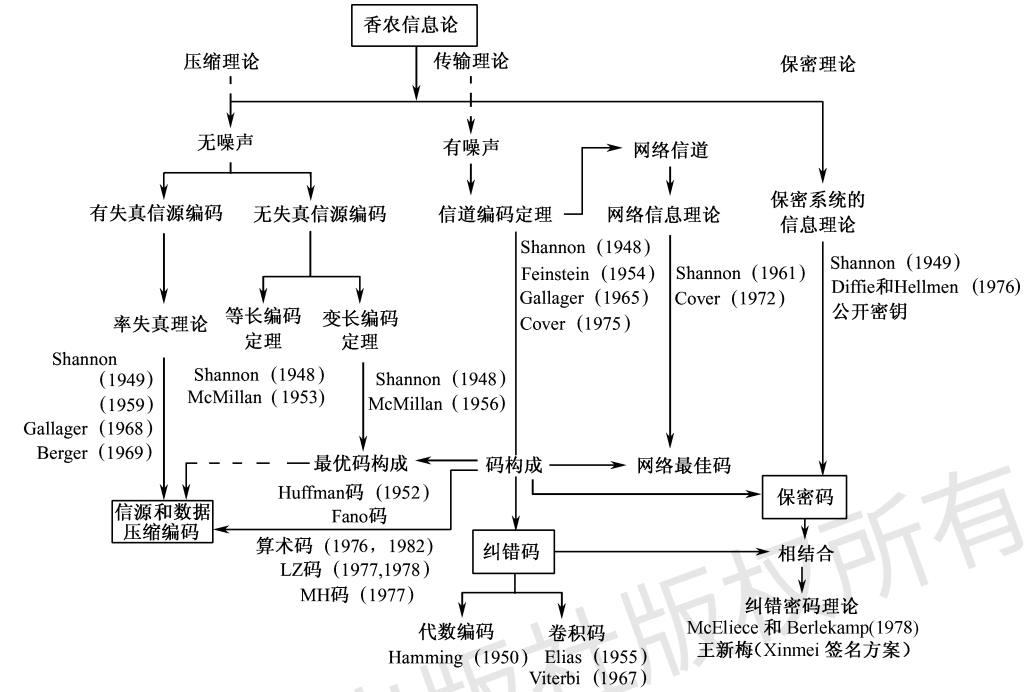
(1) **狭义信息论**,也称经典信息论:它主要研究信息的测度、信道容量及信源和信道编码理论等问题。这部分内容是信息论的基础理论,又称香农基本理论。其研究的各部分内容可用图 1.5 来描述。

(2) **一般信息论**,也称工程信息论:它主要研究信息传输和处理问题。除了香农理论以外,还包括编码理论、保密理论、噪声理论、信号滤波和预测理论、统计检测与估计理论、调制理论及信息处理理论等。后一部分内容是以美国科学家维纳(N. Wiener)为代表的,其中最有贡献的是维纳和前苏联科学家柯尔莫哥洛夫(A. Колмогоров)。

虽然维纳和香农等人都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)所干扰后,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

最佳线性滤波理论(维纳滤波器)、统计检测与估计理论、噪声理论等。



注：用方框表示的是各自为独立体系的重要分支

图 1.5　香农信息论的科学体系

而香农研究的对象则是从信源到信宿之间的全过程,是收、发端联合最优化问题,其重点放在编码上。他指出,只要在传输前后对消息进行适当的编码和译码,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**:广义信息论是一门综合、交叉的新兴学科,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科学和社会科学领域,如模式识别、计算机翻译、心理学、遗传学、生物学、神经生理学、语言学、语义学甚至包括社会学、人文学和经济学中有关信息的问题。它也就是新发展起来的包括光学信息论、量子信息论和生物信息学等新学科在内的信息科学理论。

综上所述,信息论是一门应用概率论、随机过程、数理统计和近世代数的方法,来研究广义的信息传输、提取和处理系统中一般规律的学科;它的主要目的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;它的主要内容(或分支)包括香农理论、编码理论、密码学理论、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,因此本书主要论述信息论的基础理论即香农信息理论(即图 1.5 中间非方框部分的内容)。

1.3　信息论发展简史与信息科学

信息论从诞生到今天,已有半个多世纪的历程,现已成为一门独立的理论学科。回顾它的发展历史,我们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。

1. 信息论形成的背景和基础

信息论是在长期的通信工程实践和理论研究的基础上发展起来的。

通信系统是人类社会的神经系统,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

方面的社会实践是悠久漫长的。

电的通信系统(电信系统)已有近 200 年的历史了。在这近 200 年的发展过程中,一个很有意义的历史事实是:当物理学中的电磁理论及后来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。这是因为通信系统对人类社会的发展,其关系实在是太密切了。日常生活、工农业生产、科学研究及战争等,一切都离不开信息传递和流动。

例如,当法拉第(M. Faraday)于 1820 年至 1830 年期间发现电磁感应的基本规律后,不久莫尔斯(F. B. Morse)就建立起电报系统(1832—1835)。1876 年,贝尔(A. G. Bell)又发明了电话系统。

1864 年麦克斯韦(Maxwell)预言了电磁波的存在,1888 年赫兹(H. Hertz)用实验证明了这一预言。接着 1895 年英国的马可尼(G. Marconi)和俄国的波波夫(А. С. Подов)就发明了无线电通信。20 世纪初(1907 年),根据电子运动的规则,福雷斯特(L. Forest)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)。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 年代初的第二次世界大战初期,微波通信系统、微波雷达系统等就迅速发展起来。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。

随着工程技术的发展,有关理论问题的研究也在逐步深入。

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率问题。

1922 年卡逊(J. R. Carson)对调幅信号的频谱结构进行了研究,并明确了边带的概念。

1924 年奈奎斯特(H. Nyquist)和屈夫缪勒(K. Küpfmüller)分别独立地指出,如果以一个确定的速度来传输电报信号,就需要一定的带宽,证明了信号传输速率与信道带宽成正比。

1928 年哈特莱(R. V. Hartley)发展了奈奎斯特的理论,并提出把消息考虑为代码或单语的序列。在 s 个代码中选 N 个码即构成 s^N 个可能的消息。他提出"定义信息量 $H=N\log s$",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的概念。他的理论对后来香农的思想是有很大影响的。

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。

1939 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消息的带宽相同。达德利和莫尔斯都是研究信源编码的先驱者。

但是,一直到 20 世纪 30 年代末,理论工作的一个主要弱点是把消息看成是一个确定性的过程。这就与许多实际情况不相符合。当时所依靠的数学工具主要是经典的傅里叶分析方法,这是有局限性的。

20 世纪 40 年代初期,由于军事上的需要,维纳在研究防空火炮的控制问题时,提出了"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的观点引入通信和控制系统中来,揭示了信息传输和处理过程的统计本质。他还利用早在 20 世纪 30 年代初他本人提出的"广义谐波分析理论"对信息系统中的随机过程进行谱分析。这就使通信系统的理论研究面貌焕然一新,引起了质的飞跃。

2. 香农信息论的建立和发展

1948 年 6 月和 10 月香农在贝尔实验室出版的著名的《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,首先严格定义了信息的度量——熵的概念,又定义了信道容量的概念,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的基础。

香农理论的核心是: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地传输信息,并得出了信源编码定理和信道编码定理。从数学观点看,这些定理是最优编码的存在定理。但从工程观点看,这些定理不是结构性的,不能从定理的结果直接得出实现最优编码的具体途径。然而,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系统提供了重要的理论依据。

(1) 香农信息理论的数学严格化

从 1948 年开始,信息论的出现引起了一些著名数学家如柯尔莫哥洛夫、范恩斯坦(A. Feinstein)、沃尔夫维兹(J. Wolfowitz)等人的兴趣,他们将香农已得到的数学结论做了进一步的严格论证和推广,使这一理论具有更为坚实的数学基础。在这方面,1954 年范恩斯坦的论著是有很大贡献的。

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(J. Wolfowitz)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 年格拉格尔(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。而科弗尔(T. M. Cover)于 1975 年采用典型序列方法来证明。1972 年阿莫托(S. Arimoto)和布莱哈特(R. Blahut)分别发展了信道容量的迭代算法。

高斯信道是香农在 1948 年原论文中首先分析和研究的。1964 年霍尔辛格(J. L. Holsinger)发展了有色高斯噪声信道容量的研究。1969 年平斯克尔(M. S. Pinsker)提出了具有反馈的非白噪声高斯信道容量问题。科弗尔(T. M. Cover)于 1989 年对平斯克尔的结论给出了简洁的证明。

(2) 无失真信源编码定理和技术的发展

香农在 1948 年论文中提出了无失真信源编码定理,也给出了简单的编码方法(香农编码)。麦克米伦(B. McMillan)于 1956 年首先证明了唯一可译变长码的克拉夫特(Kraft)不等式。关于无失真信源的编码方法,1952 年费诺(Fano)提出了一种费诺码。同年,霍夫曼(D. A. Huffman)首先构造了一种霍夫曼编码方法,并证明了它是最佳码。

20 世纪 70 年代后期开始,人们把兴趣放在与实际应用有关的信源编码问题上。于 1968 年前后,埃利斯(P. Elias)发展了香农—费诺码,提出了算术编码的初步思路。而里斯桑内(J. Rissanen)在 1976 年给出和发展了算术编码。1982 年他和兰登(G. G. Langdon)一起将算术编码系统化,并省去了乘法运算,更为简化、易于实现。关于通用信源编算法——LZ 码是于 1977 年由齐弗(J. Ziv)和兰佩尔(A. Lempel)提出的。1978 年他们俩又提出了改进算法 LZ-77 码和LZ-78码,而且齐弗也证明此方法可达到信源的熵值。1984 年由韦尔奇(T. A. Welch)提出了改进的 LZW 码。随后,1990 年贝尔(T. C. Bell)等在 LZ 算法基础上又做了一系列变化和改进,如 LZSS 码、LZRW1-4 码、LZP1-4 码等。这些字典码已广泛应用于文本的数据压缩中。

正是在香农的无损信源压缩编码定理指引下,无损压缩编码技术和算法得到迅速发展与应用。

(3) 信道纠错编码的发展

在研究香农信源编码定理的同时,另外一部分科学家从事寻找信道最佳编码(纠错码)的研究工作。这一工作已取得了很大的进展,并已经形成一门独立的分支——纠错码理论。

纠错码的出现应归功于理查德·汉明。早在 1950 年,汉明第一个提出了纠正一位错误的编码方法,目的是为使贝尔实验室的计算机具备有检测错误能力的运行程序。由此汉明码的纠错思想成为了线性分组码的基本指导思想。接着,Golay(戈雷)提出了纠二位和三位错误的戈雷码。1954 年 Muller 和 Reed 突破了码的参数固定不变的限制,提出新的分组码 RM 码。随之,1957 年,E. Prange 在线性分组码中找到子类的循环码。人们在对循环码和线性分组码的广泛、深入地研究

基础上,形成了系统的理论,即代数编码理论,使其成为应用数学的一个分支。但代数编码的渐近性能较差,难以实现香农信道编码定理所指出的结果。为此,1955 年埃利斯(P. Elias)提出卷积码的思想。1960 年左右提出了序列译码方法,门限译码方法,特别是以维特比(Viterbi)为代表的、基于概率和软判决的最大似然译码算法的提出,使卷积码迅速得到广泛应用。如"先驱者"号太空探测器,木星和土星探测器,以及移动通信领域中欧洲的 GSM 标准系统和北美 IS—95 标准等都采用了卷积码技术。然而科学家们并没有停止对构造好码和逼近香农极限的优异码的研究。先后研究提出了级联码(将两个短码串行级联使用),乘积码及交织(或交错)技术等新的方法。在 20 世纪 80 年代前后,又提出了一种网格编码调制方案(TCM),它将编码和调制结合起来,在不扩展信道带宽情况下提高了系统的功率,从而增强了系统的抗干扰能力。近年来,Turbo 码、LDPC 码的提出和研究,发现了这两种码的误比特率与香农极限相差无几的优异性能。由此不但引起了新的研究热潮,而且使人们更加清晰地认识到香农信道编码理论是真正具有实用意义的科学理论。

(4) 限失真信源编码的提出和发展

限失真信源编码的研究较信道编码和无失真信源编码落后十年左右。香农在 1948 年论文中已体现出了关于率失真函数的思想。一直到 1959 年他发表了"保真度准则下的离散信源编码定理",首先提出了率失真函数及率失真信源编码定理。从此,发展成为信息率失真编码理论。1971 年伯格尔(T. Berger)给出更一般信源的率失真编码定理。1971 年伯格尔著作的《信息率失真理论》[10]一书是一本较全面地论述有关率失真理论的专著。率失真信源编码理论是信源编码的核心问题,是频带压缩、图像和多媒体等数据压缩的理论基础。有关率失真信源编码理论本身尚有许多问题有待进一步的研究,所以它直至今日仍是信息论的重要研究课题。有关数据压缩、多媒体数据压缩,图像压缩等又是另一独立的分支——数据压缩理论与技术。

近 30 多年来,有关数据压缩理论和技术都发展得非常迅速,取得大量的成果。而且还制定了一系列关于限失真数据压缩的技术标准和建议:语音压缩编码有 CCITT G. 722、G. 723、G. 728 等标准;静态图像压缩标准 JPEG;动态图像压缩标准 MPEG-2、MPEG-4、MPEC-21 等;视频编码标准H. 261、H. 263、H. 264 等。这些压缩技术标准的出现标志着数据压缩理论和技术研究已进入了成熟时期。

当然,这其中尚存在许多问题,这不仅需要在数据压缩理论和技术方面做进一步研究,而且更需要从率失真信源编码理论的深入研究中获得理论指导。

(5) 多用户、网络信息论的发展

香农 1961 年的论文"双路通信信道"开拓了网络信息论的研究。

1970 年以来,随着卫星通信、计算机通信网的迅速发展,网络信息理论的研究异常活跃,成为当时信息论的中心研究课题之一。

1971 年艾斯惠特(R. Ahlswede)和 1972 年廖(H. Liao)给出了多元接入信道的信道容量区。1973 年斯莱平(D. Slepian)和沃尔夫(J. K. Wolf)研究了两个特定相关信源在多元接入信道中信息的传输问题,以及无记忆相关信源编码问题,并最早给出了无记忆相关信源的编码定理(Slepian-Wolf 定理)。随后,Keilers(1976 年)、Ozarow(1979 年)和 Carleisl(1977 年与 1982 年)等分别讨论了特定的高斯多元接入信道、具有反馈的 AWGN 多元接入信道及具有反馈的多元接入信道。而科弗尔(T. M. Cover)、艾斯惠特(R. Ahlswede)又于 1980 和 1983 年分别发表文章讨论相关信源在多元接入信道的传输问题。

1972 年科弗尔提出了广播信道的研究。伯格曼斯(P. Bergmans)(1973)、格拉格尔(R. G. Gallager)(1974)、科弗尔(1975)、马登(K. Marton)(1979)、伊·盖马尔(A. El Gamal)(1979)和范·德·缪伦(E. C. Van der Meulen)(1979)等分别研究了广播信道的容量区问题。只有降阶广播信道的容量区得以解决。有关中继信道的研究,由范·德·缪伦(1977)首先引入,科弗尔和伊·盖马尔找到了降阶中继信道的容量区(1979)。

1985 年范·德·缪伦曾对广播信道研究的进展和多元接入信道研究的进展做了较全面的概述。

20 世纪 70 年代以后,这一领域研究活跃,发表了大量的论文,但 20 世纪发表的论文所讨论的具体分析策略和结论很难推广应用到一般的实际通信网模型中。

21 世纪最初几年,以香港中文大学杨伟豪和李硕教授发表的“网络信息流”(2000 年)和“线性网络编码”(2003 年)及美国学者 Gupta 和 Kumar 提出的“无线网络的传输容量”(2000 年)和“无线通信的网络信息论”(2004 年)等为代表,他们将编码处理技术引入到网络层,拓宽了网络信息论的研究方法和研究视角,使网络信息论的研究取得突破性的进展。近年来,随着互联网通信,移动通信的迅猛发展,更激起了学术界对网络编码,网络信息论广泛重视和研究,网络信息论的研究已成为通信信息理论和技术研究的新热门领域。

(6) 信息保密与安全理论的提出和发展

关于保密理论问题,香农在 1949 年发表的“保密通信的信息理论”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。他将信息保密与安全问题引入了科学的轨道,为保密理论和密码学的发展奠定了理论基础。

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“密码学的新方向”一文,提出了公开密钥密码体制,揭开了密码学的神秘面纱,使密码学得到了广泛地研究和发展,从而进入了一个崭新的研究阶段。

尤其当今,进入了网络经济时代,信息的安全和保密问题更加突出和重要。人们把线性代数、数论、矩阵、近世代数等引入保密问题的研究,已形成了独树一帜的分支——密码学理论。

纠错码和密码学本来是两门不同的学科,而自从 1978 年伯利坎帕(E. R. Berlekamp)、麦克利斯(R. J. McEliece)和范·蒂尔鲍(H. C. A van Tilborg)证明了纠错码中一般线性分组码的译码问题是一个难解的数学问题。同年 McEliece 又首先构造了基于纠错码的公开密钥密码体制。从此以后,纠错码和密码学相结合的研究迅速发展起来。

近年来,在信息安全和密码学方面值得关注的新动向是量子密码学和光学信息安全学。他们是新一代的信息安全理论与技术,是极具发展前景的交叉科学。

目前,在香农信息论方面,还值得注意的研究动向是:

信息概念的深化;

网络信息理论和多重相关信源编码理论的发展和应用;

通信网的一般信息理论研究;

磁记录信道的信息理论研究;

信息率失真理论的发展及其在数据压缩和图像处理中的应用;

信息论在大规模集成电路中的应用等问题。

这些领域都是与当前信息工程的前景——光通信、空间通信、计算机互联网、移动通信、多媒体通信、语音和图像的信息处理等密切相关的。

3. 信息论与信息科学

现在,信息理论与技术不仅在通信、计算机和自动控制等电子学领域中得到直接的应用,而且还广泛地渗透到生物学、医学、生理学、语言学、人文学、社会学和经济学等各领域。在信息论与数学、物理、自动控制、系统工程、人工智能、生物学、电子计算机等学科互相渗透,互相结合的基础上,形成了一门综合性的新兴学科——**信息科学**。

信息科学作为一门独立的学科,它是以信息作为主要研究对象,以信息的运动规律和利用信息的原理作为主要的研究内容,以信息科学方法论作为主要的研究手段,以扩大人类的信息功能(特

别是智力功能)为主要的研究目标的一门新兴学科。

信息科学的研究对象是客观事物的信息属性,这是信息科学区别于传统自然科学而具有独立存在性和广阔发展前景的基本依据。

宇宙间万物世界,都是聚物质、信息、能量于客观事物一身。信息性与物质性、能量性一样,是客观事物最基本的属性。信息是无所不在的,它存在于自然界、存在于人类社会中,还存在于人的大脑之中。而信息科学正是以这无所不在的信息作为自己的研究对象,展开其自己的广阔研究领域。显然,信息科学的研究范围要更广阔,涉及的内容也更复杂,更深刻。

可以认为由这些交叉学科相结合基础上形成的,以信息量为重要度量的学科分支都可看作信息科学的分支学科。近年来,逐渐形成的**光学信息论、量子信息论、生物信息论**或**生物信息学**都是信息科学的重要分支。尤其近几年,量子信息科学不断地取得大量的、有成效的、引人瞩目的成果,量子信息科学将会是今后信息科学发展的重要领域。

广义地认为,信息科学由信息科学理论、信息应用技术和信息科学方法三者组成。

信息科学理论主要包含信息定性理论、信息定量理论和信息应用理论。

信息应用技术,狭义地说,它是扩展人的信息功能的技术。它包括获取信息、传递信息、加工处理信息、存储信息等代替和延伸人的感官及大脑的信息功能的技术。所以,主要包括四个主要方面:信息获取技术(感测技术)、信息传递技术(电信技术)、信息加工处理技术(计算机技术)及信息控制技术(自动智能控制技术)。

信息科学方法是人类以信息作为窗口去认识世界和改造世界全过程的一整套方法,由信息分析方法和信息利用方法两大部分组成。它包括:信息的获取方法、信息的传递方法、信息的加工处理方法、信息的存储方法、信息的描述和度量方法及信息的调控和利用方法。信息科学方法就是信息科学理论的应用手段。它是适应信息科学研究的需要而产生的一种同传统的科学研究方法截然不同的科学研究方法,并将随着信息科学理论的发展而不断完善。

信息科学理论、信息科学技术和信息科学方法三者之间既有区别,又相互联系和作用而构成信息科学的总体。正是它们在这样的相互依赖、相互促进中交相辉映、共同发展,使人类对信息的认识和利用上升到一个新的水平,把人类推入了高度化发展的信息社会。

毫无疑问,随着信息论和信息科学的发展,人们将会揭示出客观世界和人类主观世界更多的内在规律,从而使人们有可能创造出各种性能优异的信息获取系统、信息传输系统、信息控制系统及智能信息系统,使人类进一步从自然力的束缚下得到解放和自由。