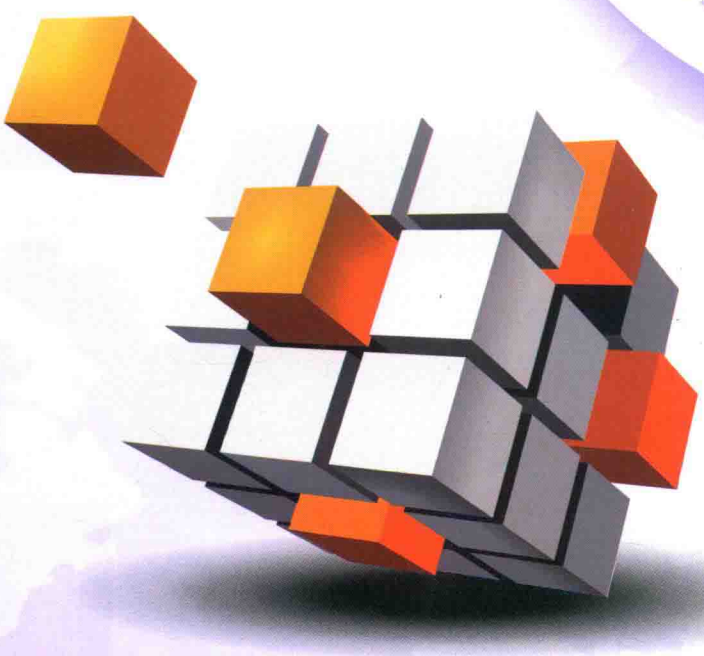
信息论

XINXILUN DAOYIN

导引（第二版）

主编◎徐政五　甘　露　汪利辉



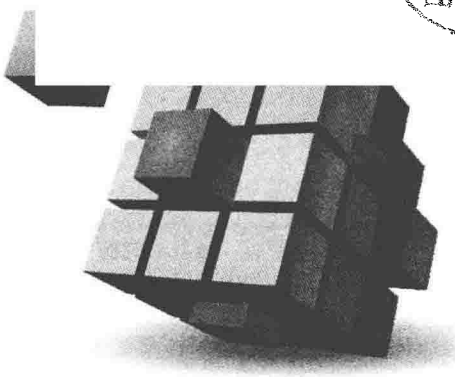
电子科技大学出版社

信息论

XINXILUN DAOYIN

导引（第二版）

主编 徐政五 甘 露 汪利辉



电子科技大学出版社

图书在版编目(CIP)数据

信息论导引/徐政五，甘露，汪利辉主编. —2版.
—成都：电子科技大学出版社，2017.2
ISBN 978-7-5647-4199-0

Ⅰ. 信… Ⅱ. ①徐… ②甘… ③汪… Ⅲ. ①信息论
Ⅳ. ①G201

中国版本图书馆CIP数据核字（2017）第034293号

内 容 简 介

本书共分七章，主要讲述信息论的基本理论和方法。内容包括：信息的性质、研究范围和有关随机信号方面的数学预备知识；以香农理论为基础，研究信息度量的方法和信源熵等；信源的匹配编码及编码问题的一般解法；信道的分类、信道容量计算及多用户信道；有关信息率失真函数的概念、性质及信息率失真函数的计算；分析线性分组码、循环码和卷积码编码；信息加密的一般原理和方法、数据加密标准的基本概念等。

本书选材恰当、难易程度适中、推理严谨、逻辑性强且文字流畅，适用于电子学与通信学科各专业学生作为教材使用，也可作为技术人员在工程实践中参考。

信息论导引（第二版）

徐政五 甘露 汪利辉 主编

出　　版：电子科技大学出版社（成都一环路东一段159号电子信息产业大厦　邮编：610051）
策划编辑：周清芳　徐守铭
责任编辑：周清芳　徐守铭
主　　页：www.uestcp.com.cn
电子邮箱：usetcp@uestcp.com.cn
发　　行：新华书店经销
印　　刷：成都蜀通印务有限责任公司
成品尺寸：185mm×260mm　**印张** 14　　**字数** 350千字
版　　次：2017年2月第二版
印　　次：2017年2月第一次印刷
书　　号：ISBN 978-7-5647-4199-0
定　　价：32.80元

前　言

信息科学是一门涉及面极广的新兴科学，其任务是研究信息的性质、获取、传输、检测、存储、处理、控制的基本原理和方法。它的理论基础是从通信科学发展起来的近代信息论。而 C. E. 香农是近代信息论的奠基人。

随着计算机科学的发展和信息化的需求，信息论学科有了很大发展，并从通信技术领域延伸到其他领域中，诸如文字学、语言学、心理学、经济学、生物科学等。

信息论导引是一门为信息科技为主的各种不同专业学生开设的公共课程，本书是介绍信息论的基本理论和方法的导引性教材，共分七章：第一章引论，主要介绍信息的性质和研究范围，并附加了有关随机信号方面的预备知识；第二章信息论基本概念，主要以香农理论为基础，研究信息度量方法和信源熵等；第三章无失真信源编码，主要介绍信源的匹配编码和编码问题的一般解法；第四章信道，主要介绍信道的分类、几种不同信道模型的信道容量计算及多用户信道的概念。第五章离散信源的限失真信源编码，主要介绍了失真函数、信息率失真函数的概念、性质及信息率失真函数的计算。第六章信道编码，主要论述了分组码和卷积码的编码与译码。第七章信息加密技术，主要介绍了信息加密的一般原理和方法，以及数据加密标准的基本概念。本书适用于电子学与通信学科的本科生、研究生及科学技术人员。

原版教材第 1 章由李立萍编写、第 2 章、第 3 章、第 4 章和习题由徐政五编写；第 5 章、第 6 章和第 7 章由汪利辉编写，并由西南交通大学诸昌铃教授和成都理工大学郭勇教授主审。在此，对李立萍教授表示深切怀念和诚挚谢意。

再版教材对原书的部分内容和错误进行了修订及纠正。全书由徐政五统稿和终校，甘露教授为教材的修订提出了宝贵的意见和建议，王宏副教授、张花国副教授、李万春副教授对教材的修订付出了大量的精力和时间。

电子科技大学出版社对本书的出版给予了很大的支持，在此致以谢意。

由于编者水平有限，书中难免有错误和不当之处，殷切希望读者批评指正。

编　者

2016 年 10 月

目　录

第一章 引 论

现代信息论也称狭义信息论，是在20世纪由美国工程师C. E. Shannon（1948年）奠基的一门崭新学科。至今，随着计算机科学的发展和信息化的需求，信息论学科有了很大发展，并从通信技术领域延伸到许多其他领域中，诸如文字学、语言学、心理学、经济学和生物科学等方面。本章主要讨论信息的基本概念和特征以及信息论研究的内容，并简述研究信息论必备的概率论和随机信号统计特性方面的知识。

1.1 信息论的起源和发展史

现代信息论作为真正意义上的一门科学，是从1924年奈奎斯特（H. Nyguist）解释了信号带宽和信息率之间的关系以及1928年哈脱莱（R. V. Hartley）引入了非统计（等概率事件）信息量概念的工作开始的。直到1948年美国数学家香农（C. E. Shannon）发表了两篇有关“通信的数学理论”的文章，讨论了信源和信道特性，并用概率测度和数理统计的方法，系统地阐述了通信的基本问题，得出了几个重要且带有普遍意义的结论，由此奠定了现代信息论的基础。

20世纪50年代维纳（N. Wiener）和卡尔曼（R. E. Kalman）提出的维纳滤波理论和卡尔曼滤波理论以及20世纪70年代凯纳思（T. Kailath）等人提出的信息过程理论是信息论的重大发展。

1961年，香农发表的论文“双路通信信道”开拓了多用户理论的研究，该理论随着卫星通信、计算机通信网络的迅速发展取得了许多突破性的进展。

随后50多年来，信息理论与技术无论在基本理论方面还是在实际应用方面都取得了巨大的进展。在香农理论基础上给出的最佳噪声通信系统模型，近年来正在成为现实，这就是伪噪声编码通信系统的迅速发展和实际应用。在噪声中对信号过滤与检测基础上发展起来的信号检测理论和在抗干扰编码基础上发展起来的编码理论已成为近代信息论的两个重要分支。此外，简尼斯（E. T. Jaynes）提出的最大熵原理和库尔拜克（S. Kullback）提出的最小鉴别信息原理，为功率谱估计等应用提供了理论依据。还相继展开了模糊信息、相对信息、主观信息、智能信息处理以及自动化信息控制等大量崭新的课题研究，使信息理论的面貌为之一新，并将大大促进信息科学的发展。

现在，信息理论与技术不仅直接应用于通信、计算机和自动控制等领域，而且还广泛渗透到生物学、医学、语言学、社会学和经济学等领域。特别是通信技术与微电子、光电子、计算机技术等相结合，使现代通信技术的发展充满生机与活力。

1.2 信息的定义

在人类认识和改造自然界的过程中都离不开获取自然界的信息。所谓信息，是指存在于客观世界的一种事物形象，一般泛指消息、情报、指令、数据和信号等有关周围环境的知识。凡是物质的形态、特性在时间或空间上的变化，以及人类社会的各种活动都会产生信息。千万年来，人类利用自己的感觉器官从客观世界获取各种信息，如语言、文字、图像、颜色、声音和自然景物等，可以说，我们是生活在信息的海洋之中，因此获取信息的活动是人类最基本的活动之一。

所谓信号，是指消息的表现形式，是带有信息的某种物理量，如电信号、光信号和声信号等。因为消息的传送一般都不是直接的，而必须借助于一定形式的信号才能便于远距离快速传输和进行各种处理。由于信号是带有信息的某种物理量，这些物理量的变化包含着信息。因此，信号可以是随时间变化或随空间变化的物理量。在数学上，信号可以用一个或几个独立变量的函数来表示，也可以用曲线图形表示。

所谓消息，是指用来表达信息的某种客观对象，如电报中的电文，电话中的声音，电视中的图像，雷达的目标距离、高度、方位等参量都是消息。在我们得到一个消息后，可能得到一定数量的信息，而我们所得到的信息，显然与我们在得到消息前对某一事件的无知程度以及得到后对同一事件的无知程度有关。

例如，由发送端发出的消息 A，在接收端可以看成某一随机事件，在没有收到任何消息之前，它的出现概率 $P(A)$（先验概率）显然和消息 A 所含有的信息多少有关。如果在接收端事先已知 A 必然发生（消息 A 一定发送），则 A 为必然事件；$P(A)=1$，那么，事实上等于没有传递任何信息或者说传递的信息量等于零。反之，如果事先认定 A 几乎不可能发生，即 A 为小概率事件，$P(A)\approx 0$。但是，当我们在接收端突然发现它居然发生了，事实上，这的确是一条令人惊奇的消息，它含有我们完全不知的信息，或者说，这一消息含有极大的信息量。例如，一封“母病重、速归”的电报，如果收报人的母亲一直很健康，那么，这封电报就会使他感到突然和震惊。换句话说，这封电报便含有很大的信息量（“母病重”这一事件对于收报人来说，出现的概率是很小的）。反之，如果在收到这封电报前，收报人已知其母年迈体衰，新染恶疾，那么，这封电报便是意料之中的了。换言之，它并没有带来更多的信息。由此，我们可把信息与消息在含义上的区别概括为：信息是消息中不确定性的消除（也就是该消息给予受信者的新知识），消息就是知道了的信息。尽管信息一词仍然会感到含义模糊和难以捉摸，但人人都感觉到它的存在。这种目前尚难明确定义的信息我们称其为广义理解的信息。

传统科学的基本概念是物质和能量，而信息科学的基本概念就是信息。香农提出概率信息的概念（称为香农信息或狭义信息），是从不确定性（随机性）和概率测度给信息下定义的。香农从信源具有随机性不定度出发，为信源推出一个与统计力学的熵相似的函数，称为信息熵，而这个熵就是信源的信息选择不定度的测度，从而我们可以认为：信息表征信源的不定度，但它不等于不定度，而是为了消除一定的不定度必须获得与此不定度相等的信息量。

信息作为一个可以用严格的数学公式定义的科学名词首先出现在统计学中，随后又出现在通信技术中。无论是在统计数学中还是在通信技术中定义的信息都是一种统计意义上的信息，我们可以把它简称为统计信息。统计信息是非常明确的，同时其适用范围要比广义信息狭隘得多。我们在本书中讨论的信息论正是关于这种统计信息的理论。

信息本身是看不见、摸不着的，它必须依附于一定的物质形式，如文字、声波和电磁波等，这种运载信息的物质称为信息的载体。一切物质都有可能成为信息的载体。有人这样认为：在人类社会中，从原始社会人们利用手势、声音和火光这类非语言传播发展到语言传播是人类信息传播史上的第一次革命。文字的出现，印刷术、纸张的发明和推广应用，使人类社会的信息传播打破了时间与空间的障碍，标志着信息传播的第二次革命。第三次信息传播革命是与电磁波传播媒介联系在一起的，如电报、电话、无线电广播、电视乃至通信卫星等一系列现代电磁波传播媒介的出现，使人类收集和传递信息的能力大大提高，这是人类信息传播史上具有划时代意义的革命。21 世纪，人类正步入信息高速公路时代，因此，信息论吸引了众多领域的学者们注意，他们竞相应用信息论的概念和方法去理解和解决本领域中的问题。

1.3 信息的特征和性质

信息和能源、物质材料不同，它具有许多异于后者的特殊性质，分析研究信息的特征有助于加深对信息概念的理解。不同的信息经过归纳后将呈现出它的特征，将有助于我们从纷繁复杂的信息表象中了解信息的本质。

1.3.1 信息的特征

信息的特征是信息所特有的征象，是信息区别于其他事物的本质属性。信息具有如下几方面的特征：

(1) 信息的客观性。信息是事物变化及其状态变化的表现。由于事物及其状态、特征的变化是不以人们意志为转移的客观存在，所以反映这种客观存在的信息，同样带来客观性。信息不仅其实质内容具有客观性，而且一旦形成，其本身也具有客观性。

(2) 信息与载体的不可分割性。在人类社会的信息活动中，各种信息必须借助于文字、图像、胶片、磁带、声波和光波等物质形态的载体，才能够表现，才能为人们的听觉、视觉、味觉、嗅觉和触觉所感知，人们才能够识别信息和利用信息，信息与信息载体是不可分割的。从某种意义上说，没有信息载体就没有信息本身。

(3) 信息的价值性。信息本身不是物质生产领域的物化产品，但它一经生成并物化在载体上就是一种资源，具有可用性。信息具有使用价值，能够满足人们某些方面的需求，为社会服务。信息具有在一定程度上代替物质和劳动力资源的作用，最明显的事例是通信业的发展可以大大减少人员的流动及实物的流通总量和运输距离。

(4) 信息的时效性。信息的时效性是指信息从发生、接受到利用的时间间隔及效率。信息是有寿命、有时效的。信息的使用价值与其所提供的时间成反比，时间的延误会使

信息的使用价值衰竭，甚至完全消失。

(5) 信息的可分享性。信息的可分享性是指信息的共享性。信息的交流与实物的交流有着本质的区别。实物交流，是一方得到的正是另一方所失去的；而信息的交流，是一方得到新的信息，而另一方并无所失，双方或多方可共享信息。这说明信息的生产成本不取决于其被使用的规模。信息的共享性使信息资源易于扩散，使信息得到比物质资源更广泛的开发利用。

(6) 信息的可传递性。可传递性是信息的一个重要特征，信息的传递是通过信道来进行的。信源发出信息后，经由信道传递至信宿，信息系统就是由信源、信道和信宿组成的有机整体。信息的传递手段和方式多种多样，信息传递的快慢，对于信息的效用和价值至关重要。

(7) 信息的可扩散性。信息具有可扩散性，通过各种渠道和传输手段迅速散布开去的信息容易获得，但也容易被滥用，而且信息一旦扩散，就不可回收。

(8) 信息的可加工性。客观世界存在的信息是大量的、多种多样的，人们对信息的需求往往具有一定的选择性。为了更好地开发和利用信息，需要对大量的信息用科学的方法进行筛选、分类、整理、概括和归纳，使其精炼浓缩，排除无用信息，选取自己所需要的信息；而且可从大量零星、分散的信息中找出带有普遍性和具有规律性的信息。信息还具有可变换性，它可以从一种形态转变为另一种形态，如物质信息可转换为语言、文字、数据和图像等形式，也可以转换为计算机语言、电信号等。同样一条信息可以用多种不同的载体来记录。

(9) 信息的可再现性。信息的可再现性包括两方面的含义：一是信息作为客观事物的一种反映，它为人们所接受、认识的过程也是客观事物的再现过程；二是信息的内容可以物化在不同的载体上，传递过程中经由载体的变化而再现相同的内容。

(10) 信息的可存储性。信息反映的内容是客观的，信息的客观性决定了信息具有可存储性，有时加工处理后的信息并非立即要用，有的当时虽然用了，但以后还可作参考，这样就可以对信息进行存储。信息的存储和积累使人们能够对信息进行系统的、全面的研究和分析，使信息可以延续和继承。

(11) 信息的积累性。信息的积累性是由信息的可存储性决定的。人类知识宝库不断丰富和扩充的过程，就是信息经过系统化、抽象化和规律化而形成知识长期积累的过程。

(12) 信息的延续性和继承性。信息不同于物质产品的消耗，它具有延续性和继承性的特点。信息的作用是延绵千古、地久天长的。它可以年复一年地被记忆、保存。直接探索、认知和获取一个未知事物的信息是极其困难的，而接受、理解并继承一个信息则要简单容易得多。

(13) 信息的可开发性。信息作为客观事物的一种反映，由于客观事物的复杂性和事物之间相互关联性的特点，反映事物本质的和非本质的信息往往交织在一起。又由于在一定的历史阶段，人们认识上存在一定的局限性，因此，获取信息是需要开发的。

(14) 信息的可再生性和可增值性。信息具有确定性的价值，但在不同的时间、地点，对不同的人又有不同的意义，并且这种意义还可以引申、推导和繁衍出更多的意义，从而使信息增值。信息的再生性，使它成为人类社会取之不尽、用之不竭的资源。

1.3.2 信息的性质

性质 1 普遍性：信息是普遍存在的。

信息是事物运动的状态和状态改变的方式，因此，只要有事物存在，只要有事物的运动，就会有它们运动的状态和方式，就存在着信息。无论在自然界、人类社会，还是在人们的思维领域，绝对的“真空”是没有的，绝对不运动的事物也是没有的，因此，信息普遍存在。

性质 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。

一切事物运动的状态和方式都会产生信息，而宇宙时空中的事物是无限丰富的，因而它们所产生的信息也必然是无限量的，即使在有限的空间中，比如在地球上，事物也是无限多样的。而在无限的时间长河中，事物的发展变化更是无限的，因而信息自然也是无限的。

当然，这里也有实在信息与实得信息的区别。人们的实得信息可能是有限的，但作为总体而言的实在信息是无限的。实际上，人类实得信息的总量是宇宙时空中总体实在信息总量的一个极小部分。

性质 3 相对性：对于同一个事物，不同的观察者所获得的信息量可能不同。

由于不同的观察者有着不同的观察力、不同的理解力和不同的目的性，因此，从同一个事物所获得的信息量（实得语法信息量、实得语义信息量以及实得语用信息量）肯定各不相同，这在理论上是不言而喻的。假定事物 X 的实在信息量 $I(X)$ 是常数，在这样的条件下，第 i 个观察者 R_i 的实得信息量 $I(X,R_i)$ 就为：

$$I(X;R_i) = I(X) - I_0(X;R_i), i = 0,1,2,\cdots$$

既然各个观察者的先验信息量 $I_0(X;R_i)$ 各不相同，它们的实得信息量 $I(X;R_i)$ 当然也各不相同。信息的这个性质告诉我们实得信息量是因人而异的。了解这一点对于处理实际问题十分重要。

性质 4 转移性：信息可以在时间上或在空间中从一点转移到另一点。

由于信息具有脱离母体而相对独立的能力，因而它就可以通过一定的方法使之在时间上或在空间中进行转移。在时间上的转移称为存储；在空间中的转移称为通信。其实，存储也是一种通信：今天与明天的“通信”，或者今天与后天的“通信”。当然，信息在空间中的转移必然也伴有时间上的转移，因为它在空间中转移的速度是一有限值。信息可以在时间上和在空间中转移，这是一个十分有用的性质，它使人类的知识能够积累和传播，使人与人之间能够进行信息的交流，使人与其环境之间能够保持信息的联系，从而能够更好地认识环境和改造环境。

性质 5 变换性：信息是可变换的，它可以由不同的载体和不同的方法来载荷。

既然信息是事物运动的状态和方式，而不是事物本身，它就可以负载在其他一切可能的物质载体和能量形式上。例如，投掷硬币这一试验的结果当然是一种信息，我们可以用数字 0 和 1 来表示，或者可用电流的正和负来表示，也可以用机械位置的高和低来表示，甚至以表情上的哭与笑来表示。实际上，只要能够保持“运动的状态和状态的改

变方式”具有不变性，那么，它就不仅可以在各种物质和能量形式之间进行变换，而且可以经受一切不会破坏“信息不变性”的数学变换。信息的这一性质也是很有用的，它使人们对信息施行各种各样的处理和加工成为可能。

性质 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。

本体论层次的信息是事物运动的状态和方式，认识论层次的信息是认识主体所感知和表述的事物运动的状态和方式。* 获得了信息，就可以消除认识主体对于事物运动状态和方式的不定性。后面还会看到，语法信息中的概率信息量就是负熵，它是混乱程度的对立面。一个系统要想从无序状态转变为有序状态，就必须从外界获得信息（负熵）。这是自组织理论导出的基本结论，信息的这一性质使信息对人类具有特别重要的价值。

性质 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。

信息是事物运动的状态和状态改变的方式，事物本身在不断地发展变化，因此，信息也会随之变化。脱离了母体的信息因为不再反映变化了的母体的新的运动状态和方式，它的效用就会逐渐降低，以至完全失去效用。这就是信息的时效性。信息脱离母体并不能完全反映母体实际的运动状态和方式，这个信息的寿命就到了尽头。到这时，它至多只能作为母体运动状态和方式的一种历史记录。所以人们在获得信息之后，并不能就此满足，更不能一劳永逸。信息要及时发挥效用，知识要不断补充更新。

性质 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。

由此可知，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目的。

1.4　现代信息技术的含义和基本内容

1.4.1　现代信息技术的含义

前面我们已提到，本书讲述的信息论是关于统计信息的理论。从技术本质的意义上看，信息技术就是能够扩展人的信息器官（感觉器官、传导神经网络、思维器官和效应器官）功能的一类技术。

1.4.2　信息技术的基本内容

近代信息技术的基本内容包括感测技术、通信技术、智能技术及控制技术，即信息

---

* 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。将涉及形成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。

技术四基元。

(1) 感测技术。感测技术包括传感技术和测量技术，如遥感、遥测技术等，它们是感觉器官功能的延长。

(2) 通信技术。通信技术的功能是传递信息，它是传导神经网络功能的延长。

(3) 智能技术。智能技术包括计算机硬件技术、软件技术、人工智能技术和人工神经网络等，它们是思维器官功能的延长，能更好地加工和再生信息。

(4) 控制技术。控制技术的功能是根据输入的指令信息（决策信息）对外部事物的运动状态和方式实施干预，是效应器官功能的扩展和延长。

信息技术是人的信息器官功能的延长。信息技术四基元的关系也是一个有机的整体，它们和谐有机地合作，共同完成扩展人的智力功能的任务。

信息技术四基元及其功能系统完全与人的信息器官及其功能系统相对应。信息技术的功能和人的信息器官的功能是一致的，只是功能的水平或性能各有高低。通信技术和智能技术处在整个信息技术的核心地位，而感测技术和控制技术则是核心与外部世界之间的接口。没有通信技术和智能技术，信息技术当然就失去了基本的意义；而没有感测技术和控制技术，信息技术同样也是没有意义的：一方面，没有信息的来源；另一方面，信息也没有归宿。可见，信息技术的四基元是一个完整的体系。这便是信息技术的内部结构。

1.4.3 在通信领域中信息技术的基本内容

归纳起来，在通信领域中信息技术研究的内容，主要包括以下几个方面。

(1) 通信的统计理论研究

主要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) 信源的统计特性研究

信源的统计特性主要包括：

① 文字（如汉字）和字母（如英文）的统计特性；

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) 受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、生理学和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，它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，它主要针对信道统计特性进行编码，所以有时也称为信道编码；

③ 计算机中的容错问题。

(5) 提高信息传输效率的研究

主要包括：

① 功率的节约（如降低信息传输所需的功率）；

② 频带的压缩（如语音信号压缩、图像信号压缩和计算机文件的压缩等）；

③ 传输时间的缩短和可靠性的保证（如模拟话路中数据传输速率的提高；计算机网络中数据传输可靠性的保证等）。

(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 理想接收机的实现。

(7) 噪声中信号检测和估计理论与技术的研究

主要包括：

① 信号检测的最佳准则；

② 信号最佳检测的实现；

③ 信号最佳估计的准则和实现。

(8) 图像信号的复原与重建和模式识别问题与树分类器的设计等。

1.5 预 备 知 识

1.5.1 概率论的基本知识

研究概率论的方法是以集合论为基础，集定义为点（或元素）的组合。直观地讲，一个集合就是一些事物的总和。在概率论中，这些“事物”就是基本事件。由此，我们可以确定任一个具体的点是否为集中的点（或元素）。实验（或测量）的可能结果组成的点集，常称为样本空间。随机变量 x_k 是定义在样本空间上的集函数，即对样本空间上的每一点 k，都有 $-\infty$ 至 $+\infty$ 之间的一个实数 x_k 与之对应。

在概率论中，以不同的方式组合在一起的点集都称为事件。在一定的条件下，每个事件有一个概率函数。也就是说，在相同条件下进行多次重复实验之前，我们可以粗略地预言，什么将要发生，但不能精确地预言它的结果。例如，掷一枚硬币，大约有一半的次数是国徽向上，但在试验前不能预言究竟出现哪一面。增加同一试验的次数，就会发生与某一总的平均值一致的趋向，称之为统计的规律性，这完全是真实的。在统计的

规律中，其数学模型往往是建立在归纳的基础上的，常用的数学研究工具是概率论和数理统计。

下面我们简介一些概率论的基本知识。

(1) 随机事件。在随机试验中，对一次试验可能出现也可能不出现，而在大量重复试验中却具有某种规律性的事情，称为此随机试验的随机事件，简称事件。

(2) 事件之间的关系与事件的运算。设随机试验 E 的样本空间为 S，A、B 是随机试验 E 的事件，则：

① 若事件 A 发生必然导致事件 B 发生，则称事件 B 包含事件 A，记为 $B \supset A$。

② 若事件 A 与事件 B 至少有一个发生，则这一事件称为事件 A 与事件 B 的和，记为 $A \cup B$。

③ 若事件 A 与事件 B 同时发生，则这一事件称为事件 A 与事件 B 的积，记为 $A \cap B$。

④ 若事件 A 发生而事件 B 不发生，则这一事件称为事件 A 与事件 B 的差，记为 $A-B$。

⑤ 若事件 A 与事件 B 不能同时发生，亦即 $AB=\varphi$，则称事件 A 与事件 B 是互不相容的，基本事件是互不相容的。

(3) 概率的定义。设 E 是随机试验、S 是它的样本空间。对于 E 的每一事件 A 赋予一实数，记为 $P(A)$，称为事件 A 的概率。

(4) 概率的性质。

① 设 $\overline{A}$ 是 A 的对立事件，则：

$$P(A) = 1 - P(\overline{A}) \tag{1-1}$$

$$P(\varphi) = 0 \tag{1-2}$$

② 设 A、B 为两个事件，则：

$$P(A \cup B) = P(A) + P(B) - P(AB) \tag{1-3}$$

③ 设 A、B 为两个事件，若 $B \supset A$，则：

$$P(A) \leqslant P(B) \tag{1-4}$$

(5) 条件概率。设 A、B 为随机试验 E 的两个事件，且 $P(A) > 0$，则称：

$$P(B \mid A) = \frac{P(AB)}{P(A)} \tag{1-5}$$

为事件 A 发生的条件下事件 B 发生的条件概率。

(6) 全概率公式。

定义 1.1 设 S 为随机试验 E 的样本空间，$B_1, B_2, \cdots, B_n$ 为 E 的一组事件，若 $B_iB_k = \varphi$ $(i \neq k)$，$B_1 \cup B_2 \cup \cdots \cup B_n = S$，则称 $B_1, B_2, \cdots, B_n$ 为样本空间的一个划分。

若 $B_1, B_2, \cdots, B_n$ 是 S 的一个划分，那么，做一次试验 E，事件 $B_1, B_2, \cdots, B_n$ 中必有一个且仅有一个发生。

若 A 为 E 的事件，则全概率公式为：

$$P(A) = P(A \mid B_1)P(B_1) + P(A \mid B_2)P(B_2) + \cdots + P(A \mid B_n)P(B_n) \tag{1-6}$$

(7) 贝叶斯 (Bayes) 公式。设 $B_1, B_2, \cdots, B_n$ 为样本空间 S 的一个划分，且 $P(B_i) > 0$ $(i = 1, 2, \cdots, n)$。对于任一事件 A，$P(A) > 0$，由条件概率的定义有：

$$P(B_i \mid A) = \frac{P(B_iA)}{P(A)} = \frac{P(A \mid B_i)P(B_i)}{P(A)}$$