

信息理论基础

周炯槃编著·人民邮电出版社

信息理论基础

周炯槃 编著

人民邮电出版社

1110787

10022/10
内 容 提 要

本书重点介绍仙依信息论的一些基本观点，力图把信息论和它的一些应用联系起来。为了在较广泛的意义上研究信息论，本书第一部分介绍了一些集合论和概率论的基本知识。

本书第二部分介绍仙依信息论，包括信源和它的度量值——熵的概念，信道与信道容量；信源和信宿之间的平均失真以及信息率失真函数；最后介绍编码定理。

本书可作为通信院校信息论课程的教材，也可供从事信息论研究的数学、科研、工程技术人员参考。

信 息 理 论 基 础

周 炳 黎 编 著

责任编辑：董乐前

•
人民邮电出版社出版

北京东长安街27号

河北省邮电印刷厂印刷

新华书店北京发行所发行

各地新华书店经售

•
开本：787×1092 1/32 1983年8月第一版

印张：14 28/32 页数：238 1983年8月河北第一次印刷

字数：340千字 印数：1—8,200册

统一书号：15045·总2640—无6210

定价：1.90元

5250111

前 言

信息的概念已在自然科学以至社会科学中广泛地被采用，它的重要性也在不断地被阐明，因而，关于信息的理论也就被人们所注意，本书就是试图满足这种需要而编写的。

这样的目标显然不能在一本书中达到，本书着重介绍近代仙依信息论的一些基本观点，作者认为这是研究信息理论的起点。为了使读者在较广泛的含义上理解它，本书的第一部分将介绍一些有关集合和概率的基本知识，这对于有兴趣阅读近代通信和信息论文献的读者，可能是必需的和有帮助的。本书的第二部分，是仙依信息论，即信源，信道和编码定理。

信息理论的近代发展除上述理论的进一步精确化外，一般可分为两个分支，一是它在通信科学方面的应用，也就是各编码定理的实现问题，由此已有许多具体的方法，如信源处理，信道改善和一般的检测问题。二是信息概念的广义化，以利于应用到其它边缘学科上去。这些将留待以后论述。

本书曾作为研究生教材使用，部分内容是北京邮电学院陆传资同志和李道本同志协助整理。舒华英同志和信息论研究室的其他许多同志对本书出版做了很多工作，谨此致谢。

作者 1981年1月于北京邮电学院

目 录

引论	(1)
----	-------

第一部分 数学基础

第一章 集合论大要	(7)
------------------	-------

第一节 集合论的基本知识	(7)
--------------	-------

1.1.1 集合的概念	(7)
-------------	-------

1.1.2 集合的运算及其性质	(10)
-----------------	--------

1.1.3 集合的分类与一一对应	(12)
------------------	--------

1.1.4 族(类)及其运算	(14)
----------------	--------

1.1.5 直积集合	(17)
------------	--------

第二节 关系与函数	(18)
-----------	--------

1.2.1 概述	(18)
----------	--------

1.2.2 函数	(23)
----------	--------

1.2.3 次序关系(\leq)	(25)
----------------------	--------

第三节 测度	(28)
--------	--------

1.3.1 波雷尔族	(28)
------------	--------

1.3.2 测度	(30)
----------	--------

1.3.3 可测函数	(33)
------------	--------

1.3.4 勒贝格积分	(34)
-------------	--------

第一章 习题	(36)
--------	--------

第二章 概率论大要	(42)
------------------	--------

第一节 概率空间和事件概率	(42)
---------------	--------

2.1.1	概率空间	(42)
2.1.2	概率的性质	(44)
第二节	随机变量和分布函数	(45)
2.2.1	定义	(45)
2.2.2	离散型分布和连续型分布	(47)
2.2.3	常见分布举例	(49)
第三节	数学期望和特征函数	(51)
2.3.1	数学期望的定义	(51)
2.3.2	随机变量的数字特征——各阶矩	(52)
2.3.3	特征函数	(57)
2.3.4	常见分布的特征函数	(59)
第四节	随机矢量和多维分布	(61)
2.4.1	定义	(61)
2.4.2	随机矢量的特征函数与矩	(62)
2.4.3	多维分布举例	(64)
2.4.4	随机变量的独立性	(66)
2.4.5	随机序列的收敛性	(68)
第五节	随机变量的变换	(72)
2.5.1	边缘分布	(73)
2.5.2	函数变换	(73)
第六节	条件概率, 条件分布函数, 条件期望	(79)
2.6.1	条件概率	(79)
2.6.2	条件分布函数	(80)
2.6.3	条件期望	(83)
第七节	极限定理	(88)
2.7.1	大数法则	(89)
2.7.2	中心极限定理	(91)
2.7.3	小数极限	(94)

第二章	习题	(96)
第三章	随机过程大要	(101)
第一节	一般理论	(101)
3.1.1	随机过程的一般描述方法	(101)
3.1.2	可离性, 可测性, 连续性	(102)
第二节	独立变量过程	(104)
第三节	可加过程 (独立增量过程)	(105)
3.3.1	定义	(105)
3.3.2	正态可加过程	(107)
3.3.3	帕桑过程	(117)
3.3.4	勒维过程	(122)
第四节	平稳随机过程	(123)
3.4.1	定义	(123)
3.4.2	相关函数	(125)
3.4.3	弱平稳过程的谱分解	(129)
3.4.4	强平稳过程的遍历性	(137)
第五节	马尔柯夫过程	(139)
3.5.1	马尔柯夫链	(140)
3.5.2	马尔柯夫过程	(147)
3.5.3	高阶马尔柯夫过程	(153)
第三章	习题	(156)

第二部分 仙依信息论

第四章	信源和信息熵	(164)
第一节	信源特性和分类	(164)
第二节	离散信源的信息熵	(178)
4.2.1	信息量和熵	(178)
4.2.2	熵函数的数学特性	(183)

4.2.3	熵函数的公理构成	(193)
第三节	互信息和序列的熵	(197)
4.3.1	两个符号的熵和互信息	(197)
4.3.2	序列信息的熵	(204)
第四节	连续信源的熵	(210)
4.4.1	连续随机变量的熵和信息	(211)
4.4.2	最大熵定理	(215)
第四章	习题	(224)
第五章	信道和信道容量	(232)
第一节	信道的主要参数和分类	(232)
第二节	无干扰离散信道	(238)
第三节	单符号信道	(243)
5.3.1	信道容量的定义和计算举例	(243)
5.3.2	离散信道容量的一般计算方法	(249)
5.3.3	离散信道容量的迭代计算	(255)
第四节	多符号信道	(261)
5.4.1	独立并联信道的容量	(262)
5.4.2	限频限功率高斯信道的容量	(264)
5.4.3	有公共制约的多符号信道	(268)
5.4.4	一般信道问题	(272)
第五节	多用户信道	(275)
5.5.1	多址接入信道	(277)
5.5.2	广播信道	(286)
5.5.3	相关信源的多用户信道问题	(291)
第五章	习题	(295)
第六章	信息率失真函数	(304)
第一节	一般概念和定义	(304)
第二节	$R(D)$ 函数的性质	(310)

第三节	离散信源的 $R(D)$ 函数的计算	(315)
6.3.1	$R(D)$ 的参量表达式	(316)
6.3.2	二元信源和对称失真函数的 $R(D)$ 函数	(319)
6.3.3	迭代计算公式	(324)
第四节	连续信源的 $R(D)$ 函数	(327)
6.4.1	定义和一般公式	(328)
6.4.2	$d(x, y)$ 只与 $(x-y)$ 有关的情况	(331)
第五节	信息价值	(337)
第六节	广义信息率失真函数	(343)
6.6.1	通信系统的性能指标的界	(343)
6.6.2	一般化信息函数和信息率失真函数	(346)
6.6.3	通信系统性能指标的界之例	(349)
第六章	习题	(351)
第七章	编码定理	(358)
第一节	无失真离散信源编码定理	(359)
7.1.1	定长编码定理	(360)
7.1.2	变长编码定理	(368)
第二节	限失真信源编码定理	(379)
7.2.1	$D(C)$ 的上界	(379)
7.2.2	$E(\beta, P)$ 的性质	(385)
7.2.3	离散无记忆信源的限失真编码定理	(390)
第三节	离散信道编码定理	(392)
7.3.1	差错率 P_e 的上界	(392)
7.3.2	离散无记忆平稳信道的编码定理	(398)
7.3.3	$E(R)$ 的计算	(402)
第四节	连续信道的编码定理	(411)
7.4.1	半连续信道的编码定理	(412)
7.4.2	连续信道的编码定理	(414)

7.4.3	高斯信道可靠性函数的计算	(418)
7.4.4	高斯信道的实际编码问题	(423)
第五节	信道编码定理的改善	(429)
7.5.1	差错概率的下界	(430)
7.5.2	差错率上界的改善	(440)
7.5.3	差错率下界的改善	(445)
第六节	多用户信道编码定理	(449)
7.6.1	二址接入信道的编码定理	(450)
7.6.2	退化广播信道的编码定理	(454)
7.6.3	有边信息的编码定理	(456)
第七章	习题	(458)
结束语		(464)

引 论

信息是一个常用的词，它代表着某一抽象的有待传送、交换、存贮以及提取的内容。例如我们说互通信息，利用信息来做出某种判断等等。其实信息是一个含义相当深刻的概念，它牵涉到生命现象本身。从远古的生物进化直到当代形形色色的科学和社会活动中，无处不涉及到信息的交换和利用。然而信息这个概念迄今尚未被人们充分掌握。信息论的理论基础一般来说，是从仙依研究通信系统时建立的。仙依和惠佛在49年发表的“通信的数学理论”对信息引入了定量的规定，从而开辟了对信息的初步了解。显然，目前信息的含义已进一步发展，这一定量规定已嫌不足，不过仍然可认为仙依理论不失为信息论的基础。所以，这里仍先讨论通信系统模型，研究它的实质性问题，即信源、信道、编码理论，作为进一步研究信息论的出发点。

图 0-1 是通信系统的模型。这是一个单向通信系统，信息从信源送到信宿。

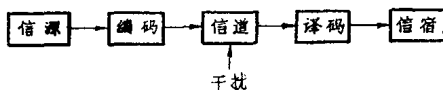


图0-1 通信系统的模型

在习惯意义上说，通信是两个人之间传递信息。例如信源是一个人甲，他要把某些信息传送给某个人乙，后者是信息的归宿点，这就构成一个通信系统。最简单最原始的通信方式是面对面谈话。这时某甲有一些事情要告诉某乙，也就是有一些信息要传递给某乙，他把这信息编成语言，用嘴说出来，这个

1110787

· 1 ·

过程就是编码。说出来的语言已是声音，作为一种信号在空气中传播，这空间就构成了一个能传送声音的信道。声音到达乙处，乙用耳朵来接收，译出语言所表达的内容，完成译码过程，取得信息；这时的信宿应为某乙的脑。在声信号传送过程中，不可避免地有一些杂声混入，这将影响某乙所收到的声信号，造成某些失真。在大噪声的情况下，某乙也可能收不到什么信息，虽然他收到了声信号，即原来某甲的语音和噪声。这噪声就是干扰。由上述简单讨论可见，面对面谈话（甲说乙听），也可用图0-1的模型来表达。

仔细分析一下这类谈话的过程，我们发现，信息是一种抽象的东西，不易掌握。语言只是代表信息的符号。同样的事情可用不同语言来表达，也就是同样的信息可以用不同的编码方式转换成符号。这些符号有时就称为消息。消息是具体的，但还不是物理性的，当然也不是信息本身。而说出来的语言却已成为物理性信号，可以在自然界传递，或者说在实际信道中传送。在信宿端，先须用耳朵来接收这个声音信号，译成语言符号，理解它的含义，从而提取所需的信息。这里应分辨信息、符号或消息、信号这三者的不同含义，以便正确地理解通信系统的实质问题，从而把许多通信方式抽象成图0-1那样的模型，以便统一研究一些问题。

有了这样的理解，就可以把几乎所有通信系统归纳成统一的模型。例如信源和信宿相距很远，不能直接谈话，那就需要用另外一些通信方式。用书信传递信息是一种古老的通信方式，这里所用的符号仍是语言符号。但用文字的形式写在纸上后，纸上的字就是一种语言信号，它可以通过邮路送到对方去，而收信人须用眼睛看，来完成译码过程，从而获得信息。这时的信道实际上起了存贮信息的作用，发信者把信息存在纸

上，收信者利用光信号由人眼来接收。这种存贮方式使通信克服了时间上的限制。假如某人写了一本书，它可以在图书馆中存放很久，后人还可以从中获得信息，其实这也可以说是一种通信方式。

书信通信是用时间来克服空间的限制，其所需的时间随着科学的发展而逐渐缩短。古代用驿马传送，后来用火车飞机传送，但这一般还是需要较长的时间。用电通信就最大限度地缩短了时间。它与书信的差异，仅在于用电信号来传送。因而编译码过程，将包含把声音信号（或其他符号如电报电码、传真图象或电视信号）换成电信号（由话筒完成）；而译码时再把电信号换成声信号（由听筒完成），而传送时可用电缆或无线收发信系统的信道，其他与面对面谈话相仿。

在双向通信中，两个人要相互传送信息，图0-1的模型也完全适用，只是信道、编译码器要有两套，一套用于正向通信，一套用于反向通信，每端的人既是信源也是信宿而已。

只要把编、译码和信道的含义一般化，就可以使图0-1的模型广泛地适用于其他领域。所谓编码，就是用符号来表达信息，这通常称为信源编码部分；然后将符号转换成信道所要求的信号，这通常称为信道编码部分。总之所谓编码，不过是把信息变换成信号的措施，译码就是编码的反变换，而信道就是传送物理信号的物理设施。我们碰到的信道总是具体的、物理性的，而信息则是抽象的，信号只是信息的载荷子。符号或消息也是具体的，但它并不是物理性的，它是代表信息的具体方式。不同的通信系统，编、译码器和信道不同，但它们所起的作用是一样的。

图0-1的模型只在信道方块中引入了干扰，这是一种简化的表达方式。实际上编、译码过程中也会引入干扰。为了分析

简单，我们常把系统中其他地方的干扰，都等效地折合成信道干扰。

信道除了传送信号外，还应理解为它可能有存贮信号的作用，前面说到的书信方式中，这种存贮是明显的。其实在电信系统中，也有存贮问题，例如在点对点的通信中，电路中总有延时，即使这延时值很小，也应看作是存贮作用。至于在近代电信系统中，有许多交换点，有计算机，它可以存贮信号，待到合适时机再传送，存贮时间将更长。

在复杂的电信系统中，信道的数量很大，信源和信宿的数量也很大，这样组成了通信网。但它的基本单元还是如图0-1所示的模型。对于某个基本单元，信源和信宿可能已不是人，而是某些计算机。因此出现所谓人——机；机——人；机——机通信，但其实质还是上述模型，只是信源、信宿的含义更一般化了。信道也可能不像图0-1所示的那样简单，只有一个输入和一个输出，而是有几个输入和几个输出，这常称为多用户信道。即一个信道有几个编码器或几个译码器与它连接，使各编、译码器之间能在规定条件下相互传送信息。信道理论也应包括这类情况。

有些一般认为并非是通信系统的，也可用上述模型来研究。这时可称为信息流通系统。例如雷达是一种遥测系统，目标物在空间的坐标、速度、形状、性质等是包含着信息的，这就构成了信源，我们用无线电波射向它，而反射波中包含着这些信息，这就是编码过程。从接收到的反射波译出所需的信息，完成译码过程。电磁波传播和收发过程就是信道。又如一个自动化系统，其中可能包含着测量和控制。这常包含两个信道，即正向和反向信道。从正向信道中提取所需信息，经过处理后又由反向信道传送控制信息，因而对被测量的部件作某项

校正。这里信源和信宿可能都是机械性的，但它必然有一些信息可被测量和被处理。

甚至有些社会活动也被认为是信息流通系统，例如管理机构的实质，也是通过下层人员收集信息，传送给决策人员，再发出行为信息去进行社会活动。

由上述可见，信息论的基本问题就是信源和信宿、信道以及编码问题。

信源的核心问题是它包含的信息到底有多少？应能把它定量地表示出来，也就是要规定信息量。信宿的问题是能收到或提取多少信息。后一问题一般不计及信息是否有用或有意义。例如某种语言，甲完全熟悉，他就能从中提取有用信息，乙可能不懂这种语言，他就不能从中提取有用信息。作为狭义的信息论，可不必问信宿的实际情况，而认为甲、乙收到了同样的信息。

信道的问题主要是它最多能传送多少信息的问题，这就是信道容量。多个输入多个输出的多用户信道，也有其容量，但它已不能由一个数量来表达，而可能以几个数量所限制的区域作为信道容量。但含义是相仿的。

另一类是与信源有关的失真函数问题。它研究在规定的失真下必须传送的信息量，也牵涉到信息价值问题，即收到信息后比未收到信息前有多大好处。

最后就是编、译码问题。即理论上如何编码才能使信源的信息被充分表达。信道的容量才能被充分利用；这些编、译码的方法是否存在。为了研究这个问题，有几个编码定理需要介绍。具体地讲就是信源编码定理和信道编码定理。这些编码定理只解决编码器的存在性，至于实际实现则属于信息论在各领域中的应用问题，不属本书的范围。

以下各章将分别讨论这些问题。但要研究这些问题，必须使用一些数学工具，主要是集合论、概率论和随机过程。这些方面虽均有专著论述，但为了把它们简化和工程化一些，本书第一部分将概述它们的要点，作为第二部分讨论问题的基础，也为应用和展开信息论作一些准备。

第一部分 数学基础

第一章 集合论大要

第一节 集合论的基本知识

1.1.1 集合的概念

集合是近代数学最基本概念之一，它是测度论和概率论的基础。

集合是具有某些性质（或特点）的一系列元素（或对象）所组成的总体。在数学上常用下式表示某一集合 A

$$A = \{x: x \text{ 具有某些性质（或特点）}\}$$

用语言来表达，凡是具有某些性质的 x 称为 A 中的一个元素，而这样一些元素的全体便构成集合 A 。今后为方便起见，有时简称集合为集，集合中的元素为元。

下面举些集合的例子以加深对集合这一概念的理解。

(1) $I = \{x: x \text{ 是正整数}\}$ 即 I 是由全体正整数所组成的集合。有时可简单写成 $I = \{x \text{ 是正整数}\}$ ，省去前面的 x ，，这在不引起误解时使用。

(2) $Z = \{x: x \text{ 是整数}\}$ ，即 Z 是由全体整数（包括负整数）所组成的集合。

(3) $A = \{x: x = a, b, c, \text{ 或 } d\}$ 这是由 a, b, c, d 四个元素组成的集合。常写成 $A = \{a, b, c, d\}$ 。