信息论与编码

Information Theory and Coding

西南交通大学 电子信息工程专业 2020 - 教师: 赵舵

- 手 机: 15390029122

- 电 邮: <u>zhaoduo@swjtu.edu.cn</u>

- 课程教学qq群:446528349

- 请通过以上邮件联系
- 如果通过教务邮件联系我回复会有延迟

重要说明之一

- **该门课程的重要性**(信息时代,信息无处不在,与 人人密切相关)
 - 信息论是信息科学与技术的基本理论, 信息科学 大厦的地基;
 - 信息论的原理和方法应用广泛,若无信息论理 论支持,从事通信与信息领域的研究和创新是 不可能的事情;
 - 信息论的学习有助于认识事物的本质, 信息论是 高层次信息技术人才必不可少的基础知识。

重要说明之二

教材:

[1]李梅,李亦农,王玉皞.信息论基础教程.第3版[M]. 北京邮电大学出版社,2015.



参考书:

- [1] 李梅. 信息论基础教程习题解答与实验指导[M]. 北京邮电大学出版社, 2008
- [2] 姜丹. 信息论与编码. 中国科学技术大学出版社[M]. 2004.
- [3] 科费, 托马斯, 科费,等. 信息论基础[M]. 机械工业出版社, 2005.
- [4] RobertJ.McEliece, 李斗, 殷悦,等. 信息论与编码理论[M]. 电子工业出版社, 2004.

重要说明之三

网络教学带来的新挑战:

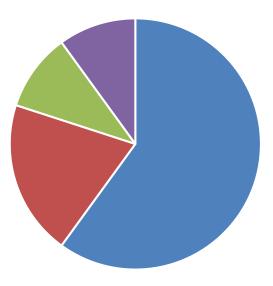
- 1、定时提前到课堂:一般提前15分钟发布课堂链接
- 2、目前采用平台腾讯课堂+雨课堂+QQ群热备
- 3、网络打卡、课堂签到

上课同时准备:

- 1、笔记本(做好公式推导和证明的准备)
- 2、科学计算器1台(或者MATLAB软件,做好算法 仿真准备)
- 3、及时反馈老师课堂提问

学期成绩评分标准

期末成绩构成



- ■期末考试60%■期中考试20%
- ■课后作业10% ■课堂表现10%

课程的主要研究内容

- 什么是信息论
- 为什么要研究信息论
- 信息论的发展过程是怎样的
- 信息论的内容、体系以及范畴
- 如何实现信息的有效、可靠、安全传输
- •

课程在电子信息工程专业中的地位

・课程是本专业核心课程

——专业基础课程

• 课程的先修课程要求:

概率论与数理统计、线性代数

• 课程支撑后续课程学习:

计算机网络、通信电路、传感器与信号检测 技术、信息处理课程设计等

第1章 绪论

- 信息的基本概念
- 信息论的形成和发展
- 信息论的研究内容
- 通信系统的一般模型以及其中各部分的功能和作用

1-1 信息的概念





Q1: 哪一个屏幕提供给你更多的信息量?

Q2: 多了多少?

- The English word was apparently derived from the Latin stem (information-) of the nominative (informatio): this noun is in its turn derived from the verb "informare" (to inform) in the sense of "to give form to the mind", "to discipline", "instruct", "teach": "Men so wise should go and inform their kings." (1330)
- Inform itself comes (via French informer) from the Latin verb informare, to give form, to form an idea of. Furthermore, Latin itself already contained the word informatio meaning concept or idea, but the extent to which this may have influenced the development of the word information in English is not clear.

zhaoduo@swjtu.edu.cr

- According to the Oxford English Dictionary, the first known historical meaning of the word information in English was the act of informing, or giving form or shape to the mind, as in education, instruction, or training.
- A quote from 1387 English text: "Five books come down from heaven for information of mankind".



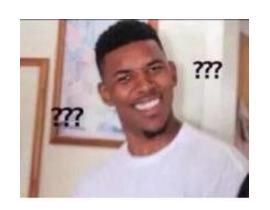
Information is

a difference which

makes a difference.

Gregory Bateson

A perceived difference that can make a difference.



(1)



(2)

Q3: 你现在对信息概念的理解?

我国的《辞海》对"信息"作了如下解释:

• 信息:通信系统传输和处理的对象,泛指消息和信号的具体内容和意义。通常须通过处理和分析来提取。信息、物质和能量被称为系统的三大要素。信息和物质的量值与信息的随机性有关,如在接收端无法预估消息或信号中所蕴含的内容或意义,即预估的可能性越小,信息量就越大。

- 1. 日常生活中的"信息"
 - a. 远古时期人类的结绳记事
 - b. 古代的烽火告警
 - c. 语言文字的发明
 - d. 造纸术和印刷术的发明
 - e. 近代的电报电话的发明
 - f. 计算机技术和网络的快速发展

1-1 信息的概念

2. "信息"、"消息"、"信号"的联系和区别

信息与消息

消息: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,对客观物质运动和主观思维活动状态的一种表达。

消息中包含信息,是信息的载体;

同一则信息可由不同的消息形式来载荷;

同一则消息可以载荷不同的信息;

1-1 信息的概念

2. "信息"、"消息"、"信号"的联系和区别

信息与信号

信号: 需要将消息变换成适合于信道传输

物理量,这种物理量就称为信号。

同一则信息可由不同的信号来表示;

同一则信号可以表示不同的信息;

信息定义:信息是事物运动状态或存在方式的 不确定性的描述

信息一般具有如下一些特征:

1、可识别; 2、可转换; 3、可传递; 4、可加工处理; 5、可多次利用(无损耗性); 6、在流通中扩充; 7、主客体二重性; 8、信息的能动性

1-1 信息的概念

◆ 第一个重要概念: 信息传递的通道中传送的是随机变量的值

注意:

- ▶我们在收到消息之前,并不知道消息的内容。否则消息 是没有必要发送的。
- ▶消息随机变量有一个概率分布。
- ▶消息随机变量的一个可能取值就称为一个事件。

1-1 信息的概念

- ◆ 第二个重要概念: 事件发生的概率越小, 此事件 含有的信息量就越大。
- ▶事件"中国足球队5:0力克巴西足球队"含有的信息量
- 大。 (小概率事件发生了,事件信息量大)
- ▶事件"中国足球队0:3负于巴西足球队"含有的信息量
- 小。 (大概率事件发生了,事件信息量小)

(不太可能发生的事件竟然发生了,令人震惊)

- ◆ 第三个重要概念: 消息随机变量的随机性越大, 此消息随机变量含有的信息量就越大。
- ▶消息随机变量X= "中国足球队与巴西足球队比赛的结果",则消息随机变量X含有的信息量小。

(随机性小,可预见性大,因此该消息随机变量含有的信息量小。)

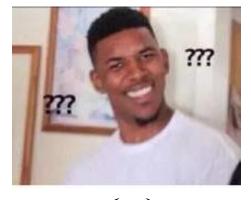
▶消息随机变量X= "意大利足球队与德国足球队比赛的结果",则消息随机变量X含有的信息量大。

(随机性大,可预见性小,因此该消息随机变量含有的信息量大。)

1-1 信息的概念

- ◆第四个重要概念:两个消息随机变量的相互依赖性越大,它们的互信息量就越大(这里指的是绝对值大)。
- ➤例 X=成都明日平均气温, Y=犀浦明日平均气温, Z=北京明日平均气温, W=迈阿密明日平均气温。则

X与Y互信息量大, X与Z互信息量小得多, X与W互信息量几乎为0







(2)



(3)

Q3: 你现在对信息概念的理解?

1. 早期的编码问题 (F.B.Morse, 1837 二进制电报码)

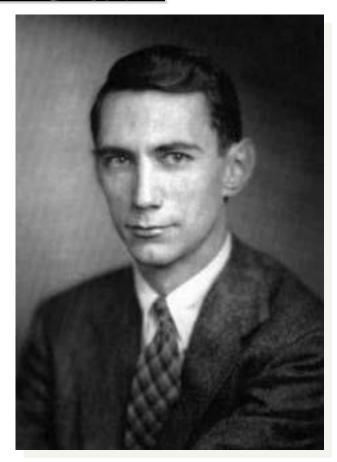


- 2. 通信的有效性和可靠性 (Nyquist, 1924 揭示了信号带宽和信息速率之间的关系; Hartley, 1928 首先提出了信息的概念,指出信息的度量与信号的概率分布、对数函数有关等(《信息传输》))
- 3. 信息熵的提出 (控制论的奠基人Wiener, 1948 定义:信息是信息,不是物质也不是能量(《控制论—动物和机器中通信与控制问题》),美国统计学家Fisher和Shannon同时提出信息的一种度量----熵)
- 4. 信息论的创立 (C.E.Shannon 1948 在研究通信系统的传输时,对信息进行了科学的定义,并进行了定性和定量的描述《通信的数学理论》)

The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point.

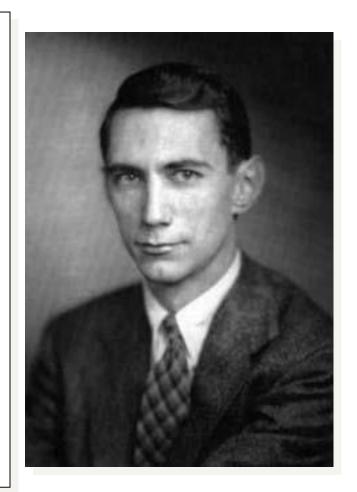
(Claude E. Shannon, 1948)

A Mathematical Theory of Communication



通信的基本问题就是报文的再生,在某一点与另外选择的一点上报文精确地或近似地重现.

(Claude Shannon, 1948) 诵信的数学理论



Remission with corrections from The Rell System Technical Journal, Vol. 27, pp. 579-423, 023-656, July. October, 1946.

A Mathematical Theory of Communication

By C. E. SHANNON

INTRODUCTION

THE recent development of various methods of modulation such as PCM and PPM which exchange bandwidth for signal-to-noise ratio has intensified the interest in a general theory of communication. A basis for such a theory is contained in the important papers of Nyquist and Hartley on this subject. In the present paper we will extend the theory to include a number of new factors, in particular the effect of noise in the channel, and the savings possible due to the statistical structure of the original message and due to the nature of the final destination of the information.

The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point. Frequently the messages have meaning; that is they refer to or are correlated according to some system with certain physical or conceptual entities. These semantic aspects of communication are irrelevant to the engineering problem. The significant aspect is that the actual message is one selected from a set of possible messages. The system must be designed to operate for each possible selection, not just the one which will actually be chosen since this is unknown at the time of design.

If the number of messages in the set is finite then this number or any monotonic function of this number can be regarded as a measure of the information produced when one message is chosen from the set, all choices being equally likely. As was pointed out by Hurtley the most natural choice is the logarithmic function. Although this definition must be generalized considerably when we consider the influence of the statistics of the message and when we have a continuous range of messages, we will in all cases use an essentially logarithmic measure.

The logarithmic measure is more convenient for various reasons:

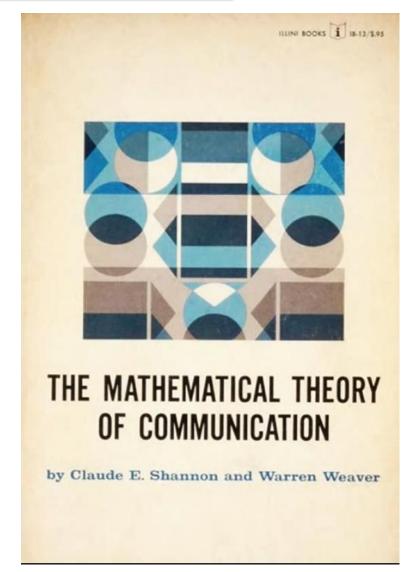
- 1. It is practically more useful. Parameters of engineering importance such as time, bandwidth, number of relays, etc., tend to vary linearly with the logarithm of the number of possibilities. For example, adding one relay to a group doubles the number of possible states of the relays. It adds 1 to the base 2 logarithm of this number. Doubling the time roughly squares the number of possible messages, or doubles the logarithm, etc.
- 2. It is nearer to our intuitive feeling as to the proper measure. This is closely related to (1) since we intuitively measures entities by linear comparison with common standards. One feels, for example, that two punched cards should have twice the capacity of one for information storage, and two identical channels twice the capacity of one for transmitting information.
- 3. It is mathematically more suitable. Many of the limiting operations are simple in terms of the logarithm but would require clumsy restatement in terms of the number of possibilities.

The choice of a logarithmic base corresponds to the choice of a unit for measuring information. If the base 2 is used the resulting units may be called binary digits, or more briefly bits, a word suggested by J. W. Tukey. A device with two stable positions, such as a relay or a flip-flop circuit, can store one bit of information. N such devices can store N bits, since the total number of possible states is 2^N and $\log_2 2^N \equiv N$. If the base 10 is used the units may be called decimal digits. Since

$$log_2 M = log_{10} M/log_{10} 2$$

= 3,32 log₁₀ M,

"Nyspast, H., "Certain Pactors Affecting Tolograph Speed," Boll System Technical Journal, April 1924, p. 324; "Certain Topics in Tologoph Transmisson Theory, A.L.E. Even., v. 45, April 1928, p. 617.
"Harfity, R.V.L., "Transmisson of Information," Fell System Technical Assensi, July 1928, p. 538.



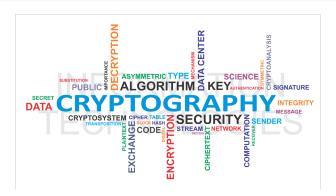


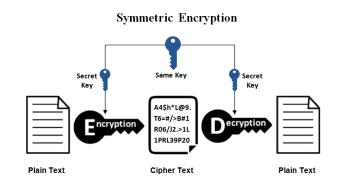
无失真数据压缩,Lossless data compression

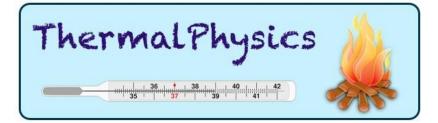


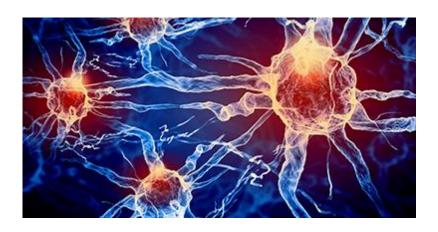


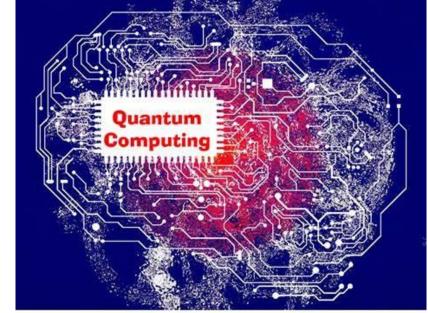
限失真数据压缩,Lossy data compression











Shannon—生写了127篇文章,他的每篇文章都极富洞察力,为我们提供了全新的新思想,很多文章都开辟了崭新的研究方向!

□1938年发表《继电器和开关电路的符号分析》一文曾获电气和电子工程师学会(IEEE)的Alfred Noble奖,是20世纪中的一篇最重要也是最为著名的硕士论文,成为数字电路设计的一个里程碑。这篇文章是在1937年成文的,当时他还是MIT的一名学生。在这篇文章他告诉人们:"如果我们有一天能发明计算机,要使它能够思索的话,一定会是采用二元码和串在一起的开关,并应用布尔(Boole)逻辑系统实现的结果。"

- □1940年在MIT的博士论文《An Algebra for Theoretical Genetics》,是数字控制系统和计算机科学的先驱工作。
- □ 1948年发表的《通信的数学理论》文章,创建了信息 论,这是一篇20世纪少有的几篇对科学和工程,乃至对人 类社会发展产生了重要影响著作,是可与牛顿力学相媲美 的不朽之作,也是他最重要的科学贡献。这使他成为信息 论之父,时年仅32岁。作为数学家,他为数学开辟了一个 工程应用的新领域。这篇文章虽然在1947年完成,但至今 仍然闪烁着智慧的光芒,它将照耀人类今后的数个世纪。

"通信的基本问题是在彼地精确地或近似地重现此地所选的消息",这句话将通信的本质表述得多么清晰!它所给出的信道容量方程 (C = Wlog₂(1+ S/N), W:信道带宽, S/N:信噪比, C:信道容量),指出了通过信道实现错误概率为零时可传输的最大信息速率,即Shannon极限,这是一个罕见的、漂亮、简洁而又有效的理论结果。

著名信息论和编码理论教授Robert G. Gallager曾说过:

"Shannon发现了在所有通信中最基本的元素就是二元数字"。"这的确是他的发现,从此萌发了整个通信领域的(数字化)革命"。

今天,这一理论已被广泛地应用,从空间探测、卫星通信、无线移动通信,到硬盘驱动器、光盘存储等。信息论的应用已远远超出了通信领域,从基因学、分子生物学、神经系统、脑科学到心理学、艺术、音乐、社会学、语言学、经济学,甚至庭院设计。

zhaoduo@swjtu.edu.cn

□1949年发表了 "Programming a computer for playing chess, "这也是人工智能的一个先驱工作。 1965年他曾应邀赴莫斯科参加一个工程会议,并顺便会见 了多次获国际象棋世界冠军、电器工程师Mikhail Botvinnik , 一起对弈和讨论了计算机编程下棋。 1980年Shannon还作为特邀贵宾参加了在奥地利Linzjuxingde 国际计算机象棋冠军赛, 贝尔实验室的 "Belle"获得了冠军 , 已接近象棋大师水平。 1997年IBM造出了"深蓝"计算机,装入了计算机程序 chatterbotALICE, 并战胜了俄国国际象棋大师和世界冠军 Garry Kasparov。这是人类第一次用自己制造的机器在智能 上(更确切地说是在下国际象棋的能力上)战胜了自己。

□1950年他构建了老鼠走迷宫机器Theseus, 1951年发表的 《Presentation of a maze solving machine》,是一篇计算机 学习的先驱著作。这也是人工智能的一个先驱工作。 □1953年Shannon曾构建了"心灵阅读(Mind reading) 机,可通过观察、记忆和分析对方过去所选硬币的正、反 面的图样,试图猜测对方下一次可能选择。这是一种博弈 游戏。Shannon的阅读机曾和贝尔的同事,这种机器的发明 人D. W. Hagelbarger进行对弈,并赢得胜利。 □与E. F. Moore合作研究,用增加接点的冗余度来提高继电 器电路可靠性,这一研究与有扰信道传信问题密切相关 □1956年与J. 麦卡锡合编的著名论文集《自动机研究》是 自动机理论方面的重要文献。

- □1959年发表的《Coding theorems for a discrete source with fidelity criterion》文章创建了率失真理论,在连续消息和离散消息之间架上了一座桥梁,从而给数字化提供了一个基础和有效的工具。
- □1960年发表的《Two-way communication channel》文章,创建了多用户信息论。
- □Shannon曾提出将信息论用在生物系统,在他看来,机器的和生命的事物是有共同性的,今天,生命信息论已有不少研究了。
- □Shannon还做过将信息论用于最佳投资策略问题的研究,他认为股票市场是一种"受扰信号",与时间序列相关联,问题是要通过适当选择和调整证卷投资组合,使效用函数达到极大值。
- □1966年获美国国家科学奖章,由前总统Lyndon B. 约翰逊颁发。

zhaoduo@swjtu.edu.cn

信息论创始人Shannon的主要贡献

口为了表彰Shannon的伟大功绩,IEEE Information Society 的25名成员于2000年10月6日在Shannon的儿童时代的老家 Michigan的Gaylord举行了Shannon塑像的落成典礼。

Claude Elwood Shannon

Father of Information Theory, Electrical engineer, Mathematician, and native son of Gaylord. His creation of information theory, the mathematical theory of communication, in the 1940s and 1950s inspired the revolutionary advances in digital communications and information storage that have shaped the modern world.

This statue was donated by the Information Theory Society of the Institute of Electrical and Electronics Engineers, whose members follow gratefully in his footsteps.

Dedicated October 6, 2000 EdgeneDaub, Sculptor



信息论创始人Shannon的主要贡献

- □Shannon虽然已于2001年辞世,但正如信息论著名教授 Richard Blahut 博士的题词所说的,它所留给人类的思想会永 远留在人类的脑海中,激励我们的子孙们。
- □ "在我看来,两三百年之后,当人们回过头来看我们的时候,他们可能不会记得谁曾是美国的总统。他们也不会记得谁曾是影星或摇滚歌星。但是仍然会知晓Shannon的名字。学校里仍然会教授信息论。" (Dr. Richard Blahut, Oct. 6, 2000, Gaylord, Michigan)

1-2 信息论的形成和发展

Shannon信息论的优点和局限

优点:

- (1) 它是一个科学的定义,有明确的数学模型和定量计算;
- (2) 它与日常用语中的信息含义是一致的;
- (3) 定义排除了对信息一词某些主观上的含义;

1-2 信息论的形成和发展

Shannon信息论的优点和局限

局限:

- (1) 数学模型的确立、定义是以假定事务的状态可以 用一个经典集合论为基础的概率模型来描述;
- (2) 定义和度量没有考虑到收信者的主观性和主观意愿, 也抛开了信息的具体含义、用途、重要程度等因素。

1-2 信息论的形成和发展

钟义信教授

认为"信息就是事物运动状态和方式,就是关于事物运动的千差万别的状态和方式的知识"

提出了"语法信息"、"语义信息"、"语用信息" 定义

目前国际上尚没有形成一个普遍公认的、完整的、确切的信息的定义。

信息论是关于信息的本质和传输规律的科学的理论,是研究信息的计量、发送、传递、交换、接收和储存的一门新兴学科.

1-3 信息论的研究内容

一般将信息论分成:

• 狭义信息论 (经典信息论)

主要研究信息的测度、信道容量以及信源和 信道编码问题,是信息论的理论基础

· 广义信息论(信息科学)

是以信息作为主要的研究对象、以信息过程 的运动规律作为主要研究内容、以信息科学 方法论作为主要研究方法、以扩展人的信息 功能作为主要目标的一门科学

1、广义信息论研究对象:以信息作为主要研究对象

对信息的进一步认识

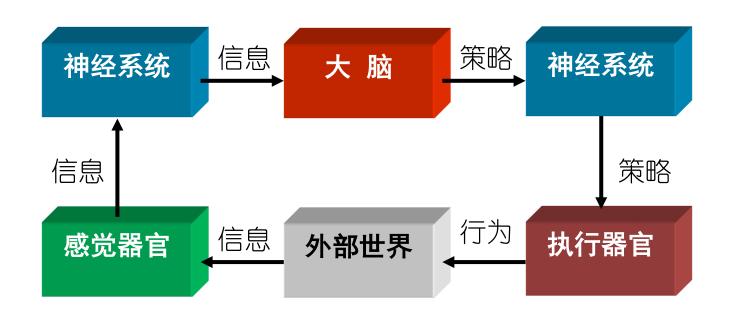
1、信息是普遍存在的一类研究对象;

信息无处不在:存在于人类社会、人类思维领域......

- 2、信息与物质是既有联系又有区别的两个概念; 物质是信息载体;信息为事物运动方式和状态变化的方式,而非事物本身
- 3、信息与能量是既有联系又有区别的两个概念;

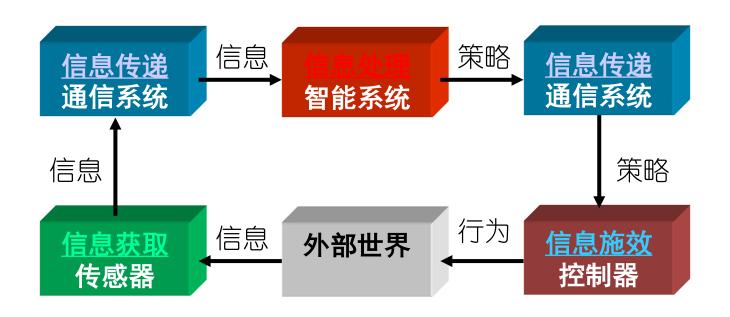
传递和处理信息需要能量;对于能量的控制则需要信息

2、广义信息论的研究内容:



人类处理信息过程模型

2、广义信息论的研究内容:



广义信息过程模型

2、广义信息论的研究内容:

- a、探讨信息的定性本质
- b、研究信息的定量测度
- c、信息的获取、传递、处理、施效的基本规律
- d、构建信息科学的方法论

广义信息论的研究目标:

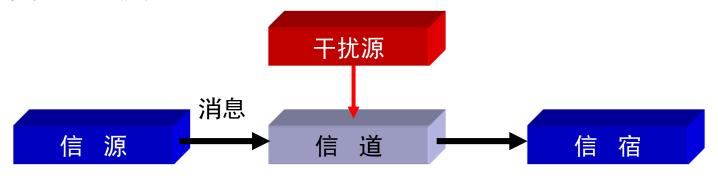
补充增强和扩展人的各种天然信息功能 - - 智力功能,智能系统

3、狭义信息论的研究内容:

- a、信息的定义
- b、信息的度量
- c、信息传输过程中的基本极限条件
- d、信息的压缩和恢复的极限条件
- e、从环境中抽取信息的极限条件
- f、实际中能否达到极限条件
- g、实际中如何接近极限条件

比较	广义信息论	狭义信息论
研究对象	智能系统	通信系统
研究目标	扩展智力功能	扩展信息
	实现智能系统	传递功能
研究内容	信息处理全部	信息传递
	的过程	的过程
研究方法	信息科学	信息论传统方
	方法学	法统计方法

1、简单信道模型



信源(Source):

向通信系统中提供消息的人和机器;

信道(Channel):

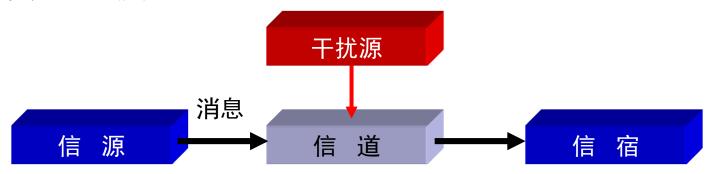
信道是信息传递的通道,承担了信息的传输和储存的任务,是构成通信系统的表现。

统的重要组成部分;

信宿(Destination): 消息传递的对象,也就是接收消息的人或机器;

干扰源(Interference):通信系统中干扰的集中反映(噪声)

1、简单信道模型



- □ 消息从信源通过信道到信宿,如何有效、可靠地传输,是 通信系统要解决的根本问题。
- 先说有效性 (Validity) 消息若在信源中先去粗取精,则必能提高通信的有效性 对数字通信来说,即信源编码 (Source Coding) 要解决的主要问题
- ➤ 再说可靠性 (Reliability)

信宿对接收到的"消息"若能够进行判断、评估,去伪存真的处理, 则必能提高通信的可靠性

对数字通信来说,信道编码(Channel Coding)的主要任务就是解决这个问题

1、简单信道模型 干扰源 信源 信道 信宿

- 口信源: 消息的源, 通常指向通信系统提供消息的人、设备或事物。
- ▶信源輸出的是以符号形式出现的具体消息,它载荷信息。
- ▶ 信源输出的消息有多种形式:

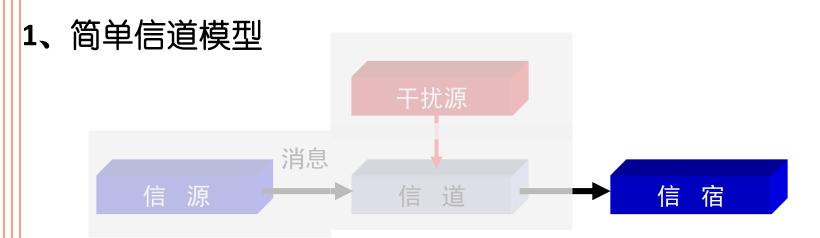
例如,从消息在时间上和幅度上的分布情况这一角度,可分为离散信源(Discrete Source)和连续信源(Continuous Source)。

前者指信源发出的消息在时间和幅度上都是离散分布的,如字母、文字、数字等符号组成的符号序列或单个符号

后者指在时间和幅度上都是连续分布的,如话音、图像等。

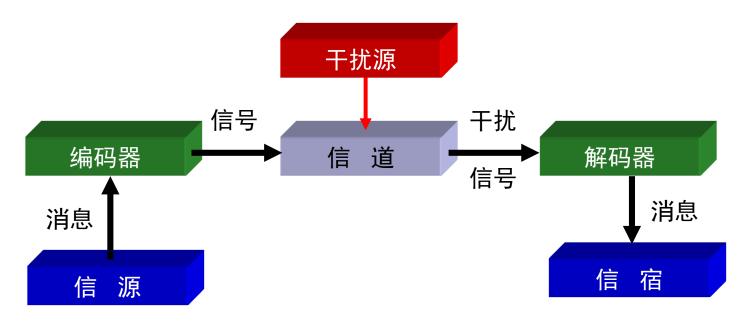
1、简单信道模型 干扰源 信源信道 信宿

- 口信道: 传递消息的通道, 广义上是指从信源到信宿间传递物理信号的媒质和设施。
- ▶信道的种类很多,如电信中常用的架空明线、同轴电缆、 波导、光纤、传输电磁波的空间等都是信道。
- ➤也可以从信道的性质或其传送的信号情况来分类,例如: 无干扰信道和有干扰信道、恒参信道和变参信道、离散信道 (Discrete Channel) 和连续信道(Continuous Channel)、单 用户信道和多用户信道等。



口信宿:消息传递的对象,即接收消息的人、设备或事物。 根据实际需要,信宿接收的消息,其形式可以与信源发出相同,也可以不同。当两者形式不同时,存在一个映射关系。

2、编码信道模型



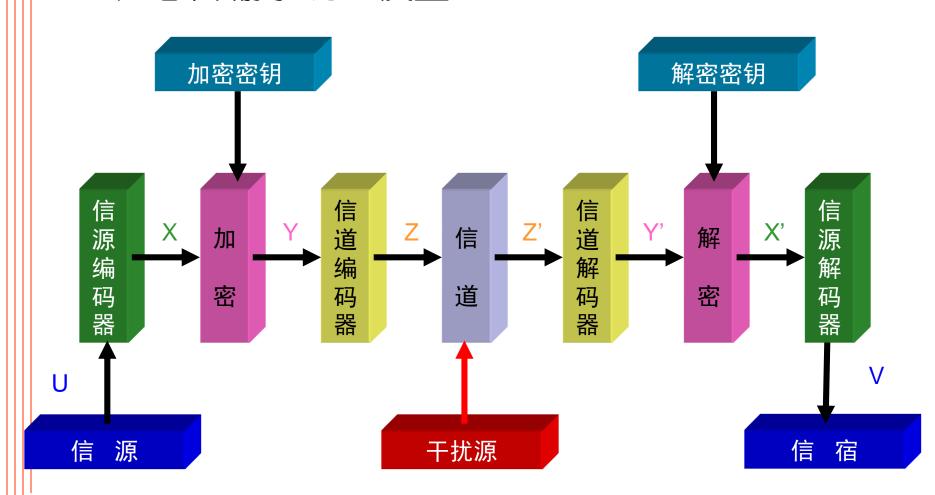
编码器(Encoder):将消息转换成为信号实现编码的设

备;

解码器(Decoder): 与编码器相反,是将编码信号进行

反变换的设备;

3、信息传输系统的模型



- 信源编码器(Source Encoder):将信源发出的消息,变换为由二进制(或者多进制)码元组成的的代码组的设备。
- 信源译码器(Source Decoder):将相应代码组译成信宿所能接收的消息的形式的设备。
- 信道编码器(Channel Encoder):为了提高信息传输的可靠性而对消息进行变换和处理的设备。
- 信道译码器(Channel Decoder): 对经过信道传输后的信号进行信道编码逆变换过程的设备。

- 加密编码器(Encryption Encoder): 将信源编码器输出的明文代码组变成密文代码组的设备。
- 加密密钥(Encryption Key):加密变换过程中使用的参数。

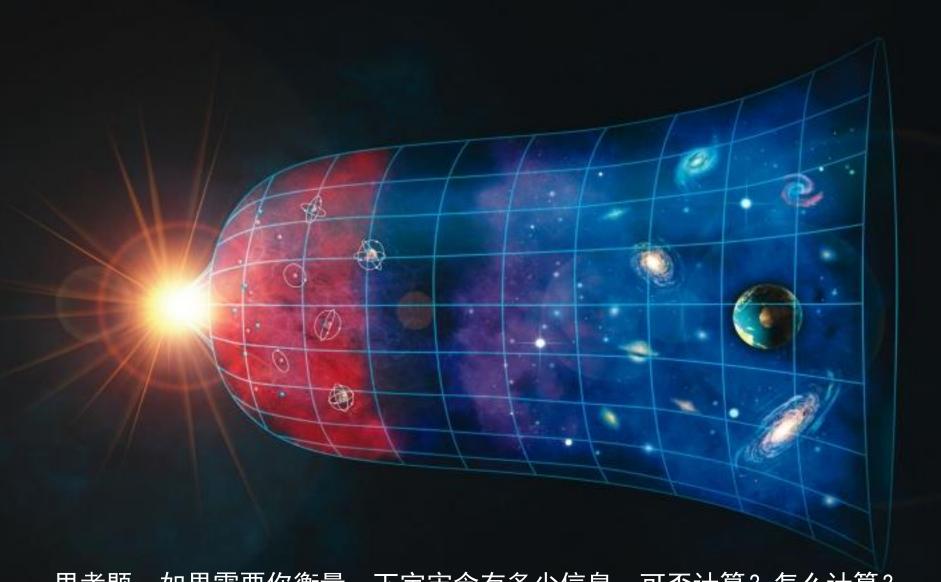
- 解密译码器(Decryption Decoder):将信道译码器输出的密文代码组变成明文代码组的设备。
- 解密密钥(Decryption Key): 解密变换过程中使用的参数。

1-5 课程内容安排

数据压缩-检错纠错-提高效率 提高可靠性 信源编码 信道编码 信息理论 ● 有噪声信道 ● 无失真 (数学基 信源编码理论 有噪声信道编码定理 础分析) 克拉夫特不等式 信道容量 ● 限失真编码 差错控制 限失真信源编码定理 编码方法 ● 变长符号编码 ● 纠错编码方法 (编码算 Huffman编码 Hamming编码 法实现) 费诺编码 BCH编码 游程编码 Turbo编码 算数编码 LZW编码 zhaoduo@swjtu.edu.cn

作业题

- 试说明信息、消息和信号三者的联系与区别.
- 从你的实际生活中列举出三种不同类型的通信系统模型,并说明它们各自包括的主要功能模块及 其作用.



思考题:如果需要你衡量一下宇宙含有多少信息,可否计算?怎么计算?