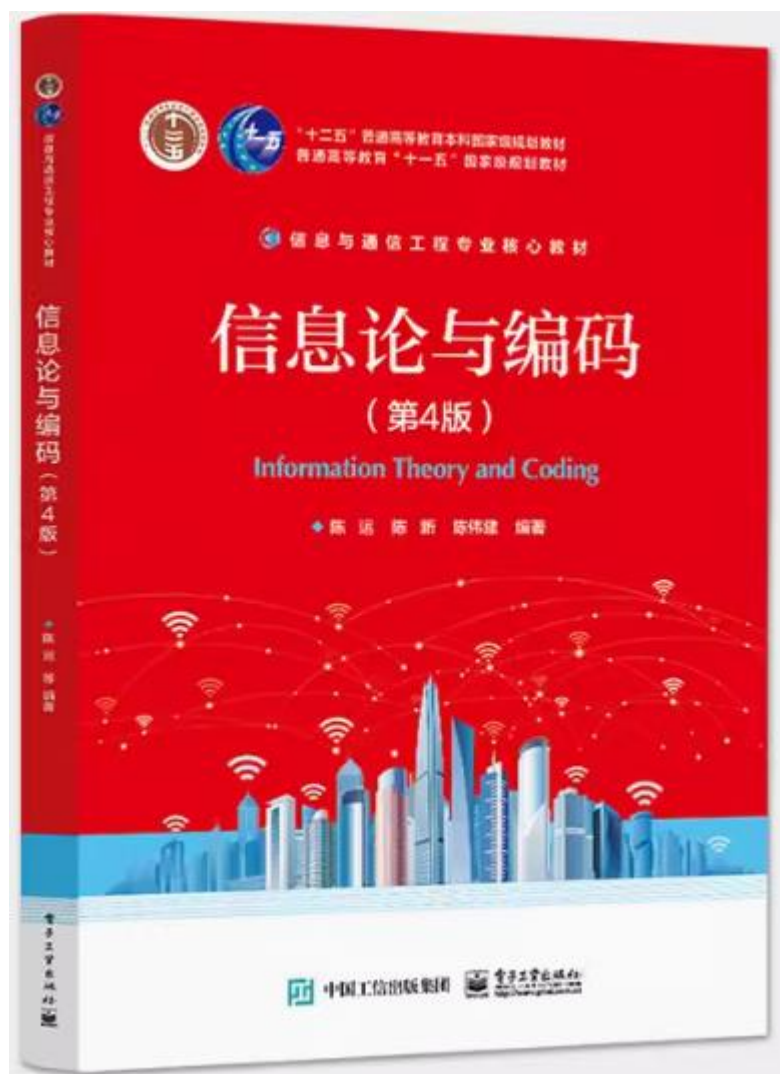


信息论基础

计算机科学与技术学院 孙伟平



教材：信息论与编码（第4版）

编著：陈运，陈新，陈伟建

电子工业出版社



第 1 章 概 论

第1章

1.1

信息的概念和分类

1.2

信息论的起源和发展

1.3

信息论的研究内容

1.1.1 信息的概念

生活中哪些场景下你会提到“信息”一词？

什么是信息？信息能度量吗？



没有物质一切都不会存在；没有能量一切都不会发生；
没有信息一切都没有意义。 ——欧廷格

要想有效地生活，就要有足够的信息。 ——维纳

在这三十年间，信息极大地释放了人类的能量，它所
创造的价值超过了之前五千年的财富总和。 ——雷军

中国《辞海》

音讯、消息；

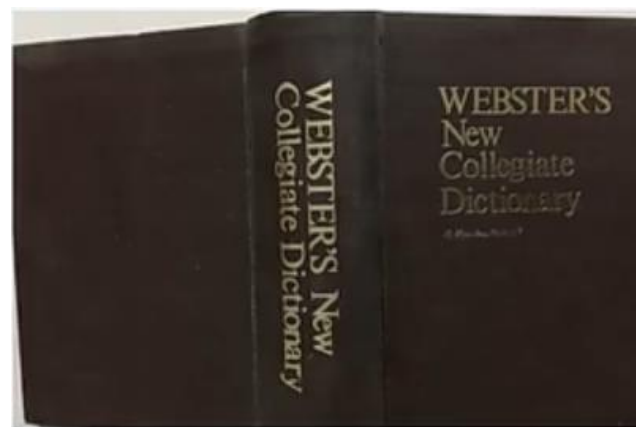
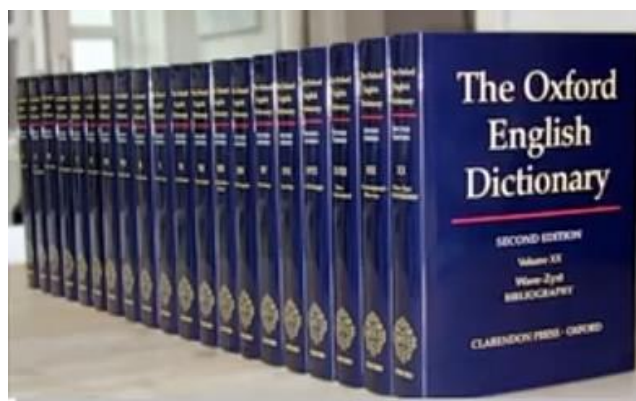
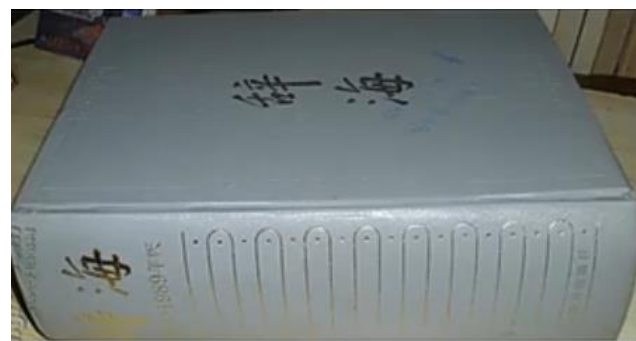
通信系统传输和处理的对象，泛指消息和信号的具体内容和意义。通常通过处理和分析来提取。

牛津英语词典

通过各种方式可以被传递、传播、传达、感受的，以声音、图像、文件所表征，并与某些特定事实、主题或事件相联系的消息、情报、知识都可统称为信息。

美国Webster's New Collegiate

由调查、研究和学习所得到的资料^{和知识}；
知识、学问和新闻； 事实、情况和数据；
表示数据的记号、信号和标识。



信息不等同于情报

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。

信息不等同于知识 新知识

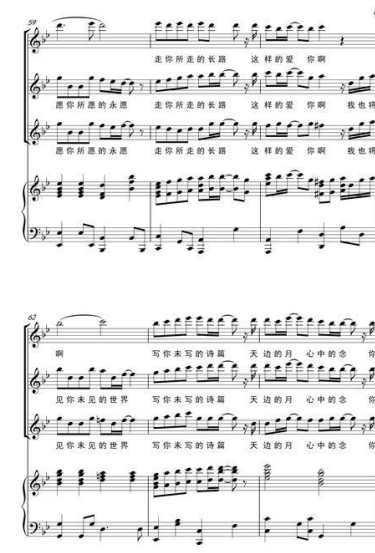
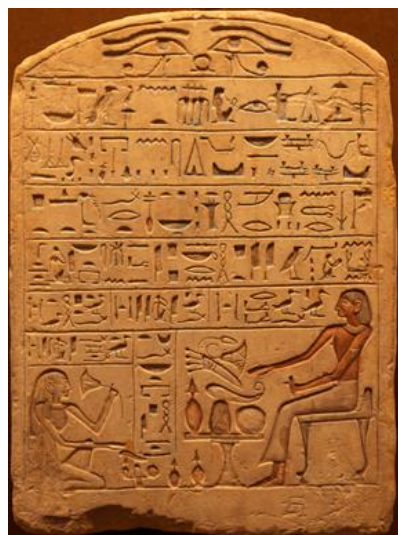
知识是以实践为基础，通过抽象思维，对客观事物规律性的概括。

信息不等同于消息 消息是信息的外壳，信息是消息的内核

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。

信息不等同于信号 信号是信息的载体，信息是信号所载荷的内容

把消息换成适合信道传输的物理量（如电信号、光信号、声信号、生物信号等），这种随时间变化的物理量称为信号。



那么信息究竟是什么呢？

太阳从东方升起。

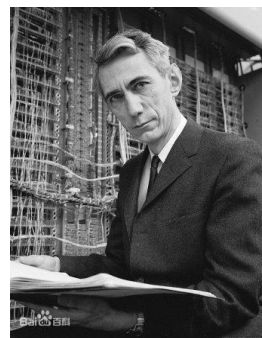
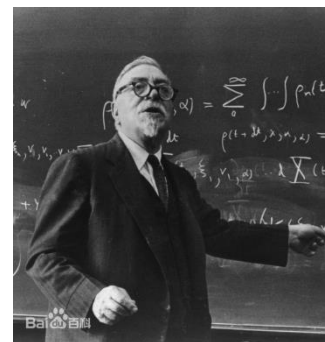
确定

我看到了一只白色的麻雀。

不确定



纽约比克曼酒店



信息是不确定性的辨析度。利用信息消除不确定性，建立新时代的世界观和方法论。

用严格的数学公式定义的科学名词

- 与内容无关
- 独立于形式
- 信息是可以度量的
——统计信息

信息是事物运动状态或存在方式**不确定性**的描述。

- 信息的基本概念在于它的不确定性，任何确定的事物都不会有信息。

信源输入	码字输出	消息 先验概率	收到消息后的后验概率		
			收到0	收到01	收到011
X1	000	1/8	1/4		
X2	001	1/8	1/4		
X3	010	1/8	1/4	1/2	
X4	011	1/8	1/4	1/2	1
X5	100	1/8			
X6	101	1/8			
X7	110	1/8			
X8	111	1/8			

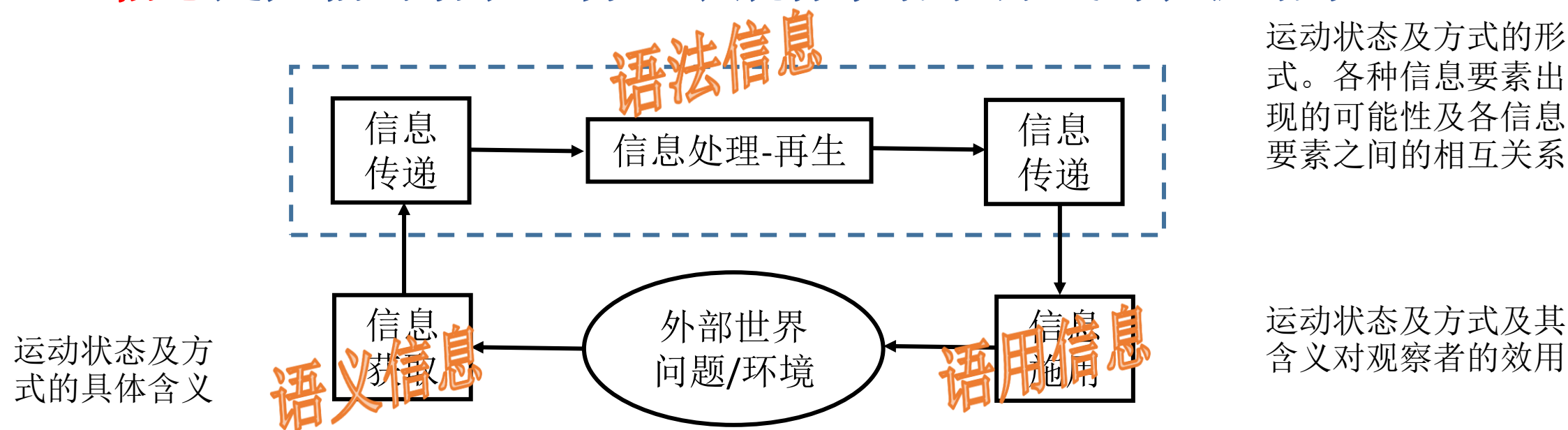
收到消息 → 不确定性减少
获得了信息

统计信息：

信息是事物运动状态或存在方式**不确定性**的描述。

全信息：

信息是人们对客观世界运动规律和存在方式的认识结果。



1.1.2 信息的分类

按照信息的性质	语法	语义	语用
按照观察的过程	实在	先验	实得
按照信息的地位	客观	主观	
按照信息的作用	有用	无用	干扰
按照信息的逻辑意义	真实	虚假	不定
按照信息的传递方向	前馈	反馈	

按照信息的生成领域

宇宙

自然

社会

思维

按照信息的应用部门

工业

农业

军事

政治

科技

文化

经济

市场

管理

按照信息的来源

语声

图象

文字

数据

计算

按照信息载体的性质

电磁

语声

图象

文字

光学

生物

按照携带信息的信号的性质

连续

半连续

离散

第1章

1.1

信息的概念和分类

1.2

信息论的起源和发展

1.3

信息论的研究内容

在人类历史的长河中，信息传输和传播手段经历了五次重大变革。



语言的产生



文字的产生



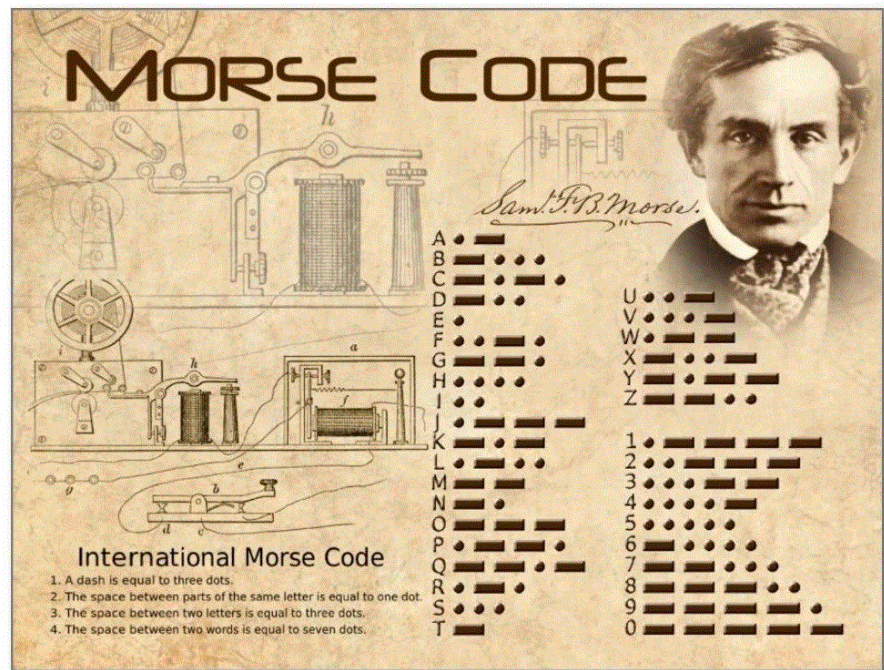
印刷术的发明



电报、电话的发明



计算机技术与通信技术相结合，促进了网络通信的发展



酝酿期

19世纪30年代至20世纪30年代

创立期

20世纪30年代 ~ 40年代

发展期

20世纪50年代起

➤ 19世纪:

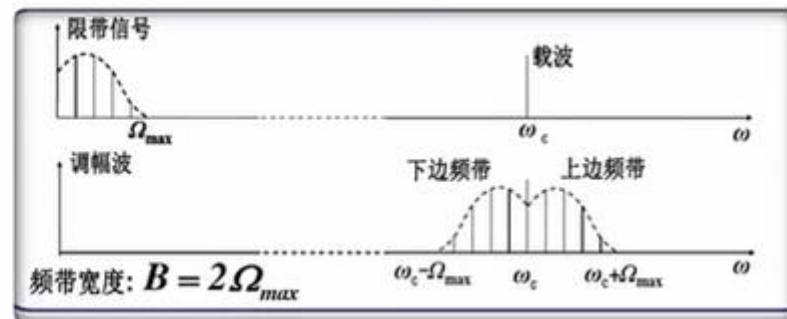
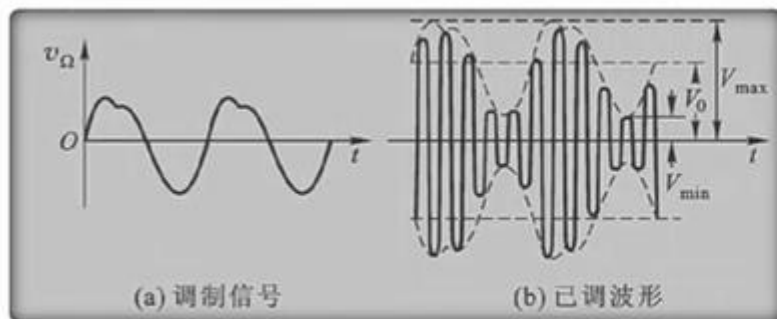
主要问题: 如何获得信息的电气表现形式及进行远距离传输。

- 1832年J.Henry发明电报;
- 1838年F.B.Morse发明电码;
- 1876年Bell发明电话;
- 1895-1896年Marconi和Popov发现无线电通信;
- 1904年Fleming发明二极管, 1906年Forest发明三极管放大器。

➤ 20世纪30年代以前：

主要问题：如何提高信道利用率。

- 1917年G.A.Campbell申请了第一个关于滤波器的专利；
- 1922年J.R.Carson对振幅调制信号进行了研究；
- 1924年H.Nyquist开始研究电报信号传输中脉冲速率与信道带宽的关系，建立带限信号的采样定理；
- 1928年哈特莱发表“信息的传输”，对信息量作了定义。



拉普拉斯决定论（宿命论观点）：

“世间一切系统的因果关系都可以包含在确定性的微分方程之中，只要能够给定相应方程的初始条件，就可以唯一地确定这个系统在未来任何时刻的结果。”

➤ **20世纪30年代~40年代：**

主要问题：通信中的噪声和抗干扰问题。

以香农为代表的学者的唯物论观点：

事物发展变化的因果关系是复杂的，既具有必然性，又存在偶然性，因而事件的结局存在不确定性。正是存在不确定性，人们才需要获得信息来消除这样的不确定性。

➤ **20世纪30年代~40年代:**

主要问题: 通信中的噪声和抗干扰问题。

- **1930年N.Wiener把Fourier分析方法全面引入随机信号的研究中;**
- **1936年V.D.London发表有关噪声的论文, E.H.Armstrong提出频率调制;**
- **1939年H.Dudley发明声码器, H.Reevet提出脉冲编码调制;**
- **1944-1945年S.O.Rice发表“Mathematical analysis of random noise”,
对噪声的研究作了全面的总结;**
- **1948年N.Wiener发表《控制论》, C.E.Shannon发表“通信中的数学理论”, 奠定信息论的基础。**

➤ 20世纪50年代起:

主要问题：信源编码和信道编码的具体构造方法以及保密通信问题的研究。

“通信系统的中心问题是在噪声下如何有效而可靠地
传送信息，而实现这一目标的主要方法是编码”。

——香农

1. 无失真信源编码

- 1952年，Huffman编码
- 1963年，P.Elias算术编码
- 1965年，A.N.Kolmogorov通用编码

2. 信道编码

- **1950's, Hamming**汉明码（最早用于纠错的线性分组码）
- **1955年, Elias**卷积码
- **1957年, Prange**循环码
- **1959年, Hocquenghem、Bose和Chaudhuri**提出BCH码
- **1961年, Wozencraft**提出序列译码方法
- **1967年, Viterbi**提出卷积码的最大似然译码- **Viterbi**码
- **1960年, Reed和Solomon**提出RS码，**1965年Berlekamp**迭代译码算法为RS码的实际应用扫清了障碍

- 1960's, 香农的学生Robert Gallager发明了LDPC码, 后来高通在此基础上开发形成了**5G标准**
- 1966年, Forney提出级联码, 尽可能接近香农极限
- 1980's, Goppa等提出代数几何码
- 1982年, G.Ungerboeck等提出TCM (编码调制)
- 1993年, C.Berrou等提出了Turbo码, 距香农极限0.7dB
- 1995年, Mackey和Neal重新发现LDPC码, 距香农极限0.0045dB
- 2007年, Erdal Ariken发明了Polar码, 华为在此基础上开发形成了**5G标准**

年份	1/2码率	BER<10 ⁻⁵
1948	Shannon	0dB
1967	(255,125)BCH	5.4dB
1977	卷积码	4.5dB
1993	Turbo码	0.7dB
2001	LDPC码	0.0045dB



华为Polar Code是一个5G短码块的信道编码方案，其在2016年11月14日到18日期间美国Reno举行的3GPP RAN1 #87会议中战胜了美国的LDPC方案和法国的Turbo2.0方案，成为了5G控制信道eMBB场景编码最终方案。

3. 限失真信源编码

- 1959年，Shannon发表“保真度准则下的离散信源编码定理”
- 1966年，线性预测编码实验
- 1968年，变换编码，采用二维离散傅里叶变换
- 1971年，T.Berger“信息率失真理论”
- 80年代以后，信源编码得到迅猛发展

包括了数据压缩理论、语音压缩编码技术、图像压缩编码技术、视频压缩编码技术等分支。

4. 保密编码（略）

1928年，**哈特莱 (Hartley)** 首先提出了**用对数度量信息**的概念。

Hartley的工作给Shannon很大的启示, 他在1941~1944年对通信和密码进行深入研究, 用**概率论**和**数理统计**的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**。

- 1 阐明通信系统传递的对象;
- 2 提出了信息熵的概念;
- 3 指出通信系统的中心问题;
- 4 指明了解决问题的方法。

以上这些成果1948年以“通信的数学理论” (A mathematical theory of communication) 为题公开发表，标志着信息论的正式诞生。这是一篇信息论开创性的权威论文，为信息论理论建立了基础。

维纳 (Wiener) 在研究火控系统和人体神经系统时，提出了在干扰作用下的信息最佳滤波理论，成为信息论的一个重要分支。

20世纪60年代以后

1. 1961年Shannon“双路通信信道”。

2. 1971年R.Ahlsvede和1972年H.Liao找出了多元接入信道的信道容量区；1973年J.K.Wolf和D.Slepian推广到具有公共信息的多元接入信道；T.M.Cover、R.Ahlsvede于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。

3. 1972年T.M.Cover提出了广播信道的研究。P.Bergmans(1973)、R.G.Gallager(1974)、科弗尔(1975)、K.Mar-ton(1979)、A.El Gamal(1979)和E.C.Van der Meulen(1979)等分别研究了广播信道的容量区问题。

4. 中继信道的研究,由E.C.Van der Meulen (1977)首先引入, T.M.Cover和A.El Gamal找到了降阶中继信道的容量区(1979年)。

当今。。。。。

网络信息论、物理层安全、广义信息论

信息论的未来发展趋势

- 学科的交叉和技术的融合产生新的信息技术。
- 量子信息理论将迅速发展。
- 信息运动要素的挖掘和利用将成为关注的热点。

信息论自诞生到现在，在人类科学史上是相当短暂的。但它的发展和对学术界及人类社会的影响是相当广泛和深刻的。信息作为一种资源，如何开发、利用、共享，是人们普遍关心的问题。

第1章

1.1

信息的概念和分类

1.2

信息论的起源和发展

1.3

信息论的研究内容

▶ 信息不是静止的，它会产生也会消亡，人们需要获取它，并完成它的传输、交换、处理、检测、识别、存储、显示等功能。研究这方面的科学就是信息科学。

▶ 信息论是信息科学的主要理论基础之一。它研究信息的基本理论，主要研究可能性和存在性问题，为具体实现提供理论基础。

▶ 信息技术主要研究如何实现、怎样实现的问题。

信息论

一门应用概率论、随机过程、数理统计和近代代数的方法，来研究信息传输、提取和处理系统中一般规律的学科。

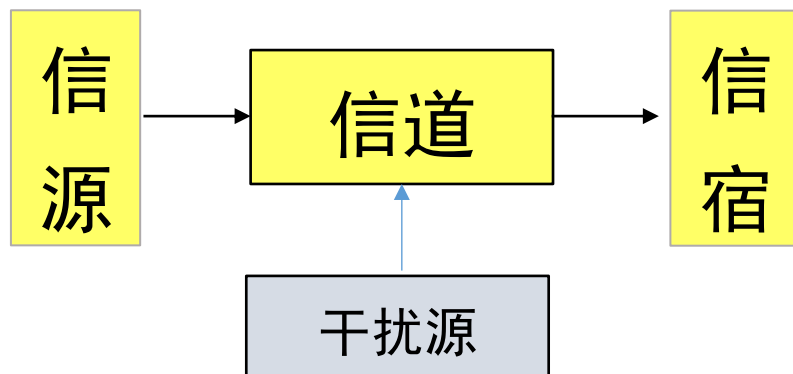
基本内容

在信息可以量度的基础上，研究有效地和可靠地传递信息的科学。

13.1 通信系统模型

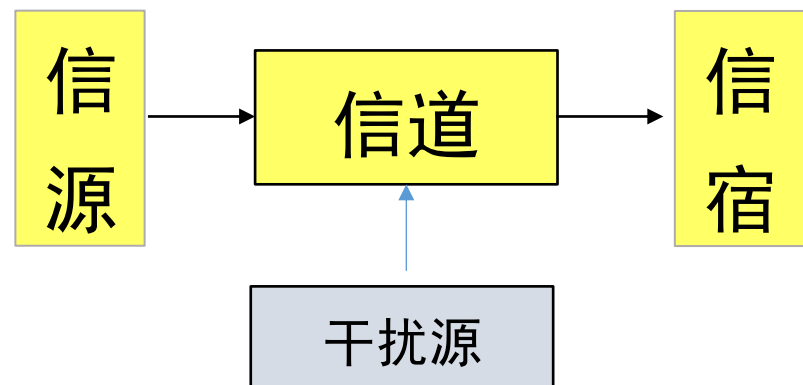
A Mathematics Theory Of Communication

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



- 信源 **Source**
- 信宿 **Destination**
- 信道 **Channel**

简单通信系统模型



- 信源

- 产生消息的源，消息可以是文字，语言，图像。可以离散，可以连续。随机发生。
- 研究的主要问题是消息的统计特性和产生信息的速率。

- 信宿：信息的接收者

- 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。
- 信道的中心问题是研究信道的统计特性和传信能力，即信道容量。

- 干扰源

- 系统各部分引入的干扰，包括衰落，多径，码间干扰，非线性失真，加性噪声，主要是统计特性。

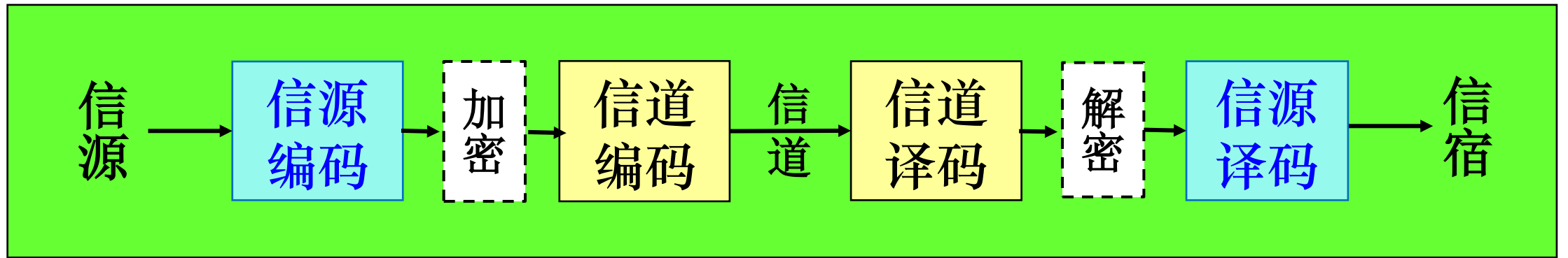


图1.3.1 通信系统基本模型

【注意】

(1) 图1.3.1给出的模型只适用于收发两端单向通信的情况，只有一个信源和一个信宿，信息传输也是单向的。

更一般的情况是信宿和信源各有若干个，即信道有多个输入和多个输出，信息传输也可以是双向的。

(2) 研究这样一个概括性很强的通信系统的目的，就是要找到信息传输过程中的共同规律，以提高信息传输的可靠性、有效性、保密性和认证性，从而达到信息传输系统最优化。

信息的可靠性、有效性、保密性、认证性

(1) **可靠性**：使信源发出的消息经过信道传输以后，尽可能准确、不失真的再现在接收端；

(2) **有效性**：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；

(3) **保密性**：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接收，而不能被未授权接收者接收和理解；

(4) **认证性**：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，而不是伪造和篡改的。

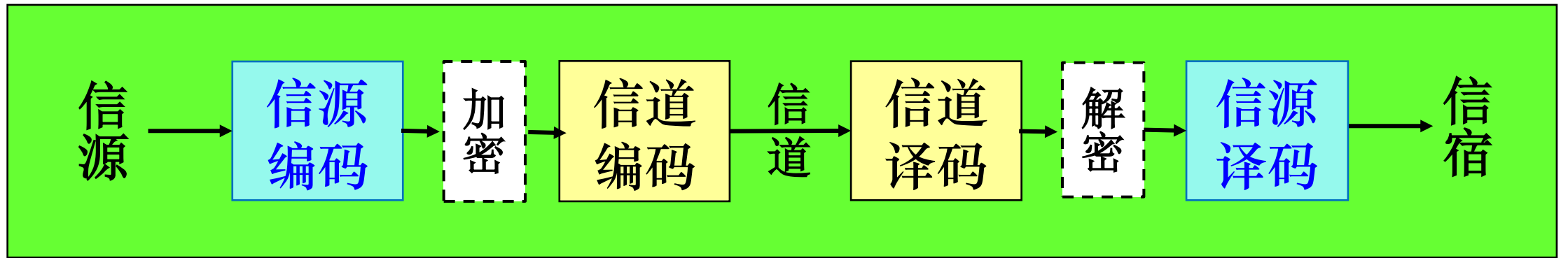


图1.3.1 通信系统基本模型

(3) 不是所有的通信系统都采用图1.3.1所示的那样全面的技术，例如，点对点的有线电话只需一对电话机和一条电话线路（铜线）即可，话音基带信号通过电话机变为相应的电信号（模拟信号），即在电话线上传送，接收端的电话机再把电信号恢复成人耳能听到的话音。

如果是点对点的无线电话，需要在发送端加一台发射机，将模拟信号调制到射频上，再用大功率发射机经天线发射出去，经无线信道传输,接收端的收信机把收到的调制射频信号解调恢复为发送端的原始话音；

如系统需保密则可在系统中增加加密和解密装置，就构成无线保密通信系统；

如传输中干扰大、信道容量有限，则需加入信源编码和信道编码技术，以提高传输消息的有效性和可靠性。

13.2 信息论研究内容

信息论的研究对象是广义通信系统。不仅电子的、光学的信号传递系统，任何系统，只要能够抽象成通信系统模型，都可以用信息论研究，如神经传导系统、市场销售系统等等。关于信息论的研究内容，一般有以下三种解释：

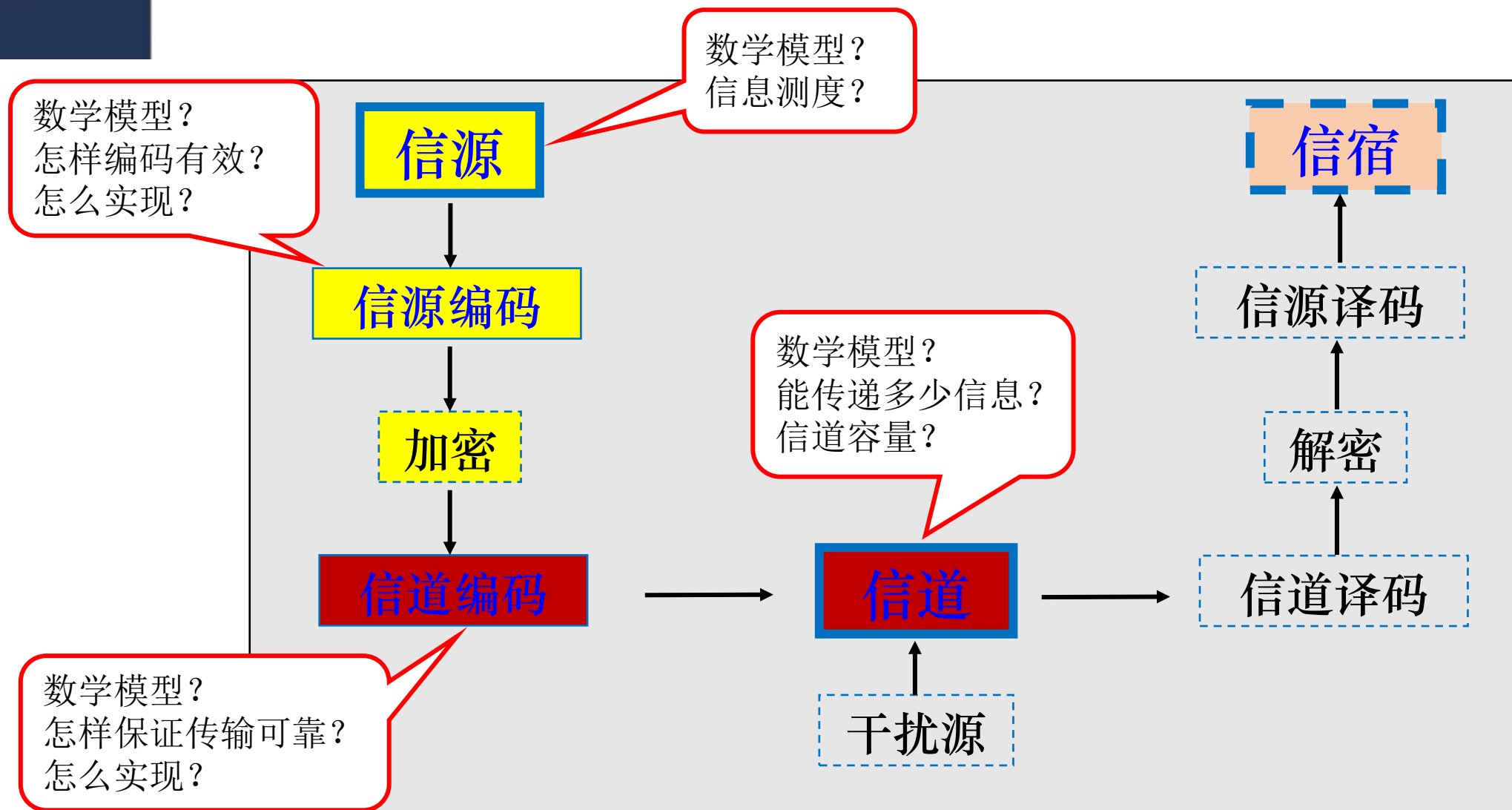
1 信息论基础

亦称香农信息论或狭义信息论。主要研究信息的测度、信道容量、信息率失真函数，与这三个概念相对应的香农三定理以及信源和信道编码。

	对应关系		对应关系		对应关系	
理 论	无失真 信源编码 定理		信道编码 定理		限失真 信源编码 定理	
概 念	信源熵		信道容量		率失真函数	
技 术	无失真 信源编码、 密码		信道编码		限失真 信源编码	

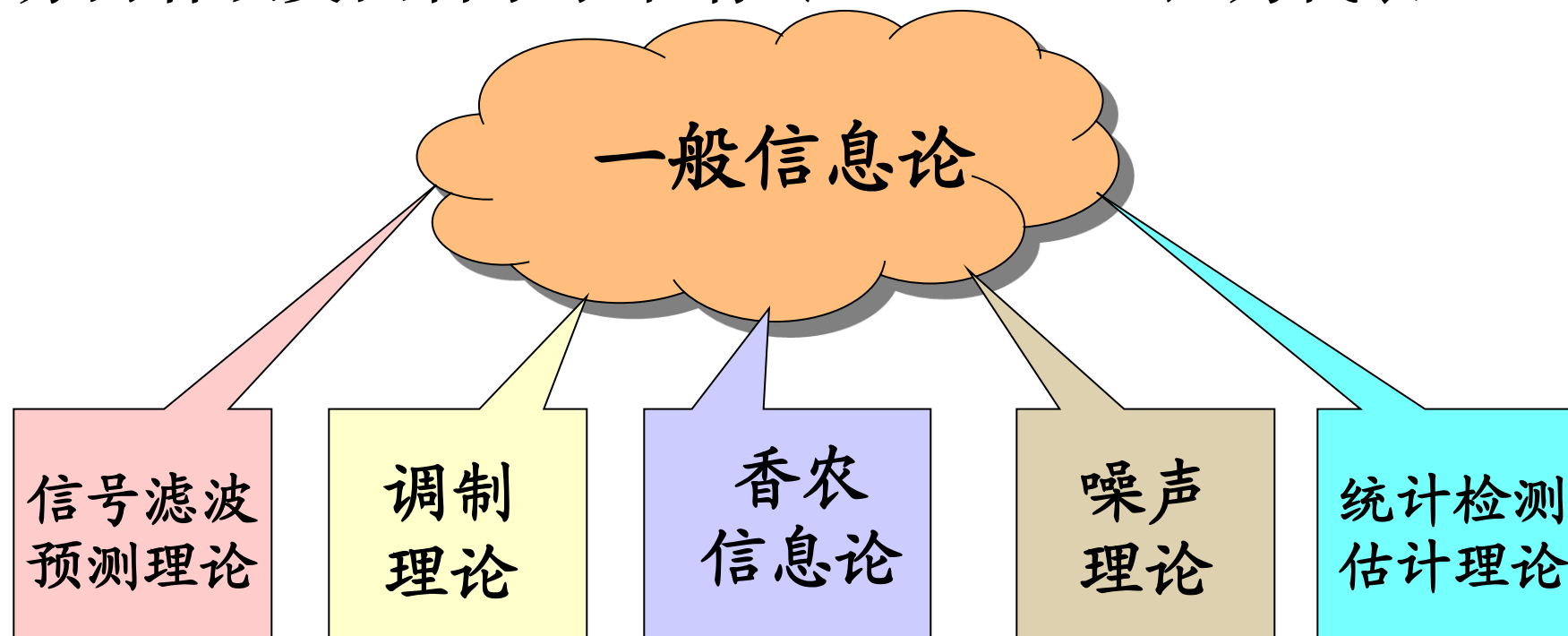
基本内容

在信息可以量度的基础上，
研究有效地和可靠地传递
信息的科学。

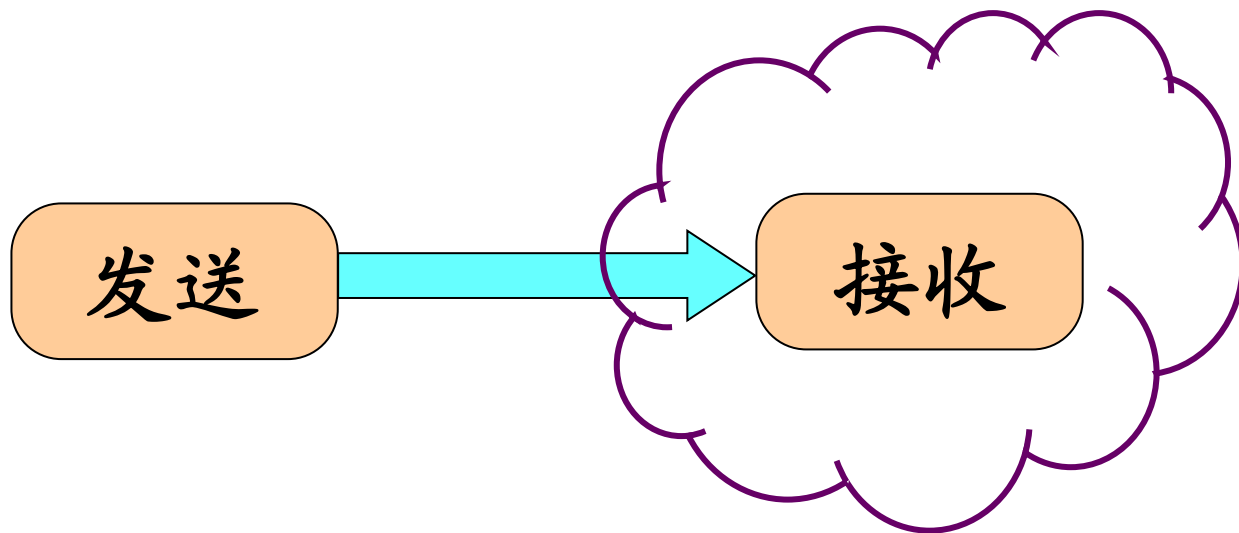


2 一般信息论

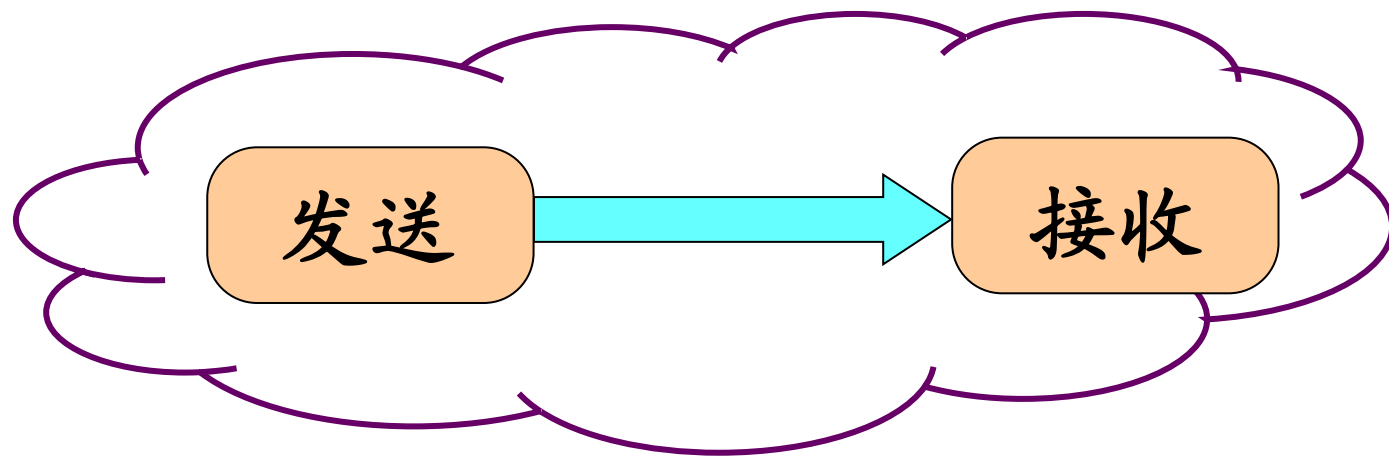
主要是研究信息传输和处理问题。除了香农基本理论之外，还包括噪声理论、信号滤波和预测、统计检测与估计理论、调制理论。后一部分内容以美国科学家维纳（N·Wiener）为代表。



维纳和香农等人都是运用概率和统计数学的方法研究准确或近似再现消息的问题，都是通信系统的最优化问题。但他们之间有一个重要的区别。



维纳研究的重点是在接收端。研究消息在传输过程中受到干扰时，在接收端如何把消息从干扰中提取出来，并建立了最佳过滤理论（维纳滤波器）、统计检测与估计理论、噪声理论等。

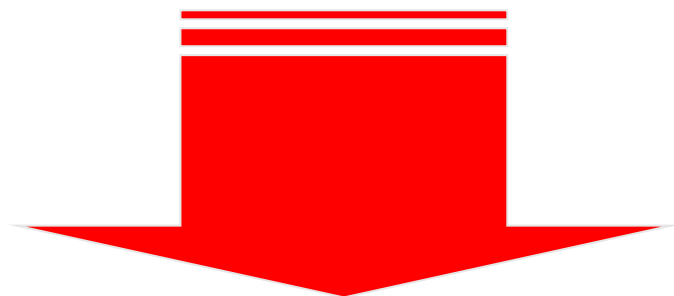


香农研究的对象是从信源到信宿的全过程，是收、发端联合最优化问题，重点是编码。为此，发展了信息测度理论、信道容量理论和编码理论等等。

3 广义信息论

概括说来，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。

反过来，所有研究信息的识别、控制、提取、变换、传输、处理、存贮、显示、价值、作用、安全以及信息量的大小的一般规律以及实现这些原理的技术手段的工程学科，信息论的完备和延伸，也都属于广义信息论的范畴。



总之，人们研究信息论的目的是为了高效、可靠、安全并且随心所欲地交换和利用各种各样的信息。

第1章 小结

1. 掌握信息的定义；
2. 能简述一个通信系统包括的各主要功能模块及其作用；
3. 了解信息论的研究内容（三种理解）；
4. 掌握信息论基础课程的研究内容（11个问题）。

课时安排

章 节	课时	
第1章 概论	2	
第2章 离散信源熵	10	作业点评，专题讨论
第3章 无失真离散信源编码	4	
第4章 离散信道容量	8	
第5章 纠错编码	6	作业点评
总复习	2	拓展连续信源熵

成绩评定

- 平时成绩（占总成绩的30%）
 - 课堂参与
 - 作业
 - 课堂小测验
- 期末考试（占总成绩的70%）
 - 闭卷笔试

作业：每周一交作业，作业有有效期

请注明班号，学号，姓名

All students participating in the class must agree to abide by the following code of conduct:

1. My answers to homework, quizzes and exams will be my own work (except for assignments that explicitly permit collaboration)
2. I will not make solutions to homework, quizzes or exams available to anyone else.
3. I will not engage in any other activities that will dishonestly improve my results or dishonestly improve/hurt the results of others.

摘自coursera

资源

 中国大学MOOC

课程 ▾

学校

学校云



首页 > 工学



3 位授课老师



刘刚
副教授



冯磊
讲师



黄云
助教

概率论中的基本概念和公式

随机试验-样本空间-随机事件

概率-条件概率-联合概率

全概公式-贝叶斯公式

先验概率-后验概率-转移概率

随机变量：定义在样本空间取值在实数域的函数，
自变量是随机试验的结果，其取值也有随机性。

概率分布函数-概率密度函数

数学期望 -方差

1) 条件概率

$$P(A | B) = \frac{P(AB)}{P(B)}$$

$$P(B | A) = \frac{P(AB)}{P(A)}$$

2) 联合概率

$$P(AB) = P(B)P(A | B)$$

$$P(AB) = P(A)P(B | A)$$

3) 全概公式

设 B_1, B_2, \dots 是一列互不相容的事件 ($B_i B_j = \emptyset$) ,

且有 $B_1 \cup B_2 \cup \dots = \Omega$ (样本空间) ;

$P(B_i) > 0, i=1, 2, \dots$, 则对任一事件A, 有:

$$P(A) = \sum_i P(B_i)P(A|B_i) = \sum_i P(AB_i)$$

4) 贝叶斯(Bayes)公式

设 B_1, B_2, \dots 是一列互不相容的事件 ($B_i \cap B_j = \emptyset$) ,
且有 $B_1 \cup B_2 \cup \dots = \Omega$ (样本空间) ;

$P(B_i) > 0$, $i=1, 2, \dots$, 则对任一事件A, 有:

先验概率

似然函数

$$P(B_i | A) = \frac{P(B_i)P(A | B_i)}{\sum_{i=1} P(B_i)P(A | B_i)} = \frac{P(B_i)P(A | B_i)}{P(A)}$$

后验概率