信息论基础

倪江群 中山大学信息科学与技术学院

9/2016

教材和参考资料

✓ 课堂教材

□ 田宝玉,〈信息论基础〉,人民邮电出版 社,第一版,2008年。作业布置依据

✓ 参考教材

- Thomas M. Cover and Joy A. Thomas, (Elements of Information Theory), Jone Wiley & Sons, Inc. 1991.
- □ Gallager, ⟨Information Theory of Reliable Communication⟩, Jone Wiley & Sons, Inc. 1968.

教学内容

内容		估计学时	
	第1章:	绪论	3
	第2章:	离散信息的度量	3
	第3章:	离散信源	4
	第4章:	连续信息和连续信源	4
	第5章:	无失真信源编码	4
	第6章:	离散信道及其容量	4
	第7章:	有噪信道编码	3
	第8章:	波形信道	4
	第9章:	信息率失真函数	3
	课外阅	读	
	第10章	: 有约束信道及其编码	
	第11章	: 网络信息论	

有关授课教师

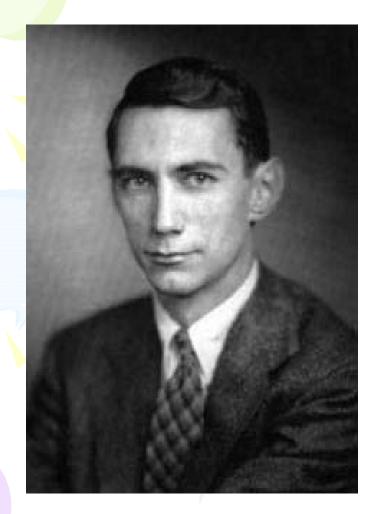
倪江群教授简介

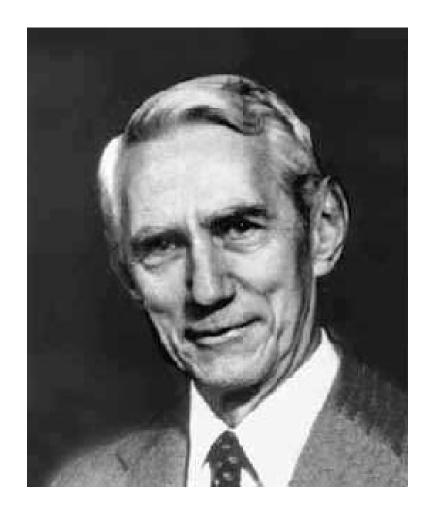
倪江群于1998年6月在香港大学电机与电子工程学系获博士学位, 1998年10月至2000年10月在中山大学和广东省电信科学技术研究院博 士后工作站工作。 2000年至今在中山大学信息科学与技术学院工作, 目前为教授、博士生导师,电子与通信工程系主任。倪江群博士的研 究方向为多媒体信号处理和通信、多媒体信息隐藏和信息取证、数字 电视关键技术、嵌入式系统和应用。他主持了多项包括科技部重大国 际合作项目、国家自然科学基金、国家115电子发展基金、广东省自然 科学基金重点项目在内的国家和省部级科技项目, 他曾参与著名华裔 科学家丁肇中教授领导的大型国际科技合作项目"阿尔法磁谱仪(AMS-02)",并主持其中硅微条轨迹探测器热控系统(TTCS)的电子 控制系统,中山大学参与研制的热控制系统是国内大学参加AMS-02项 目中唯一在太空运行的装置。

第1章缩论

信息论即香农(Claude Edwood Shannon, 1916—2001)信息论,也称经 典信息论,是研究通信系统极限性能的理 论。从信息论产生到现在几十年来,随着 人们对信息的认识不断深化,对信息论的 研究日益广泛和深入,信息论的基本思想 和方法已经渗透到许多学科,在人类社会 已经进入信息时代的今天,信息理论在自 然科学和社会科学研究领域还会发挥更大 的作用。

Shannon和信息论





C. Shannon (1916-2001) - 比特之父 1948年创立信息论

· 柯尔莫果洛夫对Shannon的评价:

"在我们时代,当人类的知识变得越来越专门化时,Claude E. Shannon是卓越的例外。他把深邃的抽象数学思维与对实际技术关键问题的广泛、具体的理解相结合。他可以同时被认为是近几十年来伟大的数学家和伟大的工程师。"

• A. Viterbi 对信息论的评价:

I have often remarked that the transistor and information theory, two Bell Laboratories breakthroughs within months of each other, have launched and powered the vehicle of modern digital communications. Solid state electronics provided the engine while information theory gave us the steering wheel with which to guide it.

• Shannon基本理论

- 消息A的信息度量为: $I(A) = -Log_a P(A)$
- 不确定性度量(熵): $H(X) = E\{-Log_a P(X)\}$
- 信息量度量: I(X;Y) = H(X) H(X|Y)
- 高斯信道容量: $C = W \log \left(1 + \frac{P}{N}\right)$
- Shannon信道编码定理:
- Shannon信源编码定理(率失真):
- Shannon理论对(端对端)通信发展的影响信源与信道编码分离定理;纠错编码发展;率失真理论; 压缩编码技术;编码调制(TCM);扩谱技术(CDMA);
 正交频分复用(OFDM);多天线技术(MIMO);资源优化;

本章主要的容

- ▶信息的基本概念
- ▶香农信息论研究的内容
- ▶香农信息论产生的背景、主要研究进展和应用

§ 1.1 信息的基本概念

本节内容:

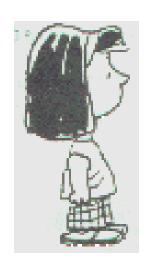
- ◆ 信息论的产生
- ◆ 信息的基本概念
- ◆ 信息论的基本内容

1.1.1 信息论的产生

客观世界三大基本要素 — 能量 信息

信息时代社会的发展离不开物质(材料)、能量(能源)和信息资源。美国学者欧廷格说:"没有物质什么都不存在,没有能量什么都不发生,没有信息什么都没意义。"

按理说,关于信息的课程应该象物理、化学、生物等课程一样,是基础课。但是,由于信息的抽象性以及当前人们对信息的认识并不完全清楚,所以在当前只能是专业课。



1948年,美国工程师和数学家香农(Claude Edwood Shannon, 1916-2001)发表了《通信的数学理论》(A Mathematical Theory of Communication, BSTJ, 1948)标志着信息论的产生。

通信的基本问题:在一点精确地或近似地恢复另一点所选择的消息。看另一点所选择的消息。

● 通信系统三项性能指标:

传输的有效性 传输的可靠性 传输的安全性

有效性

对于离散信源,信源符号平均码长度应尽量短;

信息传输应尽量快,即高的传信率;信息传送应该有高的频谱利用率;

夢 可靠性

传输差错要尽量少 , 对数字传输就是要求低的误码率。

安全性

传输的信息不能泄露给未授权人。

◆ 三项指标所对应的三项基本技术:

数据压缩 - 有效性

数据纠错 - 可靠性

数据加密 - 安全性

香农信息论解决了前两项技术的理论问题: 提高有效性可通过信源编码来实现,即信源压缩 编码,并给出了压缩编码的极限;提高可靠性通 过信道编码来实现,并给出实现可靠信息传输速 率的极限(信道容量)。所以说,香农奠定了数 据压缩和传输的基本定律。 实际上传输安全性的问题也是香农最先解决的。 1945年,他写了《密码学的数学理论》(A Mathematical Theory of Cryptography),1949年 改名为《保密系统的通信理论》(Communication Theory of Secrecy System)公开发表。这篇文章 建立了保密系统的数学理论,对密码学产生了很大 的影响。

所以说,香农个人建立了通信中的三个基本问题的理论基础,而信息论主要是前二个问题的理论基础。

1.1.2 信息的基本概念

信息已成为众多学者争相研究的对象,迄今已有上百种有关信息的定义或说法。

例如: "信息是事物之间的差异"、"信息是收信者事先不知道的东西"等。

如前所述,由于当前还没有一个公认的 关于信息的定义,但这并不影响我们对信息 的基本特征的认识。信息有许多与物质、能 量相同的特征,例如信息可以产生、消失、 携带、处理和量度。信息也有与物质、能量 不同的特征,例如,信息可以共享,可以无 限制地复制等。 • 1949年,Weaver在《通信的数学》中解释香农的工作时,把通信问题分成三个层次:

第一层:通信符号如何精确传输? (技术问题)

第二层:传输的符号如何精确携带所需要的含义? (语义问题)

第三层: 所接收的含义如何以所需要的方式有效 地影响行为? (效用问题)

• Weaver认为香农的工作属于第一层,但他又证明 香农的工作是交叉的,对第二、三层也有意义。

- 信息是认识主体(人、生物、机器) 感受和表达事物运动状态/运动状态变化的方式。
- 以这种定义为基础,信息分成三个基本层次,即语法信息,语义信息,语用信息,分别反映<u>认识</u>主体和事物运动<u>状态</u>及其变化方式间<u>交互</u>的外在形式、内在含义和效用价值。
- 与Weaver对信息的解释基本一致。

信息的三个基本层次:

- ➤ <u>语法(Syntactic)信息</u>
- ➤ <u>语义(Semantic)</u> 信息
- ➤ 语用(Pragmatic)信息

语法(Syntactic)信息

它是事物运动的状态和变化方式的外在形式,不涉及状态的含义和效用。象语言学领域的"词与词的结合方式",而不考虑词的含义与效用。在语言学中称为语法学。语法信息还可细分为,概率信息、偶发信息、确定信息、模糊信息等。基于对语法符号的描述方式

语义(Semantic) 信息

是事物运动的状态和变化方式的含义。 在语言学里,研究"词与词的结合方式含 义"的学科称为语义学。

语用(Pragmatic)信息

是事物运动状态及其状态改变方式效用

信息三个层次的含义

有一个情报部门,其主要任务是对经济情报 进行收集、整理与分析以提供给决策机构。该部 门设三个组: 信息收集组、信息处理组和信息分 析组。信息收集组的任务是将收集到的资料按中 文、英文或其他文字、明文、密文进行分类,不 管这些资料的含义如何都交到信息处理组。信息 处理组根据资料的性质进行翻译或破译得到这些 资料的含义,然后交到信息分析组。信息分析组 从这些资料中挑选出有价值的情报提交给决策机 构。

可见,信息收集组是根据所得到的消息提取出语法信息,信息处理组是根据所得到的语法信息提取出语义信息,而信息分析组是根据所得到的语义信息提取出语用信息。

可以看到,研究语义信息要以语法信息为基础,研究语用信息要以语义信息和语法信息为基础。三者之间,语法信息是最简单、最基本的层次,语用信息则是最复杂、最实用的层次。

香农在1948年指出:

"通信的基本问题是在一点精确地或近似地恢复 另一点所选择的消息。通常,这些消息是有含义 的,即它对于某系统指的是某些物理的或概念的 实体。这些通信的语义方面与通信问题无关,而 重要的方面是实际消息是从一个可能消息集合中 选择出的一条消息。" 可见,香农在研究信息理论时,排除了语义信息与语用信息的因素,先从语法信息入手,解决当时最重要的通信工程一类的信息传递问题。同时他还把信源看成具有输出的随机过程,所研究的事物运动状态和变化方式的外在形式遵循某种概率分布。因此香农信息论或经典信息论所研究的信息是语法信息中的概率信息。

不过,随着信息论研究的深入,香农信息论的方法已经渗透到语义信息领域,例如最大熵建模方法用于机器翻译等自然语言处理问题。

通信信息三个层次

信号消息信息



消息: 信息的数学表达

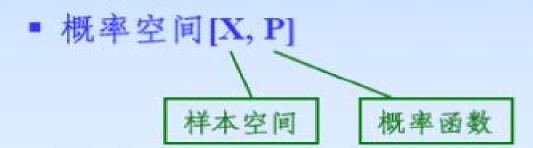
信息:信号和消息的内在抽象

Shannon信息的定义

■ 是对事物运动状态或存在方式不确定性的描述

■ 概率空间[X, P]

Shannon信息的描述工具

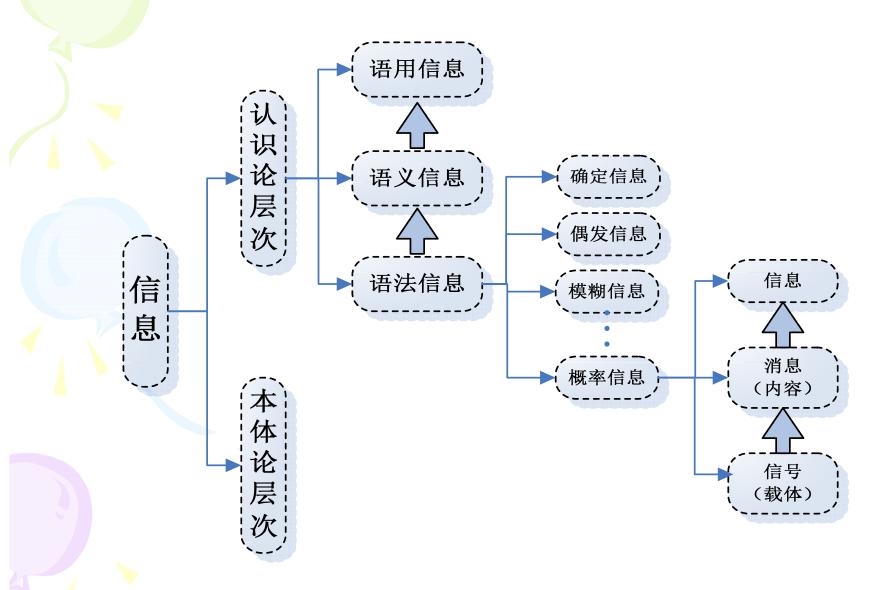


■ 离散概率空间

$$\begin{bmatrix} X \\ P \end{bmatrix} = \begin{bmatrix} x_1 & x_2 & \dots & x_n \\ p_1 & p_2 & \dots & p_n \end{bmatrix} \qquad \sum_{i=1}^n p_i = 1$$

■ 自信息和信息熵

信息各层次之间的关系如图



§ 1.2 信息论研究的内容

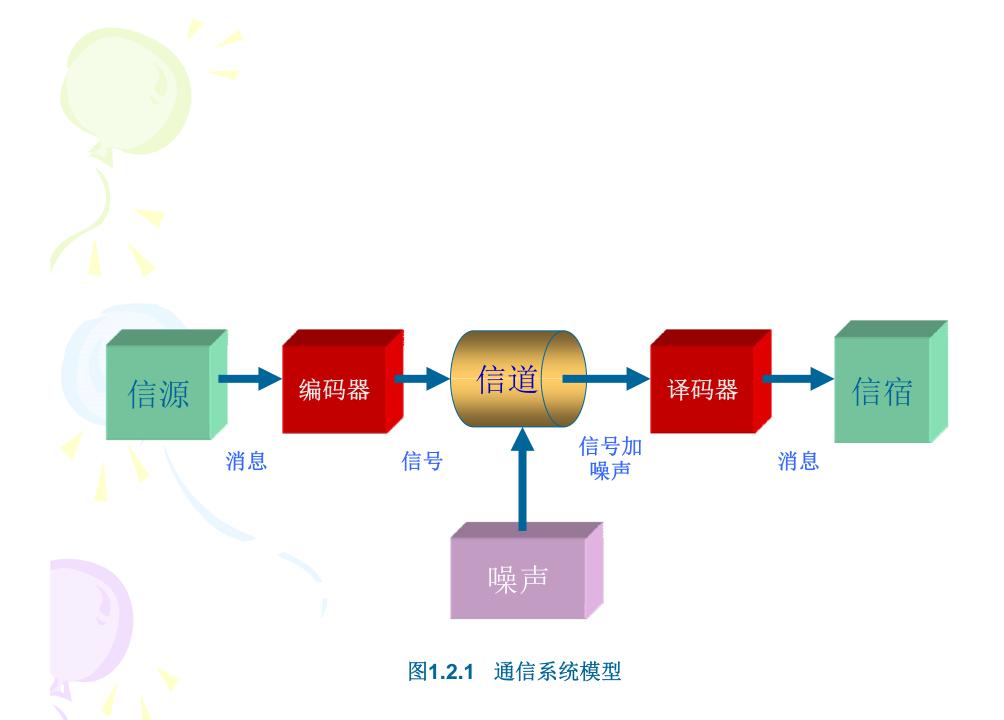
本节内容:

- ◆ 通信系统模型
- ◆ 香农信息论的主要内容

1.2.1 通信系统模型

如前面所述,信息论的建立是从研究通信系统 开始的,并首先建立了通信系统模型。由于技术发 展水平的限制,当时的通信基本限制在点对点的通 信,所以这种通信系统模型是指"从一个地方向另 一个地方传送信息的系统"。例如,电话、电报、 电视、无线通信、光通信等。而存储系统在某种意 义上也可看成从现在向将来发送信息的通信系统。 例如,磁盘或光盘驱动器、磁带记录器、视频播放 器等

通信系统是从空间的一点到另一点传送信息的,而存储系统是从时间的一点到另一点传送信息的。



1. 信源(information source)

信源是信息的来源, 其功能是直接产生

可能包含信息的消息

→ 按输出符号的取值分类:

离散信源和连续信源:

连续信源又分为:

离散时间连续信源;

波形信源或模拟信源。

- → 按输出符号之间的依赖关系分类
 - 无记忆信源
 - 信源输出符号的概率与以前输出的符号无关 *有记忆信源*

信源输出符号的概率与以前输出的符号有关

★ 核心问题: 信源的消息中所包含的信息量 以及信息如何量度 2. 编码器(Encoder)

编码器的功能:

将消息变成适合于信道传输的信号

信源编码器(source encoder)

信道编码器(channel encoder)

调制器(modulator)

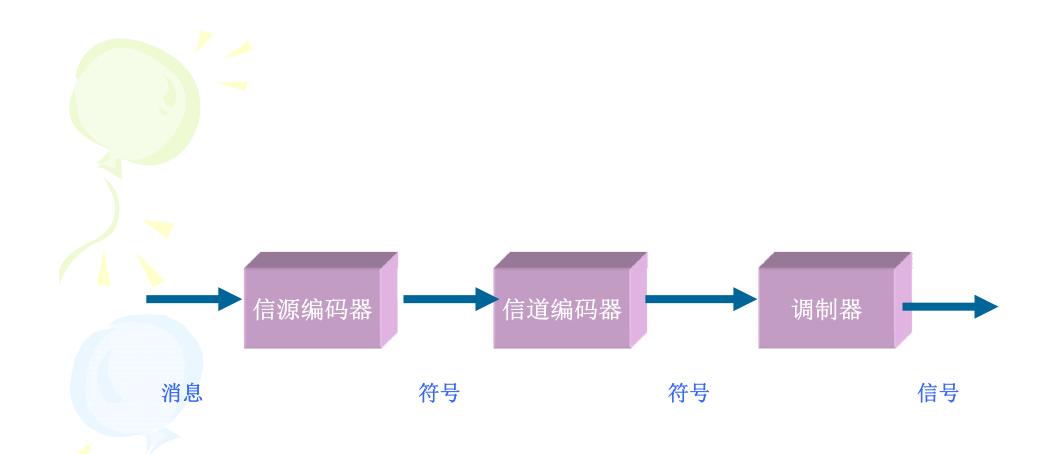


图1.2.2 编码器的组成

各部分的主要功能

信源编码器的功能是将信源消息变成符号,目的是提高 传输有效性,也就是压缩每个信源符号传输所需代码 (通常为二进制代码)的数目(对二进制代码称比特 数)。例如,一个信源含4个符号 {a, b, c, d}, 概率分别 为1/2, 1/4, 1/8, 1/8。如果不采用信源编码,每个信 源符号至少需要用2个二进制代码传输。如果采用信源编 码, 分别将a, b, c, d编码成为: 0, 10, 110, 111, 那么 平均每信源符号只需1.75个二进制代码传输。可见,采 用合适的信源编码确实能通过压缩码率提高传输有效性。 所以, 信源编码也称信源压缩编码。

信道编码器给信源编码符号增加冗余符号,目的是 提高传输可靠性。信源编码输出直接传送,不能保证传 输可靠性。利用信道编码对信源编码器的输出符号增加 一些冗余符号,并让这些符号满足一定的数学规律,使 传输具有纠错或检错能力。因为出现传输错误就会破坏 这种数学规律。在接收端就会发现错误。例如,最简单 的奇偶纠错,将信源编码输出的每个码组的尾补一个1 或0, 使得整个码组"1"的个数为奇或偶(或模二加为1 或0)。当传输发生奇数差错,打乱了"1"数目的奇偶 性,就可以检测出错误。这是最简单的检错方式,而实 际的信道编码技术要复杂得多.

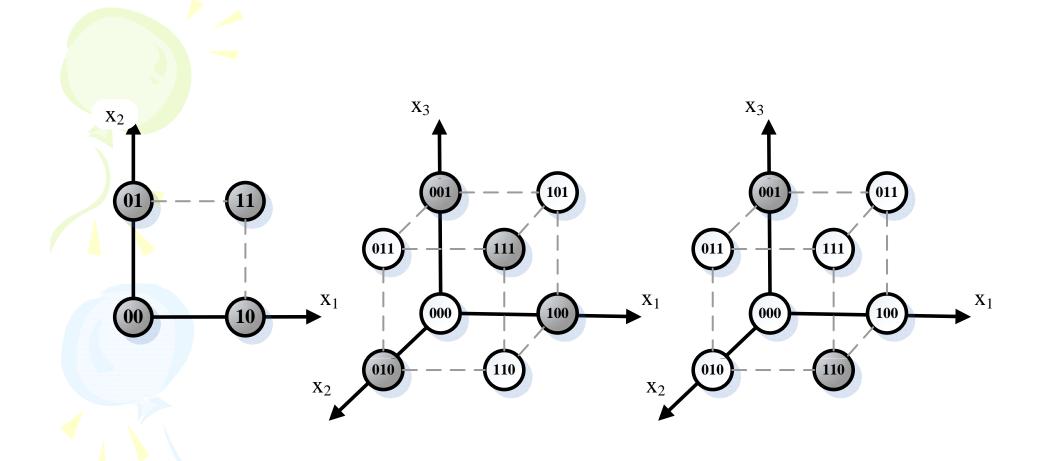


图1.2.3 增加冗余符号提高传输可靠性 (图中,有阴影的点表示码字)

图中, (a) 4个消息用4个2维矢量传送,没有冗 余符号。如果出现任何差错都会使传送的码字变 成另一个码字, 所以无检错能力: (b) 在(a) 的基础上每个码字增加一个校验符号,构成奇校 验,4个消息用4个3维矢量传送。如果出现任何奇 数差错都会使传送的码字变成不是码字的3维矢量, 这样就能检测出错误,但不能纠正错误: (c)用 2个汉明距离为3的3维矢量传送2个消息。如果出 现一个错误,可以根据接收矢量和码字汉明距离 的大小判决是哪个消息被传输,因此可以纠1个错 误。

调制器功能是,将编码器的输出符号变成适合信道传输的信号,目的是,提高传输效率(使远距离传输成为可能)。信道编码符号不能直接通过信道输出,要将编码器的输出符号变成适合信道传输的信号,例如,0、1符号变成两个电平,为远距离传输,还需载波调制,例如,ASK,FSK,PSK等。

3. 信道

信道是信号从编码器传输到译码器的中间媒 介。 信道可以分为狭义信道和广义信道。狭义 信道是某些物理通信信道,也可以是物理的存储 介质。例如有线、无线、光纤、磁盘、光盘等。 广义信道是一种逻辑信道,它和信息所通过的介 质无关, 只反映信源与信宿的连接关系。信息论 中只研究广义信道,例如表示为输入/输出间的 转移概率: $P(Y \mid X)$

信道还分为无噪声信道和有噪声信道。通 常,系统中其它部分的噪声和干扰都等效 成信道噪声。通信系统中主要有两种噪声: 加性噪声和乘性噪声。一般,背景噪声为 加性,而衰落为乘性。这里主要研究加性 噪声。在信息论中研究最多的是理想加性 高斯白噪声(AWGN)信道。研究高斯噪声 的主要原因是它的普遍性和易于处理的特 性。

高斯分布的普遍性主要基于两种原因: (1)根据中心极限定理,无数独立随机 变量的和的分布趋近高斯分布,因此高 斯噪声普遍存在; (2)在限功率条件下 产生最大熵的信源分布为高斯分布,而 最大熵分布是最容易被观察到的分布。

- 与信源的分类类似,信道还分为离散信道、离散时间连续信道和波形信道(或模拟信道),其中,离散信道和离散时间连续信道输入与输出都是符号序列,只不过符号取值不同,前者取离散值,而后者取连续值;而波形信道的输入与输出均为时间的连续波形。
- 信道也可有无记忆信道和有记忆的区分,离散信道和离散时间连续信道可以是无记忆的,也可以是有记忆的;而波形信道是通常有记忆的。

• 波形信道: 输入/输出是时间连续随机过程的信道

4. 译码器 (decoder)

译码器实现的功能即从信号中恢复消息。

包括:▶解调器

- ▶ 信道译码器
- ▶ 信源译码器



图1.2.3 译码器的组成

解调器功能是,将信道输出信号恢 复成符号:信道译码器的功能是, 去掉解调器输出符号中的冗余符号: 信源译码器的功能是,将信道译码 器输出符号变成消息。总之,功能 与发信机中的对应部分功能相反, 目的相同。在模拟通信系统中仅包 含解调器。

5. 信 宿(Destination)

信宿的功能是接收信息,包括人或设备。当前人们对信宿的研究也取得某些成果。例如,利用人的视觉残留效应可以对图像采用不连续传输的方式达到连续的视觉效果,从而进一步压缩码率。利用人听觉的掩蔽效应可以压缩在高频率信号而不影响听觉效果。总之,对信宿的研究和压缩编码结合可以在不影响视听效果的条件下,显著压缩码率。

6.通信系统性能指标的评价

有效性用频谱利用率来衡量。提高有效性的措施是,采用信源编码以压缩码率,采用频谱利用率高的调制减小传输带宽;

可靠性用传输错误率来衡量。提高可靠性的措施是,采用信道编码以降低错误率;

安全性可通过信息的加密强度来衡量。提高安全性的措施是,采用高强度的加密和伪装技术。

1.2.2 香农信息论

信息论是在概率论、随机过程和通信技术相结 合的基础上发展起来的学科,可分为狭义信息 论和广义信息论。狭义信息论即香农信息论或 经典信息论,所研究的基本问题是:信源、信 道及编码问题,核心是三个编码定理。广义信 息论包括: 香农或经典信息论、信源编码、信 道编码、近代信息论、统计通信理论、通信网 理论、信号与信息处理、保密通信等。

香农信息论的内容可用一句话概括为: "一个概念,三个定理",就是信息熵的概念和三个编码定理。

香农工作涉及通信理论中有效性和可靠性这二个基本问题。

□狭义信息论体系 传输理论 压缩理论 无失真编码 有失真编码 网络信息理论 信道编码定理 率失真理论 变长编码 等长编码 Shannon 定理 定理 网络最佳码 纠错码 Gallager Shannon Shannon 编码调制理论 Berger 1948 1948 McMillan McMillan 1953 1956 压缩编码 Huffman码(1952)、Fano码 **JPEG** 算术码(1976,1982) MPEG LZ码(1977,1978)

1. 关于信源信息的度量

如前所述,香农将信源限制为具有某一先验概率的随机过程,对信息进行量度是信息论的首要问题。香农定义了信息熵作为信源所含信息的量度,是信息论中最重要的概念。

2. 无失真信源编码定理(香农第一定理) 无失真信源编码定理,也称香农第一定理,是信源 压缩编码的理论基础,其内容是:如果信源编码码 率(编码后传送每个信源符号的平均比特数)不小 于信源的熵,就存在无失真编码;反之,不存在无 失真编码。可以简述为:

 $R \ge H \Leftrightarrow$ 存在无失真信源编码

其中,R为信源编码码率,H为信源的熵。

例如,英文字母加空共27符号,用代码传送,每个符号需5比特(log27)。但通过试验发现,实际的英文字母信源熵大约为1.4比特/符号,所以根据香农第一定理,存在某种信源编码方式,使得每字母仅用1.4个二进制符号就能无失真传送,这样可以显著提高传输效率。

该定理解决的是信源无损压缩极限的理论问题, 并未给出普遍的信源编码的方法,所以寻找接近或 达到信源熵的压缩编码技术、分析其性能并有效实 现是研究的主要问题。

3. 关于信道容量与信息的可靠传输

有噪信道编码定理(香农第二定理)是信道编码的理论 基础,其内容是:如果信息传输速率小于信道容量,则总可 找到一种编码方式使得当编码序列足够长时传输差错任意小, 反之不存在使差错任意小的编码。可以简述为:

R ≤ C ⇔ 存在译码差错任意小的编码

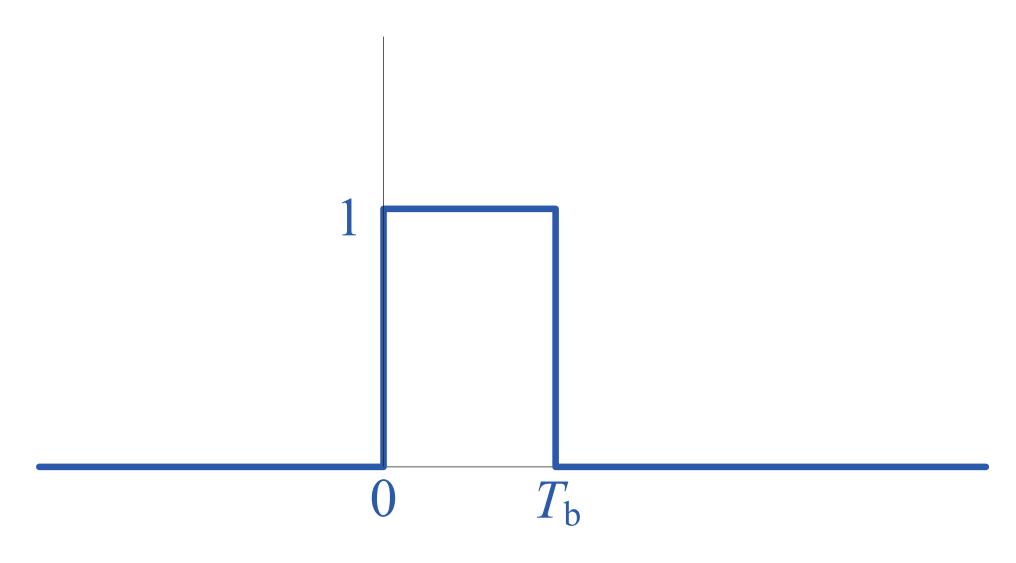
其中,R为信息传输速率,也称信道编码码率,C为信道容量。

有关码率R和信道容量C的简单说明:

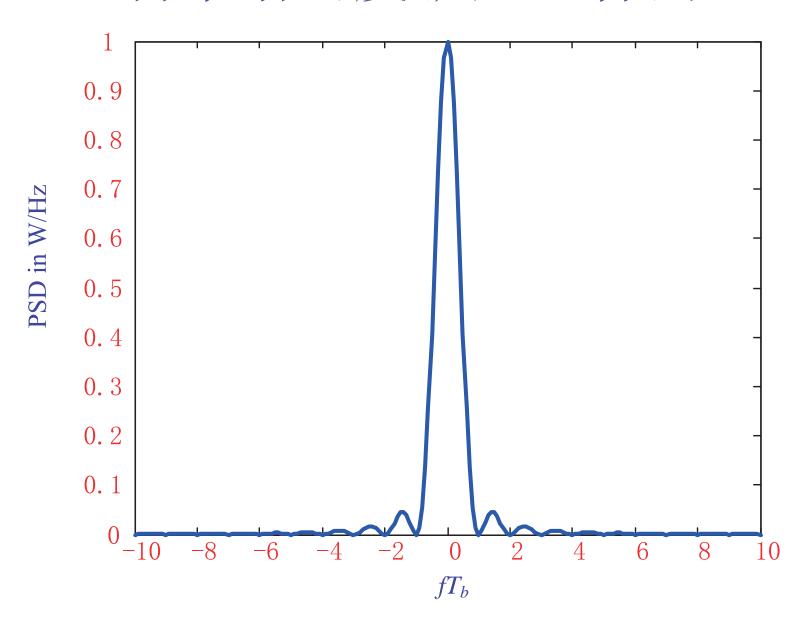
- 1. 信道(X, p(y|x), Y), (M,n)码
- 1. 1 下标集{1,2,…,*M*}
- 1. 2 编 码 函 数 $X^n:\{1,2,\cdots,M\}\to X^n$ 生 成 码 字 $X^n(1),X^n(2),\cdots,X^n(M),$ 即码书 Codebook Code —》 codeword
 - 1. 3 编码经信道以 $Y^n \sim p(y^n | x^n)$ 传给接收者
 - 1. 4 译码函数 $g:Y^n \to \{1,2,\cdots M\}$
 - 2. (M,n)码的码率: $R = \log M/n$ 比特/传输
 - 3. 码率相当于传输每个编码符号有多少信息;最大可达码率定义为容量

例如,一个带宽为3kHz的系统,用二进符号传输,如果不进行信道编码,无码间干扰的最大传输速率为6kbps,按照香农AWGN信道容量公式可知,通过合适的信道编码,在信噪比为26dB的条件下,实现可靠传输的最大速率可达到25.6kbps。

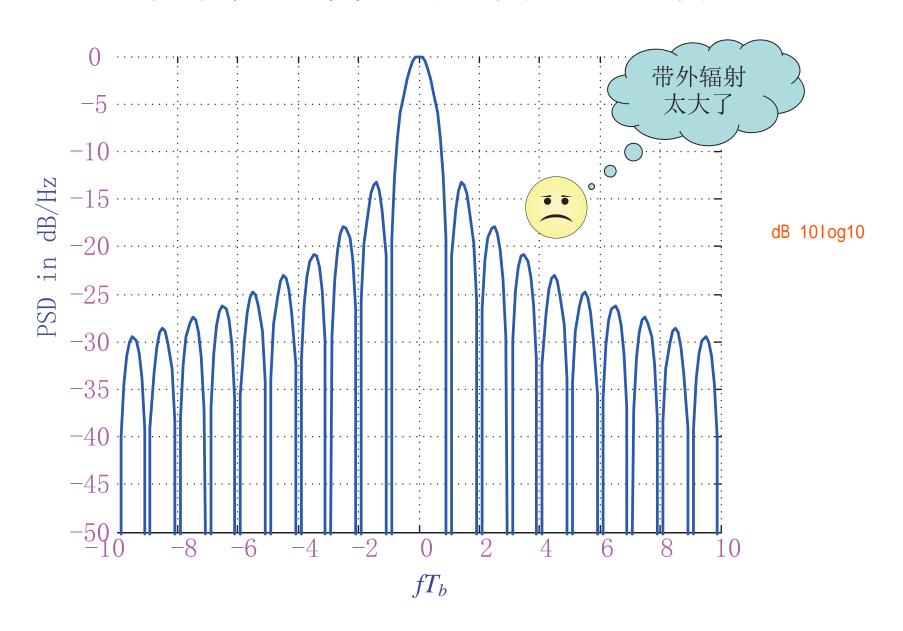
如果脉冲是这样的



功率谱密度就是这样的

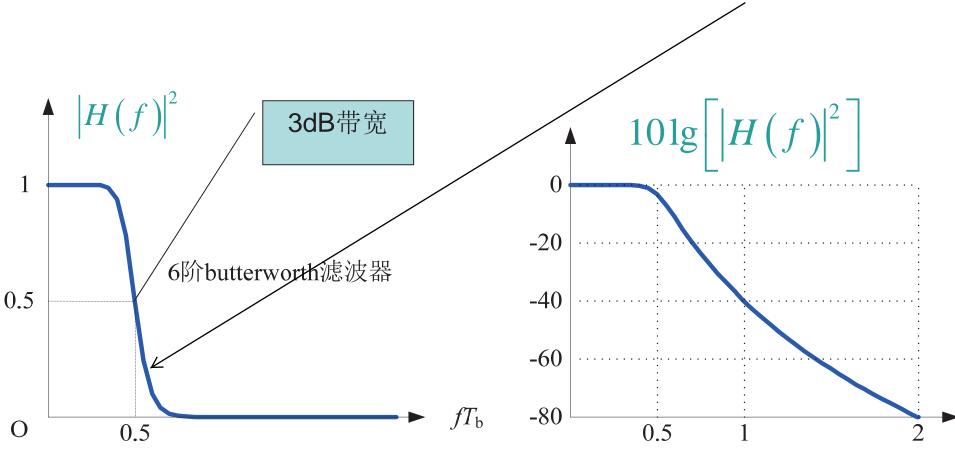


工程师们喜欢用分贝坐标

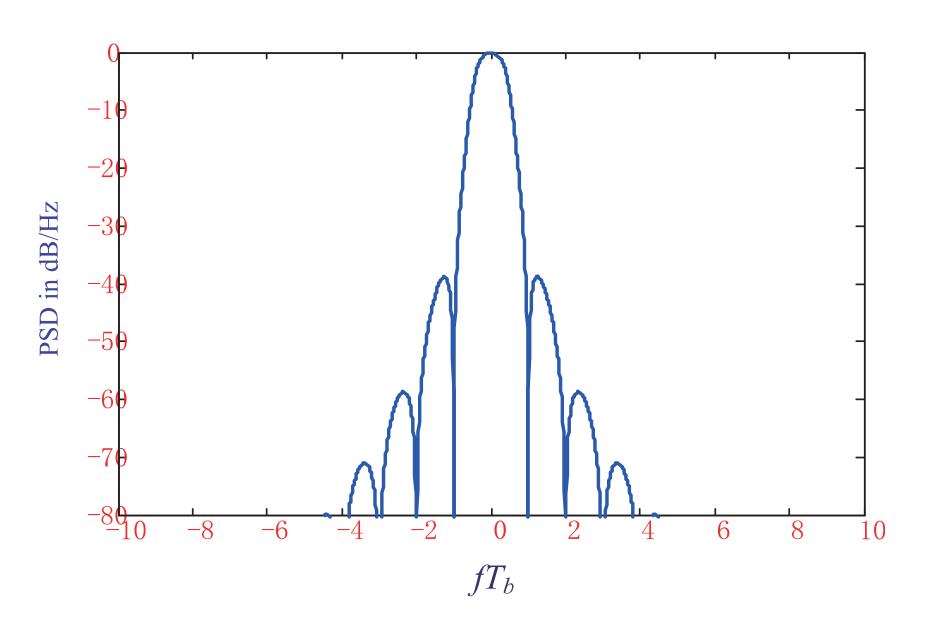


经过一个Butterworth滤波器

注意:脉冲信号是无限带宽信号,实际的传输带宽有限,故高频分量被抑制

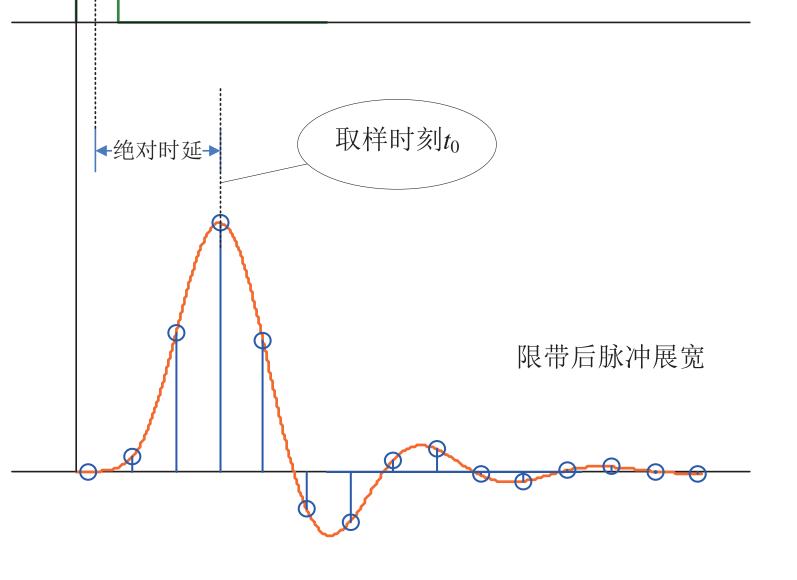


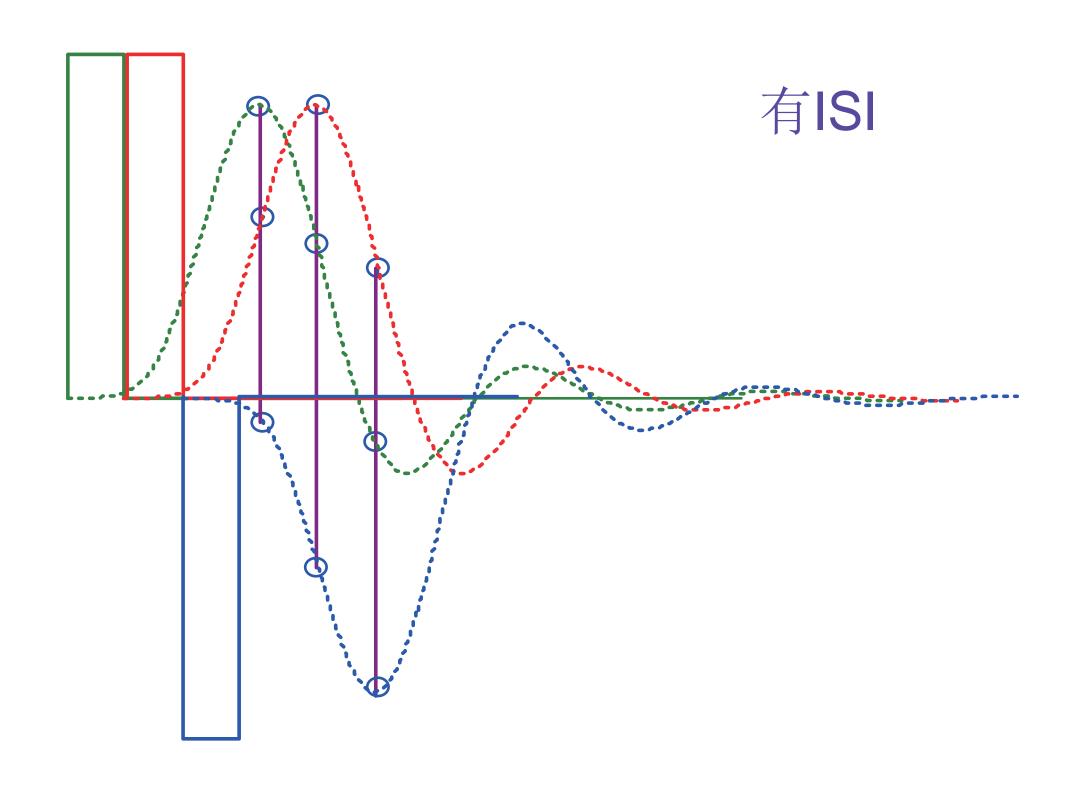
带宽被有效限制了





但是脉冲变成 这个样子了





由于信道类型的复杂性,所以根据实际 研究的问题建立信道模型,分析特性,计算 容量以及在这些信道条件下各类通信系统的 性能是研究的主要问题。此外,定理解决的 是信息传输极限的理论问题,并未给出普遍 的信道编码的方法,所以寻找接近或达到信 源信道容量的信道编码技术、分析其性能并 有效实现也是研究的主要问题。不过这些内 容主要归入信道编码理论与技术的范畴。

4. 信息率失真理论(数据压缩的理论基础)

在很多情况下,我们并不需要信息精确的 传输,而是容许有一定限度差错的传输。这 样在保证获取足够信息的前提下,可以提高 传输效率,降低通信成本。为实现限失真传 输的有效性,对给定信源,希望在满足一定 的失真要求条件下, 使编码器的码率最小, 这是一个最优有损数据压缩编码的理论问题, 其理论基础就是信息率失真理论,核心是限 失真信源编码定理。

限失真信源编码定理(香农第三定理)是有 损压缩编码的理论基础,其内容是:对任何失真 测度D,只要码字足够长,总可找到一种编码,使 得当信源编码的码率〉R(D)时,码的平均失真〈D; 反之,如果信源编码的码率〈R(D),就不存在 平均失真〈D的编码。可以简述为:

 $R \geq R(D) \Leftrightarrow$ 存在平均失真 $\leq D$ 信源编码

其中, R为信源编码码率, R (D) 称为信息率失真函数, 是满足失真准则(平均失真〈D)下, 每信源符号所需最小编码比特数。

给定信源和失真D —》最小的编码码率R(D):率失真函数

与无失真信源编码类似,限失真信源编码定理解决了有损压缩极限的理论问题,也未给出实际的有损信源编码的构造方法。在各种失真度准则下对信源R(D)函数的研究,利用率失真理论对实际有损压缩编码性能的分析,寻找接近或达到理想有损压缩的信源编码方法是该领域研究的主要问题。

- 5. 信息论的特点
 - ▶以概率论、随机过程为基本研究工具;
 - →研究通信系统的整个过程,而不是单个环节, 并以编、译码器为重点;
 - ▶关心的是最优系统的性能和渐近性能,但并不 具体设计系统;
 - >语法信息中的概率信息,要求信源为随机过程。

§ 1.3 香农信息论研究的进展与应用

本节主要内容:

- ▶香农信息论创立的背景
- ▶香农的主要贡献
- > 香农信息论的研究进展
- ▶香农信息论的应用

1. 3. 1 香农信息论创立的背景

香农的信息论的创立主要是由于香农的杰出贡 献,但也与当时的技术发展背景和前人的工作密不 可分。当时通信理论与技术已有较大发展,存在的 主要通信技术与手段有: 电报(Morse, 1830's)、电 话(Bell, 1876)、无线电报(Marconi, 1887)、AM 无 线电(1900's 早期)、单边带调制(Carson, 1922)、 电视(1925-1927)、电传(1931)、调频 (Armstrong, 1936)、脉码调制(Reeves, 1937-1939)、 声码器(Dudley, 1939)、 扩频(1940's)等。

1948年以前,Nyquist,Hartley等人也做了许 多有影响的工作。例如Nyquist发现传输速率正比于 在单位时间信号电平数目的对数(1924); Hartley 提出"传输速率", "码间干扰", "系统传输信 息的容量"等术语; Wiener, Rice等人把随机过程 作为通信工程师的工具。所有这些都为信息理论的 建立产生了重要影响

热力学对香农信息论的创立也产生很大影响,香农提出用熵作为信息的度量,实际上也参考了热熵的概念

吉布斯提出在微观系统状态概率不等情况下的热熵计算公式: S =-ki*pi*log(pi), 该公式称为吉布斯方程。实际上,除常数k外,香农熵和吉布斯方程的热熵表达式相同

1.3. 2 香农的主要贡献

香农在信息论发展过程中的主要学术贡献:

- 1948年,发表〈通信的数学理论〉,奠定了信息论的理论基础
- 1956年,发表〈The Zero-Error Capacity of a Noisy Channel〉,开创了零差错容量的研究领域

- 1959年,发表〈Coding Theorem for a Discrete Source with a Fidelity Criterion 〉
- 给出了有关率失真定理的简单证明,推广到更一般的信源和失真测度,进一步推广到模拟信源,推动了信息率失真理论研究

1961 年 , 发 表〈Two-Way Communication Channels〉,将信息论应用到连接两个点A、B的信道,其中A、B需要双向通信,但两个方向互相干扰的情况,证明了信道的容量区域是凸的,并建立了此区域的内外边界,从而开拓了多用户理论(网络信息论)的研究。

1.3.3 香农信息论的研究进展

五十多年来,无论是理论方面,还是应用方面, 香农信息论得到很大的发展。可分以下四个方面来 叙述。

1. 信息的量度

香农熵作为信息的量度,是信息论中最重要的概念,在这方面有两个重要研究内容,一是以香农熵为基础,研究信源信息熵的估计方法,二是将信息熵用做推断工具的最大熵原理,三是提出新的信息量度方法,以适应新的应用,主要进展包括:

(1) 信息熵的估计

自从香农信息论创立以来,已经提出了多种信息熵估计方法,并得到广泛应用,信息熵估计技术就是研究的热点之一。当前,信息熵估计方法已经从主要针对文本、图象等一般信源,转移到针对特殊信源(例如DNA序列熵的估计)的研究。

(2) 最大熵原理

1957年,统计物理学家Jaynes,根据香农 熵的概念,提出了当已知条件不充分时利用部 分信息推断概率分布的方法,称为最大熵原理。 它的基本思想是, 求满足某些约束的信源事件 概率分布时,应使得信源的熵最大,这样可以 使我们依靠有限的数据达到尽可能客观的效果, 克服可能引入的偏差。当前,最大熵原理已经 应用于多个领域,其中包括信号检测与处理、 模式分类、自然语言处理,生物医学,甚至经 济学领域,都取得很好的效果。

(3) Kolmogorov熵

上世纪60年代,Kolmogorov等提出一种与概率无关的信息量度,称为Kolmogorov 算法熵。在数值x给定条件下使计算机输出 y值的最短程序长度,定义为在x条件下y的 条件算法熵。算法熵可以作为算法复杂度 的度量。

(4) Renyi熵

Renvi熵有一个参数,是香农熵的单参数推广。 Renvi熵称为与概率分布有关的阶的信息度量,不 满足可加性; 当阶数为1时,收敛于香农熵。 Renvi熵在很多领域都有应用,例如生物学、医学、 遗传学、语言学、经济学和电器工程、计算机科 学、地球物理学、化学和物理学等: Renvi熵也广 泛用于量子系统的研究,特别是用于量子纠缠态、 量子通信协议、量子相关性的分析等。

(5) Tsallis熵

大范围的相互作用或长时间的记忆系统可能不 满足遍历性,例如引力系统、Levy fligHts、分形 现象、湍流物理、甚至经济学等领域,称为非广延 系统。已经证明,波尔兹曼—吉布斯统计学不适于 这类系统。1988年,由Tsallis提出一种适用于非 广延系统的信息度量,推广了波尔兹曼—吉布斯熵, 称作 Tsallis熵。目前一般认为: Tsallis熵适用 于非规则、不完全随机或混沌的运动的处理。 Tsallis 熵在信息处理的应用也是当前研究的热点 之一。

2. 无损数据压缩

无损数据压缩的理论基础是香农第一定理,主要包括概率匹配编码(也称熵编码)和通用编码的理论与技术。主要进展如下:

(1) 熵编码的进展

- Huffman解决了从固定到可变长度最优编码的构造,即 Huffman编码
- · Rissanen等提出算术编码(非分组码)

(2) 通用编码的进展

- 由A. Lempel和J. Ziv提出的方法(L-Z算法)是当前最广泛使用的通用编码方法,该方法基于对信源序列的分段,简单的分段原则使编译码都很简单,已经证明L-Z算法对任何平稳遍历信源都能以熵率编码;
- Broose和Wheeler提出基于Broose-Wheeler变换的压缩编码,性能优于L-Z系列的编码;
- Cleary和 Witten提出部分匹配预测 (Prediction by Partial Matching, PPM) 压缩编码,是目前压缩率最优的无损编码

• 在提高瞬时压缩效率的编码方面, Rissanen提出上下文树模型, F. Willems等提出了上下文树加权编码方法, 理论与实验证明这种方法的编码速率达到熵率。

(3) 分布信源编码

• D. Slepian和J. Wolf提出相关信源编码是数据压缩理论的最重要的进展之一。他们证明,即使对两个相关信源分别编码但联合译码,所需总的编码速率也可以小于两个信源熵的和。此外具有边信息的信源编码和数据压缩的研究还在开展。

信息论对信号处理关键技术的指导作用

一 分布式信源编码和信道编码的对偶性(1)

分布式信源编码

- 设X和Y为统计相关的离散信源, Slepian和Wolf证明: 当X和Y进行单独编码和联合解码时(图3.2), X和Y无据码的最低码率与传统的编码方案(联合编码-联合解码,图3.1)码率相同
- $R=R_X+R_Y>=H(X, Y)$
- · Wyner-Ziv进一步发展了有 损分布式编码理论

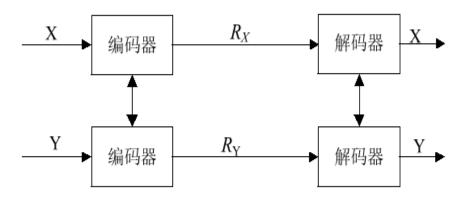


图3.1 两个信源的单独编码和解码

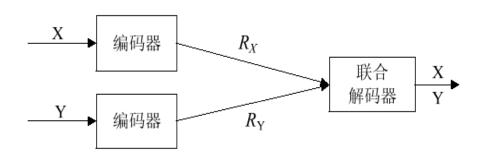


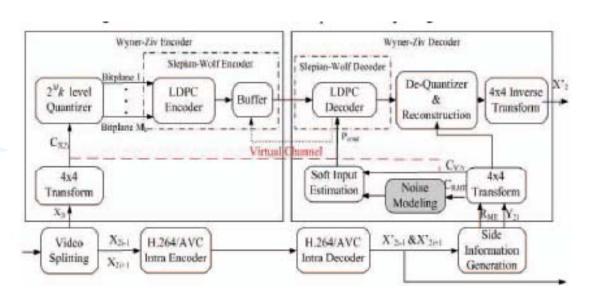
图3.2 两个信源的单独编码-联合解码

信息论对信号处理关键技术的指导作用

一 分布式信源编码和信道编码的对偶性(2)

分布式视频编码(DVC)

DVC架构中,为降低计算复杂度,将诸如运动估计/补偿这类的高复杂计算工作转移到解码端完成,因此不能象传统视频编码架构一样,有效统计两帧之间的相关性,而近似地采用原始信息X(编码端可知)和边信息Y(解码端可知)的相关性来替代



Source coding with side information at decoder

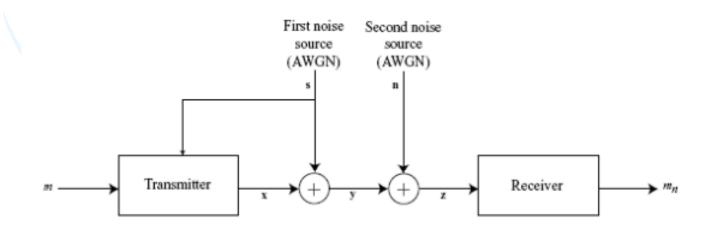
Fig. 1. Diagram of transform domain Wyner-Ziv video codec architecture

信息论对信号处理关键技术的指导作用

一 分布式信源编码和信道编码的对偶性(3)

编码端具有边信息的信道编码

- Channel coding with side information at encoder
- 信息论原型 污纸编码(Writing on Dirty Paper)
- 在编码端掌握第一个噪声源s时,通过有效编码信道可以达到的容量和无s或编/解码端都掌握s时相同



Costa's dirty paper channel

信息论对信号处理关键技术的指导作用一分布式信源编码和信道编码的对偶性(4)

结论:

- 分布式信源编码是解码端具有边信息的信源编码问题
- 污纸编码是编码端具有边信息的信道编码问题
- · 二者是对偶问题(Duality)
- 根据信息论的结果设计实际可操作算法,为提高信源 编码和信道编码算法的性能提供了方法论依据

3. 可靠通信

可靠通信的理论基础是香农第二定理,它的进展主要包括以下方面:

- (1) 各种特殊信道容量与有关的编译码技术研究
- 高斯信道的研究;
- 衰落信道的研究
- 反馈信道的研究;
- 迭代译码的研究;

- 有约束信道(香农称做离散无噪声信道)的容量的研究(成为有约束序列编码的理论基础,这些技术广泛应用在磁与光记录设备中);
- 零差错信道容量(这是香农开辟的另一个研究领域,信息可以无错误编码的速率称零差错容量,这种容量的研究不同于非零差错容量的研究,它要以组合图论作为研究工具)的研究

(2) 多用户信道的研究

- 多接入信道、无记忆高斯多接入信道容量区域、干扰信道、广播信道、未知参数信道、窃听信道等,都是多用户信道研究的内容,现已构成信息论中的一个重要分支网络信息论。
 - (3) 多入多出(MIMO)信道与空时编码的研究
- Paulraj、Telatar、Foschini等人的工作奠定了空时信道研究的理论基础,Tarokh提出了空时格码技术,推动了空时编码的研究,对无线系统中多天线以及空时编码与调制技术的研究已成为新的研究领域。

(4) 编译码理论与技术的研究

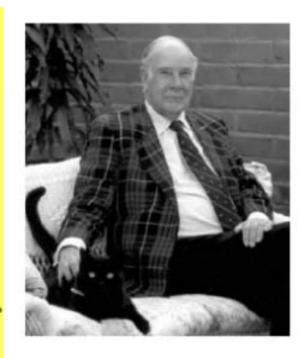
- · Berlekamp系统总结了代数编码理论;
- BCH、RS码、卷积码、级联码以及TCM编码调制的出现大大提高了通信的可靠性;
- Berrou等提出的Turbo码和Gallager首先提出后来被重新认识的LDPC(低密度奇偶校验)码是信道编码理论研究的重要里程碑,其性能已经接近香农的信道容量界限。

信道编码的历史及研究现状

- ▶ 1948年,Bell实验室的C.E.Shannon发表的《通信的数 学理论》,是关于现代信息理论的奠基性论文,它的发表 标志着信息与编码理论这一学科的创立。Shannon在该 文中指出,任何一个通信信道都有确定的信道容量C,如 果通信系统所要求的传输速率R小于C,则存在一种编码 方法, 当码长n充分大并应用最大似然译码(MLD, Maximum Likelihood Decdoding)时,信息的错误概 率可以达到任意小。从Shannon信道编码定理可知,随 着分组码的码长n或卷积码的约束长度N的增加,系统可 以取得更好的性能(即更大的保护能力或编码增益),而 译码的最优算法是MLD,MLD算法的复杂性随n或N的增 加呈指数增加,因此当n或N较大时,MLD在物理上是不 可实现的。因此,构造物理可实现编码方案及寻找有效译 码算法一直是信道编码理论与技术研究的中心任务。
- Shannon指出了可以通过差错控制码在信息传输速率不 大于信道容量的前提下实现可靠通信,但却没有给出具体 实现差错控制编码的方法。



20世纪40年代,R.Hamming和M.Golay提出了第一 个实用的差错控制编码方案,使编码理论这个应用数 学分支的发展得到了极大的推动。通常认为是 R.Hamming提出了第一个差错控制码。当时他作为一 个数学家受雇于贝尔实验室, 主要从事弹性理论的研 究。他发现计算机经常在计算过程中出现错误,而一 旦有错误发生,程序就会停止运行。这个问题促使他 编制了使计算机具有检测错误能力的程序, 通过对输 入数据编码, 使计算机能够纠正这些错误并继续运行。 Hamming所采用的方法就是将输入数据每4个比特分 为一组, 然后通过计算这些信息比特的线性组合来得 到3个校验比特,然后将得到的7个比特送入计算机。 计算机按照一定的原则读取这些码字, 通过采用一定 的算法,不仅能够检测到是否有错误发生,同时还可 以找到发生单个比特错误的比特的位置,该码可以纠 正7个比特中所发生的单个比特错误。这个编码方法 就是分组码的基本思想, Hamming提出的编码方案 后来被命名为汉明码。

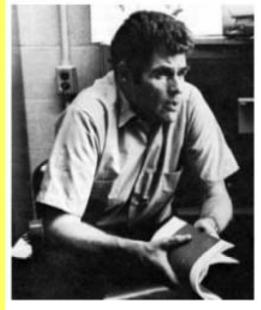


Hamming, 1915-1998



虽然分组码在理论分析和数学描述方面已经非常成熟,并且在实 际的通信系统中也已经得到了广泛的应用,但分组码固有的缺陷 大大限制了它的进一步发展。首先,由于分组码是面向数据块的, 因此,在译码过程中必须等待整个码字全部接收到之后才能开始 进行译码。在数据块长度较大时,引入的系统延时是非常大的。 分组码的第二个缺陷是它要求精确的帧同步,即需要对接收码字 或帧的起始符号时间和相位精确同步。另外,大多数基于代数的 分组码的译码算法都是硬判决算法,而不是对解调器输出未量化 信息的软译码,从而造成了一定程度的增益损失。

分组码所存在的固有缺点可以通过采用其他的编码方 法来改善。这种编码方法就是卷积码。卷积码是Elias 等人在1955年提出的。卷积码与分组码的不同在于: 它充分利用了各个信息块之间的相关性。通常卷积码 记为(n, k, N)码。卷积码的编码过程是连续进行的, 依次连续将每k个信息元输入编码器,得到n个码元, 得到的码元中的检验元不仅与本码的信息元有关,还 与以前时刻输入到编码器的信息元(反映在编码寄存器 的内容上)有关。同样,在卷积码的译码过程中,不仅 要从本码中提取译码信息,还要充分利用以前和以后 时刻收到的码组. 从这些码组中提取译码相关信息, 而且译码也是可以连续进行的,这样可以保证卷积码 的译码延时相对比较小。通常,在系统条件相同的条 件下, 在达到相同译码性能时, 卷积码的信息块长度 和码字长度都要比分组码的信息块长度和码字长度小, 相应译码复杂性也小一些。



Elias, 1923-2001

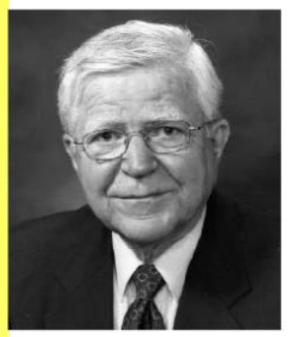
当前组的监督码元不仅取决于本组的信息码元,也取决于前N组的信息码元(n,k,N)

- ▶ 卷积码的译码通常有如下几个比较流行的译码算法:
 - ◆ 由Wozencraft和Reiffen在1961年提出,Fano和 Jelinek分别在1963年和1969年进行改进了的序 贯译码算法。该算法是基于码字树图结构的一种 次最优概率译码算法。
 - ◆ 由Massey在1963年提出的门限译码算法。这个 算法利用码字的代数结构进行代数译码。
 - ◆ 由Viterbi在1967年提出的Viterbi算法。该算法是基于码字格图结构的一种最大似然译码算法,是一种最优译码算法。
- 在Viterbi译码算法提出之后,卷积码在通信系统中得到了极为广泛的应用。如GSM、3G、商业卫星通信系统等。



Viterbi, CDMA之父

· 近年来,在信道编码定理的指引下,人们一 直致力于寻找能满足现代通信业务要求,结 构简单、性能优越的好码,并在分组码、卷 积码等基本编码方法和最大似然译码算法的 基础上提出了许多构造好码及简化译码复杂 性的方法,提出了乘积码、代数几何码、低 密度校验码(LDPC, Low Density Parity Check)、分组-卷积级联码等编码方法和逐 组最佳译码、软判决译码等译码方法以及编 码与调制相结合的网格编码调制(TCM, Trellis Coded Modulation)技术。其中对纠 错码发展贡献比较大的有级联码、软判决译 码和TCM技术等。



Gallager

- ➤ 虽然软判决译码、级联码和编码调制技术都对信道码的设计和发展产生了重大影响,但是其增益与Shannon理论极限始终都存在2~3dB的差距。
- 在 1993 年 于 瑞 士 日 内 瓦 召 开 的 国 际 通 信 会 议 (1CC'93)上,两位任教于法国不列颠通信大学的教 授C.Berrou、A.Glavieux和他们的缅甸籍博士生 P.Thitimajshima首次提出了一种新型信道编码方 案——Turbo码,由于它很好地应用了Shannon信 道编码定理中的随机性编、译码条件,从而获得了 几乎接近Shannon理论极限的译码性能。仿真结果 表明,在采用长度为65536的随机交织器并译码迭代 18次情况下,在信噪比Eb/N0>=0.7dB并采用二元相 移键控(BPSK)调制时,码率为1/2的Turbo码在加性 高斯白噪声信道上的误比特率(BER)<=10-5,达到了 与Shannon极限仅相差0.7dB的优异性能。(1/2码率 的Shannon极限是0dB)。



Berrou and Forney

Turbo码:级联、交织、软判决译码

- ▶ 1997年,Host、Johannesson、Ablov提出了编织卷级码 (Woven Convolutional Code,WCC)的概念,随后编织码 (Woven code)便发展起来了。它是一种组合码,其系统结构 可完全包容传统分组码、卷级码以及各类Turbo码,开创了编码 领域的一个新天地。
- ➤ 编织码的结构综合了并行级联卷级码(Turbo码)和串行级联卷级码的结构特点,当外编码器个数足够多时,该码型完全拥有了Shannon编码定理中随机长码的特性,因此,其纠错性能理论上比Turbo码要优异。
- ▶ 但编织码的编码结构复杂性较高,编码效率也不高,目前研究最 多的是1/3的编织卷级码,译码采用BCJR算法的迭代译码。

4. 有损数据压缩

有损数据压缩的理论基础是信息率失真理论,它的进展主要包括以下方面:

- (1) Berger给出了更一般的率失真编码定理,发展了信息率失真编码理论;
- (2) Wyner和Ziv研究了在译码器具有边信息的有损信源编码问题,推动了多端有损压缩编码的研究;
- (3) Hajek和Berger建立了随机场率失真编码理论的基础:

- (4) Yang和Kieffer证明,对于信源统计特性和失真测度都通用的有损压缩编码是存在的,为通用有损压缩编码的研究提供了理论依据;
- (5) 信源和信道联合编码;
- (6) 有损压缩编码的实现技术得到很大发展,其中包括: 标量与矢量量化、预测编码、变换编码等。这些技术都成功应用到语音、图象、视频以及多媒体的压缩编码中。

1.3.4 香农信息论的应用

香农信息论最重要的应用领域是通信,此外,香农信息论已经渗透到多种其他学科,概括如下:

- 1. 信息论是评估通信系统性能优劣的基本标准。
- 香农信息论解决了通信系统传输有效性/可靠性指标的理论问题。在实际工作中,将通信系统实际的性能指标与香农的理论界限比较,可以评估该系统性能的优劣,从而确定系统性能改进的方向,达到预期的目的

2. 信息论提供从全局的观点观察和设计通信系统的理论方法。

信息论提供的是一系列支持通信实践的指导原则。例如,在通信系统的设计中,给定信源编码的失真度要求、信道容量,那么信源编码和信道编码的方法可以自由选择,因此可以设计不同的方案,但是可能对应不同的设备复杂度和成本。利用香农信息论可以从全局考虑设计问题,从而达到通信系统的最佳设计。

- 3. 信息论是从事与信息处理有关的研究、开发与管理人员的必备知识。
 - 信息论并不仅是通信的数学理论,而且提供了通信和信息处理的方法论,它是从事信息相关行业人员的必备知识。实践证明,不掌握信息论的基本原理,往往不能从全局的角度处理具体的信息处理问题,限制了解决问题的思路。

4.信息论在其他领域的应用已获得很大的成功

除通信、计算机、信号处理和自动控制领域 (电子信息领域)等外,信息理论方法已经渗透 到生物学、医学、气象学、水文环境学、语言学、 社会学和经济学等诸多领域,并取得成功。

谢谢大家!

