通 信 安 全

L4—信道编码理论

- 教师：崔爱娇

- 编号：ELEC3019
- 学时：32学时

概 要

信道编码定理

- 概 论
- 信道模型
- 信道编码译码
- 信道容量
- 信道编码定理

概 要

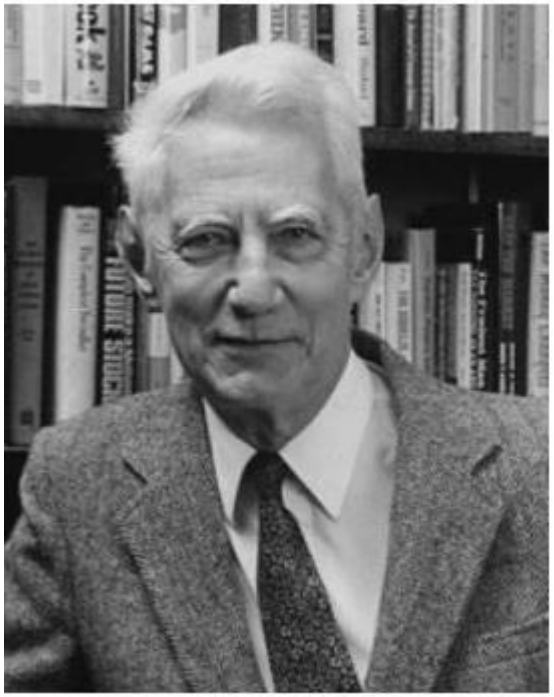
信道编码定理

- 概 论
- 信道模型
- 信道编码译码
- 信道容量
- 信道编码定理

概　论

在上个世纪40年代以前，人们认为只有通过增加发射功率和重传的方式，才能减少这种通信错误。

直到1948年香农提出了伟大的香农定理，人们才认识到，可以通过信道编码的方式来实现可靠通信。



$$C = B\log_2\left(1+\frac{S}{N}\right)\ (\text{b/s})$$

所谓**信道编码**，也叫差错控制编码，就是在发送端对原数据添加冗余信息，这些冗余信息是和原数据相关的，再在接收端根据这种相关性来检测和纠正传输过程产生的差错，从而对抗传输过程的干扰。

信息理论与编码技术的重要性

纵观现代通信的发展历程，可以发现通信系统的每次重大变革都是以信息理论与编码调制技术的重要突破为基础。

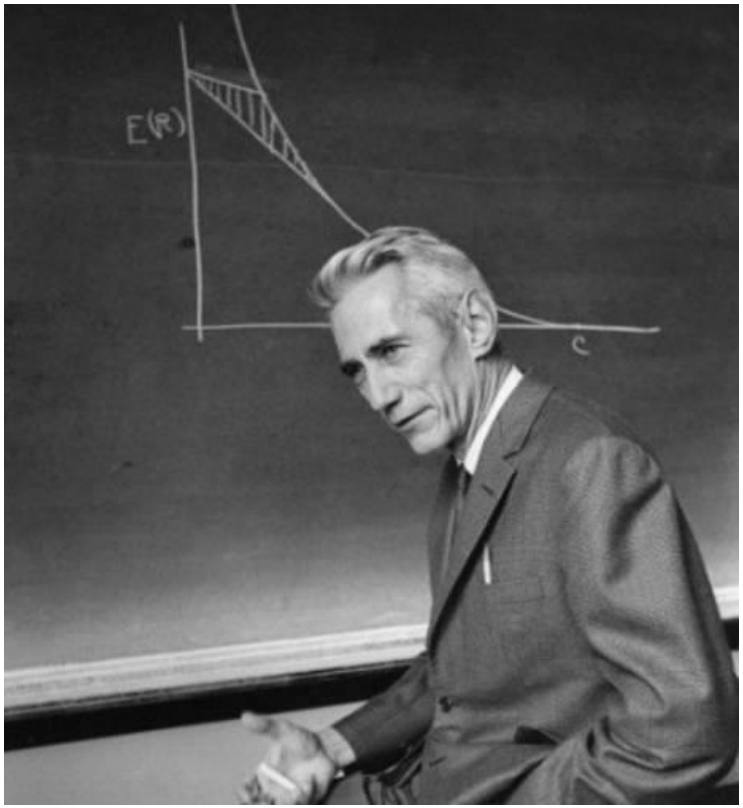
TCM(1976) Trellis Coded Modulation	电话Modem
CDMA(1980s)	IS-95,3G
Turbo码(1993)	3G, DVB, 802.16
MIMO(1995)	B3G/4G
合作与网络编码（2000）	新一代无线系统

概　论

信息理论与编码技术的重要性

著名信息论和编码学者Dr. Richard Blahut在香农的塑像落成典礼上这样评价香农：

在我看来，两三百年之后，当人们回过头来看我们这个时代的时候，他们可能不会记得谁是美国总统，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，学校里仍然会讲授信息论。

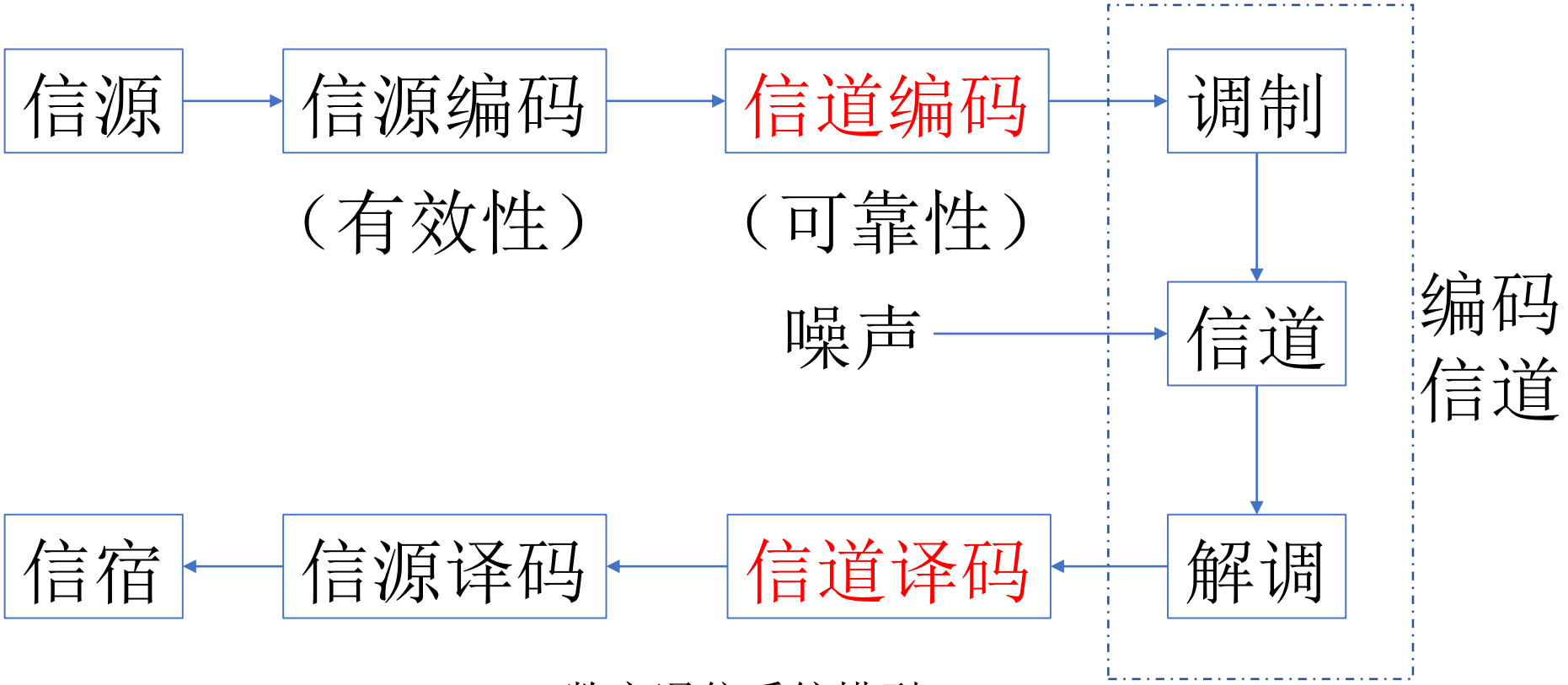


概　论

由于移动通信存在干扰和衰落，在信号传输过程中将出现差错，故对数字信号必须采用纠、检错技术，即纠、检错编码技术，以增强数据在信道中传输时抵御各种干扰的能力，提高系统的可靠性。

对要在信道中传送的数字信号进行的纠、检错编码就是信道编码。

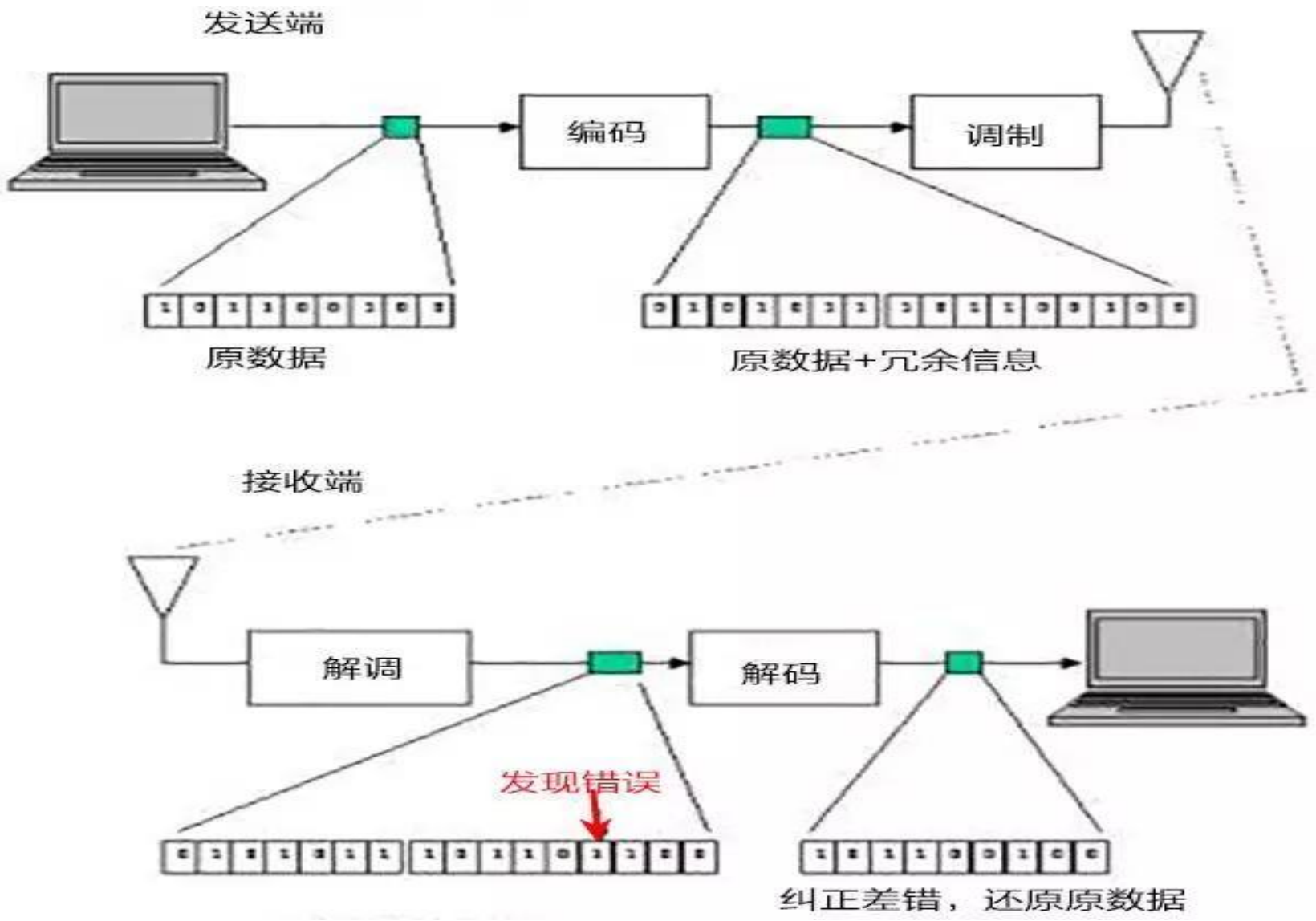
概　论



数字通信系统模型

信源编码之后的码字序列抗干扰能力很脆弱，在信道噪声的影响下容易产生差错，为了提高通信系统的有效性和可靠性，要在信源编码器和信道之间加上一个信道编码器。

概　论



概　论 信道的分类

根据信道用户的多少

- 单用户信道：只有一个输入端和输出端。对讲机
- 多用户信道：至少一端有两个以上的用户，且可双向通信，计算机网络

根据输入端与输出端的关联

- 无反馈信道：输出端对输入端信号无影响，无线电广播
- 有反馈信道：输出信号反馈到输入端，手机通信

根据信道的统计特性

- 恒参信道：信道的统计特性不随时间变化，光纤通信
- 随参信道：信道的统计特性随时间变化，短波（天波）通信

概　论　信道的分类

根据输入输出信号的特点

- 离散信道：输入输出的随机序列取值都是离散信号，数字电路
- 连续信道：输入输出的随机序列取值都是连续信号，电视
- 半离散半连续信道，A/D，D/A
- 波形信道：输入和输出信号都是时间上连续的随机信号，无线广播

根据信道的记忆特性

- 无记忆信道：只与当前输入有关
- 有记忆信道：不仅与当前输入有关，还与过去输入有关

概 要

信道编码定理

- 概 论
- 信道模型
- 信道编码译码
- 信道容量
- 信道编码定理

信道的数学模型及分类

这里研究**无反馈、固定参数的单用户离散信道**

（1）无干扰信道，输入信号与输出信号有一一对应关系

$$y = f(x),\quad P(y|x) = \begin{cases} 1, y = f(x) \\ 0, y \neq f(x) \end{cases}$$

（2）有干扰无记忆信道：输入与输出无一一对应关系，输出只与当前输入有关系

（3）有干扰有记忆信道：这是最一般的信道。

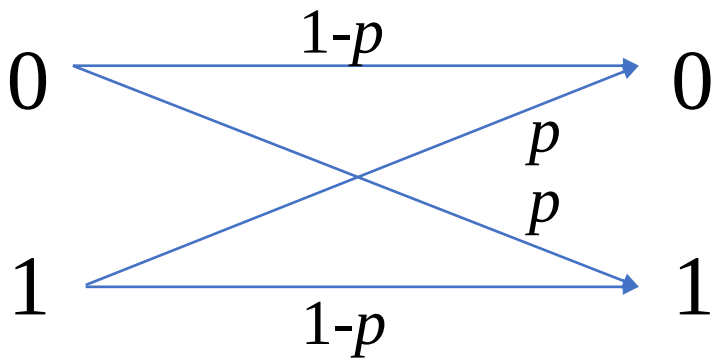
信道转移概率表示成矩阵

$$C\left[u, v, p(v|u)\right]$$

$$P = \begin{array}{c} \\ u_1 \\ u_2 \\ \cdots \\ u_n \end{array} \begin{array}{c} \begin{array}{cccc} v_1 & v_2 & \cdots & v_m \end{array} \\ \begin{bmatrix} p(v_1|u_1) & p(v_2|u_1) & \cdots & p(v_m|u_1) \\ p(v_1|u_2) & p(v_2|u_2) & \cdots & p(v_m|u_2) \\ \cdots & \cdots & \cdots & \cdots \\ p(v_1|u_n) & p(v_2|u_n) & \cdots & p(v_m|u_n) \end{bmatrix} \end{array}$$

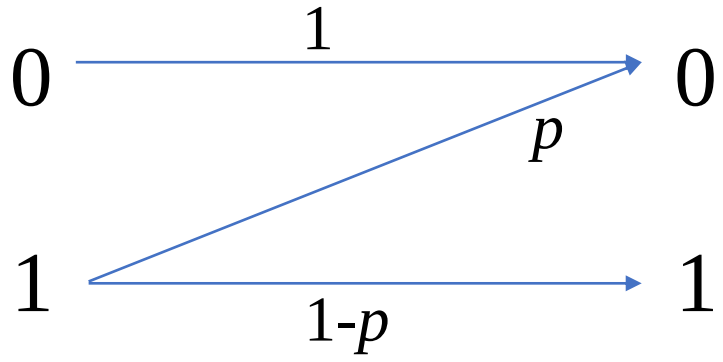
信道模型(典型的无记忆信道)

二进制对称信道（BSC）



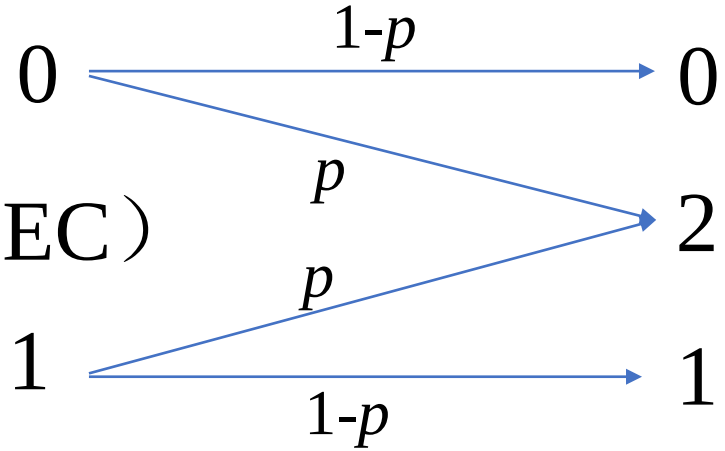
$$\begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix}$$

Z信道



$$\begin{pmatrix} 1 & 0 \\ p & 1-p \end{pmatrix}$$

M信道（BEC）



$$\begin{pmatrix} 1-p & 0 & p \\ 0 & 1-p & p \end{pmatrix}$$

信道模型

离散输入连续输出信道

-假定信道编码器的输出符号取自$X = \{x_0, x_1, \ldots, x_{q-1}\}$,译码器输入为连续值$Y = R$，称这类信道为离散输入连续输出信道，典型的有，二元输入高斯白噪声信道（BIAWGN）

- BIAWGN输入输出可表示为 $Y=X+N$
- 其中，N为加性高斯白噪声，其均值为零，方差为σ^2。给定一个输入$X = x_k$, $k = 0, 1,\ldots, q-1$，则Y是均值为x_k，方差为σ^2的高斯变量

$$p(y \mid X = x_k) = \frac{1}{\sqrt{2\pi\sigma}} \exp\left\{-(y - x_k)/2\sigma^2\right\}$$

概 要

信道编码定理

- 概 论
- 信道模型
- 信道编码译码
- 信道容量
- 信道编码定理

信道编码问题

信道编码的目标：保证通信误差充分小的情况下，传送尽可能多的信息。

信道编码问题

信息在信道中通过的含义

信道容量：多少信息可以在信道中通过

减少信源传输的信息量可以降低通信时的误差概率

↓

牺牲数量可以换质量

差错类型

差错类型

◆ 独立随机差错：
在无记忆信道中出现，数据流中发生的错误彼此无关。

◆ 突发错误：
在有记忆信道中，数据流中一个错误的发生，带来一连串错误的发生。

◆ 混合差错：

信道编码

信道编码分类

- 纠独立随机差错码
- 纠突发差错码；
- 纠混合差错码。

信道编码的基本思路

根据一定的规律在待发送的信息码中加入一些多余的码元，以保证传输过程的可靠性。其任务就是构造出以最小多余度代价换取最大抗干扰性能的“好码”。

信道编码

好的错误控制编码方案的目标

- 用可以纠正的错误个数来衡量纠错能力；
- 快速有效地对消息进行编码；
- 快速有效地对接收到的消息进行译码；
- 单位时间内所能传输的信息比特数尽量大（即有少的冗余度）

基本知识：

- ✓ 目标（1）是最基本目标。
- ✓ 为了增加一个编码方案的纠错能力，必须引入更多的冗余度。（但增加的冗余度会造成实际信息传输速率的降低）
- ✓ 目标（1）和（4）不完全相容。
- ✓ 为了能纠正更多的错误，编码策略会变得更复杂，于是（2）和（3）目标也很难达到。

译码规则

译码规则（译码函数）

依据一定的判决准则设计一个单值函数 $F(b_j) = a_i$ $(i = 1, 2, \ldots, r; j = 1, 2, \ldots, s)$，使每一种可能的输出符号 b_j（$j = 1, 2, \ldots, s$）与一个唯一的输入符号 a_i $(i = 1, 2, \ldots, r)$一一对应。函数 $F(b_j) = a_i$ 即为译码函数或译码规则。

注：对输入符号集为 $X = \{a_1, a_2, \ldots, a_r\}$，输出符号集为 $Y = \{b_1, b_2, \ldots, b_s\}$ 的信道来说，一共可构成 r^s 种不同译码规则。

例：二进制对称信道，其输入符号集为 $X = \{0, 1\}$，输出符号集为 $Y = \{0, 1\}$，则可构成 $2^2=4$ 种译码规则。

- $F(0)=0$，$F(1)=0$；
- $F(0)=0$，$F(1)=1$；
- $F(0)=1$，$F(1)=0$；
- $F(0)=1$，$F(1)=1$；

译码规则

注：不同的译码规则会引起不同的可靠程度。

例：若已知二进制对称信道传递矩阵为 $P=\begin{pmatrix} \frac{1}{4} & \frac{3}{4} \\ \frac{3}{4} & \frac{1}{4} \end{pmatrix}$

其信源符号‘0’和‘1’的正确传递概率为p=1/4；‘0’和‘1’的错误传递概率为p=3/4

如采取译码规则（2），$F(0)=0$，$F(1)=1$,则信道输出端出现‘0’和‘1’的正确译码概率分别是

$$p=\{X=0|Y=0\}=\overline{p}=1/4$$

$$p=\{X=1|Y=1\}=\overline{p}=1/4$$

从统计观点看，输出端出现的4个符号‘0’或‘1’中，只能有一个得到正确译码。

译码规则

例：若已知二进制对称信道传递矩阵为 $P=\begin{pmatrix} \frac{1}{4} & \frac{3}{4} \\ \frac{3}{4} & \frac{1}{4} \end{pmatrix}$

其信源符号‘0’和‘1’的正确传递概率为p=1/4；0’和‘1’的错误传递概率为p=3/4

如采取译码规则（3），$F(0)=1$，$F(1)=0$,则信道输出端出现 ‘0’和‘1’的正确译码概率分别是

$$p=\{X=1|Y=0\}=\overline{p}=3/4$$

$$p=\{X=0|Y=1\}=\overline{p}=3/4$$

从统计观点看，输出端出现的4个符号‘0’或‘1’中，有3个得到正确译码。

正确译码概率

正确译码概率P_{rj}

当信道的输入符号是a_i，在信道输出端收到某符号$b_j(j=1, 2, \ldots, s)$后，正确译码的概率p_{rj}是在信道输出端出现$b_j(j=1, 2, \ldots, s)$的前提下，推测信道输入符号a_i的后验概率，即

$$p_{rj} = p\left\{X = F\left(b_j\right) = a_i \mid Y = b_j\right\}$$

错误译码概率

正确译码概率P_{ej}

当信道的输入符号是a_i，在信道输出端收到某符号$b_j(j=1, 2, \ldots, s)$后，错误译码的概率p_{ej}是在信道输出端出现$b_j(j=1, 2, \ldots, s)$的前提下，推测信道输入符号是除了a_i以外的其他任何可能输入符号的后验概率，即

$$p_{ej} = P\{X = e \mid Y = b_j\}$$

式中：e表示除了$F(b_j)=a_i$以外的所有可能的输入符号的集合。

$$p_{ej} = 1 - p_{rj} = 1 - p\{F(b_j) = a_i \mid b_j\}$$

平均错误译码概率

$$P_e = \sum_{j=1}^{s} p(b_j) p_{ej} = \sum_{j=1}^{s} p(b_j) \left\{ 1 - p\left[F(b_j) = a_i \mid b_j \right] \right\}$$

$$= \sum_{j=1}^{s} p(b_j) - \sum_{j=1}^{s} p(b_j) p\left[F(b_j) = a_i \mid b_j \right]$$

$$= 1 - \sum_{j=1}^{s} p(b_j) p\left[F(b_j) = a_i \mid b_j \right]$$

说明

- 平均错误译码的概率P_e：表示在信道输出端每收到一个符号其产生错误译码的可能性的大小；
- 平均错误译码的概率P_e可作为信道传输可靠性的衡量标准；
- 平均错误译码的概率P_e取决于信道输出随机变量的概率空间$P(Y)$、信道的后验概率分布$P(X|Y)$以及译码规则；
- 选择合适的译码规则可降低平均错误译码的概率

费诺不等式

描述了平均错误译码概率P_e与信道疑义度$H(X|Y)$的内在联系，即

$$H\left(X\mid Y\right)\le H\left(P_e\right)+P_e\log_a\left(r-1\right)$$

（1）不论采用什么准则选择译码规则，费诺不等式都是普遍成立的。

（2）费诺不等式表明，在收到信道输出随机变量后，对输入随机变量仍然存在的平均不确定性$H(X|Y)$由两部分组成：第一部分是收到输出随机变量后，按选择的译码规则译码时，是否产生错误译码的平均不确定性$H(P_e)$；第二部分是当平均错误译码概率为P_e时，到底是哪一个信源符号被错误译码的最大平均不确定性，它是（n-1）个符号不确定性的最大值$\log_a(r\text{-}1)$与P_e的乘积。

概 要

信道编码定理

- 概 论
- 信道模型
- 信道编码译码
- 信道容量
- 信道编码定理

信道容量

信息传输率：信道种平均每个符号所能传送的信息量。

$$R = I(X;Y) = H(X) - H(X|Y)$$

每个固定信道都有一个最大的信息传输率。信道容量定义为信道中每个符号所能传递的最大信息量，也就是最大的$I(X;Y)$值。此时输入的概率分布称为最佳输入分布。

$$C = \max_{P(x)}\{I(X;Y)\}$$

信道容量

信道容量：信道输入与信道输出的互信息，它表征了信道可靠传输的最多速率。最常见的信道容量计算式就是带宽、功率受限下的加性高斯白噪声（AWGN）信道容量计算式。设AWGN信道带宽受限于[-W，W]，噪声双边功率谱密度为$N_0/2$，信号功率为P，则。

$$C = W\log\left(1+\frac{P}{N_0 W}\right) bits/s$$

这个容量仅在输入服从高斯分布的情况下可以达到。如果输入信号调制受限，那么容量将会小于上面这个值。

信道容量

-BSC: 对转移概率为p的二进制对称信道二言，当输入等概时，互信息取得最大值，信道容量为，其中$H(p)$是二元熵函数。

$$C = 1 + p\log_2 p + (1-p)\log_2 (1-p) = 1 - H(p)$$

-BEC: $C = 1- p$

-BIAWGN:

$$C = \frac{1}{2}\int_{-\infty}^{+\infty} p\left(y \mid \sqrt{E_s}\right)\log_2 \frac{p\left(y \mid \sqrt{E_s}\right)}{p(y)} dy$$

$$+\frac{1}{2}\int_{-\infty}^{+\infty} p\left(y \mid -\sqrt{E_s}\right)\log_2 \frac{p\left(y \mid -\sqrt{E_s}\right)}{p(y)} dy$$

概 要

信道编码定理

- 概 论
- 信道模型
- 信道编码译码
- 信道容量
- 信道编码定理

信道编码定理

设R是信息传输的速率，C是离散无记忆信道的信道容量，$\varepsilon > 0$是任意小的数，则只要$R < C$就总存在码字长为N，码字数为$M=2^{NR}$的分组码使译码的平均错误概率$P_e < \varepsilon$。

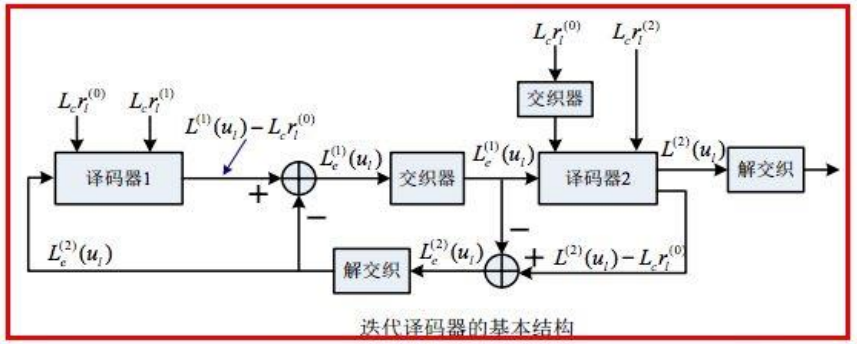
任意离散输入无记忆平稳有噪信道都有一个被称为信道容量的值C，它标志着信道传输能力的上限，只要信息传输速率$R \le C$，就存在一种编码方式，当平均码长足够大时，译码错误概率可以做到任意小；反之，则无论采用何种编码方式也不可能保证错误概率任意小。

编码历史

香农前辈虽然指出了可以通过差错控制码实现可靠通信的理论参考，但却没有给出具体实现的方法。于是，人们开始研究编码方案，不断逼近香农极限。

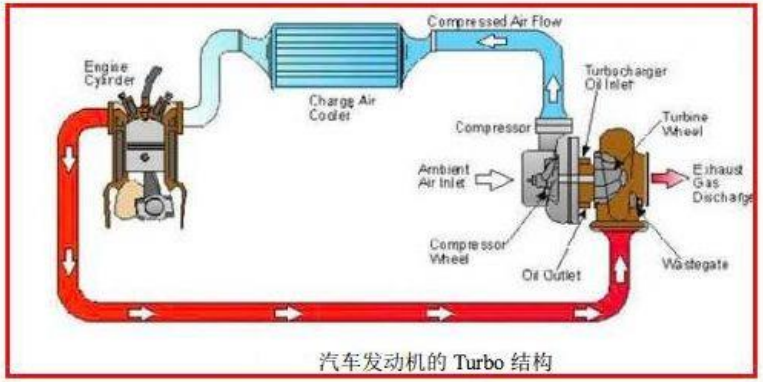
汉明码-格雷码-卷积码（ Viterbi译码算法）　　计算复杂性

1993年，两位当时名不见经传的法国电机工程师C.Berrou和A.Glavieux声称他们发明了一种编码方法——Turbo码，可以使信道编码效率接近香农极限。



迭代译码器的基本结构

这两位法国工程师正是绕过数学理论，凭借其丰富的实际经验，通过迭代译码的办法解决了计算复杂性问题。



汽车发动机的 Turbo 结构

作业

1-为什么进行信道编码。

2-信源为1，信宿收到0的概率为0.3，请画出二进制对称信道和Z信道的转移概率矩阵。