第7章

有噪信道编码

本章主要内容：

§7.1 概述

- 信道编码：就是按一定的规则给信源输出序列增加某些冗余符号，使其变成满足一定数学规律的码序列（或码字），再经信道进行传输。（提高传输的可靠性）

- 信道译码：就是按与编码器同样的数学规律去掉接收序列中的冗余符号，恢复信源消息序列。

一般地，所加的冗余符号越多，纠错能力就越强，但传输效率降低。因此在信道编码中明显体现了传输有效性与可靠性的矛盾。

本节主要内容：

1. 信道编码的基本概念
2. 判决与译码规则
3. 译码错误概率

7.1.1 信道编码的基本概念

简化的通信系统模型如图7.1.1所示。

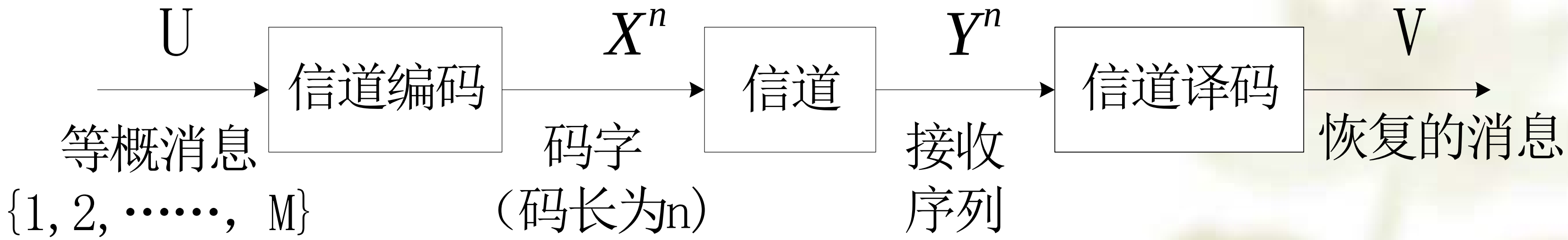


图7.1.1 简化通信系统模型图

设信源输出或信道编码器的输入消息集合为U，信道编码器采用分组编码，输出码字为X^n的一个子集，其中每个码符号$x \in X_i$取自符号集$A = \{a_1, a_2, \cdots, a_r\}$；码字通过离散无记忆信道传输；信道输出或译码器的输入为Y^n，其中每个符号$y \in Y$取自符号集$B = \{b_1, b_2, \cdots, b_s\}$；译码器输出是被恢复的消息，其集合用V表示。

信息传送过程

（1） 消息产生：由信源发出M个等概率消息：U = {1，2，…，M}；

（2） 信道编码：编码器将消息映射成码字，编码函数f：{1，2，…，M}→C=$\{\mathbf{c}_1,\mathbf{c}_2,\cdots,\mathbf{c}_M\}$，其为码长为n的码字，码符号集A的大小为r；

（3） 信道传输：$\mathbf{x}$ 为n维矢量，取自码字集C，作为n次扩展信道的输入，$C \in A^n$，$\mathbf{y}$ 是n维矢量，为信道输出，$\mathbf{y} \in Y^n$；

（4） 信道译码：译码器根据接收的 $\mathbf{y}$ 完成译码功能，译码函数 $g: Y^n \rightarrow V = \{1, 2, \cdots, M\}$ 。

衡量信道编码有效性的重要指标就是信息传输速率

对于离散信道，当离散信源的符号通过信道编码器编成长度为n的码字通过信道传输时，那么信息传输速率为

$$R = H(X) / n \quad (7.1.1)$$

单位为：比特（或奈特）/信道符号，其中，$H(X)$为信源的熵。

当信源符号等概率时，一个（M，n）码信息传输速率R为

$$R = \log M \ / n \quad (7.1.2)$$

对于时间连续信道，信息传输速率表示单位时间所传送的信息量，即信息传输速率为

$$R' = H(X)/(nT_s)$$

单位为：比特（或奈特）/秒，其中，T_s为传输一个码符号所需时间

7.1.2 判决与译码准则

考虑单符号的判决，这时输入为编码符号集A

对于图7.1.1所示的模型，单符号判决规则为：

$$g(y=b_j)=a^* \qquad j=1,\cdots,s \tag{7.1.3}$$

其中，$a^* \in A$。（7.1.3）的含义是，当接收到b_j就判定为a^*发送符号。因此，对每一个信道输出都必须有一个信道输入与之对应。所以判决规则是一个有惟一结果的函数。

（7.1.3）式可简记为 $g(y)=x^*$，称 $g(y)$ 为判决函数。

设信道的转移概率为 $P_{Y/X}(y=b_j \mid x=a_i)=p_{ij}$，那么，在接收到 b_j 的条件下，若实际上发送的是a^*，则判决正确，反之就出现差错。

在发送 $x = a_i$ 条件下，利用判决规则（7.1.3），条件错误率定义为:

$$p(e \mid x = a_i) = \sum_{y, g(y) \neq a_i} p(y \mid x = a_i) \tag{7.1.4}$$

平均错误率定义为:

$$P_E = \sum_i p(x = a_i) p(e \mid x = a_i) = \sum_x p(x) \sum_{y, g(y) \neq x} p(y \mid x) = 1 - \sum_y p(x^* y) \tag{7.1.5}$$

还可计算平均正确率为：

$$\bar{P}_E = 1 - P_E = \sum_y p(x^* y) \tag{7.1.6}$$

例7．1．1 一个二元对称信道输入和输出分别为X，Y，其中$p_X(0)=\omega$，信道的转移概率为$p_{Y|X}(0|0)=p_{Y|X}(1|1)=1-p$，$p_{Y|X}(1|0)=p_{Y|X}(0|1)=p$，分别求下面两种判决函数所对应的平均错误率并比较两者的大小：

（1）$g(y=0)=0, g(y=1)=1$；

（2）$g(y=0)=1, g(y=1)=0$。

解

（1） $$p(e\mid x=0)=p_{Y|X}(1\mid 0)=p$$

$$p(e\mid x=1)=p_{Y|X}(0\mid 1)=p$$

平均错误率：$P_{E1}=\omega p+(1-\omega)p=p$

（2） $$p(e|x=0)=p_{Y|X}(0|0)=1-p$$

$$p(e|x=1)=p_{Y|X}(1|1)=1-p$$

平均错误率：$P_{E2}=\omega(1-p)+(1-\omega)(1-p)=1-p$

很明显，当 $p\le 1/2$ 时，$P_{E1}\le P_{E2}$；否则 $P_{E1}>P_{E2}$。

此例说明，错误率和判决函数的选取有关。幻灯片 4

7.1.3 译码错误概率

如前所述，译码就是通过接收序列恢复消息序列。如果恢复的消息序列与发送序列不同，则称译码差错。通常有两种错误概率的描述：误码率和误字率。误码率是指传输码元出错概率（对二进制也称误比特率）。误字率是指码字出错概率。本章所研究的错误率就是误字率。

与单符号判决情况类似，条件错误率为：

$$\boxed{P(g(\mathbf{y}) \neq i \mid \mathbf{x} = \mathbf{c}_i)} \tag{7.1.7}$$

平均错误率为：

$$\boxed{P_E = \sum_{i,\mathbf{y}} p(\mathbf{c}_i) P(g(\mathbf{y}) \neq i \mid \mathbf{x} = \mathbf{c}_i)} \tag{7.1.8}$$

错误概率的大小首先与编码器的纠错性能有关，其次与译码规则的选择有关也和接收信噪比大小有关。

应选择纠错性能好的编码，性能好的译码算法以使平均错误概率最小。幻灯片2

§7.2　最佳判决与译码准则

本节主要内容：

1. 最大后验概率准则
2. 最大似然准则

注：假定输入x，输出y
1. p(x): x的先验概率
2. p(y|x):有明确因果关系，称之为似然概率
3. p(x|y)：事件y发生后，反推x的概率，称后验

7.2.1 最大后验概率准则

为提高传输可靠性，除采用有效的 信道编码之外，还应采用适当的译码准则。本节介绍最大后验概率（MAP）准则和最大似然（ML）准则。

根据（7.1.6）式，平均正确率可以写为

使最大

$$\sum_y p(x^* y) = \sum_y p(y) p(x^* | y) \leq \sum_y p(y) \max_x p(x | y)$$

为使判决正确率最大或使判决错误率最小，对于判决准则，应使得对于每一个输出y，都选择对应后验概率最大的x。

即对所有i，当满足

$$p(x = a^* \mid y) \geq p(x = a_i \mid y) \qquad (7.2.1)$$

时，则选择判决函数为，称此准则为最大后验概率 (MAP, Maximum a Posteriori) 准则，可简写为：

MAP准则：

$$g(y) = \arg\max_x p(x \mid y) \qquad (7.2.2)$$

MAP准则就是，对给定的信道输出将具有最大后验概率的输入符号作为判决结果。

由（7.2.1）式，得

$$p(x=a_i\mid y)$$

$$\frac{p(x=a^*)p(y\mid x=a^*)}{p(y)} \geq \frac{p(x=a_i)p(y\mid x=a_i)}{p(y)}$$

意义在于：实际应用时，后验概率一般没有显式表达，而似然概率有表达

所以，对所有i，当

$$\boxed{\Lambda = \frac{p(y\mid x=a^*)}{p(y\mid x=a_i)} \geq \frac{p(x=a_i)}{p(x=a^*)}} \qquad (7.2.3)$$

时，则选择判决函数为g(y)=a*。其中,Λ为似然比，（7.2.3）式表示的是似然比检验。

注：（1）MAP准则是使平均错误率最小的准则；

（2）MAP准则可归结为似然比检验。

例7.2.1 设信道输入X等概率取值为{+1，-1}，通过一个加性高斯信道传输，加性噪声Z是均值为零，方差为σ^2的高斯随机变量，信道输出Y=X+Z，接收机用MAP准则接收，试确定判决函数。

均值为x，方差为σ的高斯

解　后验概率密度为

$$p(x|y)=\frac{p(x)p(y|x)}{p(x=1)p(y|x=1)+p(x=-1)p(y|x=-1)}$$

P(y)

$$=\frac{\exp[-(y-x)/(2\sigma^2)]}{\exp[-(y-1)^2/(2\sigma^2)]+\exp[-(y+1)^2/(2\sigma^2)]}$$

$$=\frac{1}{1+\exp(-2xy/\sigma^2)}$$

令 $\Lambda = \dfrac{p(x=1\,|\,y)}{p(x=-1\,|\,y)} = \dfrac{1+\exp(2y/\sigma^2)}{1+\exp(-2y/\sigma^2)}$

则 $\Lambda \geq 1$ 时，$g(y)=+1$；$\Lambda < 1$ 时，$g(y)=-1$；而当 $\Lambda \geq 1$ 时，有 $y \geq 0$；$\Lambda < 1$ 时，有 $y < 0$；

所以，判决函数为 $$g(y)=\begin{cases}+1 & y \geq 0\\ -1 & y < 0\end{cases}$$

§7.2

7.2.2 最大似然准则

若输入符号等概，（7.2.3）变为：

对所有i, 当

$$\boxed{p(y\,|\,x=a^{*}) \geq p(y\,|\,x=a_i)} \qquad (7.2.4)$$

则选择判决函数为g(y)=a*，称此准则为最大似然（Maximum Likelihood，ML）准则，可简写为：

ML准则：

$$\boxed{g(y) = \arg\max_{x}\ p(y\,|\,x)} \qquad (7.2.5)$$

注：（1）当输入符号等概或先验概率未知时，采用 此准则。

（2）当输入符号等概时，最大似然准则等价于最大后验概率准则。

例7.2.1（续）接收机用ML准则接收，试确定判决函数。

解　似然函数为

$$p(y|x)=\frac{1}{\sqrt{2\pi\sigma}}\exp[-(y-x)^2/(2\sigma^2)]$$

令　$$\Lambda=\frac{p(y|x=1)}{p(y|x=-1)}=\exp(2y/\sigma^2)$$

类似于MAP判决情况，可得到与MAP相同的结果，这是意料之中的，因为信道输入等概率。但当信道输入概率不相等时，MAP和ML判决函数和平均错误率通常是不同的，而MAP准则是使平均错误率最小的。

如果信道输入概率和转移概率矩阵给定，那么可对两种准则使用要点总结如下：

p(x)已知

1. 转移概率阵的每个元素为p(y|x)，乘p(x)，得到p(x,y)
2. 每列最大p(x,y)相加得正确概率

✓ MAP准则

由转移概率矩阵的每行分别乘p(x)，得到联合概率矩阵；对于每一列（相当于y固定）找一个最大的概率对应的x作为判决结果；所有判决结果所对应的联合概率的和为正确概率，其他矩阵元素的和为错误概率。

$$\begin{array}{cc} & y \\ x & [p(xy)] \end{array}$$

假定输入有r个元素，p(x)=1/r

1. 转移概率p(y|x)为似然

2. 每列最大—》最大似然

✓ ML准则 (先验概率未知)

对转移概率矩阵中每列选择最大的一个元素对应的x作为判决结果；所有信道输出和所对应判决结果的联合概率之和为平均正确率，其他的联合概率之和为平均错误率。<u>幻灯片 2</u>

$$\begin{array}{cc} & y \\ x & [p(y|x)] \end{array}$$

§7.3　信道编码与最佳译码

本节主要内容：

1. 线性分组码
2. 序列最大似然译码
3. 几种简单的分组码

7.3.1　线性分组码

信道编码有很多种类，其中最重要的一类是线性分组码，其冗余符号（也称校验位或监督位）和信息符号是线性关系。本节利用简单的线性分组码的最佳译码说明如何实现传输可靠性。

一个二元（n，k）线性分组码有k个信息位，n-k个校验位，根据某种确定的数学关系构成总长度为n的码字，码率为k/n。在线性分组码中，校验位为信息位的线性组合。如果码字的开头或结尾的k位是信息位，那么就称为系统码，否则称非系统码。在（n，k）线性分组码中码字的个数有 2^k 个。（许用码），而可能的码字有2^n个

例7．3．1 求一个二进（n，k）线性分组码的信息传输速率。

解

$$\boxed{R=\frac{\log_2 2^k}{n}=\frac{k}{n}}$$ （比特/符号） （7.3.1）

R=k/n常称做码率或编码效率。

1. 汉明距离

设两个二元码字为 $\boldsymbol{x}=(x_1,\ldots,x_n),\boldsymbol{y}=(y_1,\ldots,y_n)$ ，其中，x_i,y_i均取自符号{0，1}，定义它们的汉明距离为

$$d(\mathbf{x},\mathbf{y})=\sum_{k=1}^{n} x_k \oplus y_k \qquad (7.3.2)$$

其中，$\oplus$为模二加运算。

例如，码字 $\boldsymbol{x}=(1101110)$ 和码字 $\boldsymbol{y}=(1010001)$的汉明距离为6。

引理7.3.1 设$\boldsymbol{x}$、$\boldsymbol{y}$、$\boldsymbol{z}$是长度为n的二元矢量，那么

（1）$d(\boldsymbol{x},\boldsymbol{y}) \geq 0$ （非负性）

（2）$d(\boldsymbol{x},\boldsymbol{y}) = d(\boldsymbol{y},\boldsymbol{x})$ （对称性）

（3）$d(\boldsymbol{x},\boldsymbol{z}) \leq d(\boldsymbol{x},\boldsymbol{y}) + d(\boldsymbol{y},\boldsymbol{z})$ （三角不等式）

（证明留做练习）

2. 码的最小距离

- 码的最小距离：一个码字集合中任意两个许用码字的最小汉明距离用 $d_{\min}$ 来表示。

一个（n，k）线性分组码的最小 $d_{\min}$ 距离定义为

$$\boxed{d_{\min} = \min_{i \neq j} d(\boldsymbol{v}_i, \boldsymbol{v}_j)} \qquad (7.3.3)$$

其中，$d(v_i, v_j)$表示码字v_i, v_j间的汉明距离。

注：对于（n，k）线性分组码，有个 2^n 码字，其中许用码字 2^k 个，禁用码字2^{n-k} 个

由于线性分组码可看成n维空间的一个子空间，任何两码字的和都是码字，所以

$$\boxed{d_{\min} = \min_{i \neq j} d(\boldsymbol{v}_i, \boldsymbol{v}_j) = \min_{i \neq j} d(\boldsymbol{v}_i \oplus \boldsymbol{v}_j) = \min_{v_k \neq 0} w(\boldsymbol{v}_k)} \quad (7.3.4)$$

其中，$v_k = v_i \oplus v_j$，$w(.)$表示某码字的重量，即该码字中不为“0”的“1”的个数。

因此，线性分组码的最小距离$d_{\min}$就是其最小重量的非零码字。

例7．3．2 一个线性分组码C={00000，01010，10101，11111}，求该码的最小距离$d_{\min}$。

解 $d_{\min} = w(01010)=2$

7.3.2 序列最大似然译码

设所有符号规定与图7.1.1所示的模型的说明相同。如果对于所有k，满足

$$p(\mathbf{y}\,|\,\mathbf{x}=\mathbf{c}^*) \ge p(\mathbf{y}\,|\,\mathbf{x}=\mathbf{c}_k) \qquad (7.3.5)$$

就选择译码函数为 $g(\mathbf{y}) = f^{-1}(\mathbf{c}^*)$ ，则称为序列的最大似然译码准则，其中，$f^{-1}(\mathbf{c}^*)$ 表示码字 $\mathbf{c}^*$ 所对应的消息。转移概率 $p(\mathbf{y}\,|\,\mathbf{x})$ 称为似然函数。

f 为编码器 $\Rightarrow$

$f(k) = c_k$

可以简写为

ML译码：

$$g(\mathbf{y}) = f^{-1}(\arg\max_{\mathbf{c}_k \in \mathbf{C}} p(\mathbf{y}\,|\,\mathbf{c}_k)) \qquad (7.3.6)$$

与单符号情况相同，当消息等概或概率未知时用最大似然译码准则。

在通信系统中，设发送序列为X，接收序列为Y，并且X和Y来自同一个符号集，由于信道噪声的干扰，通常Y与X不同。当接收到Y后，计算所有可能的发送序列X与Y之间的汉明距离，将与Y汉明距离最小的X作为译码输出，这种译码方法称$\boxed{\text{最小汉明距离准则}}$。

定理7.3.1 对于无记忆二元对称信道（错误概率小于1/2），最大似然译码准则等价于最小汉明距离准则。

证

设信道的输入与输出分别为序列$\boldsymbol{x}=(x_1,\dots,x_n)$，$\boldsymbol{y}=(y_1,\dots,y_n)$，因为信道是无记忆的，所以似然函数为

$$\boxed{p(\mathbf{y}\,|\,\mathbf{x})=\prod_{i=1}^{n}p(y_i\,|\,x_i)} \qquad （7.3.7）$$

设$\mathbf{x},\mathbf{y}$的汉明距离为d，如果x_i出错，那么y_i与x_i不同，从而使汉明距离增加1。设二元对称信道的传输错误率为p，根据二元对称信道的特性，有

$$p(y_i\,|\,x_i)=\begin{cases} p & x_i\neq y_i \\ 1-p & x_i=y_i \end{cases}$$

其中$p\le 1/2$。

此项为负

所以（7.3.7）式变为 $p(\mathbf{y}|\mathbf{x})=(1-p)^{n-d}p^{d}$ ，取对数，得

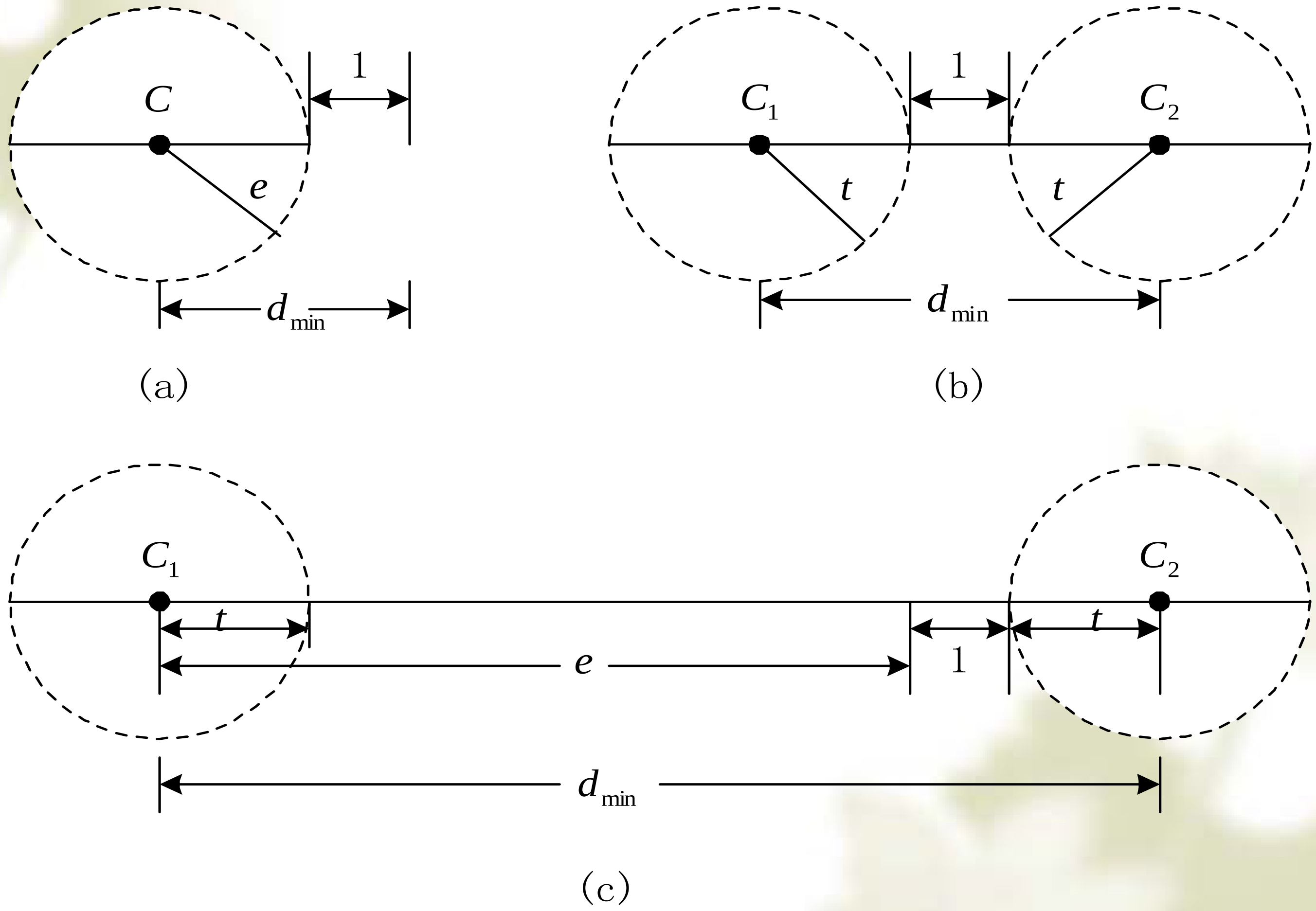
$$\log p(\mathbf{y}\,|\,\mathbf{x}) = n\log(1-p) + d\,\boxed{\log[p/(1-p)]} \tag{7.3.8}$$

因为n是定值，信道固定后，p也是定值，又 $p \le 1/2$ ，所以，对于所有的码序列，当对应的*d*最小时就使（7.3.7）的值最大，从而使似然函数最大。

下面的定理说明，码的纠错能力与码的最小码距d有直接关系。首先引入差错矢量的概念。设一个长度与码字相同的矢量e为差错矢量，其每个分量取值为0或1，设发送和接收矢量分别为 x 和y，那么接收矢量可以表示为$y = x + e$。如果e的某分量为1表示码字对应的位出错，反之如果为0表示码字对应的位传输正确。

定理7.3.2　一个最小距离为d的二元分组码能检测e个错的充要条件是: $d>e+1$；能纠t个错的充要条件：

$$d>2t+1 \qquad (7.3.9)$$



码距和检错和纠错能力的关系

7.3.3 几种简单的分组码

1. 重复码

重复码是一种最简单的分组码，只有一个信息位，n-1个校验位（是信息位的简单重复），码率为1/n，所以码字数与信源符号数相同。二元重复码中只有两个码字，即0…0和1…1，码的最小距离为n，能纠（n-1）/2个差错。很明显，一个n次重复码的距离是n。

2. 奇偶校验码

奇偶校验码是一种（n，n-1）二元分组码，有n-1个信息位，1个校验位，码率为（n-1）/n。 校验位的选取应使得每个码字的重量都是奇数或偶数。在奇校验中，每个码字的重量是奇数，而在偶校验中，每个码字的重量是偶数。当传输差错是奇数时，就改变码字中原来1个数的奇偶性，使接收方发现差错。所以，该码只能检测到奇数个差错。

3. 方阵码

这是一个二维奇偶校验码，又称行列监督码。该码不仅能克服奇偶校验码不能检测偶数个差错的缺点，而且还能纠正突发错误。编码过程简述如下：将要传送的信息排成方阵，对方阵的各行和各列分别进行奇偶校验编码，校验位分别放到相应行或列的后面或下面，构成一个新的矩阵，按顺序将新矩阵逐行或逐列输出。该码的缺点是，不能检测在方阵构成矩形四角的错误。

例7.3.3　对等概二元信源符号a_0和a_1进行重复码编码，对应的码字为000，111；编码序列通过错误概率为（$p \le 1/2$）的无记忆二元对称信道传输，接收端利用最大似然译码准则；

（1）求重复码的码率；

（2）求重复码的最小码距离与可纠错误数；

（3）求译码错误率p_E；

（4）将p_E与未编码译码错误率比较。

解

（1）码率R=1/3；

（2）最小码距离3，可纠错误数1；

（3）由于是对称信道，可利用最小汉明距离准则进行译码。二元对称信道三次扩展信道转移概率矩阵的元素如下表前两行所示（其中X为码字，Y为接收序列），最后一行为译码输出：

分别计算y的每一个可能序列与000和111的汉明距离，将汉明距离小的信源符号作为译码输出。

例如，接收为010，与000的距离为1，而和111的距离为2，所以译码输出为a_0；依次类推，得到表中的下面一行

译码正确率： $$1-p_E=(1-p)^3+3(1-p)^2 p$$

传输正确2或3位

译码错误率： $$p_E = p^3 + 3(1-p)p^2$$

传输错2或3位

（4）因为未编码译码错误率为p，计算差值，得

$$p_E - p = p^3 + 3(1-p)p^2 = p(1-p)(2p-1) \le 0$$

以上p<0.5。从本例可以看到，即使采用很简单的编码也能提高传输可靠性。

可以证明，当采用足够长的重复码（n→∞）时，译码错误率趋于零。（见习题7. 15）

注：这时码字中的信息比特也相应增加

§7.4　费诺（Fano）不等式

本节主要内容：

1. 信道疑义度

2. 费诺（Fano）不等式

7.4.1 信道疑义度

设信道的输入与输出分别为X、Y， 定义条件熵H(X/Y)为信道疑义度。它有如下含义：

- 信道疑义度表示接收到Y条件下X的平均不确定性；
- 根据I(X;Y)=H(X)-H(X/Y)，信道疑义度又表示X经信道传输后信息量的损失；
- 接收的不确定性由信道噪声引起，在无噪情况下，H(X/Y)=0。

7.4.2 费诺（Fano）不等式

定理7．4．1 设信道的输入与输出分别为X、Y，输入符号的数目为r，那么信道疑义度满足

$$H(X|Y) \le H(p_E) + p_E \log(r-1) \quad (7.4.1)$$

其中，p_E为平均错误率。（7．4．1）称做费诺不等式

P_E：译码错误概率，P_E=1-ΣP(x*y)

证　设译码或判决规则由（7.1.3）确定，那么

$$H(X|Y)-H(p_E)-p_E\log(r-1)$$

$$=-\sum_x\sum_y p(xy)\log p(x|y)+p_E\log p_E+(1-p_E)\log(1-P_E)-p_E log(r-1)$$

拆开

$$=-\sum_y\sum_{x\neq x^*}p(xy)\log p(x|y)+\sum_y\sum_{x\neq x^*}p(xy)\log\frac{p_E}{r-1}$$

$$-\sum_y p(x^*y)\log(x^*|y)+\sum_y p(x^*y)\log(1-p_E)$$

$$=\sum_y\sum_{x\neq x^*}p(xy)\log\frac{p_E}{(r-1)p(x|y)}+\sum_y p(x^*y)\log\frac{1-p_E}{p(x^*|y)}$$

注意：$p_E=\sum_y\sum_{x\neq x^*}p(xy)$, $1-p_E=\sum_y p(x^*y)$

对于正数 x ，$\ln x \le x-1$

$$\le \left\{ \sum_{y}\sum_{x\ne x^*} p(xy)\left[\frac{p_E}{(r-1)p(x|y)}-1\right]+\sum_{y} p(x^*y)\left[\frac{1-p_E}{p(x^*|y)}-1\right] \right\}(\log e)$$

=(r-1)

$$=\left\{ \sum_{x\ne x^*}\sum_{y} p(y)\frac{p_E}{(r-1)}-\sum_{y}\sum_{x\ne x^*} p(xy)+\sum_{y}(1-p_E)p(y)-\sum_{y} p(x^*y) \right\}(\log e)$$

=1

$$= p_E - p_E + (1-p_E) - (1-p_E) = 0$$

仅当下面两个条件同时成立时，等号成立：

（1） $\frac{p_E}{(r-1)p(x|y)}-1=0 \Rightarrow p(x|y)=\frac{p_E}{(r-1)}$ （7．4．2a）

（2） $\frac{1-p_E}{p(x^*|y)}-1=0 \Rightarrow p(x^*|y)=1-p_E$ （7．4．2b）

注释：

（1）费诺不等式给出了信道疑义度的上界，无论什么译码规则，费诺不等式成立；译码规则变化只会改变 p_E 的值；

（2）信道疑义度的上界由信源、信道及译码规则所限定；因为信源决定p(x)，r，而p(x)，p(y|x)及译码规则决定 p_E ；

（3）如果H(X/Y) >0，那么 $p_E > 0$；

（4）不等式的含义可以这样来理解：当接收到Y后，关于X平均不确定性的解除可以分成两步来实现：第1步是确定传输是否有错，解除这种不确定性所需信息量为 $H(p_E)$；第2步是当确定传输出错后，究竟是哪一个错，解除这种不确定性所需最大信息量是log(r-1)。

图7.4.1为费诺不等式示意图：

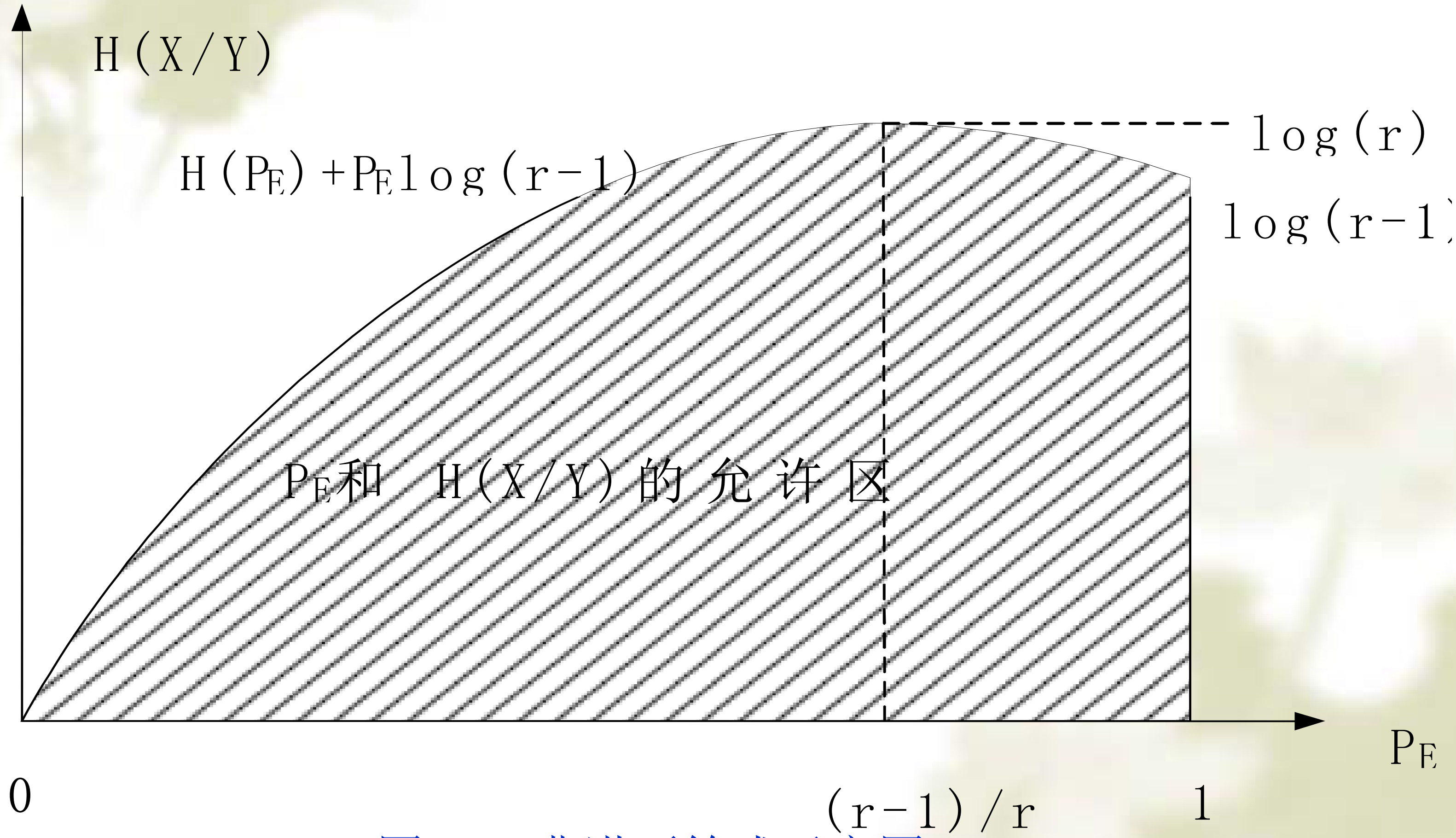


图7.4.1费诺不等式示意图

图中，曲线下面的区域为信道疑义度被限定的区域。信道疑义度不能超过区域边界的曲线。现求曲线所表示的函数的极大值。

$$H(p_E)+p_E\log(r-1)=p_E\log\frac{r-1}{p_E}+(1-p_E)\log\frac{1}{1-p_E}$$
$$\leq\log[p_E\frac{r-1}{p_E}+(1-p_E)\frac{1}{1-p_E}]=\log r$$

上凸函数性质

仅当 $\frac{r-1}{p_E}=\frac{1}{1-p_E}$，即

$$p_E=\frac{r-1}{r} \quad (7.4.3)$$

时等式成立。

由于当$p_E = 1$时，有

$$H(p_E) + p_E \log(r-1) = \log(r-1)$$

结合（7．4．2）和（7．4．3），可以推出信道疑义度达到最大值的充要条件是，信道输入与输出统计独立。（见习题7．8）

例7.4.1 已知信道的转移概率矩阵为

$$\begin{pmatrix} 1/2 & 1/3 & 1/6 \\ 1/6 & 1/2 & 1/3 \\ 1/3 & 1/6 & 1/2 \end{pmatrix}$$

现有两种判决规则：

规则A：$\begin{cases} g(y=b_1)=a_1 \\ g(y=b_2)=a_2 \\ g(y=b_3)=a_3 \end{cases}$，规则B：$\begin{cases} g(y=b_1)=a_1 \\ g(y=b_2)=a_3 \\ g(y=b_3)=a_2 \end{cases}$

设输入等概，求信道的疑义度和两种译码规则下信道疑义度的上界？

对称信道: $C=H(Y)-H(p_1 \ \cdots \ p_s)$

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

解

当信道输入等概率时输出也等概率，所以 $H(X)=H(Y)$。又因为 $H(X)-H(X|Y)=H(Y)-H(Y|X)$，所以信道疑义度：

$$H(X|Y)=H(Y|X)=H(1/2,1/3,1/6)=1.459$$ 比特

对于判决规则A，$P_E(A)=1/2$，

所以信道疑义度上界为：$H(1/2)+(1/2)\times\log 2=1.5$ 比特

对于判决规则B，$P_E(B)=2/3$，

所以信道疑义度上界为：

$$H(2/3)+(2/3)\times\log 2=\log 3=1.585$$ 比特

$$
\begin{array}{cc}
 & \begin{array}{ccc} b_1 & b_2 & b_3 \end{array} \\
\begin{array}{c} a_1 \\ a_2 \\ a_3 \end{array} &
\begin{pmatrix} 1/2 & 1/3 & 1/6 \\ 1/6 & 1/2 & 1/3 \\ 1/3 & 1/6 & 1/2 \end{pmatrix}
\end{array}
$$

对于译码规则A：

$$
\begin{aligned}
P_E(\mathrm{A}) &= \sum_{x} p(x) \sum_{x \neq g(y)} p(y|x) \\
&= p(a_1)(p(b_2|a_1)+p(b_3|a_1)) \\
&\quad + p(a_2)(p(b_1|a_2)+p(b_3|a_2)) \\
&\quad + p(a_3)(p(b_1|a_3)+p(b_2|a_3)) \\
&= 1/2
\end{aligned}
$$

§7.5　有噪信道编码定理

本节主要内容：

1.　联合典型序列

2.　有噪信道编码定理

3.　无失真信源信道编码定理

前面我们研究了利用重复码可以提高传输可靠性的例子，并且仅当码长足够长时才能实现，而当码长足够长时码率又趋于零。

$$\Rightarrow R = H(X)/n$$

这就是说，可靠性和有效性的要求是矛盾的。

那么高可靠性是否一定意味着低有效性呢？

有噪信道编码定理，即香农第二定理回答了这个问题，该定理指出高可靠性和高有效性的信道编码是存在的。

7.5.1 联合典型序列

在第5章，我们介绍了典型序列，利用（5.3.4）表示某信源符号在序列中出现的频率与其概率接近的程度，并设定一个门限值将序列分成典型和非典型序列。本节我们利用与（5.3.4）不同的不等式定义典型序列。实际上，两种定义无本质区别，但后者在使用上更简单。

设离散无记忆$\boxed{\text{平稳信道}}$的转移概率为 p_{ij}，输入与输出序列分别为 $\boldsymbol{x}=(x_1,\ldots,x_n)$和 $\boldsymbol{y}=(y_1,\ldots,y_n)$，n为序列长度；达到信道容量的输入概率为 $P(x_k=a_i)=p_i$ ，信道输出概率为$P(y_k=b_j)=\sum_i p_i p_{ij}$ ，输入与输出的联合概率为 $P(x_k=a_i,y_k=b_j)=p_i p_{ij}$，$1\le k\le n$ ；设输入/输出序列对$(\mathbf{x},\mathbf{y})$构成序列$\mathbf{xy}=[x_1y_1,x_2y_2,\cdots;x_ny_n]$；并设$n_i$为序列 $\mathbf{x}$ 中的$x_k=a_i$数目，n_j为序列 $\mathbf{y}$中$y_k=b_j$的数目，n_{ij}为序列$(\mathbf{x},\mathbf{y})$中（$x_k=a_i,y_k=b_j$）的数目。

q_j

q_j和信道p_ij有关

如果 $n_i = np_i(1\pm\delta)$，对每个 i，那么就称 $\mathbf{x}$ 为 δ –典型序列；如果 $n_j = n\boxed{\sum_i p_i p_{ij}}(1\pm\delta)$，对每个 j，那么就称 $\mathbf{y}$ 为 δ –典型序列；如果 $n_{ij} = np_i p_{ij}(1\pm\delta)$，对每个 i, j，那么就称 $(\mathbf{x}, \mathbf{y})$ 为 δ –联合典型序列。实际上，联合典型序列 $(\mathbf{x}, \mathbf{y})$ 是两个典型序列 $\mathbf{x}$ 和 $\mathbf{y}$ 所对应的元素组成的有序对构成的一个新序列。这个序列的元素取自联合集XY，序列的概率为：$p(\mathbf{x},\mathbf{y}) = \prod_{i=1}^{n} p(x_i, y_i)$。

引理7. 5. 1　如果 $(\mathbf{x},\mathbf{y})$ 为 δ – 联合典型序列，那么 $\mathbf{x}$ 和 $\mathbf{y}$ 也分别是 δ – 典型序列。

证:

$n_i = \sum_j n_{ij} = \sum_j np_i p_{ij}(1\pm\delta) = np_i(1\pm\delta)$，所以，$\mathbf{x}$ 也是 δ –典型序列。同理，$\mathbf{y}$ 也是 δ – 典型序列。

引理7. 5. 2 对于δ –联合典型序列$(\mathbf{x},\mathbf{y})$，有下面的关系成立：

$$p(\mathbf{x},\mathbf{y}) = 2^{-nH(XY)(1\pm\delta)} \tag{7.5.1}$$

$$p(\mathbf{x}) = 2^{-nH(X)(1\pm\delta)} \tag{7.5.2}$$

$$p(\mathbf{y}) = 2^{-nH(Y)(1\pm\delta)} \tag{7.5.3}$$

对联合典型序列：$n_{ij}=np_i p_{ij}(1\pm\delta)$

证

因为 $p(\mathbf{x},\mathbf{y})=\prod_{i,j}(p_i p_{ij})^{n_{ij}}$，所以

$$\frac{\log p(\mathbf{x},\mathbf{y})}{n}=\sum_{i,j}p_i p_{ij}(1\pm\delta)\log(p_i p_{ij})=-H(XY)(1\pm\delta)$$

从而 (7.5.1)式成立。同理可证 (7.5.2) 和 (7.5.3)成立。

根据典型序列和联合典型序列的性质我们看到：典型 $\mathbf{x}$序列的个数大约为$2^{nH(X)}$，典型序列 $\mathbf{y}$ 的个数大约为$2^{nH(Y)}$，但并不是所有的$(\mathbf{x},\mathbf{y})$对都是联合典型的，因为联合典型序列$(\mathbf{x},\mathbf{y})$的个数大约为$2^{nH(XY)}$，而$H(XY)\le H(X)+H(Y)$。

引理7．5．3　如果$\mathbf{y}$为$\delta-$典型序列，$\mathbf{x}$为与$\mathbf{y}$独立的$\delta-$典型序列，那么与$\mathbf{y}$构成$\delta-$联合典型序列的$\mathbf{x}$的个数不大于$2^{n[H(X/Y)+\delta(H(XY)+H(Y))]}$。

证　因为$\mathbf{y}$为$\delta-$典型序列，根据(7.5.3)，有$p(\mathbf{y})\le 2^{-nH(Y)(1-\delta)}$；又因为$\mathbf{x}$与$\mathbf{y}$构成$\delta-$联合典型序列，所以根据(7.5.1)，有$p(\mathbf{x},\mathbf{y})\ge 2^{-nH(XY)(1+\delta)}$，所以

$$p(\mathbf{x})=p(\mathbf{x},\mathbf{y})/p(\mathbf{y})\ge 2^{-nH(XY)(1+\delta)+nH(Y)(1-\delta)}$$

右边：分子小，分母大

设$F_{\mathbf{y}}$表示满足引理条件的$\mathbf{x}$的集合，那么

$$1\ge\sum_{\mathbf{x}}p(\mathbf{x})\ge\left|F_{\mathbf{y}}\right|2^{-nH(XY)(1+\delta)+nH(Y)(1-\delta)}$$

注意: (X,Y)联合典型,
Y典型 —》X和Y联合典型

因此

$$\boxed{\left|F_{\mathbf{y}}\right|\le 2^{n[H(X/Y)+\delta(H(XY)+H(Y))]}}\qquad(7.5.4)$$

§ 7.5

1. 移到左边，负变正，整理
2. H(XY)-H(Y)+delta(H(XY)+H(Y))
=H(X|Y)+delta(H(XY)+H(Y))

7.5.2　有噪信道编码定理

定理7.5.1（信道编码定理）

设有一离散无记忆平稳信道的容量为C，则只要信息传输率（码率）R<C，总存在一种（M，n）码，使得当n足够长时，译码错误概率 p_E 任意小；反之，当信息传输率R>C时，对任何编码方式，译码差错率 >0。

1. 随机编码

$$R = \frac{\log M}{n}$$

每个n长码字的每一个符号概率按照达到信道容量的输入概率 $p(x)$ 独立选取，从而随机地产生 $M = 2^{nR}$ 个码字。第m个码字的概率为：

$$p(\mathbf{c}_m) = \prod_{i=1}^{n} p(x_i(m)) \qquad (7.5.5)$$

其中，x_i 为码字 $\mathbf{c}_m$ 的第i个符号。

因为每个码字独立产生，所以产生某特殊码的概率为各个码字概率的乘积：

$$p(C) = \prod_{m=1}^{2^{nR}} \prod_{i=1}^{n} p(x_i(m)) \qquad (7.5.6)$$

这种编码方式称随机编码。

从随机编码的概念可以看出，随机编码是指：在编码时，码符号的选择是随机的，从而码字的选择是随机的，码字集合的选择也是随机的。但当码字集合选定后，译码规则就使用确定的码字集合。

由于按照概率选择码符号，所以，当码长足够大时，选择后的码字基本上是典型序列，且这些序列基本上是等概率出现的。

2.联合典型序列译码

设接收序列为 $\mathbf{y}$，如果下面条件满足，则译码器输出第m个消息：

联合序列(C_m,Y)中，n_ij=n*p_i*p_ij

1）$(\mathbf{c}_m, \mathbf{y})$是联合典型序列；

2）没有其他的消息对应的码字$\mathbf{c}_k (k \neq m)$使得$(\mathbf{c}_k, \mathbf{y})$是联合典型的；否则，输出译码错误信息。

在接收端应该知道达到容量的输入概率和信道的转移概率，所以根据接收序列判定符合联合典型的输入码字是可以做到的。

需要计算n_ij：依据p_i和p_ij

n_ij=n*p_i*p_ij*(1+/-δ)

利用图7.5.1的图形可以对有噪信道编码定理的证明做如下解释。

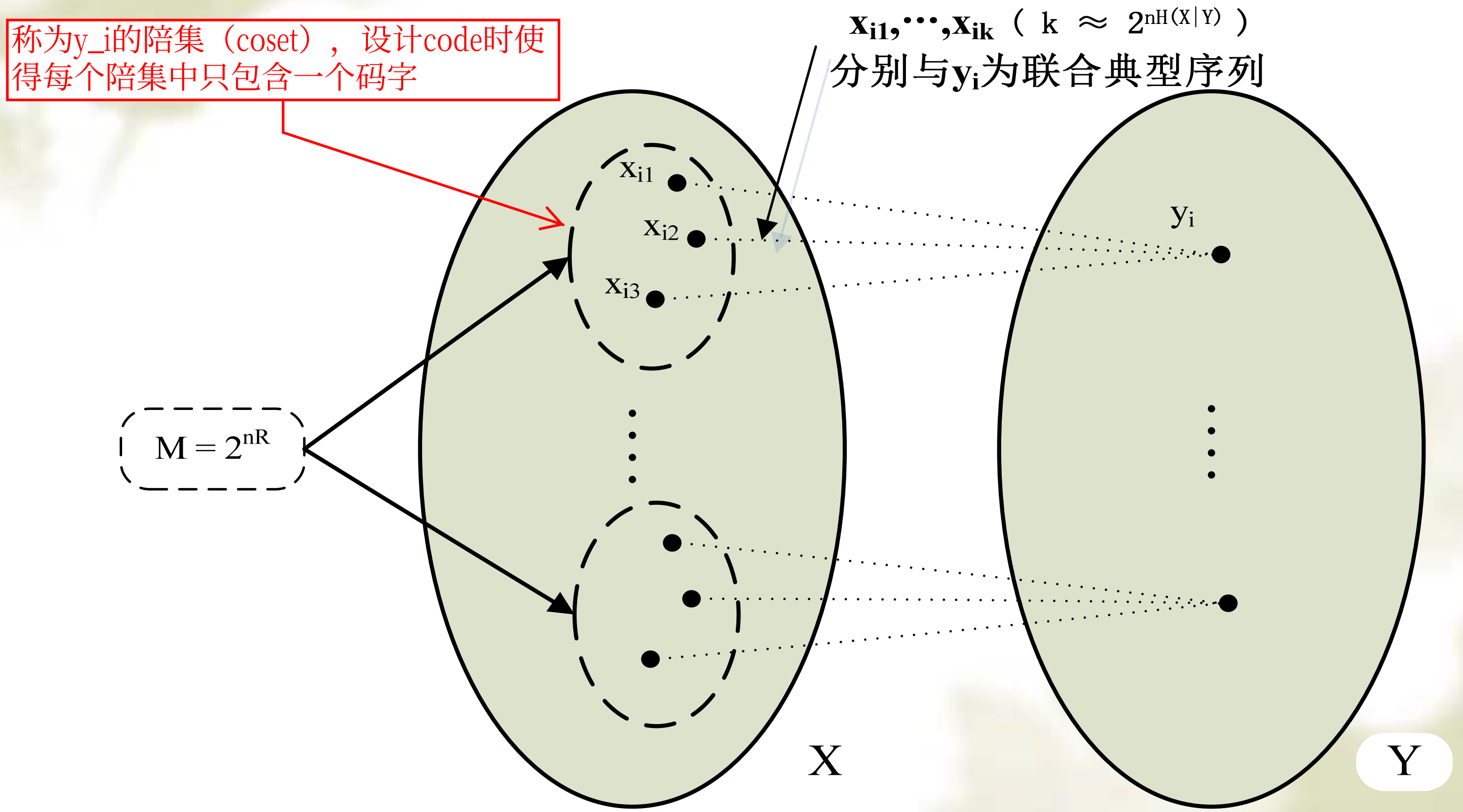


图7.5.1有噪信道编码定理的图形解释

为使典型序列译码不出现差错，我们总希望对于一个输出典型序列 **y**，仅有一个码字和 **y**构成联合典型序列。但实际上有$\left|F_{\mathbf{y}}\right| \approx 2^{nH(X/Y)}$个与 **y** 独立但又与 **y** 构成联合典型序列的输入序列 **x** ，因此就应该让$2^{nH(X/Y)}$个**x**的典型序列中含一个码字。由于**x** 的典型序列的总为$2^{nH(X)}$，因此，如果码字数不超过$2^{n[H(X)-H(X/Y)]}$，就可以作到这一点。

2^nH(X)/2^nH(X|Y)

抽屉原则：
否则可能出现一个抽屉中包含2个码字

如果R < C，那么就有码字数$2^{nR} = M < 2^{n[H(X)-H(X/Y)]}$（此时的平均互信息就是信道容量），从而可使译码差错任意小。

信道容量C

3.译码平均错误率 p_E

由于寻找最佳的即 p_E 最小的编码很困难，所以采用求 $\overline{p_E}$ 的方法，即在所有的随机编码集合中对 p_E 进行平均，$\overline{p_E} = \underset{p(C)}{E}\{p_E(C)\}$ ，p（C）为选择码C的概率。若n足够大且 $\overline{p_E}$ 任意小，那么至少有一种编码满足要求。

7.5.3　无失真信源信道编码定理

如果信源发出的消息通过信道传输，那么实现有效可靠传输的条件由下面的信源信道编码定理来说明。

<u>定理7.5.2</u>（信源信道编码定理）设有一离散无记忆平稳信道的每秒容量为C，一个离散信源每秒的熵为H，那么，如果H < C，总存在一种编码系统，使得信源的输出以任意小的错误概率通过信道传输；反之，如果H > C时，对任何编码系统，译码差错率>0。

注意：信道错误概率和
信道传输速率有关

例7．5．1 有一个二元对称信道，错误率为p=0.02。设该信道以1500二元符号/秒的速率传送消息，现有一条0、1独立等概、长度为14000二元符号消息序列通过信道传输：

（1）信道能否在10秒内将消息序列无差错传输？

（2）实现该消息序列无差错传输的最短时间是多少？

解

（1）二元对称信道容量：C = 1-H2(0.02) = 1-0.1414

=0.8586 比特/信道符号

每秒信道容量：C(bps) = 0.8586x1500 = 1288 bps

信源熵：H(X)=1 比特/信源符号

每秒信源熵率：H(bps) = 14000/10= 1400 bps

因为1400 bps >1288 bps，根据信源信道编码定理，不能无差错传输。

（2）设所需最短时间为T，则

每秒信源熵率： H(bps) =14000/T

根据信源信道编码定理，应有14000/T < 1288 ，得

T = 14000/1288 = 10.87秒

§7.6　纠错码技术简介

本节主要内容：

信道编码通常称作纠错码，可以按多种方式分类。例如：

- 按编码方式可分为分组码和卷积码
- 按纠错或检错能力可分为检错码和纠错码
- 按纠错类型可分为纠随机错误和纠突发错误码
- 按信息位和校验位之间的关系可分为线性码和非线性码
- 按码元的取值还可分为二进制码和多进制码

本节在前面已介绍的分组码基本概念的基础上，进一步介绍线性分组码的编译码方法、实用的几种线性分组码和卷积码的简单知识。

7.6.1 无失真信源信道编码定理

1. 生成矩阵

一个（n，k）线性分组码中的码字可用n维矢量空间的一个n维行矢量v表示，记为$v=(v_{n-1},\cdots,v_0)$，对应的信息分组用一个k维行矢量u表示，记为$u=(u_{k-1},\cdots,u_0)$。

在二进编码中，所有都取值0或1。v、u 之间的关系可用矩阵表示

$$\boxed{v = uG} \qquad (7.6.1)$$

其中，G 为分组码的生成矩阵，阶数为k× n。

将 $\boldsymbol{G}$ 写成

$$\boldsymbol{G}=(\boldsymbol{g}_1^T,\cdots,\boldsymbol{g}_k^T)^T \qquad (7.6.2)$$

其中$g_i(i=1,\cdots,n)$，为k维行矢量，T为转置。

由（7.6.1），有

$$\mathbf{v}=u_{k-1}\boldsymbol{g}_1+\cdots u_0\boldsymbol{g}_k \qquad (7.6.3)$$

可见，码字是生成矩阵各行的线性组合。为保证不同的信息分组对应不同的码字，g_i 应该是线性无关的。

对于码字的前k位是信息位，后n-k位是校验位的系统码，有 $v_{n-i}=u_{k-i}(i=1,\cdots,k)$。

所以通常的系统分组码生成矩阵 $\boldsymbol{G}$ 为如下形式：

$$\boxed{\boldsymbol{G}=(\boldsymbol{I}_k \vdots \boldsymbol{P}_{kr})} \quad （7.6.4）$$

其中，I_k 为k 阶单位矩阵，P_{kr} 为k× r(r=n-k)阶矩阵。

将（7.6.4）代入（7.6.1），得

$$\boxed{\boldsymbol{v}=(\boldsymbol{u} \vdots \boldsymbol{u}\boldsymbol{P}_{kr})} \quad （7.6.5）$$

所以，矩阵 P_{kr} 确定了分组码校验位和信息位的关系。

例7.6.1 设C1为一个（7，4）系统分组码，其生成矩阵为

$$\boldsymbol{G}=\begin{pmatrix}1&0&0&0&1&1&1\\0&1&0&0&1&1&0\\0&0&1&0&1&0&1\\0&0&0&1&0&1&1\end{pmatrix} \qquad (7.6.6)$$

求信息分组0011，1100对应的码字。

解

设信息分组0011，1100对应的码字分别为$\boldsymbol{v}_1,\boldsymbol{v}_2$，那么

$$\boldsymbol{v}_1=(0011)\boldsymbol{G}=(0011110)$$

$$\boldsymbol{v}_2=(1100)\boldsymbol{G}=(1100001)$$

2. 奇偶校验矩阵

例7.6.1（续） 导出该码校验位与信息位的关系。

解

设3个校验位分别为w_2, w_1, w_0， 根据（7.6.5）， 有

$$(w_2\, w_1\, w_0) = (u_3\, u_2\, u_1 u_0)\boldsymbol{P}_{kr} = (u_3\, u_2\, u_1 u_0)\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

所以

$$w_2 = u_3 + u_2 + u_1$$

$$w_1 = u_3 + u_2 + u_0$$

$$w_0 = u_3 + u_1 + u_0$$

在一般情况下，有

$$\left(\boldsymbol{P}_{kr}^{T} \vdots \ \ \boldsymbol{I}_{r}\right)\boldsymbol{v}^{T}=\left(\boldsymbol{P}_{kr}^{T} \vdots \ \ \boldsymbol{I}_{r}\right)(\boldsymbol{u} \vdots \boldsymbol{u}\boldsymbol{P}_{kr})^{T}=\left(\boldsymbol{P}_{kr}^{T}\boldsymbol{u}^{T}+\boldsymbol{P}_{kr}^{T}\boldsymbol{u}^{T}\right)=\boldsymbol{0}^{T} \quad (7.6.7)$$

上面，***0*** 是一个n维行零矢量。

记

$$\boldsymbol{H}=\left(\boldsymbol{P}_{kr}^{T} \vdots \ \ \boldsymbol{I}_{r}\right) \quad (7.6.8)$$

H称为分组码的奇偶校验矩阵，这是一个r×n（n=k+r）阶矩阵。

（7.6.7）意味着，对任何码字都必须满足

（7.6.9）

$$\boldsymbol{H}\boldsymbol{v}^T=\boldsymbol{O}^T$$

因此，（7.6.8）可用来验证某n维矢量是否为码字。

根据（7.6.1）、（7.6.8）又可得

$$\boldsymbol{G}\boldsymbol{H}^T=\boldsymbol{O}_{n,n-k}$$

（7.6.10）

这里，$\boldsymbol{O}_{n,n-k}$表示一个k ×（n-k）阶的全零矩阵。

例7.6.1（续）求分组码的奇偶校验矩阵***H***，并计算 GH^T。

解：根据（7.6.8），得

$$\mathbf{H}=\begin{bmatrix} P_{kr}^{\tau} & I_r \end{bmatrix}=\begin{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}^{\tau} & \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \end{bmatrix}$$

$$=\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$$
\boldsymbol{G}\boldsymbol{H}^T = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}
$$

3. 伴随式

在传输过程中，接收码字**v**可能发生差错，设差错矢量为**e**，则接收矢量为

$$\boldsymbol{r} = \boldsymbol{v} + \boldsymbol{e} \qquad (7.6.11)$$

设

$$e = (e_{n-1}, \cdots, e_0) \qquad (7.6.12)$$

如果$e_i \neq 0$，就表示第i个码元 v_i出错。

令

$$\boldsymbol{s}^T = \boldsymbol{H}\boldsymbol{r}^T \qquad (7.6.13)$$

称**s** 为分组码的伴随式。利用（7.6.10）和（7.6.8），得

$$\boldsymbol{s}^T = \boldsymbol{H}(\boldsymbol{v}+\boldsymbol{e})^T = \boldsymbol{H}\boldsymbol{e}^T \qquad (7.6.14)$$

注：

- 伴随式仅与错误有关，是***H***各列的线性组合；
- 伴随式是r=n-k维行矢量；
- 可以建立伴随式与错误矢量之间的对应关系，这些错误矢量称为可纠错误图样，通常选择重量最小的错误矢量作为可纠错误图样。

4. 分组码译码

根据伴随式可以对分组码译码，译码过程如下：

（1）根据（7.6.13）计算伴随式$\boldsymbol{s}$；

（2）根据伴随式$\boldsymbol{s}$查找对应的可纠错误图样$\boldsymbol{e}$；

（3）计算$\hat{\boldsymbol{v}} = \boldsymbol{r} + \boldsymbol{e}$；　为纠错后的码字。

例7.6.1（续）设接收序列为0111110，对应码字为：0011110，错1位，试利用伴随式译码。

解

计算伴随式：$\boldsymbol{s}^T=\begin{pmatrix}1&1&1&0&1&0&0\\1&1&0&1&0&1&0\\1&0&1&1&0&0&1\end{pmatrix}\begin{pmatrix}0\\1\\1\\1\\1\\1\\0\end{pmatrix}=(110)^T$

根据表7.6.1，得可纠错误图样$\boldsymbol{e}$ =(0100000)，译码结果：

$$\hat{\boldsymbol{v}}=(0111110)\oplus(0100000)=(0011110)$$

下面介绍标准阵列译码方法：

将码字集合C={v}看成n维线性空间Ω 的一个子集，设**s**$\in\Omega$，子集{v+**s**}称作陪集。通过选择不同的**s**，可以构成Ω中2^{n-k}个互不相交的陪集，每个陪集中重量最小的n维矢量称做陪集首。按陪集首的重量由小到大将陪集排序，第1个陪集对应的是码字集合，陪集首是零矢量，构成标准阵列的第1行。

注意：在选取**s**构成陪集时，要选择已经产生的陪集之外的元素，而且陪集首未必就是**s**。把产生的陪集与第1行对齐，陪集首放在每行的左边。这样就形成标准阵列。

可以看到，每一个接收序列都可以在标准阵列中找到位置，并且每个陪集中的每个元素是对应列中的码字和陪集首的和。如果差错图样是某陪集首，那么接收序列就是对应的陪集中的元素。如果接收序列就是某陪集中的元素，那么该矢量与其陪集首相加得到的码字（与接收序列位于同一列的码字）就是译码结果。这就是标准阵列译码原理。

例7.6.2（续）若接收序列为0111，试标准阵列进行译码。

解　接收序列为0111在陪集4，第3列，对应码子字为0101。

5. 分组码的译码错误率计算

从上面的分析可知，如果可纠错图样就是实际发生的错误，那么译码正确，否则译码错误。

所以译码错误率为

$$p_E = 1 - \text{可纠错图样的概率}$$

设i为重量i的错误图样的个数，那么

$$\boxed{p_E = 1 - \sum_{i=0}^{n} \alpha_i p^i (1-p)^{n-i}} \qquad （7.6.15）$$

其中，p为信道传输单符号错误率。

例7.6.2（续）设消息通过一个错误率为10^{-2}的二元对称信道传输，计算译码错误率并与未编码系统比较。

解

陪集首就是可纠错图样，译码错误率为：

$$p_E = 1-[(1-p)^4+3p^3(1-p)]\Big|_{p=10^{-2}} = 0.0103$$

对于未编码系统，4个消息可用00，01，10，11传送，传输错误率为：

$$p_E = 1-(1-p)^2\Big|_{p=10^{-2}} = 0.0199$$

可见，编码系统比未编码系统的传输错误率低。§7.6

7.6.2　几种重要的分组码

1．汉明码

这是一个纠单错的码，分组长度 $n=2^m-1$，信息位数 $k=n-m$，校验位数 $r=m, m\geq 3$，码的最小距离 d_{min}=3，码率为$R=(n-m)/n=1-m/(2^m-1)$。汉明码可以是循环码。

2．BCH码

这是一类纠多重错误的码，分组长度 $n=2^m-1, m\geq 3$，校验位数$n-k\leq mt$，码的最小距离 $d_{\min}\geq 2t+1$。BCH码是一种纠错能力很强的码，在码的参数选择上有较大的灵活性，可以选择码长、码率以及纠错能力等。

3.里德-所罗门码

简称RS码，是BCH码的一个子类，是非二进制码。该码的参数：每符号m比特，分组长度 $n=2^m-1$ 符号，信息符号数 $k=n-2t$，码的最小距离 $d_{\min}\geq 2t+1$。RS码非常适合纠突发错误，并经常在级联码中用做外码。

§7.6

7.6.3卷积码概要

一、卷积码的引入

（1）分组码的编/译码，前后各组是无关的

编码时，码组的检验位只决定于本组信息位

译码时，从一个长为 n 码组中还原本组信息位

（2）分组码要增加纠错能力—》增加检验位—》使编/译码设备复杂

（3）如既要求 n,r 较小，又要求纠错能力较强，考虑使用卷积码

卷积码 – 码组中的监督码元不仅取决于本组的信息码元，也取决于前 m 组的信息码元

记为 (n,k,m)

基本术语

在 (n,k,m) 码中，m 称为编码记忆

称 $K=m+1$ 为编码约束度，说明编码过程中互相有约束的码段个数

称 $N_c=K\bullet n$ 为编码约束长度，说明编码过程中相互约束的码元个数

对于译码过程：

根据当前输入码组，及以后 $L+m$ 段 $(L\geq 1)$ 所接收的码组，译出一个码组的信息码元，称 $L+m$ 译码约束度

<u>通信链路的卷积编码/译码和调制/解调结构</u>

—输入信息源 $\mathbf{m}=m_1,m_2,\cdots,m_i,\cdots$，$m_i$为数字比特，且独立/等概；

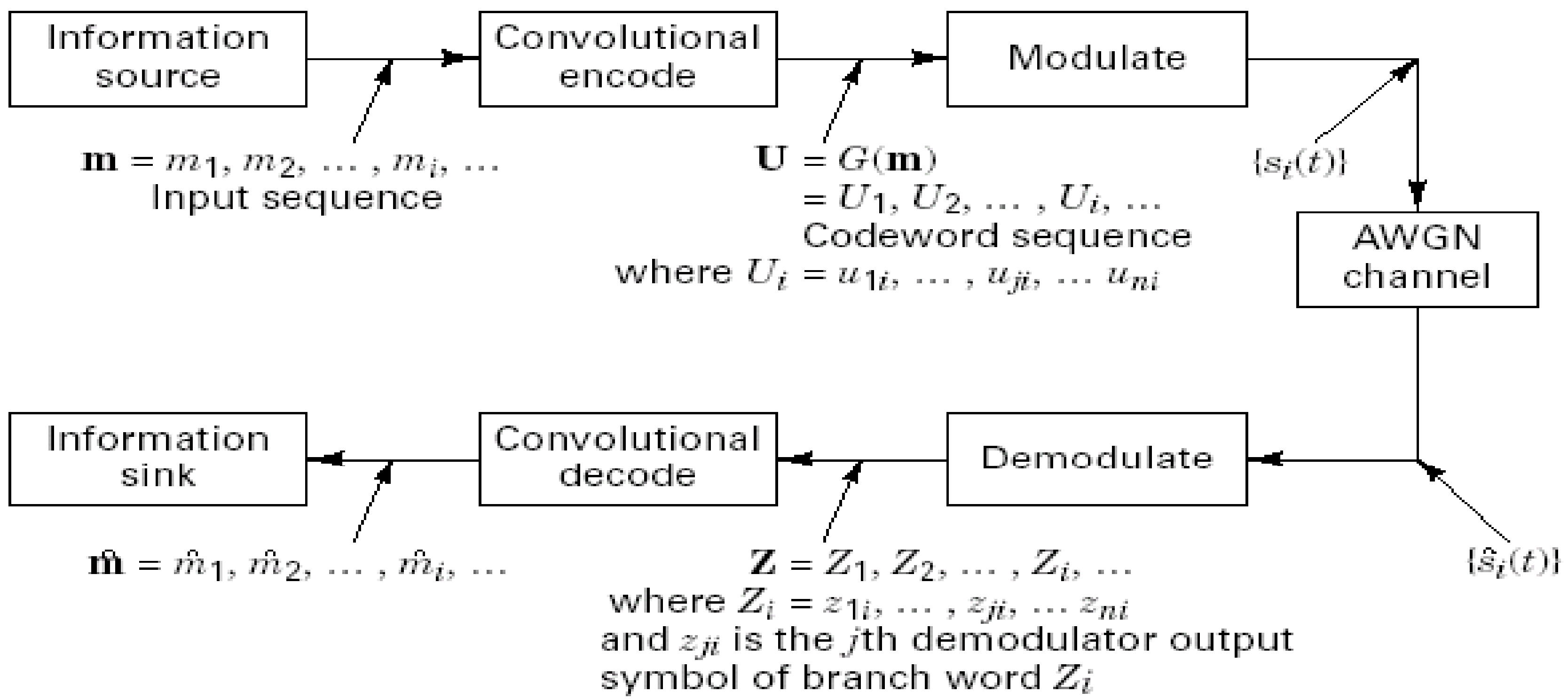
—卷积码编码器将输入 $\mathbf{m}$ 转换成唯一的码字序列$\mathbf{U}=G(\mathbf{m})$，

序列$\mathbf{U}=U_1,U_2,\cdots U_i,\cdots$，其中$U_i$为分支码字；

—码字序列$\mathbf{U}$对波形$s(t)$进行调制—》干扰—》$\hat{s}(t)$

—对$\hat{s}(t)$解调得解调序列$\mathbf{Z}=Z_1,Z_2,\cdots,Z_i,\cdots$

—译码器根据接收序列 $\mathbf{Z}$ 及编码过程先验知识，生成对原信息序列的估计$\hat{\mathbf{m}}=\hat{m}_1,\hat{m}_2,\cdots,\hat{m}_i,\cdots$



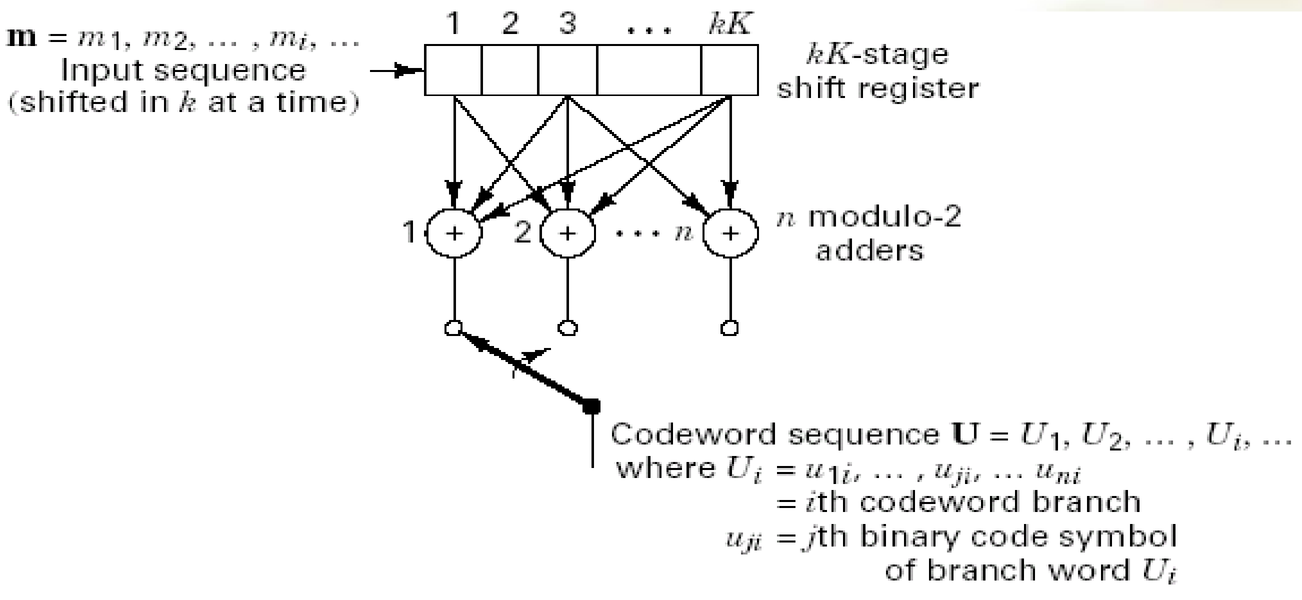
通信链路的编码/译码和调制/解调分析

典型卷积码编码器结构

—包含K个k位移位寄存器和 n个模 2 加法器；

—每个时间单元，输入k个信息比特，寄存器中其他比特向右移 k 位；

—顺序采样n个加法器输出得到 n元编码比特，效率k/n



二、一个简单的卷积码

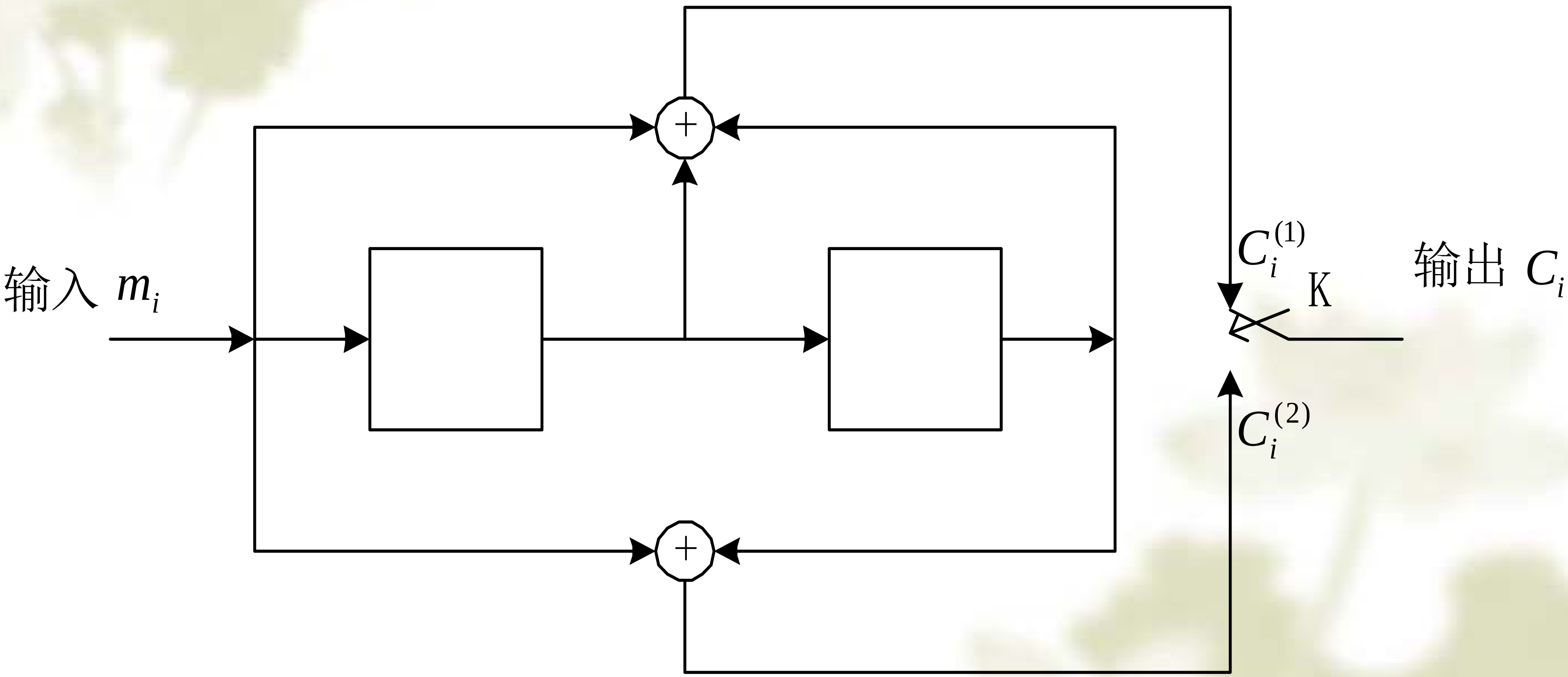
考虑一个（2，1，2）卷积码编码器，包括二级移位寄存器和 2 个模 2 加法器，输出码组包含 2 个输出码元$C_i^{(1)}, C_i^{(2)}$

假定寄存器初始状态为 0，输出码组和输入信息码元关系：

$$C_i^{(1)} = m_{i-2} + m_{i-1} + m_i$$

$$C_i^{(2)} = m_{i-2} + m_i$$

如输入信息序列为 $m = (m_0, m_1, \cdots) = (1,1,1,\cdots)$ 时，有输出序列： $C = (11,01,10,\cdots) = (C_0, C_1, C_2, \cdots)$



（2，1，2）卷积码编码器

§7.7 信道编码性能界限

本节主要内容：

这里主要介绍编码距离界，包括汉明球包（Hamming Sphere Packig）界、瓦尔沙夫一吉尔伯特（Varshar mov-Gilbert）界以及普罗特金（Plotkin ）界。

Hamming界给出了当可纠错数给定后，最大码字数的上界；Varsharmov-Gilbert界提供了一个最好码的最大码字数的下界；而Plotkin界表明了在给定码长和码率条件下最大可能的最小码距离。

7.7.1 汉明球包界

当分组码的码长n和可纠错数t给定后，就限定了可用的最大码字数M，汉明界给出了M的上界。

定理7.7.1 设一个q进制纠t个错误，长度为n的纠错码，码字数为M，那么

$$\boxed{M[1+C_n^1(q-1)+\cdots+C_n^t(q-1)^t]\leq q^n} \quad (7.7.1)$$

证

给定一个码字**u**，定义一个以为中心的**n**维球：

$$S_t(u)=\{v\in V\mid d(u,v)\le t\}$$

此球中包含与的距离小于或等于**t**的所有矢量，球内所含矢量的总数为：

$$\left|S_t(\boldsymbol{u})\right|=1+C_n^1(q-1)+\cdots+C_n^t(q-1)^t$$

因为编码能纠**t**个错，所以这**M**个码字所构成的球是不相交的，而**M**个球所包含的全部矢量不会超过，从而得到（**7.7.1**）式。

如果一个纠错码满足（**7.7.1**）式中的等号，则称

码是完备的，否则就称不完备的。

例7. 7. 1 一个二元（n， k）分组码，能纠一个错误，求码字最大数目M的上界。

解

根据（7.7.1），有 $M(n+1)\le 2^n$，所以

$$\boxed{M \le 2^n/(1+n)} \qquad （7.7.2）$$

例7.7. 2 验证汉明码是否完备。

解

汉明码能纠一个错误，将参数 $M=2^{n-m}$，$n=2^m-1$ 代入式（7.7.2），等号成立。

所以汉明码是完备码。

对于一个二元(n,k)分组码，（7.7.1）式变为

$$\boxed{n-k \ge \log_2(1+C_n^1+\cdots+C_n^t)} \qquad (7.7.3)$$

（7.7.3）规定了能纠 t 个错误的二元（n，k）码的校验位数目的最低限。

令k=nR，由（7.7.3），得

$$\boxed{1-R \ge \frac{1}{n}\log_2(1+C_n^1+\cdots+C_n^t) \ge \frac{1}{n}\log_2 C_n^t} \qquad (7.7.4)$$

应用斯特灵公式：$n! \approx (n/e)^n\sqrt{2\pi n}$，当$n \to \infty$，并保持t/n为常数，得

$$\boxed{1-R \ge H_2(t/n)} \qquad (7.7.5)$$

其中,$H_2(t/n)$为一个符号的概率等于 t/n的二元信源的熵（以 2 为底）。

因为$2t+1=d \le n$，所以$t/n \le 1/2$。

根据（7.7.5）可以在直角坐标系的第一象限画出R与t/n所在的范围，这是曲线$R = 1 - H_2(t/n)$与坐标轴围成的区域，如图7.7.1所示。

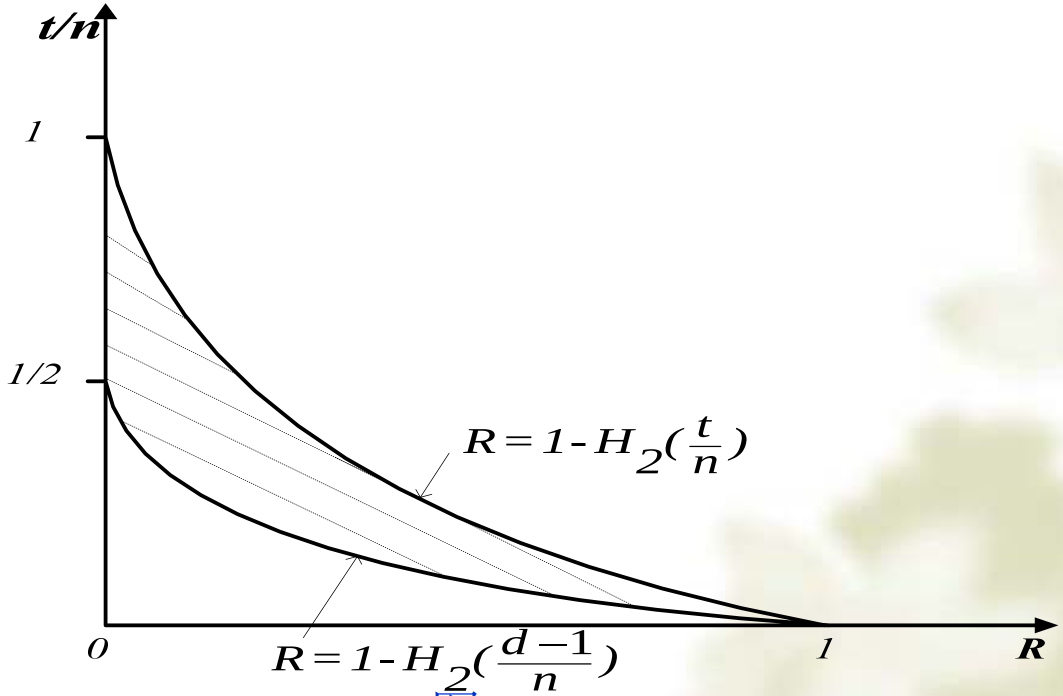


图7.7.1

例7．7．3　如果要求分组码可纠错误数始终为码长为1/2，那么当码长足够长时，码率接近多少？

解

根据（7.7.5），

$$H_2(1/2)=1$$

所以此时R趋于零。

7.7.2 Varsharmov-Gilbert界

定理7.7.2 设一个q进制、最小距离为d、长度为n的纠错码，码字数的最大值为$A_q(n,d)$，那么

$$\boxed{A_q(n,d)[1+C_n^1(q-1)+\cdots+C_n^{d-1}(q-1)^{d-1}]\geq q^n} \tag{7.7.6}$$

证

设C是所有q进制、最小距离为d、长度为n的纠错码中码字数最大的编码，即M=|C| = $A_q(n,d)$，设V是q进制、长度为n的序列的集合，那么n维球 $S_{d-1}=\{v\in V\,|\,d(u,v)\le d-1\}(u\in C)$ 表示以每个码字为中心，半径d-1的球，所包含的序列数是：$\sum_{i=0}^{d-1}C_n^i(q-1)^i$。M个码字的这种n维球一定覆盖V。因为，如果存在 $v\in V$ 不在这M个n维球中，必有 $d(u,v)\ge d$，对所有 $u\in C$；这样 $C\bigcup\{v\}$可以构成新的编码，而且q、d、n不变，但码字比C增多，与原假设矛盾。所以这M个n维球一定包含所有的q^n矢量,从而得（7.7. 6 ）。

注：在长度n和最小距离d给定的分组码中，码字数最大的码称为最优码，其码字数用$A_q(n,d)$表示。

例7．7．4　一个二元(n,k)分组码，最小码距离为3，求码字最大数目$A_2(n,3)$的下界。

解

根据（7．7．6），有$A_2(n,3)[1+n+n(n-1)/2]\ge 2^n$，

所以

$$A_2(n,3)\ge 2^{n+1}/(n^2+n+2) \tag{7.7.7}$$

对于二元(n,k)分组码，当d ≤ n/2时，根据（7．7．6）用类似于（7．7．5）式的推导，可得

$$R\ge 1-H_2[(d-1)/n] \tag{7.7.8}$$

与（7.7.5）式对照，曲线$R=1-H_2(t/n)$和曲线$R=1-H_2((d-1)/n)$所围成的区域是最优的R、n、d（或t）所在的区域，如图7.7.1中的阴影部分所示。 §7.7

7.7.3　Plotkin界

定理7.7.3（Plotkin 界）当码长n和码字数*M*给定后，最小码距离d的上界为：

$$d \le nM/[2(M-1)] \qquad (7.7.9)$$

证

现对二进制编码进行证明。

将编码C所有码字排成 $M \times n$ 阶矩阵，其中每行代表一个码字。

$$\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ x_{M1} & x_{M2} & \cdots & x_{Mn} \end{pmatrix}$$

设 $s=\sum_{\mathbf{u}\in C}\sum_{\mathbf{v}\in C} d(\mathbf{u},\mathbf{v})$。码的最小距离为d，所以 $s \geq M(M-1)d$。

现按上面矩阵中的每列计算s。设第j列的元素有 a_i 个“0”，$M-a_i$ 个“1”。先固定某一个元素，相当于固定一个码字，如果此元素是“0”，那么其他码字对s的贡献累加就是 $M-a_i$；因为有 a_i 个码字，所以对s的总贡献就是 $a_i(M-a_i)$。如果此元素是“1”，那么其他码字对s的贡献累加就是 a_i；因为有 $M-a_i$ 个码字，所以对s的总贡献就 $a_i(M-a_i)$。

综合起来有，按矩阵中的每列计算对s的总贡献是，$2a_i(M-a_i)$，所以

$$M(M-1)d \le \sum_{i=1}^{n} 2(M-a_i)a_i$$

求$2a_i(M-a_i)$的极大值，有

$$2(M-a_i)a_i \le \begin{cases} M^2/2 & M\text{为偶} \\ (M^2-1)/2 & M\text{为奇} \end{cases}$$

所以

$$d \le \begin{cases} nM/[2(M-1)] & M\text{为偶} \\ n(M+1)/(2M) & M\text{为奇} \end{cases} \qquad （7.7.10）$$

因为(M+1)/M小于 M/(M-1)，所以（7.7.10）式可以写成（7.7.9）。

对于二元（n,k）码，（7.7.9）变为：$d \le n2^{k-1}/(2^k-1)$

本章小结

1. 最佳译码原则

MAP准则：$g(y)=\arg\max\limits_{x} p(x\,|\,y)$　（使平均错误率最小）

ML准则：$g(y)=\arg\max\limits_{x} p(y\,|\,x)$　（用于输入等概率或概率未知）

最小汉明距离准则：$g(y)=\arg\max\limits_{x} d(x,y)$（用于二元对称信道）

2. 最小码距离 d_{min}

$$d_{min} = 2t+1$$ 能纠t个错误

3. 费诺不等式

$$H(X/Y) \le H(P_E) + P_E \log(r-1)$$

4. 有噪信道编码定理

$R \le C \Leftrightarrow$ 存在使传输差错任意小的信道编码

其中，R为码率，C为信道容量。

5．无失真信源信道编码定理

$H \le C \Leftrightarrow$ 存在使传输差错任意小的信源信道编码

其中，H为单位时间信源的熵，C为单位时间信道容量。

6． 线性分组码

生成矩阵

校验矩阵

7． 线性分组码性能界

汉明球包界

Varsharmov-Gilbert界

Plotkin界

课后习题

P.153 思考题

7.1, 7.4, 7.6, 7.10,

P.154

7.3, 7.4,