习题（第 1 章）

1. 一位朋友很不赞成“通信的目的是传送信息”及“消息中未知的成分才算是信息”这些说法。他举例说：我多遍地欣赏梅兰芳大师的同一段表演，百看不厌，大师正在唱的正在表演的使我愉快，将要唱的和表演的我都知道，照你们的说法电视里没给我任何信息，怎么能让我接受呢？请从信息论的角度对此做出解释。（主要从狭义信息论与广义信息论研究的内容去理解和解释）

答： 从狭义信息论角度说，虽然将要表演的内容观众已知，但每一次演出不可能完全相同。而观众在欣赏的同时也在接受着新的感观和视听享受。从这一角度来说观众还是可以得到新的信息的。另一种解释可以从广义信息论角度来说，它涉及了信息的社会性，实用性等主观因素，同时受知识水平、文化素质的影响。京剧朋友们在欣赏京剧时也因为主观因素而获得了享受，因此属于广义信息论范畴。

2．利用图 1.2 所示的通信系统分别传送同样时间（例如十分钟）的重大新闻公告和轻音乐，它们在接收端各方框的输入中所含的信息是否相同，为什么？

答： 重大新闻是语言，频率为 300-3400Hz,而轻音乐的频率为 20-20000Hz。同样的时间内轻音乐的采样编码的数据要比语音的数据量大，按码元熵值，音乐的信息量要比新闻大。但在信宿端，按信息的不确定量度信息量就应分别对待，对于新闻与音乐的信息量大小在广义来说因人而异。

习题（第 2 章）

1．一珍珠养殖场收获 240 颗外观及重量完全相同的特大珍珠，但不幸被人用外观相同但重量仅有微小差异的假珠换掉 1 颗。（1）一人随手取出 3 颗，经测量恰好找出了假珠，问这一事件大约给出了多少比特的信息量；（2）不巧假珠又滑落进去，那人找了许久却未找到，但另一人说他用天平最多 6 次能找出，结果确是如此，问后一事件给出多少信息量；（3）对上述结果作出解释。

解：（1）从 240 颗珠子中取 3 颗，含 1 颗假珠的概率为

$$P=\frac{C_{239}^{2}}{C_{240}^{3}}=1/80$$

$$I=-\log_2 P=\log_2 80=6.32\,(bit)$$

（2）240 颗中含 1 颗假珠，用天平等分法最多 6 次即可找到假珠，是必然事件，因此信息量为 0。

（3）按照 shannon 对信息量的定义，只有事件含有不确知成分，才有信息量，且不确知成分越大，信息量越大，必然事件则没有信息量。但从广义信息论来说，如果那人不知用天平二分法找假珠，另一人告之此事，使他由不知到知，也应该含有一定的信息量。

2．每帧电视图像可以认为是由 3×10^5 个象素组成，所有象素均独立变化，且每一象素又取 128 个不同的亮度电平，并设亮度电平等概率出现。问每帧图像含有多少信息量？如果一个广播员在约 10000 个汉字的字汇中选取 1000 个字来口述此电视图像，试问广播员描述此图像所广播的信息量是多少（假设汉字字汇是等概率分布，且彼此独立）？若要恰当地描述此图像，广播员在口述中至少需用多少汉字？

解：设电视图像每个像素取 128 个不同的亮度电平，并设电平等概率出现，则每个像素亮度含有的信息量为

$$\mathrm{H}(X)=lb128=7 \text{ 比特/像素}$$

一帧中像素均是独立变化的，则每帧图像信源就是离散亮度信源的无记忆 N 次扩展信源。得每帧会图像含有的信息量为

$$H(X^N)=NH(X)=2.1\times10^6 \quad \text{比特/每帧}$$

广播口述时，广播员是从 10000 个汉字字汇中选取的，假设汉字字汇是等概率分布的，则汉字字汇中每个汉字含有的信息量

$$H(Y) = lb10000 = 13.29 \text{ 比特/字}$$

广播员口述电视图像是从此汉字字汇信源中独立地选取 1000 个字来描述的。所以，广播员描述此帧图像所广播的信息量为

$$H(Y^N) = NH(Y) = 1000lb10^4 = 1.329 \times 10^4 \text{ 比特/千字}$$

若广播员仍从此汉字字汇信源 Y 中独立地选取汉字来描述电视图像，每次口述一个汉字含有信息量是 H(Y)，每帧电视图像含有的信息量是 $H(X^N)$，则广播员口述此图像至少需要的汉字数等于

$$\frac{H(X^N)}{H(Y)} = \frac{2.1 \times 10^6}{13.29} = 1.58 \times 10^5 = 158000 \text{ 字}$$

3．已知　　**X**：　1，0

　　　　$P(\mathbf{X})$：　p，　$1-p$

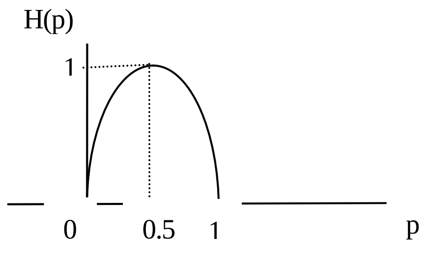
(1) 求证：$H(\mathbf{X}) = H(p)$

(2) 求 $H(p)$并作其曲线，解释其含义。

（1）证明

$$H(X) = pI(1) + (1-p)I(0)$$
$$= -plbp - (1-p)lb(1-p) = H(p)$$

（2）



该 H(p)曲线说明，当 0 与 1 等概出现时，即 p=0.5 时，熵最大。当 p 由 0.5 分别趋向于 0 和 1 时，熵逐渐减小至 0。

4．证明$H(\mathbf{X}_3|\mathbf{X}_1\mathbf{X}_2) \le H(\mathbf{X}_2|\mathbf{X}_1)$，并说明等式成立的条件。

证明：设离散平稳信源输出的随机符号序列为…X1,X2,X3,…。又设

$x_1 \in X_1$ ，$x_2 \in X_2$ ，$x_3 \in X_3$ ，而且 x_1, x_2, x_3 都取自于同一符号集 $A = \{a_1, a_2, \cdots, a_g\}$，并满足有

$$\sum_{X_2} P(x_2 | x_1) = 1, \sum_{X_3} P(x_3 | x_2) = 1, \sum_{X_3} P(x_3 | x_1 x_2) = 1,$$

$$\sum_{X_1} P(x_1) = \sum_{X_2} P(x_2) = \sum_{X_3} P(x_3) = 1$$

$$\sum_{X_1} \sum_{X_2} P(x_1 x_2) = \sum_{X_2} \sum_{X_3} P(x_2 x_3) = \sum_{X_1} \sum_{X_3} P(x_1 x_3) = 1$$

$$\sum_{X_1} \sum_{X_2} \sum_{X_3} P(x_1 x_2 x_3) = 1$$

$$\sum_{X_1} P(x_1 x_2 x_3) = P(x_2 x_3)$$

$$\sum_{X_2} P(x_1 x_2 x_3) = P(x_1 x_3)$$

$$\sum_{X_3} P(x_1 x_2 x_3) = P(x_1 x_2)$$

在区域[0，1]内设 f(x)=－xlogx, f(x)在[0，1]内是$\bigcap$型凸函数，所以满足詹森不等式

$$\sum_{i=1}^{q} P_i f(x_i) \le f(\sum_{i=1}^{q} P_i x_i) \quad 其中 \sum_{\mathrm{i}=1}^{q} P_i = 1$$

现今 $x_i = P(x_3 | x_2 x_1)$,设其概率空间为 $P(x_1 | x_2)$，并满足

$$\sum_{X_1} P(x_1 | x_2) = 1$$

所以根据詹森不等式得

$$\sum_{X_1} P(x_1 | x_2)[-x_i \log x_i] \le -[\sum_{X_1} P(x_1 | x_2) x_i] \log[\sum_{X_1} P(x_1 | x_2) x_i]$$

$$-\sum_{X_1} P(x_1 | x_2) P(x_3 | x_1 x_2) \log P(x_3 | x_1 x_2)$$

$$\le -\sum_{X_1} P(x_1 | x_2) P(x_3 | x_1 x_2) \log \sum_{X_1} P(x_1 | x_2) P(x_3 | x_1 x_2)$$

所以

$$\sum_{X_1} P(x_1x_2x_3) = P(x_2x_3)$$

$$\sum_{X_1} P(x_1x_3 \mid x_2)P(x_2) = P(x_3 \mid x_2)P(x_2)$$

上式对所有 x_1, x_2, x_3 的取值都成立，所以

$$\sum_{X_1} P(x_1x_3 \mid x_2) = P(x_3 \mid x_2)$$

$$\sum_{X_1} P(x_1 \mid x_2)P(x_3 \mid x_1x_2) = P(x_3 \mid x_2)$$

所以 $-\sum_{X_1} P(x_1x_3 \mid x_2)\log P(x_3 \mid x_1x_2) \le -P(x_3 \mid x_2)\log P(x_3 \mid x_2)$

因为 $0 \le P(x_2) \le 1, x_2 \in X_2$，所以上式两边相乘，等号不变。有

$$-\sum_{X_1} P(x_2)P(x_1x_3 \mid x_2)\log P(x_3 \mid x_1x_2) \le -P(x_2)P(x_3 \mid x_2)\log P(x_3 \mid x_2)$$

上式对所有 x_2, x_3 都成立，所以对所有 x_2, x_3 求和下式也成立

$$-\sum_{X_1}\sum_{X_2}\sum_{X_3} P(x_1x_2x_3)\log P(x_3 \mid x_1x_2) \le -\sum_{X_2}\sum_{X_3} P(x_2x_3)\log P(x_3 \mid x_2)$$

因为 $H(\mathbf{X}_3|\mathbf{X}_1\mathbf{X}_2) \le H(\mathbf{X}_3|\mathbf{X}_2)$

所以是平稳信源 $H(\mathbf{X}_3|\mathbf{X}_2) = H(\mathbf{X}_2|\mathbf{X}_1)$

得 $H(\mathbf{X}_3|\mathbf{X}_1\mathbf{X}_2) \le H(\mathbf{X}_2|\mathbf{X}_1)$

只有当 $P(x_3 \mid x_1x_2) = P(x_3 \mid x_2)$ (对所有 x_1, x_2, x_3)时等式成立。

5．设有一概率空间，其概率分布为$\{p_1, p_2, \ldots, p_q\}$，且$p_1>p_2$。若取 $p_1^{'} = p_1 - \varepsilon$，$p_2^{'} = p_2 + \varepsilon$，其中 $0 < 2\varepsilon \le p_1 - p_2$，而其它概率值不变。证明由此得到的新的概率空间的熵是增加的，并用熵的物理意义加以解释。

证明：令 $a = \dfrac{\varepsilon}{p_1 - p_2} > 0$的小数$1 - a = \dfrac{p_1 - p_2 - \varepsilon}{p_1 - p_2}$

得

$$ap_1+(1-a)p_2=\frac{\varepsilon}{p_1-p_2}p_1+\frac{p_1-p_2-\varepsilon}{p_1-p_2}p_2=p_2+\varepsilon$$

$$(1-a)p_1+ap_2=\frac{p_1-p_2-\varepsilon}{p_1-p_2}p_1+\frac{\varepsilon}{p_1-p_2}p_2=p_1-\varepsilon$$

因为 f(x)=－xlogx 是⋂型函数，根据⋂型凸函数的定义有

$$f[ap_1+(1-a)p_2]\geq af(p_1)+(1-a)f(p_2)$$

所以 $f(p_2+\varepsilon)\geq af(p_1)+(1-a)f(p_2)$

即 $-(p_2+\varepsilon)\log(p_2+\varepsilon)\geq -[\frac{\varepsilon}{p_1-p_2}p_1\log p_1+\frac{p_1-p_2-\varepsilon}{p_1-p_2}p_2\log p_2]$

同理得

$$-(p_1-\varepsilon)\log(p_1-\varepsilon)\geq -[\frac{p_1-p_2-\varepsilon}{p_1-p_2}p_1\log p_1+\frac{\varepsilon}{p_1-p_2}p_2\log p_2]$$

以上两不等式两边相加，不等号不变。

所以得

$$-(p_1-\varepsilon)\log(p_1-\varepsilon)-(p_2+\varepsilon)\log(p_2+\varepsilon)\geq -p_1\log p_1-p_2\log p_2$$

6. 某办公室和其上级机关的自动传真机均兼有电话功能。根据多年来对双方相互通信次数的统计，该办公室给上级机关发传真和打电话占的比例约为 3:7，但发传真时约有 5%的次数对方按电话接续而振铃，拨电话时约有 1%的次数对方按传真接续而不振铃。求:（1）上级机关值班员听到电话振铃而对此次通信的疑义度;（2）接续信道的噪声熵。

解: 设发传真和打电话分别为事件 X1 与 X2,对方按传真和按电话接续分别为事件 Y1 和 Y2,则

P(X1)=30%,P(X2)=70%

P(Y1|X1)=95%, P(Y2|X1)=5%,

P(Y1|X2)=1%,　　P(Y2|X2)=99%

P(X1Y1)=0.285, P(X1Y2)=0.015

P(X2Y1)=0.007, P(X2Y2)=0.693

P(Y1)= P(X1Y1)+ P(X2Y1)= 0.292

P(Y2)=1－ P(Y1)= 0.708

H(X)=－ P(X1)lb P(X1) － P(X2)lb P(X2)

=0.8814 bit/符号

H(Y)=－ P(Y1)lb P(Y1) － P(Y2)lb P(Y2)

=0.8713 bit/符号

H(XY)= $-\sum_{i=1}^{2}\sum_{j=1}^{2} P(XiYj)lbP(XiYj)$ =1.0239 bit/两个信符

I(X;Y)=H(X)+H(Y) － H(XY)=0.7288 bit/信符

（1）听到电话振铃的疑义度

H(X|Y2)=－ P(X1Y2)lb P(X1Y2)－ P(X2Y2)lb P(X2Y2)= 0.4575 bit/信符

（2）接续信道的噪声熵

H(Y|X)=H(Y)－I(X;Y)=0.1425 bit/信符

7．四个等概分布的消息M_1，M_2，M_3，M_4被送入如图所示的信道进行传输，通过编码使$M_1 = 00$，$M_2 = 01$，$M_3 =10$，$M_4 =11$。求输入是M_1和输出符号是 0 的互信息量是多少？如果知道第 2 个符号也是 0，这时带来多少附加信息量？

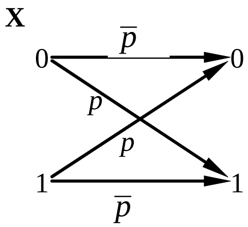


图 2.6

解：信源P(M_1)= P(M_2)= P(M_3)= P(M_4)=1/4, 信道为二元对称无记忆信道，消息Mi与码字一一对应，所以设 $M_i = (x_{i_1} x_{i_2})$ 设接收序列为Y=(y_1y_2)

接收到第一个数字为 0，即y_1=0。那么，接收到第一个数字 0 与M_1之间的互信息为

$$I(M_1; y_1 = 0) = \log \frac{P(y_1 = 0 \mid M_1)}{P(y_1 = 0)}$$

因为信道为无记忆信道，所以

$$P(y_1 = 0 \mid M_1) = P(y_1 = 0 \mid x_{1_1} x_{1_2} = 00)$$
$$= P(y_1 = 0 \mid x_{1_1} = 0) = P(0 \mid 0) = \overline{p}$$

同理，得 $I(y_1 = 0 \mid M_i) = P(y_1 = 0 \mid x_{i_1} x_{i_2}) = P(y_1 = 0 \mid x_{i_1})$

输出第一个符号是y_1=0 时，

有可能是四个消息中任意一个第一个数字传送来的。

所以

$$P(y_1=0)=\sum_{i=1}^{4}P(M_i)(y_1=0|M_i)$$
$$=\frac{1}{4}[P(y_1=0|x_{1_1}=0)+P(y_1=0|x_{2_1}=0)+P(y_1=0|x_{3_1}=1)+P(y_1=0|x_{4_1}=1)]$$
$$=\frac{1}{2}$$

故得 $I(M_1;y_1=0)=1+lb\overline{p}$ 比特

接收到第二个数字也是 0 时，得到关于M_1的附加互信息为

$$I(M_1;y_2=0|y_1=0)=I(M_1;y_1y_2=00)-I(M_1;y_1=0)$$

其中 $I(M_1;y_1y_2=00)=\log\frac{P(y_1y_2=00|M_1)}{P(y_1y_2=00)}$

同理，因为信道是无记忆信道，
所以

$$P(y_1y_2=00|M_i)=P(y_1y_2=00|x_{i_1}x_{i_2})$$
$$=P(y_1=0|x_{i_1})P(y_2=0|x_{i_2})$$

得
$$P(y_1y_2=00|M_1)=P(y_1=0|x_{1_1}=0)P(y_2=0|x_{1_2}=0)$$
$$=P(0|0)P(0|0)=\overline{p}^2$$

输出端出现第一个符号和第二个符号都为 0 的概率为

$$P(y_1y_2=00)=\sum_{i=1}^{4}P(M_i)(y_1y_2=00|M_i)$$
$$=\frac{1}{4}[P(y_1=0|x_{1_1}=0)P(y_2=0|x_{1_2}=0)+P(y_1=0|x_{2_1}=0)P(y_2=0|x_{2_1}=1)$$
$$+P(y_1=0|x_{3_1}=1)P(y_2=0|x_{3_1}=0)+P(y_1=0|x_{4_1}=1)P(y_2=0|x_{4_1}=1)]$$
$$=\frac{1}{4}$$

所以 $I(M_1;y_1y_2=00)=\log\frac{\overline{p}^2}{1/4}=2(1+lb\overline{p})$ 比特

得附加互信息为 $I(M_1; y_2 = 0 \mid y_1 = 0) = 1 + lb\overline{p}$ 比特

8．证明若随机变量 X，Y，Z 构成马氏链，即 $X \to Y \to Z$，则有 $Z \to Y \to X$。

证明：因为(X,Y, Z)是马氏链，有 P(z|xy)=P(z|y),对所有 $x \in X, y \in Y, z \in Z$ 成立，而

P(x|yz)=P(xyz)/P(yz)

= P(z|xy) P(xy)/ P(y) P(z|y)

= P(z|xy) P(y) P(x|y)/ P(y) P(z|y)

对所有 $x \in X, y \in Y, z \in Z$ 成立

故得 P(x|yz)=P(x|y) 对所有 $x \in X, y \in Y, z \in Z$ 成立

所以(Z,Y, X)也是马氏链。

习题（第 3 章）

1．发出二重符号序列消息的信源熵为$H(\mathbf{X}^2)$，而一阶马尔可夫信源的信源熵为$H(\mathbf{X}/\mathbf{X})$。试比较这两者的大小，并说明原因。

2． 设随机变量序列(**XYZ**)是马氏链，且**X**：$\{a_1, a_2, \ldots, a_r\}$，**Y**：$\{ b_1, b_2, \ldots, b_s\}$，**Z**：$\{ c_1, c_2, \ldots, c_L\}$。又设**X**与**Y**之间的转移概率为$p(b_j/a_i)$ ($i=1, 2, \ldots, r$；$j=1, 2, \ldots, s$)；**Y**与**Z**之间的转移概率为$p(c_k/b_j)$ ($j=1, 2, \ldots, s$；$k=1, 2, \ldots, L$)。试证明**X**与**Y**之间的转移概率为

$$p(c_k / a_i) = \sum_{j=1}^{s} p(b_j / a_i) p(c_k / b_j)$$

3． 有一个马尔可夫信源，已知$p(x_1|x_1)=\frac{2}{3}$，$p(x_2|x_1)=\frac{1}{3}$，$p(x_1|x_2)=1$，$p(x_2|x_2)=0$，试画出该信源的香农线图，并求出信源熵。

一步转移矩阵为 P，$P = \begin{bmatrix} \frac{2}{3} & \frac{1}{3} \\ 1 & 0 \end{bmatrix}$

可得
$$\begin{cases} Q(x_1) = \frac{2}{3}Q(x_1) + Q(x_2) \\ Q(x_2) = \frac{1}{3}Q(x_1) \\ Q(x_2) + Q(x_1) = 1 \end{cases}$$

故
$$\begin{cases} Q(x_1) = \frac{3}{4} \\ Q(x_2) = \frac{1}{4} \end{cases}$$

所以，信源熵为

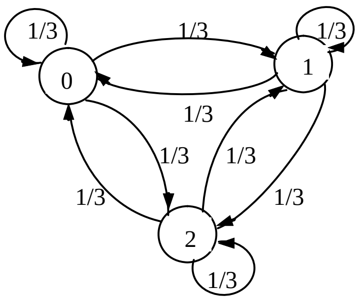
$$H_\infty = H_2 = -\sum_{i=1}^{2}\sum_{k=1}^{2} Q(E_i)P(a_k \mid E_i)\log P(a_k \mid E_i)$$

$$= \sum_{i=1}^{2} Q(E_i)H(a_k \mid E_i) = Q(x_1)H(\frac{2}{3},\frac{1}{3}) + Q(x_2)H(1,0)$$

$$= \frac{3}{4}[\frac{2}{3}\log\frac{3}{2} + \frac{1}{3}\log 3] = 0.6887\text{比特/符号}$$

4．一个马尔科夫链的基本符号为 0，1，2 三种，他们以等概率出现，且具有相同的转移概率，没有任何固定约束，试（1）画出单纯马尔科夫链信源的香农线图，并求稳定状态下的信源熵H_1。（2）画出二阶马尔科夫链信源的香农线图，并求稳定状态下的信源熵H_2。

解：（1）由已知得 $P(j \mid i) = \frac{1}{3} \quad i, j = 0,1,2$ 则香农线图如下

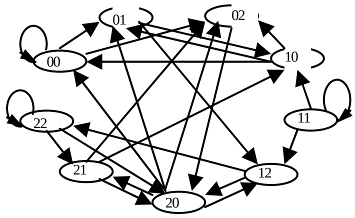


稳定时 $H(X) = 3 \times \frac{1}{3}\log 3 = 1.585$ bit/符号

（2）二阶马尔可夫信源，初始状态有 $3^2 = 9$ 个，等概分布

$$P(m \mid ij) = \frac{1}{3}$$

$$H_2 = \sum_{i=0}^{2}\sum_{j=0}^{2}\sum_{m=0}^{2} P(m \mid ij)\log P(m \mid ij) = 1.585 \quad \text{bit/符号}$$



图中每条路径概率均为 1/3

5．某一阶马尔可夫信源的状态转移如图 3.4 所示，信源符号集为 **X**：{0, 1, 2}，并定义 $\bar{p}=1-p$ 。试求：

（1） 信源的极限熵H_∞；

（2） p取何值时H_∞取最大值。

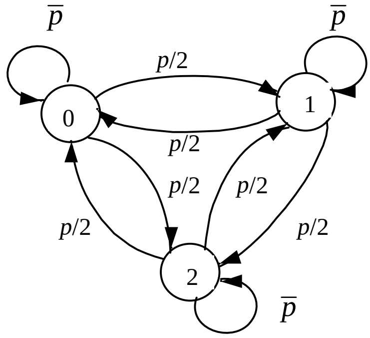


图 3.4

解：（1）

一步转移矩阵为 P， $P=\begin{bmatrix} \bar{p} & p/2 & p/2 \\ p/2 & \bar{p} & p/2 \\ p/2 & p/2 & \bar{p} \end{bmatrix}$

可得 $$\begin{cases} Q(0)=\bar{p}Q(0)+\dfrac{p}{2}Q(1)+\dfrac{p}{2}Q(2) \\ Q(1)=\dfrac{p}{2}Q(0)+\bar{p}Q(1)+\dfrac{p}{2}Q(2) \\ Q(2)=\dfrac{p}{2}Q(0)+\dfrac{p}{2}Q(1)+\bar{p}Q(2) \\ Q(0)+Q(1)+Q(2)=1 \end{cases}$$

计算得$Q(0)=Q(1)=Q(2)=\frac{1}{3}$

则得$P(0)=P(1)=P(2)=\frac{1}{3}$

所以，信源熵为

$$H_\infty=H_2=\sum_{i=1}^{2}Q(E_i)H(X\mid E_i)$$
$$=P(0)H(X\mid 0)+P(1)H(X\mid 1)+P(2)H(X\mid 2)$$
$$=\frac{1}{3}H(\overline{p},\frac{p}{2},\frac{p}{2})+\frac{1}{3}H(\frac{p}{2},\overline{p},\frac{p}{2})+\frac{1}{3}H(\frac{p}{2},\frac{p}{2},\overline{p})$$
$$=-\overline{p}\log\overline{p}-p\log p+p\text{比特/符号}$$

（2）因为 $H_\infty=-(1-p)\log(1-p)-p\log p+p$

求其对 p 的一阶导数

$$\frac{\partial H_\infty}{\partial p}=\log(1-p)+\frac{1}{\ln 2}-\log p-\frac{1}{\ln 2}+1$$
$$=\log(1-p)-\log p+\log 2=\log\frac{2(1-p)}{p}$$

令$\frac{\partial H_\infty}{\partial p}=0,$得$\log\frac{2(1-p)}{p}=0$

所以当 p=2/3 时，信源的极限熵达到最大值。

6．设随机变量序列$\mathbf{X}=X_1X_2\ldots X_N$通过某离散信道$\{\mathbf{X};\ P(\mathbf{Y}/\mathbf{X});\ \mathbf{Y}\}$，其输出序列为$\mathbf{Y}=Y_1Y_2\ldots Y_N$。试证明若

（1）$p\,(b_{jN}/a_{i1}\,a_{i1}\ldots a_{iN};\ \ b_{j1}\,b_{j2}\ldots b_{jN-1})=p\,(b_{jN}/a_{iN})$;

（2）$p\,(b_{j1}\,b_{j2}\ldots b_{jN-1}/a_{i1}\,a_{i1}\ldots a_{iN})=p\,(b_{j1}\,b_{j2}\ldots b_{jN-1}/a_{i1}\,a_{i1}\ldots a_{iN-1})$

则该信道的转移概率为

$$P(\mathbf{X}/\mathbf{Y})=p\left(b_{j1}b_{j2}\cdots b_{jN}/a_{i1}a_{i2}\cdots a_{iN}\right)=\prod_{k=1}^{N}p\left(b_{jk}/a_{ik}\right)$$

证明：

$$P(\mathbf{X}/\mathbf{Y}) = p\left(b_{j1}b_{j2}\cdots b_{jN} / a_{i1}a_{i2}\cdots a_{iN}\right)$$
$$= p\left(b_{j1}b_{j2}\cdots b_{jN-1} / a_{i1}a_{i2}\cdots a_{iN}\right)\times p\left(b_{jN} / a_{i1}a_{i2}\cdots a_{iN}; b_{i1}b_{i2}\cdots b_{iN-1}\right)$$
$$= p\left(b_{j1}b_{j2}\cdots b_{jN-1} / a_{i1}a_{i2}\cdots a_{iN-1}\right)\times p\left(b_{jN} / a_{iN}\right)$$
$$= p\left(b_{j1}b_{j2}\cdots b_{jN-2} / a_{i1}a_{i2}\cdots a_{iN-2}\right)\times p\left(b_{jN-1} / a_{iN-1}\right)\times p\left(b_{jN} / a_{iN}\right)$$
$$= \ldots = \prod_{k=1}^{N} p\left(b_{jk} / a_{ik}\right)$$

7．设信源$\mathbf{X}$的N次扩展信源$\mathbf{X}=X_1X_2\ldots X_N$通过信道{$\mathbf{X}$; $P(\mathbf{Y}/\mathbf{X})$; $\mathbf{Y}$}，其输出序列为$\mathbf{Y}=Y_1Y_2\ldots Y_N$。试证明

（1） 当信源为无记忆信源，即$X_1X_2\ldots X_N$之间统计独立时，有

$$\sum_{k=1}^{N} I\left(X_k;Y_k\right) \geq I\left(\mathbf{X};\mathbf{Y}\right)；$$

（2） 当信道无记忆时，有$\sum_{k=1}^{N} I\left(X_k;Y_k\right) \geq I\left(\mathbf{X};\mathbf{Y}\right)$；

（3） 当信源、信道均为无记忆时，有$\sum_{k=1}^{N} I\left(X_k;Y_k\right) = I\left(\mathbf{X}^N;\mathbf{Y}^N\right) = NI\left(\mathbf{X};\mathbf{Y}\right)$；

（4） 用熵的概念解释以上 3 种结果。

证明:（1）设信道输入连续型随机序列 X=(X1X2…XN),输出也是连续型随机序列 Y=(Y1Y2…YN)，信道的传递概率密度函数为

$$p(y\,|\,x) = p(y_1y_2\cdots y_N\,|\,x_1x_2\cdots x_N)$$

$$x\in X, y\in Y, y_i \in Y_i, x_i \in X_i (i=1,2,\cdots,N)$$

因为信源无记忆，即随机序列 X 中各分量彼此互相独立，因而有

$$p(x) = \prod_{i=1}^{N} p(x_i) \qquad x_i \in X_i, x\in X$$

可得

$$I(X;Y)=\underset{X,Y}{E}[\log\frac{p(x|y)}{p(x)}]$$

$$=\underset{X,Y}{E}[\log\frac{p(x|y)}{\prod_{i=1}^{N}p(x_i)}]$$

$$x\in X, y\in Y, x_i\in X_i$$

另外

$$\sum_{i=1}^{N}I(X_i;Y_i)=\sum_{i=1}^{N}\iint_{RR}p(x_iy_i)\log\frac{p(x_i|y_i)}{p(x_i)}dx_idy_i$$

$$=\iint_{R}p(x_1y_1)\log\frac{p(x_1|y_1)}{p(x_1)}dx_1dy_1$$

$$+\iint_{R}p(x_2y_2)\log\frac{p(x_2|y_2)}{p(x_2)}dx_2dy_2$$

$$+\cdots+\iint_{R}p(x_Ny_N)\log\frac{p(x_N|y_N)}{p(x_N)}dx_Ndy_N$$

其中 R 为实数集。

因为

$$\int_{X_1}\cdots\iint_{X_{i-1}X_{i+1}}\cdots\iint_{X_NY_1}\cdots\iint_{Y_{i-1}Y_{i+1}}\cdots\int_{Y_N}p(x_1\cdots x_Ny_1\cdots y_N)dx_1\cdots dx_{i-1}dx_{i+1}\cdots dx_Ndy_1\cdots dy_{i-1}dy_{i+1}\cdots dy_N$$

$$=p(x_iy_i)$$

所以

$$\sum_{i=1}^{N}I(X_i,Y_i)$$

$$=\iint_{X_1Y_1}\cdots\iint_{X_NY_N}p(x_1\cdots x_Ny_1\cdots y_N)\log\frac{p(x_1|y_1)\cdots p(x_N|y_N)}{p(x_1)\cdots p(x_N)}dx_1\cdots dx_Ndy_1\cdots dy_N$$

$$=\iint_{XY}p(xy)\log\frac{\prod_{i=1}^{N}p(x_i|y_i)}{\prod_{i=1}^{N}p(x_i)}dxdy=\underset{X,Y}{E}[\log\frac{\prod_{i=1}^{N}p(x_i|y_i)}{\prod_{i=1}^{N}p(x_i)}]$$

$$\sum_{i=1}^{N} I(X_i;Y_i) - I(X;Y) = \underset{X,Y}{E}[\log \frac{\prod_{i=1}^{N} p(x_i \mid y_i)}{p(x \mid y)}]$$

$$\leq \log \underset{X,Y}{E}[\frac{\prod_{i=1}^{N} p(x_i \mid y_i)}{p(x \mid y)}] \text{...(1)}$$

$$= \log \iint_{XY} p(xy) \frac{\prod_{i=1}^{N} p(x_i \mid y_i)}{p(x \mid y)} dxdy$$

因此，

$$= \log \iint_{XY} p(y) p(x_1 \mid y_1) \cdots p(x_N \mid y_N) dx_1 \cdots dx_N dy$$

$$= \log \int_{Y} p(y) dy \int_{X_1} p(x_1 \mid y_1) dx_1 \int_{X_2} p(x_2 \mid y_2) dx_2 \cdots \int_{X_N} p(x_N \mid y_N) dx_N$$

$$= \log \int_{Y} p(y) dy \text{...(2)}$$

$$= \log 1 = 0$$

其中（1）式是根据詹森不等式。（2）式是因为

$$p(y_i) = \int_{X_i} p(x_i y_i) dx_i = \int_{X_i} p(y_i) p(x_i \mid y_i) dx_i$$

所以

$$\int_{X_i} p(x_i \mid y_i) dx_i = 1$$

所以证得

$$\sum_{i=1}^{N} I(X_i;Y_i) - I(X;Y) \leq 0$$

$$\sum_{i=1}^{N} I(X_i;Y_i) \leq I(X;Y)$$

（2）设信道输入连续型随机序列 $X = (X_1 X_2 \cdots X_N)$，输出连续型随机序列 $Y = (Y_1 Y_2 \cdots Y_N)$。因为信道无记忆，有

$$p(y \mid x) = \prod_{i=1}^{N} p(y_i \mid x_i)$$

$$x \in X, y \in Y, x_i \in X_i, y_i \in Y_i$$

X 和 Y 的平均互信息

$$\sum_{i=1}^{N} I(X_i, Y_i) = \underset{X,Y}{E}[\log \frac{P(y|x)}{p(y)}] = \underset{X,Y}{E}[\log \frac{\prod_{i=1}^{N} p(y_i|x_i)}{p(y)}]$$

而 $\sum_{i=1}^{N} I(X_i, Y_i) = \sum_{i=1}^{N} \iint_{X_i Y_i} p(x_i y_i) \log \frac{p(y_i|x_i)}{p(y_i)} dx_i dy_i$

与前半题同理得 $\sum_{i=1}^{N} I(X_i, Y_i) = \underset{X,Y}{E}[\log \frac{\prod_{i=1}^{N} p(y_i|x_i)}{\prod_{i=1}^{N} p(y_i)}]$

因此

$$I(X;Y) - \sum_{i=1}^{N} I(X_i, Y_i) = \underset{X,Y}{E}[\log \frac{\prod_{i=1}^{N} p(y_i)}{p(y)}]$$

$$= \iint_{XY} p(xy) \log \frac{\prod_{i=1}^{N} p(y_i)}{p(y)} dxdy$$

根据詹森不等式，有

$$\begin{aligned}
&\le \log \iint_{XY} p(xy) \frac{\prod_{i=1}^{N} p(y_i)}{p(y)} dxdy \\
&= \log \int_X p(x|y) dx \int_{Y_1} \cdots \int_{Y_N} p(y_1) \cdots p(y_N) dy_1 \cdots dy_N \\
&= \log \int_{Y_1} \cdots \int_{Y_N} p(y_1) \cdots p(y_N) dy_1 \cdots dy_N \\
&= \log 1 = 0
\end{aligned}$$

其中因为 $\int_X p(x|y) dx = 1$，$\int_{Y_i} p(y_i) dy_i = 1$

由此证得 $\sum_{k=1}^{N} I\left(X_k;Y_k\right) \ge I\left(\mathbf{X};\mathbf{Y}\right)$

（3） 设 X 和 Y 的一个取值为

$$\alpha_k = (\alpha_{k_1}\alpha_{k_2}\cdots\alpha_{k_N}), \alpha_{k_i} \in \{a_1, a_2, \cdots, a_r\}(i = 1,2,\cdots,N)$$
$$\beta_h = (b_{h_1}b_{h_2}\cdots b_{h_N}), b_{h_i} \in \{b_1, b_2, \cdots, b_s\}(i = 1,2,\cdots,N)$$

信源无记忆时满足

$$P(a_k) = P(a_{k_1})P(a_{k_2})\cdots P(a_{k_N}) \qquad k = 1,2,\cdots r^N \tag{1}$$

$$\sum_{X^N} P(a_k) = \sum_{X^1} P(a_{k_1})\cdots\sum_{X^N} P(a_{k_N}) = 1$$

而信道无记忆时满足

$$P(\beta_h \mid \alpha_k) = \prod_{i=1}^{N} P(b_{h_i} \mid a_{k_i}) \tag{2}$$

及 $\sum_{Y^N} P(\beta_h \mid \alpha_k) = 1 \quad k = 1,2,\cdots,r^N, h = 1,2,\cdots,s^N$

所以当信道和信源都是无记忆时，不但上面（1）和（2）式满足，同时满足

$$P(\beta_h) = \sum_{X^N} P(\alpha_k\beta_h) = \sum_{X^N} P(\alpha_k)P(\beta_h \mid \alpha_k)$$
$$= \sum_{X^N} P(\alpha_{k_1})\cdots P(\alpha_{k_N})P(b_{h_1} \mid a_{k_1})\cdots P(b_{h_N} \mid a_{k_N})$$
$$= \sum_{X_1} P(a_{k_1})P(b_{h_1} \mid a_{k_1})\cdots\sum_{X_N} P(a_{k_N})P(b_{h_N} \mid a_{k_N})$$
$$= \sum_{X_1} P(a_{k_1}b_{h_1})\cdots\sum_{X_N} P(a_{k_N}b_{h_N})$$
$$= P(b_{h_1})\cdots P(b_{h_N}) \mid \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3)$$

同理 $P(\alpha_k\beta_h) = \prod_{i=1}^{N} P(a_{k_i}b_{h_i}) \quad k = 1,2,\cdots,r^N, h = 1,2,\cdots,s^N \ldots\ldots\ldots\ldots(4)$

根据平均互信息的表达式得

$$I(X;Y) = I(X^N;Y^N) = \sum_{X^N Y^N} P(\alpha_k\beta_h)\log\frac{P(\beta_h \mid \alpha_k)}{P(\beta_h)}$$

所以信道和信源都是无记忆的。将(2),(3),(4)式代入得

$$I(X^N;Y^N)=\sum_{X_1}\cdots\sum_{X_N}\sum_{Y_1}\cdots\sum_{Y_N}P(a_{k_1}b_{h_1})\cdots P(a_{k_N}b_{h_N})$$

$$\log\frac{P(b_{h_1}\mid a_{k_1})\cdots P(b_{h_N}\mid a_{k_N})}{P(b_{h_1})\cdots P(b_{h_N})}=\sum_{X_1}\sum_{Y_1}P(a_{k_1}b_{h_1})\log\frac{P(b_{h_1}\mid a_{k_1})}{P(b_{h_1})}$$

$$+\cdots+\sum_{X_N}\sum_{Y_N}P(a_{k_N}b_{h_N})\log\frac{P(b_{h_N}\mid a_{k_N})}{P(b_{h_N})}$$

$$=I(X_1;Y_1)+I(X_2;Y_2)+\cdots+I(X_N;Y_N)$$

因为 Xi(i=1,2,…,N)取自同一信源 X，$a_{k_i}\in\{a_1,a_2,\cdots,a_r\}(i=1,2,\cdots,N)$，而又通过同一信道，输出 Yi(i=1,2,…,N)，Yi 也属同一信源 Y,

$b_{h_i}\in\{b_1,b_2,\cdots,b_s\}(i=1,2,\cdots,N)$ 又信道的传递概率与 i 无关（时不变信道），即

$$\left.\begin{aligned}P(b_{h_1}\mid a_{k_1})=P(b_{h_2}\mid a_{k_2})=\cdots=P(b_{h_N}\mid a_{k_N})=P(b_h\mid a_k)\\ P(a_{k_1}b_{h_1})=P(a_{k_2}b_{h_2})=\cdots=P(a_{k_N}b_{h_N})=P(a_kb_h)\\ P(b_{h_1})=P(b_{h_2})=\cdots=P(b_{h_N})=P(b_h)\end{aligned}\right\}$$

其中

$$a_k,a_{k_i}\in\{a_1,a_2,\cdots,a_r\}$$
$$b_h,b_{h_i}\in\{b_1,b_2,\cdots,b_s\}$$
$$(i=1,2,\cdots,N)$$

得 $I(X_1,Y_1)=I(X_2;Y_2)=\cdots=I(X_N;Y_N)=I(X;Y)$

所以 $\sum_{k=1}^{N}I(X_k;Y_k)=I(\mathbf{X}^N;\mathbf{Y}^N)=NI(\mathbf{X};\mathbf{Y})$

1. 简述信源译码的错误扩展现象。

答：由于信道的干扰作用，造成了一定量的错误，这些错误在译码时又造成了更多的错误，这就是通信译码的错误扩展现象。

2. 针对某种应用，给出一种你认为是有价值的减小信源译码错误扩展的方法。

答：在信源编码的每个码字施加和码字等长的附加位，编码时将要写入的信息在新码字上顺序写两边，译码时先译前半段，若码长无误则译后半段，若前后不一致则要求重发，在带宽充足的条件下可以采用这种方法。

3. 试说明已有的解决信源译码错误扩展问题的方法，简述其基本思路及利弊。

答：信道编码的方法

优点：加入了纠错码，减少了译码错误的可能性，减少了发生错误扩展的概率。]

缺点：需要对发送的码字加入冗余，是一种降低效率来换取可靠性的方法。

4. 某通信系统使用文字字符共 10 000 个，据长期统计，使用频率占 80%的共有 500 个，占 90%的有 1000 个，占 99%的有 4000 个，占 99.9%的 7000 个。（1）求该系统使用的文字字符的熵；（2）请给出该系统一种信源编码方法并作简要评价。

解：

(1)
$$H(\mathbf{X}) = -0.8\log\frac{0.8}{500} - 0.1\log\frac{0.1}{500} - 0.09\log\frac{0.09}{3000} - 0.009\log\frac{0.009}{3000} - 0.001\log\frac{0.001}{3000} = 10.198\text{比特}/\text{信符}$$

(2)可以使用 huffman 编码的方法，为使压缩效果理想，可以使用扩展信源的方法。

5. 一通信系统传送的符号只有 3 个，其使用概率分别为 0.2、0.3 和 0.5，但传送时总是以 3 个符号为一个字，故该系统的信源编码以字为基础并采用二进制霍夫曼编码。根据字的概率大小，编码结果为：概率在(0，0.020)，采用 6 比特；在(0.020，0.045]，采用 5 比特，但允许其中一个用 4 比特；在(0.045，0.100]，在 0.100 以上，采用 3 比特。求该种信源编码的效率。

解：假设三个符号分别为 a b c，则 p(a)=0.2,p(b)=0.3,p(c)=0.5

下面对每个字可能出现的情况加以讨论。

3 个符号都为 a 则 $P = 0.2^3 = 0.008$ 编 6bit 码，共 1 种

3 个符号都为 b 则 $P = 0.3^3 = 0.027$ 编 5bit 码，共 1 种

3 个符号都为 c 则 $P = 0.5^3 = 0.125$ 编 3bit 码，共 1 种

3 个符号有 2 个 a，1 个 b 则 $P = 0.2^2 \times 0.3 = 0.012$ 编 6bit 码，共 3 种

3 个符号有 2 个 a，1 个 c 则 $P = 0.2^2 \times 0.5 = 0.02$ 编 5bit 码，共 3 种

3 个符号有 2 个 b，1 个 a 则 $P = 0.3^2 \times 0.2 = 0.018$ 编 6bit 码，共 3 种

3 个符号有 2 个 b，1 个 c 则 $P = 0.3^2 \times 0.5 = 0.045$ 编 5bit 码，共 3 种

3 个符号有 2 个 c，1 个 a 则 $P = 0.5^2 \times 0.2 = 0.05$ 编 4bit 码，共 3 种

3 个符号有 2 个 c，1 个 b 则 $P = 0.5^2 \times 0.3 = 0.075$ 编 4bit 码，共 3 种

3 个符号有 1 个 a，1 个 b,1 个 c 则 $P = 0.2 \times 0.3 \times 0.5 = 0.03$ 编 5bit 码，共 6 种

平均码长为

$$0.008\times6 + 0.027\times5 + 0.125\times3 + \begin{pmatrix} 0.012\times6 + 0.02\times5 + 0.018\times6 \\ + 0.045\times5 + 0.05\times4 + 0.075\times4 \end{pmatrix}\times3 + 0.03\times5\times6$$

＝4.488 bit/字

$$H(\mathbf{X}) = (-\sum_{i=1}^{s} P_i \log P_i)\times3 = (-0.2\log_2 0.2 - 0.3\log_2 0.3 - 0.5\log_2 0.5)\times3$$

$$= 4.455 bit/\text{字}$$

$\eta_1 = R_1/C = 4.455/4.488 = 99.26\%$

6.　设有一个无记忆信源发出符号 A 和 B，已知 $p(\mathrm{A}) = 1/4, p(\mathrm{B}) = 3/4$。（1）计算该信源熵；（2）设该信源改为发出二重符号序列消息的信源，采用费诺编码方法，求其平均信息传输速率；（3）又设该信源改为发三重序列消息的信源，采用霍夫曼编码方法，求其平均信息传输速率。

解：（1）该离散无记忆信源的熵为

$$H(\mathbf{X}) = -\sum_{i=1}^{s} P_i \log P_i = -0.25\log_2 0.25 - 0.75\log_2 0.75 = 0.811 bit/\text{符号}$$

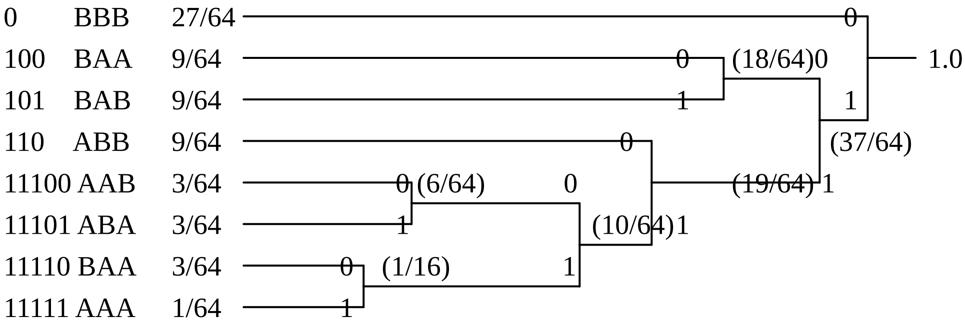
（2）费诺编码

消息符号序号 (i)	消息概率 p_i	第一次分解	第二次分解	第三次分解	二进制代码组	码组长度 b_i
BB	9/16	(9/16)0			0	1
AB	3/16	(7/16)1	(3/16) 0		10	2
BA	3/16		(4/16) 1	(3/16)0	110	3
AA	1/16			(1/16) 1	111	3

编码的平均长度为　$\overline{\mathrm{b}} = \frac{9}{16} + \frac{3}{16}\times 2 + \frac{3}{16}\times 3 + \frac{1}{16}\times 3 = 1.6875$ 码元/符号

平均传输速率为　$R = \frac{H(\mathbf{X})}{\overline{b}} = \frac{2.61}{2.74} = 0.953$ 比特/时间

（3）霍夫曼编码



编码的平均长度为　$\overline{\mathrm{b}} = \frac{27}{64} + \frac{9}{64}\times 3\times 3 + \frac{3}{64}\times 5\times 3 + \frac{1}{64}\times 5 = 2.46875$ 码元/符号

平均传输速率为　$R = \frac{H(\mathbf{X})}{\overline{b}} = 0.9855$ 比特/时间

7.　已知一个信源包含 8 个符号消息，它们的概率分布如下表：

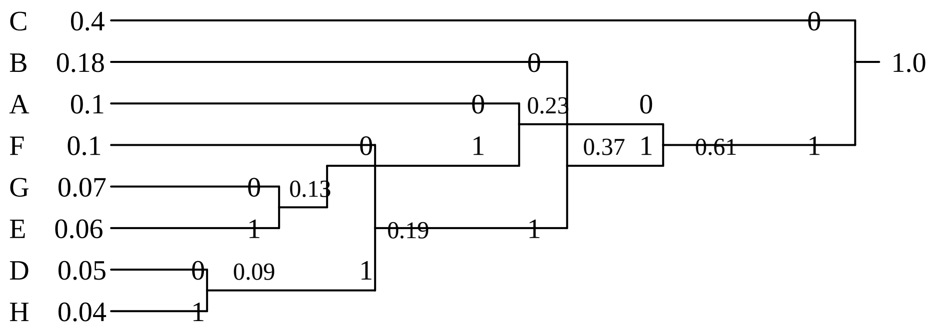
A	B	C	D	E	F	G	H
0.1	0.18	0.4	0.05	0.06	0.1	0.07	0.04

（1）信源每秒钟内发出一个符号，求该信源的熵及信息传输速率；（2）对这 8 个符号作二进制码元的霍夫曼编码，写出各个代码组，并求出编码效率。

解：（1）该信源的熵 $H(\mathbf{X}) = -\sum_{i=1}^{8} P_i \log P_i = 2.55 bit/\text{符号}$

信息传输速率 R=2.55bit/s

（2）霍夫曼编码



编码结果：

C	B	A	F	G	E	D	H
0	110	100	1110	1010	1011	1110	11111

平均码长为：$\overline{\mathrm{b}} = 0.4 + 0.18\times 3 + 0.1\times 3 + 0.1\times 4 + 0.07\times 4 + 0.06\times 4$
$+ 0.05\times 5 + 0.04\times 5 = 2.61 码元/符号$

所以编码效率为 $\eta = \dfrac{2.55}{2.61} = 97.8\%$

8. 设信道基本符号集合**A** $=\{a_1, a_2, a_3, a_4, a_5\}$，它们的时间长度分别为

$t_1 =1, t_2 =2, t_3 =3, t_4 =4, t_5 =5$ （各码元时间）

用这样的信道基本符号编成消息序列，且不能出现 $a_1a_1, a_2a_2, a_2a_1, a_1a_2$ 这四种符号相连的情况。（1）求这种编码信道的信道容量；（2）若信源的消息集合 $\mathbf{X} = \{x_1, x_2, \cdots, x_7\}$，它们的出现概率分别是 $P(x_1)=1/2, P(x_2)=1/4, P(x_3)=1/8, \cdots, P(x_6) = P(x_7)=1/64$， 试求按最佳编码原则利用上述信道来传输这些消息时的信息传输速率；（3）求上述信源编码的编码效率。

解：（1）这是一个有固定约束的不均匀编码的信道，有约束条件（即不能出现 $a_1a_1, a_2a_2, a_2a_1, a_1a_2$），可以把 a_1, a_2 作为状态 1，a_3, a_4, a_5 作为状态 2，得香农线图

时间长度分别为 $b_{11=}\infty$,b_{12} $(a_3)=3$，b_{12} $(a_4)=4$，b_{12} $(a_5)=5$，$b_{21}(a_1)=1$，$b_{21}(a_2)=2$，$b_{22}(a_3)=3$，$b_{22}(a_5)=5$,写出行列式，可得特征方程为 $1-w^{-3}-2w^{-4}-3w^{-5}-2w^{-6}-w^{-7}$

解方程可得 $w_{\max} = 1.597$

所以 $C = \log_2 w_{\max} = 0.675\,\text{bit/码元时间}$

（2） 因为规定 a_1 a_2 不能连用，故不能用和做码字，根据最佳编码的两个原则，及单译可译定理，出现概率大的消息用短码的原则，可用

x_1	x_2	x_3	x_4	x_5	x_6	x_7
1/2	1/4	1/8	1/16	1/32	1/64	1/64
a_3	a_4	a_1a_3	a_5	$a_1\ a_4$	a_2a_3	$a_2\ a_4$
3	4	4	5	5	5	6

$$H(\mathbf{X}) = -\sum_{i=1}^{s} P_i \log P_i = 1.969 bit/符号$$

$$\overline{b} = \sum_{I} P_i b_i = 3.641 码元$$

$$R = \frac{H(x)}{\overline{b}} = 0.541 bit/码元时间$$

（3）编码效率为 $\eta = R/C$ =0.541/0.675=80%

5．1 $H(X)=H(Y)=-\sum_{i=1}^{4}P(X_i)\log_2 P(X_i)=2$

$$H(XY)=\sum_{i=1}^{4}\sum_{j=1}^{4}P(x_i y_j)lbP(x_i y_j)=4\times(\tfrac{1}{8}\log_2 8+3\times\tfrac{1}{24}\log_2 24)=3.79$$ 比特/符号

$I(X;Y)=H(X)+H(Y)-H(XY)=0.21$ 比特

命题得证。

5．2 $H(X)=\frac{5}{8}\log_2\frac{8}{5}+\frac{3}{8}\log_2\frac{8}{3}=0.9544$ 比特/符号

$H(Y)=\frac{1}{2}\log_2 2+\frac{1}{2}\log_2 2=1$ 比特/符号

$$H(Y|X)=-\sum_{i=1}^{2}\sum_{j=1}^{2}P(x_i)P(y_j|x_i)\log_2 P(y_j|x_i)=\tfrac{5}{8}(\tfrac{3}{5}\log_2\tfrac{5}{3}+\tfrac{2}{5}\log_2\tfrac{5}{2})$$

$$+\tfrac{3}{8}(\tfrac{1}{3}\log_2 3+\tfrac{2}{3}\log_2\tfrac{3}{2})=0.951\text{比特/符号}$$

$I(X;Y)=H(Y)-H(Y|X)=0.049$ 比特/符号

R=0.049*1000=49 比特

5．3 $H(X)=2\times\log_2 2=1$ 比特/符号

$H(Y)=\frac{2}{3}\log_2\frac{3}{2}+\frac{1}{3}\log_2 3=0.918$ 比特/符号

$H(XY)=\frac{5}{12}\log_2\frac{12}{5}+\frac{1}{12}\log_2 12+\frac{1}{4}\log_2 4+\frac{1}{4}\log_2 4=1.825$ 比特/符号

$I(X;Y)=H(X)+H(Y)-H(XY)=0.093$ 比特/符号

5．4 $C=(1+\frac{1}{100}\log_2 100+\frac{99}{100}\log_2\frac{100}{99})\times 1000=919$ 比特/符号

5．5 （1）由图可知这是个对称信道，当输入符号等概时，$C=\max I(X;Y)$，

$p(xy)=P(x)P(y|x)$，

$$P(xy)=\begin{pmatrix}1/8 & 1/8 & 0 & 0\\ 0 & 1/8 & 1/8 & 0\\ 0 & 0 & 1/8 & 1/8\\ 1/8 & 0 & 0 & 1/8\end{pmatrix}$$

$C=\log_2 4+\sum_{j=1}^{4}P(y_j|x_i)\log_2 P(y_j|x_i)$ 对任意 x 均成立

所以，C=1 比特/符号。

（2）由图可知，信道亦为对称信道，$C=\max I(X;Y)$

$$P(xy)=P(x)P(y|x)=\begin{pmatrix} 1/6 & 1/6 & 1/12 & 1/12 \\ 1/12 & 1/12 & 1/6 & 1/6 \end{pmatrix}$$

$C=\log_2 4+\sum_{j=1}^{4} P(y_j\mid x_i)\log_2 P(y_j\mid x_i)$ =0.0817 比特/符号

（3）同上，信道为对称离散信道，

$$P(xy)=\begin{pmatrix} 1/6 & 1/9 & 1/18 \\ 1/18 & 1/6 & 1/9 \\ 1/9 & 1/18 & 1/6 \end{pmatrix}$$

$C=\log_2 3+\sum_{i=1}^{3}\sum_{j=1}^{3} P(y_j x_i)\log_2 P(y_j\mid x_i)=0.126$ 比特/符号。

5．6 设 $P(x_3)=P(x_2)=a$，则$P(x_1)=1-2a$，$P(y_1)=1-2a,$

据对称性 $P(y_3)=P(y_2)=a,$

$$I(X;Y)=H(Y)-H(Y\mid X)$$
$$=-[(1-2a)\ln(1-2a)+2a\ln a]-2a(\varepsilon\ln\varepsilon+\varepsilon^{'}\ln\varepsilon^{'})-0],$$

由$\partial I/a=0$，得$a=1/[2+\frac{1}{\varepsilon^{\varepsilon}\varepsilon'^{\varepsilon'}}]$，

代入$I(X;Y)=\ln(1+2\varepsilon^{\varepsilon}\varepsilon'^{\varepsilon'})$

所以 $C=\ln(1+2\varepsilon^{\varepsilon}\varepsilon'^{\varepsilon'})$ 奈特/符号。

5．7 该信道可看成 4 个 BSC 信道串联而成，

$$\pi_1=\begin{pmatrix} 1-\varepsilon & \varepsilon \\ \varepsilon & 1-\varepsilon \end{pmatrix}$$

$$\pi=\pi_1^{\,4}=\begin{pmatrix} 1-4\varepsilon(1-\varepsilon)[1-2\varepsilon(1-\varepsilon)] & 4\varepsilon(1-\varepsilon)[1-2\varepsilon(1-\varepsilon)] \\ 4\varepsilon(1-\varepsilon)[1-2\varepsilon(1-\varepsilon)] & 1-4\varepsilon(1-\varepsilon)[1-2\varepsilon(1-\varepsilon)] \end{pmatrix}$$

级联后的信道仍是对称信道，可代入公式：

$$C_{bsc}=1+\varepsilon\log\varepsilon+(1-\varepsilon)\log(1-\varepsilon)$$

其中ε--〉$4\varepsilon(1-\varepsilon)[1-2\varepsilon(1-\varepsilon)]$ $1-\varepsilon$--〉$1-4\varepsilon(1-\varepsilon)[1-2\varepsilon(1-\varepsilon)]$

则

$C'=1+4\varepsilon(1-\varepsilon)[1-2\varepsilon(1-\varepsilon)]\log\{4\varepsilon(1-\varepsilon)[1-2\varepsilon(1-\varepsilon)]\}+1-4\varepsilon(1-\varepsilon)[1-2\varepsilon(1-\varepsilon)]\log\{4\varepsilon(1-\varepsilon)[1-2\varepsilon(1-\varepsilon)]\}$

代入$\varepsilon=10^{-4}$，得 C’=0.9949

所以信道容量 C’=C*1024=1018.8 kbps。

5．8 由图可知信道为对称信道，且信源的符号消息等概分布，因此

$C=lb3=1.58$ 比特/符号。

5．9　后验概率 $P(x|y)=\dfrac{P(xy)}{P(y)}$，又$P(xy)=P(x)P(y|x)$,根据题目所给的数据得

$$P(xy)=\begin{pmatrix} 1/4 & 1/6 & 1/12 \\ 1/24 & 1/8 & 1/12 \\ 1/12 & 1/24 & 1/8 \end{pmatrix}$$

由 $P(y)=\sum_X P(xy)$,得

P(y)=[3/8　1/3　7/24]

所以

$$P(x|y)=\begin{pmatrix} 2/3 & 1/2 & 2/7 \\ 1/9 & 3/8 & 2/7 \\ 2/9 & 1/8 & 3/7 \end{pmatrix}$$

根据最小错误概率准则，应作如下译码：

$$y_1->x_1, y_2->x_1, y_3->x_3$$

错误概率为

$$P_E=1-P_c=1-\{P(x_1)P(y_1|x_1)+P(x_1)P(y_2|x_1)+P(x_3)P(y_3|x_3)\}$$
$$=1-\{1/2\times1/2+1/2\times1/3+1/4\times1/2\}=1-13/24=11/24$$

5．10　（1）$P_E=\dfrac{1}{M}\sum_{j=1}^{L}\sum_{\substack{i=1\\i\neq *}}^{M}P(y_j|x_i)=1/2(P(y_1|x_2)+P(y_2|x_1))=p$

（2）$P_E=\dfrac{1}{M}\sum_{j=1}^{L}\sum_{\substack{i=1\\i\neq *}}^{M}P(y_j|x_i)=1/2P(y_1|x_2)=p/2$

（3）$P_E=\dfrac{1}{M}\sum_{j=1}^{L}\sum_{\substack{i=1\\i\neq *}}^{M}P(y_j|x_i)=1/2(P(y_2|x_2)+P(y_2|x_1))=p$

5．11 ? ?

5．12 （1）对信源四个消息进行编码，选择码长 n=4，这组码为

C : $\{(x_1,x_2,1/2,1/2)\}$　　$x_i=0或1$　i=(1,2)

编码后的信息传输率

$$R=\frac{\log 4}{4}=\frac{1}{2}\quad 比特/符号$$

（2）设接收序列 $\beta=(y_1y_2y_3y_4)$　$y_i\in\{0,1\}(i=1,2,3,4)$ 根据信道的传输特性，输入序列

β 共有 16 个，正好分成 4 个互不相交的子集，每个码字只传输到其中对应的一个子集：

$\alpha_1=$(0　0　1/2　1/2)→(0　0　y_3　y_4)　　$\alpha_2=$(0　1　1/2　1/2)→(0　1　y_3　y_4)

$\alpha_3=$(1　0　1/2　1/2)→(1　0　y_3　y_4)　　$\alpha_4=$(1　1　1/2　1/2)→(1　1　y_3　y_4)

所以根据选择的译码规则

$$f(y_1y_2y_3y_4)=(y_1y_2\ 1/2\ 1/2)$$

正好将接收序列译成所发送的码字，可计算每个码字引起的错误概率

$$P_e^{(i)}=[\sum_Y P(\beta|\alpha_i)\quad F(\beta)\neq\alpha_i]=0$$

所以有 $P_E=\sum_C P(\alpha_i)P_e^i=0$。

513(1) $P(x|y)=\dfrac{P(xy)}{P(y)}$，又$P(xy)=P(x)P(y|x),P(y)=\sum_X P(xy)$,根据题目所给的数据得

P(y)=[7/12　5/12]

$$P(x|y)=\begin{pmatrix}6/7 & 3/5\\ 1/7 & 2/5\end{pmatrix}$$

又 $H(X)=-\sum_X P(x)\log P(x)\approx 0.811$　比特/符号

$$\begin{aligned}&H(X|Y)=-\sum_X\sum_Y P(x)P(x|y)\log P(x|y)=\\&[-3/4\times 2/3\log 2/3-1/4\times 1/3\log 1/3-3/4\times 1/3\log 1/3-1/4\times 2/3\log 2/3]\\&=-2/3\log 2/3-1/3\log 1/3\\&\approx 0.39+0.528\approx 0.918\end{aligned}$$

所以　$I(X;Y)=H(X)-H(X|Y)\approx 0.062$　比特/符号

(2)　此信道为二元对称信道，所以信道容量

$C=1-H(p)=1-H(2/3)=0.082$　比特/符号

根据二元对称信道的性质可知，输入符号为等概分布，即 P(0)=P(1)=1/2 时信道的信息传输率才能达到这个信道的容量值。

5．14　（1）由 $P(y)=\sum_X P(xy)$,得

P(y)=[1/2　1/4+1/4a　1/4-1/4a]

所以 $H(Y)=-\sum_{i=1}^{3}P(y_i)\log P(y_i)=1/2-(1/4+1/4a)\log(1/4+1/4a)-$
$(1/4-1/4a)\log(1/4-1/4a),$

$$H(Y|X)=-\sum_X\sum_Y P(x)P(y|x)\log P(y|x)=a(1/2\log 2+1/2\log 2)$$

（2）$+(1-a)(1/2\log 2+1/4\log 4)+(1-a)1/4\log 4$
$=3/2-1/2a$比特/符号

(3) $C=\begin{array}{l}H(Y)-H(Y|X)=-1+1/2a-1/4(1+a)\log(1/4+1/4a)-\\1/4(1-a)\log(1/4-1/4a)\end{array}$

6.1 (1) 收到传真的概率为 8/(4+8+3+1)*2/(7+1+2)=1/10

I=-log1/10=3.3 比特

（2）可采取压缩编码，安最佳编码原则编码等措施

（3）编码时码长尽可能长，这样根据香浓第二定理，总存在一种编码，只要码长足够长，总存在一种编码，是错误概率任意小。最好结合实际分析如何克服随机，突发干扰。

（4）C=Blog(1+S/N)=2.048log(1+$10^{1.2}$)=8.34Mbps，不失真条件下，该信道允许最大信息传输速率为 8.34Mbps。

6.2 （1）$h(x) = -\int p(x)\log p(x)dx = 1/2\log_2(2\pi e\sigma^2)$ 比特/样值

（2）对样值进行 256 级量化，当其服从均匀分布时，信源有最大熵，H=log256=8 比特/符号

（3）$f_s = 120KHz - 12KHz = 108KHz$

$B = 8f_s/2 = 432KHz$

所以 $C = B\log_2(1+S/N) = 4.31M$。

（4）S/N=36dB, C=5.17Mbps

所以 $S_c = (5.17-4.31)/4.31 = 20\%$。

6.3 (1) $h(x) = 1/2\log_2(2\pi e\sigma^2)$ 比特/样值

（2） 冗余度=$\dfrac{8\times 8K - 8.55K}{8\times 8K}\times 100\% = 86.6\%$

（3）$C = B\log_2(1+S/N)$ 其中 C=9.6K B=1.2288*2Mbps,

得 S/N=-25.7dB

(4) $C = B\log_2(1+S/N)$=2.4576$\log_2(1+10^{0.3}) = 3.88Mbps$

6.4 由于 P(x)=1/2=$\dfrac{1}{1-(-1)}$,所以电压为 1V~(-1)V 上的均匀分布，

又 $n = 2\varpi_0 T'$,所以 10=2ϖ_0，ϖ_0=5

h_t=2ϖ_0*（1/2）lb(4Ps)= $\varpi_0$lb(4*1)=2ϖ_0=10 bit/s

6.5

$$h_p(x) = -\int_{-1}^{1} p(x)\ln\ p(x)dx$$
$$= -\int_{-1}^{1}(1-|x|)\ln(1-|x|)dx$$
$$= -2\int_{-}^{1}(1-x)\ln(1-x)dx$$

又$n = 2\varpi_0 T'$,所以 10=2ϖ_0，ϖ_0=5

所以 $h_t = 2\varpi_0 h_p(x) = -20\int_0^1 (1-x)\ln(1-x)dx$

6.6

$$h(x) = -\int_0^2 p(x)\ln p(x)dx$$
$$= -\int_0^2 kx\ln(kx)dx$$

6.7 $C = B\log_2(1+S/N) = B\log_2(1+10^3) = 30\times 30\times 10^6 \times \log_2 10 = B*9.97$

所以 B=$3\times 10^7 Hz$.

6.8 (1)$C = \log_2 64\times \log_2 16\times 5\times 10^5 \times 25 = 6\times 10^8 bit$

(2)又 $C = B\log_2(1+S/N)$

而 $10\log_{10}\frac{S}{N} = 30dB$，

所以 S/N=10^3,

所以 $C = B\log_2(1+10^3)$ =9.97B

B=$6\times 10^7 Hz$

6.9 $C = B\log_2(1+S/N)$

所以 $5.6 = 4\log_2(1+\frac{P}{N}) = 4(1+\frac{P}{n_0 B})$

所以 P=$3.2\times 10^{-5} W$.

6.10 $C = B\log_2(1+S/N) = \frac{S}{n_0}\frac{n_0 B}{S}\log_2(1+\frac{S}{n_0 B})$

所以 $\lim_{B->\infty} C = \lim_{B->\infty}[\frac{n_0 B}{S}\log_2(1+\frac{S}{n_0 B})](\frac{S}{n_0})$ （2）

利用关系式 $\lim_{x->0} 1/x\log_2(1+x) = \log_2 e \approx 1.44$，

所以式（2）变为 $\lim_{B->\infty} C = \frac{S}{n_0}\log_2 e \approx 1.44\frac{S}{n_0}$，为一常量。

6.11 $H(X) = -\int_{-\pi/2}^{\pi/2} A\cos x\ln A\cos x dx$

$$=-A\ln A\int_{-\pi/2}^{\pi/2}\cos xdx-\int_{-\pi/2}^{\pi/2}A\cos x\ln\cos xdx$$

再由逐步分布积分得　H(X)=-2AlnA-2Aln2+2A.

因为 $\int_{-\pi/2}^{\pi/2}p(x)dx=1$，所以 2A=1　A=1/2

所以 H(X)=1　奈特/自由度

6.12　（1）$H(X)=-\int_0^a p(x)\log p(x)dx$

$$=-\int_0^a \mathrm{b}\,x^2\log bx^2dx$$

$$=\text{-logb}\int_0^a \text{p(x)dx-2b}\int_0^a x^2\log xdx$$

$$=\frac{2ba^3}{9}\log e-\frac{2ba^3}{3}\log a-\log b$$

因为 $\int_0^a$ p(x)dx=1，所以 b=$1/8\dfrac{3}{a^3}$。

故 H(X)=2/3loge+loga-log3

(2)　若 Y=X+A，则 $\dfrac{dX}{dY}=1$，所以 H(Y)=2/3loge+loga-log3

(3)　若 Y=2X，则 $\dfrac{dX}{dY}=1/2$，所以 H(Y)=H(X)-log1/2=2/3loge+loga-log3/2。

6.13　$C=B\log_2(1+S/n_0B)=6.5\times10^6\log_2(1+45.5/6.5)=1.95\times10^7 bit/s$

6.14　$C=B\log_2(1+S/N)$

(1) $C=10^6\times\log_2(1+10)=3.46\times10^6 bit/s$

(2) $10^6\times\log_2(1+10)=B\log_2(1+5)$　所以 B=$1.34\times10^6 Hz$

(3) $10^6\times\log_2(1+10)=0.5\times10^6\log_2(1+S/N)$　所以 S/N=120

第七章 习题

1. 设某二址接入信道，输入X_1, X_2和输出$\mathbf{Y}$的条件概率为$P(\mathbf{Y}/X_1X_2)$，其值是：

$p\,(0/00) = 1-\varepsilon$ $\quad p\,(0/01) = 1/2$ $\quad p\,(0/10) = 1/2$ $\quad p\,(0/11) = \varepsilon$

$p\,(1/00) = \varepsilon$ $\quad p\,(1/01) = 1/2$ $\quad p\,(1/10) = 1/2$ $\quad p\,(1/11) = 1-\varepsilon$

其中$\varepsilon<1/2$，试求其容量界限。

2. 设某广播信道，其输入X和输出Y_1、Y_2之间的条件概率$P(Y_1/X)$和$P(Y_2/X)$的具体值是：

$$p(Y_1/X):\ p(0/0)=1-\varepsilon_1 \quad p(1/0)=\varepsilon_1 \quad p(0/1)=\varepsilon_1 \quad p(1/1)=1-\varepsilon_1$$

$$p(Y_2/X):\ p(0/0)=1-\varepsilon_2 \quad p(1/0)=\varepsilon_2 \quad p(0/1)=\varepsilon_2 \quad p(1/1)=1-\varepsilon_2$$

其中$\varepsilon_1<1/2$, $\varepsilon_2<1/2$，试求其容量界限。

3. 计算图 7.12 中二址接入信道的容量。

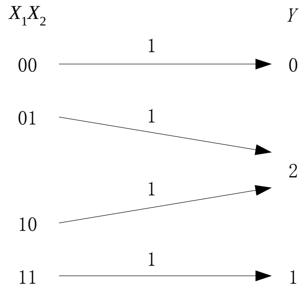


图 7.16

第 8 章 习题

1. 设输入符号表与输出符号表为 **X=Y={0, 1, 2, 3}**，且输入信号的分布为

$$p(X=i)=1/4,\ i=0,1,2,3$$

设失真矩阵为

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

求 $D_{\max}$ 和 $D_{\min}$ 及 $R(D_{\max})$。

$$\begin{bmatrix}\mathbf{X}\\P(\mathbf{X})\end{bmatrix}=\begin{bmatrix}0&1&2&3\\1/4&1/4&1/4&1/4\end{bmatrix}$$

$$D_{\min}=\sum_{i=1}^{r}p(a_i)\cdot\left\{\min_j d(a_i,b_j)\right\}$$

$$D_{\max}=\min_j\left\{\sum_{i=1}^{r}p(a_i)\cdot d(a_i,b_j)\right\}$$

$$[D]=\begin{bmatrix}0&1&1&1\\1&0&1&1\\1&1&0&1\\1&1&1&0\end{bmatrix}$$

$$D_{\min}=0$$

$$D_{\max}=\min\left\{\frac{3}{4},\frac{3}{4},\frac{3}{4},\frac{3}{4}\right\}=\frac{3}{4}$$

$$R(D_{\max})=0$$

2. 设无记忆信源 $\begin{pmatrix}\mathbf{X}\\p(\mathbf{X})\end{pmatrix}=\begin{pmatrix}-1&0&1\\1/3&1/3&1/3\end{pmatrix}$，接收符号 **$A_Y$={1/2, 1/2}**，失真矩阵 $D=\begin{pmatrix}1&2\\1&1\\2&1\end{pmatrix}$。

试求：$D_{\max}$和$D_{\min}$及达到$D_{\max}$和$D_{\min}$时的转移概率矩阵。

$$\begin{bmatrix}\mathbf{X}\\P(\mathbf{X})\end{bmatrix}=\begin{bmatrix}-1&0&1\\1/3&1/3&1/3\end{bmatrix}$$

$$[D]=\begin{bmatrix}1&2\\1&1\\2&1\end{bmatrix}$$

$$D_{\min}=1,\qquad D_{\max}=\min\left\{\frac{4}{3},\frac{4}{3}\right\}=\frac{4}{3}$$

在 $D_{\min}$ 时，

由于 $\begin{cases}\sum_{j\in J_i}p(b_j|a_i)=1\\ p(b_j|a_i),\ \ j\notin J_i\end{cases}$，所以

$$[P]=\begin{bmatrix}1 & 0\\ \frac{1}{2} & \frac{1}{2}\\ 0 & 1\end{bmatrix}$$

在$D_{\max}$时，

由于$p(b_j|a_i)=P(b_j)$，所以

$$[P]=\begin{bmatrix}1 & 0\\ 1 & 0\\ 1 & 0\end{bmatrix}$$

3.　三元信源的概率分别为$p(0)=0.4, p(1)=0.4, p(2)=0.2$，失真函数$d_{ij}$为：当$i=j$时，$d_{ij}=0$；当$i\neq j$时，$d_{ij}=1\ (i,j=0,1,2)$，求信息率失真函数$R(D)$。

$$\begin{bmatrix}\mathbf{X}\\ P(\mathbf{X})\end{bmatrix}=\begin{bmatrix}0 & 1 & 2\\ 0.4 & 0.4 & 0.2\end{bmatrix}$$

$$[D]=\begin{bmatrix}0 & 1 & 1\\ 1 & 0 & 1\\ 1 & 1 & 0\end{bmatrix}$$

$D_{\min}=0$，$R(0)=H(\mathbf{X})=\frac{2}{5}lb\frac{5}{2}+\frac{2}{5}lb\frac{5}{2}+\frac{1}{5}lb5=lb5-0.8\approx 1.52$

$D_{\max}=min\{0.6, 0.6, 0.8\}=0.6$

$R(D_{\max})=0$

由定义知：$R(D)=\min\limits_{P(b_j/a_i)\in B_D}\{I(\mathbf{X};\mathbf{Y})\}$，$I(\mathbf{X};\mathbf{Y})=H(\mathbf{X})-H(\mathbf{X}\mid\mathbf{Y})$

平均失真度一定与试验信道的平均错误概率P_e有关，即

$$\overline{D}=\sum_{i=1}^{r}\sum_{j=1}^{s}P(a_i)P(b_j/a_i)d(a_i,b_j)$$

$$=\sum_{i\neq j}^{s}P(a_i)P(b_j/a_i)=P_e$$

根据保真度准则，应有$P_e\leq D$

根据 Fano 不等式

$H(\mathbf{X}/\mathbf{Y})\leq H(P_e)+P_e\log(r-1)$

$\Rightarrow H(\mathbf{X}\mid\mathbf{Y})\leq H(P_e)+P_e lb2$

$\Rightarrow H(\mathbf{X}\mid\mathbf{Y})\leq H(P_e)+P_e\leq H(D)+D$

$\therefore R(D)=H(\mathbf{X})-H(D)-D$

$=lb5-0.8-H(D)-D$

$$R(D)=\begin{cases}lb5-0.8-D-H(D) & 0\leq \mathrm{D}\leq 0.6\\ 0 & \mathrm{D}>0.6\end{cases}$$

4.　设有一连续信源，其均值为 0，方差为$\sigma_X{}^2$，熵为 $H(\mathbf{X})$，定义失真函数为"平方误差"失真，即$d(x,y)=(x-y)^2$。证明其率失真函数满足下列关系式：

$$H(\mathbf{X})-\frac{1}{2}\log 2\pi e D\leq R(D)\leq\frac{1}{2}\log\frac{\sigma_{\mathbf{X}}^2}{D}$$

当输入信源为高斯分布时等号成立。

证明：

（1）　证明上界：

$$R(D) \geq H(\mathbf{X}) - \frac{1}{2}\log 2\pi e D$$

连续信源R(D)函数是在

$$\begin{cases} p(x \mid y) \geq 0 \\ \int_{-\infty}^{\infty} p(x \mid y) dx = 1 \\ \overline{D} = \int\int_{-\infty}^{\infty} p(x) p(x \mid y) d(x,y) dxdy = D \end{cases}$$

约束条件下，求平均互信息：

$$I(\mathbf{X};\mathbf{Y}) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} p(x) p(x \mid y) lb \frac{p(x \mid y)}{p(x)} dxdy$$

引入参量S和待定函数$\lambda(x)$。在失真不超过D时，$I(\mathbf{X};\mathbf{Y})$为下确界的试验信道满足

$$\begin{cases} p_0(x \mid y) = p_0(y)\lambda(x) e^{Sd(x,y)} \\ \int_{-\infty}^{\infty} \lambda(x) p(x) e^{Sd(x,y)} dx = 1 \\ \lambda(x) = \left[\int_{-\infty}^{\infty} p_0(y) e^{Sd(x,y)} dy\right]^{-1} \end{cases}$$

$$D(s) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} p(x) p_0(y) \lambda(x) e^{Sd(x,y)} d(x,y) dxdy$$

$$R(S) = SD(S) + \int_{-\infty}^{\infty} p(x) lb \lambda(x) dx$$

由泛函分析中的变分法求$I(\mathbf{X};\mathbf{Y})$的条件极值

令$x - y = \theta$，$d(x,y) = d(\theta) = \theta^2$

由于以上规定了下确界，则

$$\int_{-\infty}^{\infty} \lambda(x) p(x) e^{Sd(x,y)} dx \leq 1 \qquad (1)$$

设集合

$$\Lambda_s = \left\{\lambda(x) : \int_{-\infty}^{\infty} \lambda(x) p(x) e^{Sd(x,y)} dx \leq 1, 任意y\right\}$$

则有 $R(D) = \sup_{s \leq 0, \lambda(x) \in \Lambda_s} \left[SD(S) + \int_{-\infty}^{\infty} p(x) lb \lambda(x) dx\right]$ （2）

令$\lambda(x) = \dfrac{K(S)}{p(x)}$

其中$K(S) = \left[\int_{-\infty}^{\infty} e^{Sd(\theta)} d\theta\right]^{-1}$

由（1）得$K(S) \cdot \int_{-\infty}^{\infty} e^{Sd(x,y)} dx \leq 1$

即$K(S) \cdot \int_{-\infty}^{\infty} e^{Sd(\theta)} d\theta \leq 1$

当$d(\theta) = \theta^2$时，且$S < 0$，

得$\int_{-\infty}^{\infty} e^{S\theta^2} d\theta = 2\int_{-\infty}^{\infty} e^{S\theta^2} d\theta = \sqrt{\frac{\pi}{-S}} < \infty$

由（2）（3）两式，有

$$
\begin{aligned}
R(D) &\geq SD + \int_{-\infty}^{\infty} p(x) lb \frac{K(S)}{p(x)} dx \\
&= SD + \int_{-\infty}^{\infty} p(x) lb \frac{1}{p(x)} dx - \int_{-\infty}^{\infty} p(x) lb \frac{1}{K(S)} dx \\
&= SD + H(\mathbf{X}) - \int_{-\infty}^{\infty} p(x) \left[lb \int_{-\infty}^{\infty} e^{Sd(\theta)} d\theta \right] dx \\
&= SD + H(\mathbf{X}) - lb \int_{-\infty}^{\infty} e^{Sd(\theta)} d\theta
\end{aligned} \tag{4}
$$

由对数得换底公式，有

$$
\ln 2 \cdot R(D) \geq SD + H(\mathbf{X}) - \ln \int_{-\infty}^{\infty} e^{Sd(\theta)} d\theta = R \tag{5}
$$

若要（1）式等号成立，则等效于（5）式等号成立。

$$
R' = D - \int_{-\infty}^{\infty} \frac{e^{Sd(\theta)}}{\int_{-\infty}^{\infty} e^{Sd(\theta)} d\theta} d(\theta) d\theta
$$

令 $g_S(\theta) = \dfrac{e^{Sd(\theta)}}{\int_{-\infty}^{\infty} e^{Sd(\theta)} d\theta}$

则 $R' = D - \int_{-\infty}^{\infty} g_S(\theta) d(\theta) d\theta$

然后再求二阶导数，得

$$
\begin{aligned}
R'' &= -\int_{-\infty}^{\infty} g_S(\theta) d^2(\theta) d\theta + \left[\int_{-\infty}^{\infty} g_S(\theta) d(\theta) d\theta \right]^2 \\
&= -\left\{ \mathrm{E}\left[d^2(\theta)\right] - \mathrm{E}^2\left[d(\theta)\right] \right\}
\end{aligned}
$$

由于 $g_S(\theta)$ 是 $d(\theta)$ 得概率密度函数

且 $\int_{-\infty}^{\infty} g_S(\theta) d\theta = \dfrac{\int_{-\infty}^{\infty} e^{Sd(\theta)} d\theta}{\int_{-\infty}^{\infty} e^{Sd(\theta)} d\theta} = 1$

所以 $R'' \leq 0$，即（5）式右边为上凸函数，在 $R' = 0$ 的 S 上确极大值，有

$$
D = \int_{-\infty}^{\infty} g_S(\theta) d(\theta) d\theta
$$

代入 $d(\theta) = \theta^2$ 得

$$
g_S(\theta) = \sqrt{\frac{-S}{\pi}} e^{S\theta^2}
$$

$$
D = \int_{-\infty}^{\infty} \sqrt{\frac{-S}{\pi}} \theta^2 e^{S\theta^2} d\theta = -\frac{1}{2S} \tag{6}
$$

由式（5）得

$$
\begin{aligned}
\ln 2 \cdot R(D) &\geq -\tfrac{1}{2} + H(\mathbf{X}) - \ln \int_{-\infty}^{\infty} e^{S\theta^2} d\theta \\
&= H(\mathbf{X}) - \tfrac{1}{2} \ln e - \ln \sqrt{\tfrac{\pi}{-S}} \\
&= H(\mathbf{X}) - \tfrac{1}{2} \ln e - \tfrac{1}{2} \ln 2D\pi \\
&= H(\mathbf{X}) - \tfrac{1}{2} \ln 2\pi e D
\end{aligned}
$$

即 $R(D) \geq= H(\mathbf{X}) - \tfrac{1}{2} \ln 2\pi e D$

（2） 证明上界$R(D)\le\frac{1}{2}\log\frac{\sigma_{\mathrm{X}}^2}{D}$

设信道的传递函数的概率为：

$$p'(y\mid x)=\frac{1}{\sqrt{2\pi\beta D}}\exp\left[-\frac{1}{2\beta D}(y-\beta x)^2\right]$$

它是已知$\mathbf{X}=x$时y的概率分布，即均值为βx，方差为βD的高斯分布，其中$\beta=1-\frac{D}{\delta^2}$。

$$\begin{aligned}
\overline{D}&=\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}p(x)p'(y\mid x)d(x,y)dxdy\\
&=\int_{-\infty}^{\infty}p(x)dx\int_{-\infty}^{\infty}(y-x)^2p'(y\mid x)dy\\
&=\int_{-\infty}^{\infty}p(x)dx\left\{\int_{-\infty}^{\infty}\left[(y-\beta x)^2-2xy(1-\beta)+x^2\left(1-\beta^2\right)\right]p'(y\mid x)dy\right\}\\
&=\int_{-\infty}^{\infty}p(x)dx\left\{\begin{array}{l}(y-\beta x)^2\int_{-\infty}^{\infty}p'(y\mid x)dy-2xy(1-\beta)\int_{-\infty}^{\infty}p'(y\mid x)dy\\+x^2\left(1-\beta^2\right)\int_{-\infty}^{\infty}p'(y\mid x)dy\end{array}\right\}\\
&=\int_{-\infty}^{\infty}\left\{\beta D-2x(1-\beta)\beta x+x^2\left(1-\beta^2\right)\right\}p(x)dx\\
&=\int_{-\infty}^{\infty}\left[\beta D+(1-\beta)^2x^2\right]p(x)dx\\
&=\beta D+(1-\beta)^2\int_{-\infty}^{\infty}x^2p(x)dx\\
&=\beta D+(1-\beta)^2\sigma_X^2\\
&=D
\end{aligned}$$

设$B_D=\left\{p(y\mid x):\overline{D}\le D\right\}$， $p'(y\mid x)\in B_D$

由于$R(D)=\underset{p(x\mid y)\in B_D}{Inf}\left\{I(\mathbf{X};\mathbf{Y})\right\}$

所以$R(D)\le I'(\mathbf{X};\mathbf{Y})$

$$\begin{aligned}
I(\mathbf{X};\mathbf{Y})&=H(\mathbf{Y})-H(\mathbf{Y}\mid\mathbf{X})\\
&=H(\mathbf{Y})-\tfrac{1}{2}lb2\pi e\beta D
\end{aligned}$$

输出信号$\mathbf{Y}=\beta(\mathbf{X}+\mathbf{Z})$，

$\mathrm{E}\{\mathbf{Y}\}=\beta\{\mathrm{E}(\mathbf{X})+\mathrm{E}(\mathbf{Z})\}=0$

$\mathrm{E}\left\{\mathbf{Y}^2\right\}=\beta^2\left\{\mathrm{E}\left(\mathbf{X}^2\right)+\mathrm{E}\left(\mathbf{Z}^2\right)\right\}=\beta^2\sigma_X^2+\beta D=\sigma_X^2-D$

于是$\mathbf{Y}$时均值为零，方差为$\left(\sigma_X^2-D\right)$的随即变量。

当方差受限时，高斯随即变量的差熵最大，有

$H(\mathbf{Y})\le\frac{1}{2}lb2\pi e\left(\sigma_X^2-D\right)$

$$\begin{aligned}
I(\mathbf{X};\mathbf{Y})&\le\tfrac{1}{2}lb2\pi e\left(\sigma_X^2-D\right)-\tfrac{1}{2}lb2\pi e\beta D\\
&=\frac{1}{2}lb\frac{\left(\sigma_X^2-D\right)}{\beta D}=\frac{1}{2}lb\frac{\sigma_X^2}{D}
\end{aligned}$$

$$R(D)\le I'(\mathbf{X};\mathbf{Y})\le\frac{1}{2}lb\frac{\sigma_X^2}{D}$$

当且仅当$p(x)$是高斯分布时，上式等号成立。

综上所述，$H(\mathbf{X})-\frac{1}{2}\log 2\pi eD \le R(D) \le \frac{1}{2}\log\frac{\sigma_{\mathbf{X}}^2}{D}$

5. 随机变量 X 服从对称指数分布 $p(x)=\frac{a}{2}e^{-a|x|}$，失真函数为 $d(x,y)=|x-y|$，求信源的 $R(D)$。

$$p_X(x)=\frac{a}{2}e^{-a|x|}\text{，}\ d(x,y)=|x-y|$$

令 $\theta=x-y$，得 $d(\theta)=|\theta|$

且 $g_S(\theta)=\frac{e^{Sd(\theta)}}{\int_{-\infty}^{\infty}e^{Sd(\theta)}d\theta}=\frac{e^{S|\theta|}}{\int_{-\infty}^{\infty}e^{S|\theta|}d\theta}$

$$\int_{-\infty}^{\infty}e^{S|\theta|}d\theta=2\int_0^{\infty}e^{S|\theta|}d\theta=\frac{2}{|S|}$$

得 $g_S(\theta)=\frac{|S|}{2}e^{S|\theta|}$

$$\begin{aligned}D&=\int_{-\infty}^{\infty}g_S(\theta)d(\theta)d\theta\\&=\frac{|S|}{2}\int_{-\infty}^{\infty}|\theta|e^{S|\theta|}d\theta\\&=\frac{|S|}{2}\cdot 2\int_0^{\infty}|\theta|e^{S|\theta|}d\theta\\&=\frac{|S|}{2}\cdot 2\cdot\frac{1}{|S|^2}=\frac{1}{|S|}\end{aligned}$$

对 $g_S(\theta)$ 进行傅立叶变换

$$\begin{aligned}G_S(\omega)&=\int_{-\infty}^{\infty}g_S(\theta)e^{-j\omega\theta}d\theta\\&=\frac{S^2}{S^2+\omega^2}\end{aligned}$$

$$\begin{aligned}Q(\omega)&=\frac{S^2+\omega^2}{S^2}P(\omega)\\&=P(\omega)+\frac{\omega^2}{S^2}P(\omega)\end{aligned}$$

$$p_Y(y)=\frac{1}{2\pi}\int_{-\infty}^{\infty}Q(\omega)e^{-j\omega y}d\omega$$

$$p_Y(y)=p_X(x=y)-D^2p_X''(x=y)$$

$$\therefore p_Y(y)=\frac{a}{2}e^{-a|y|}-\frac{a^3}{2}D^2e^{-a|y|}$$

$$=\left(1-a^2D^2\right)\frac{a}{2}e^{-a|y|}$$

由 $p_Y(y)\ge 0$，得 $D\le\frac{1}{a}$

$$D_{\max} = \underset{y}{Inf} \int_{-\infty}^{\infty} p_X(x) d(x,y) dx$$

且 $\quad = \underset{y}{Inf} \int_{-\infty}^{\infty} |x-y| \frac{a}{2} e^{-a|x|} dx$

$$= \frac{1}{a}$$

当 $0 \le D \le D_{\max} = \frac{1}{a}$ 时

$$R(D) = R_L(D) = H(\mathbf{X}) - H(g_S)$$

$$= lb\tfrac{2e}{a} - lb2eD$$

$$= -lbaD, \quad 0 \le D \le \frac{1}{a}$$

6.　设有平稳高斯信源 *X* (*t*)，其功率谱为 $G(f) = \begin{cases} A, & |f| \le F_1 \\ 0, & |f| > F_1 \end{cases}$**，失真度量取** $d(x,y) = (x-y)^2$**，容许的样值失真为 *D*。试求：**

（1）　信息率失真函数 *R(D)*；

（2）　用一独立加性高斯信道（带宽为 F_2**，限功率为 *P*，噪声的双边功率谱密度为** $\frac{N_0}{2}$**）来传送上述信源时，最小可能方差与** F_2 **的关系。**

（1）对于时间 连续的平稳高斯信源，当功率谱密度已知时，

$$R(D) = \frac{1}{4\pi} \int_{-\infty}^{\infty} max\{0, lb(-2SG(\omega))\} d\omega$$

$$R(D) = \frac{1}{2\pi} \int_{-\infty}^{\infty} \min\left\{-\frac{1}{2S}, G(\omega)\right\} d\omega$$

在本题中

$$R(D) = \frac{1}{2\pi} \int_{-\infty}^{\infty} \min\left\{-\frac{1}{2S}, G(\omega)\right\} d\omega$$

$$= \int_{-\infty}^{\infty} \min\left\{-\frac{1}{2S}, G(f)\right\} df$$

$$= \int_{-F_1}^{F_1} -\frac{1}{2S} df$$

$$= -\frac{F_1}{S} \qquad \left(\text{设A} > -\frac{1}{2\text{S}}\right)$$

即 $S = -\frac{F_1}{D}$

$$
\begin{aligned}
R(D) &= \frac{1}{4\pi}\int_{-\infty}^{\infty} max\{0, lb(-2SG(\omega))\}d\omega \\
&= \frac{1}{2}\int_{-\infty}^{\infty} max\{0, lb(-2SG(f))\}df \\
&= \frac{1}{2}\int_{-F_1}^{F_1} lb(-2SA)df \\
&= F_1 lb(-2SA) \\
&= F_1 lb\frac{2AF_1}{D} \quad \text{bit/s}
\end{aligned}
$$

$$0 \le D \le 2AF_1$$

（2）信道容量为$C = F_2 lb\left(1+\frac{P}{F_2 N_0}\right)$bit/s

由定理可知，当$C \ge R(D)$时，可以采用最佳编码，其硬气的错误小于等于 D。

取$R(D) = C$,求得最小均方误差 D。

$$F_1 lb\frac{2AF_1}{D} = F_2 lb\left(1+\frac{P}{F_2 N_0}\right)$$

$$\therefore D = 2F_1 A\left(1+\frac{P}{F_2 N_0}\right)^{-F_2/F_1}$$

令$\beta = F_2/F_1$，$\alpha = \frac{D}{F_1 N_0}$

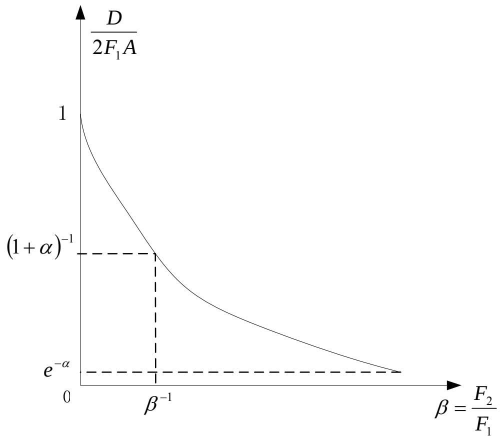
得$\frac{D}{2F_1 A} = \left(1+\frac{\alpha}{\beta}\right)^{-\beta}$

$\beta = 0$时，$\frac{D}{2F_1 A} = 1$

$\beta = 1$时，$\frac{D}{2F_1 A} = (1+\alpha)^{-1}$

$\beta \to \infty$时，由于$\lim_{\beta\to\infty}\left(1+\frac{\alpha}{\beta}\right)^{-\beta} = e^{-\alpha}$

所以$\frac{D}{2F_1 A} \to e^{-\alpha}$如下图：



7. 某工厂的产品合格率为 99%，废品率为 1%。若将一个合格产品作为废品处理，将损失 1 元；若将一个废品当作合格产品出厂，将损失 100 元；若将合格品出厂，废品报废，不造成损失。试分析质量管理中各种情况造成的损失及付出的代价。

解　根据题意有

信源空间：　好（合格）　　　废（废品）

P(好)=0.99　　　P(废)=0.01

选择失真函数为

d(好，好)=0　　　d(废，废)=0

d(好，废)=10　　　d(废，好)=100

失真矩阵为

$$[D]=\begin{array}{c} \\ 好 \\ 废 \end{array}\begin{array}{c} \begin{array}{cc} 好 & 废 \end{array} \\ \begin{bmatrix} 0 & 1 \\ 100 & 0 \end{bmatrix} \end{array}$$

可将产品检验分成如下 4 种情况：全部产品都当合格品，全部产品都当废品，完美的检验和允许出错的检验。下面分别进行讨论。

情况 1　全部产品不经检验而出厂——都当合格品。

把这一过程看作是一个“信道”，其“传递概率”为

P(好/好)=1　　P(废/好)=0　　P(好/废)=1　　P(废/废)=0

信道矩阵为

$$\Pi=\begin{array}{c} \\ 好 \\ 废 \end{array}\begin{array}{c} \begin{array}{cc} 好 & 废 \end{array} \\ \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \end{array}$$

这种情况的平均损失，即平均失真度，为

$$\overline{D}=\sum_i\sum_j P(a_i)P(b_j/a_i)d(a_i,b_j)$$

=P(好)·P(好/好) ·d(好,好)+ P(好)·P(废/好) ·d(好,废)

+P(废)·P(好/废话) ·d(废,好)+ P(废)·P(废/废) ·d(废, 废)

=0.01×1×100=1 元/个

情况 2　全部产品不经检验全部报废——都当废品

这时的信道传输概率为

P(好/好)=0　　P(废/好)=1　　P (好/废)=0　　P (废/废)=1

信道矩阵为

$$\Pi = \begin{array}{c c} & \begin{array}{cc} 好 & 废 \end{array} \\ \begin{array}{c} 好 \\ 废 \end{array} & \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \end{array}$$

平均失真度为

$$\overline{D} = \sum_i \sum_j P(a_i)P(b_j/a_i)d(a_i,b_j)$$

$=P(好)\cdot P(好/好)\cdot d(好,好)+P(好)\cdot P(废/好)\cdot d(好,废)$
$+P(废)\cdot P(好/废)\cdot d(废,好)+P(废)\cdot P(废/废)\cdot d(废,废)$
$=0.99\times1\times1=0.99$ 元/个

$$D_{\max} = 0.99$$

$$R(D_{\max}) = 0$$

全部报废造成损失小于全部出厂造成的损失。

情况 3　经过检验能正确无误地判断合格品和废品——完美的检验
这相当于无噪信道的情况，信道矩阵为

$$\Pi = \begin{array}{c c} & \begin{array}{cc} 好 & 废 \end{array} \\ \begin{array}{c} 好 \\ 废 \end{array} & \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{array}$$

平均失真度为

$$\overline{D} = 0$$

即这种情况不会另外造成损失。
情况 4 检测时允许有一定的错误——非完美的检验
设检验的正确率为 p，则信道的传输概率为

$P(好/好)$=p　　$P(废/好)$=1-p　　$P(好/废)$=1-p　　$P(废/废)$=p

信道矩阵为

$$\Pi = \begin{array}{c c} & \begin{array}{cc} 好 & 废 \end{array} \\ \begin{array}{c} 好 \\ 废 \end{array} & \begin{bmatrix} \mathrm{p} & 1-\mathrm{p} \\ 1-\mathrm{p} & \mathrm{p} \end{bmatrix} \end{array}$$

平均失真度为

$$\overline{D} = \sum_i \sum_j P(a_i)P(b_j/a_i)d(a_i,b_j)$$

$=P(好)\cdot P(废/好)\cdot d(好,废)+P(废)\cdot P(好/废)\cdot d(废,好)$
$=0.99\times(1-p)\times1+0.01\times p\times100 = 1.99(1-p)$元/个

8.　设输入符号表为 X= {0, 1 }，输出符号表为 Y={0, 1}。定义失真函数为：

$$\boldsymbol{d(0,0) = d(1,1) = 0}$$
$$\boldsymbol{d(0,1) = d(1,0) = 1}$$

试求失真矩阵[D]。

$$d(0,0) = d(1,1) = 0$$

$d(0,1)=d(1,0)=1$

$$[D]=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$$

9. 某二元信源 **X** 的信源空间为

$$[\mathbf{X}\cdot P]=\begin{cases}\mathbf{X}: & a_1,\ a_2\\ P(\mathbf{X}): & w,\ 1-w\end{cases}$$

其中 $w<1/2$，其失真矩阵为

$$[D]=\begin{bmatrix}0 & d\\ d & 0\end{bmatrix}$$

（1） 试求 $D_{\max}$ 和 $R(D_{\max})$；

（2） 试求 $D_{\min}$ 及 $R(D_{\min})$；

（3） 试求 $R(D)$；

（4） 写出取得 $R(D)$ 的试验信道的各传递概率；

（5） 当 $d=1$ 时，写出与试验信道相对应的反向试验信道的信道矩阵。

解：$\begin{bmatrix}\mathbf{X}\\ P(\mathbf{X})\end{bmatrix}=\begin{bmatrix}a_1 & a_2\\ \omega & 1-\omega\end{bmatrix}$

$$[D]=\begin{bmatrix}0 & d\\ d & 0\end{bmatrix}$$

（1）$D_{\max}=min\{d\omega,d(1-\omega)\}=d\omega$（因为 $\omega<1/2$）

$R(D_{\max})=0$

（2）$D_{\min}=0$

$R(D_{\min})=H(\mathbf{X})=-\omega lb\omega-(1-\omega)lb(1-\omega)=H(\omega)$

（3） 由于 $\sum_i \lambda_i P(x_i)e^{Sd_{ij}}=1$

令 $e^{Sd}=\beta$，则

$$[\omega\lambda_1,(1-\omega)\lambda_2]\begin{bmatrix}1 & \beta\\ \beta & 1\end{bmatrix}=[1,1]$$

得到 $\begin{bmatrix}\omega\lambda_1\\ (1-\omega)\lambda_2\end{bmatrix}=\begin{bmatrix}\dfrac{1}{1+\beta}\\ \dfrac{1}{1+\beta}\end{bmatrix}$

$$\begin{cases} \lambda_1 = \dfrac{1}{(1+\beta)\omega} \\ \lambda_2 = \dfrac{1}{(1+\beta)(1-\omega)} \end{cases}$$

$$\begin{cases} P(b_1) = \dfrac{1}{1-\beta}[\omega-(1-\omega)\beta] \\ P(b_2) = \dfrac{1}{1-\beta}[(1-\omega)-\omega\beta] \end{cases}$$

$$\begin{aligned} D(S) &= \sum_i \sum_j P(a_i)P(b_j)d(a_i,b_j)e^{Sd_{ij}} \\ &= d\omega\frac{[(1-\omega)-\omega\beta]}{1-\beta}\cdot\frac{\beta}{(1+\beta)\omega} + d(1+\omega)\frac{[\omega-(1-\omega)\beta]}{1-\beta}\cdot\frac{\beta}{(1+\beta)(1-\omega)} \\ &= \frac{d\beta}{1+\beta} = \frac{de^{Sd}}{1+e^{Sd}} \end{aligned}$$

$$R(S) = \frac{Sd\beta}{1+\beta} + H(\omega) - lb(1+\beta)$$

得到$\beta = e^{Sd} = \dfrac{D}{d-D}$

$$S = \frac{1}{d}\ln\frac{D}{d-D}$$

$$\begin{aligned} R(D) &= \frac{D}{d}\ln\frac{D}{d-D} + H(\omega) - \ln\frac{d}{d-D} \\ &= H(\omega) + \left[\frac{D}{d}\ln D - \frac{D}{d}\ln d - D - \ln d + \ln(d-D)\right] \\ &= H(\omega) + \left\{\frac{D}{d}\ln D - \left(1-\frac{D}{d}\right)\ln(d-D) - \left[\frac{D}{d} + \left(1-\frac{D}{d}\right)\right]\ln d\right\} \\ &= H(\omega) + \left[\frac{D}{d}\ln\frac{D}{d} + \left(1-\frac{D}{d}\right)\ln\left(1-\frac{D}{d}\right)\right] \\ &= H(\omega) - H\left(\frac{D}{d}\right) \end{aligned}$$

D=0 时，$R(0) = H(\omega)$

D=dω时，$R(d\omega) = 0$

所以$R(D)=\begin{cases} H(\omega)-H\left(\dfrac{D}{d}\right) & 0\le \mathrm{D}\le \mathrm{d}\omega \\ 0 & \mathrm{D}>\mathrm{d}\omega \end{cases}$

（4）$p(b_j \mid a_i)=p(b_j)\lambda_i e^{Sd_{ij}}$

$$p(b_1 \mid a_1)=p(b_1)\lambda_1 e^0=p(b_1)\lambda_1$$
$$=\frac{1}{1-\beta}[\omega-(1-\omega)\beta]\cdot\frac{1}{(1+\beta)\omega}$$
$$=\frac{[\omega-(1-\omega)\beta]}{(1-\beta^2)\omega}$$

$$p(b_1 \mid a_2)=p(b_1)\lambda_2 e^{Sd}=p(b_1)\lambda_2\beta$$
$$=\frac{1}{1-\beta}[\omega-(1-\omega)\beta]\cdot\frac{1}{(1+\beta)(1-\omega)}\cdot\beta$$
$$=\frac{[\omega-(1-\omega)\beta]}{(1-\beta^2)(1-\omega)}\cdot\beta$$

$$p(b_2 \mid a_1)=p(b_2)\lambda_1 e^{Sd}=p(b_2)\lambda_1\beta$$
$$=\frac{1}{1-\beta}[(1-\omega)-\omega\beta]\cdot\frac{1}{(1+\beta)\omega}\cdot\beta$$
$$=\frac{[(1-\omega)-\omega\beta]}{(1-\beta^2)\omega}\cdot\beta$$

$$p(b_2 \mid a_2)=p(b_2)\lambda_2 e^0=p(b_2)\lambda_2$$
$$=\frac{1}{1-\beta}[(1-\omega)-\omega\beta]\cdot\frac{1}{(1+\beta)(1-\omega)}$$
$$=\frac{[(1-\omega)-\omega\beta]}{(1-\beta^2)(1-\omega)}$$

（5）d=1 时，$\beta=\dfrac{D}{1-D}$

$\dfrac{1}{1+\beta}=1-D$，$\dfrac{\beta}{1+\beta}=D$

$$p(a_1 \mid b_1)=\frac{p(a_1)\cdot p(b_1 \mid a_1)}{p(b_1)}=\lambda_1 p(a_1)$$
$$=\frac{1}{(1+\beta)\omega}\cdot\omega=\frac{1}{(1+\beta)}=1-D$$

$$p(a_1 \mid b_2) = \frac{p(a_1)\cdot p(b_2 \mid a_1)}{p(b_2)} = \lambda_1 \beta p(a_1)$$

$$= \frac{1}{(1+\beta)\omega}\cdot \beta \cdot \omega = \frac{\beta}{(1+\beta)} = D$$

$$p(a_2 \mid b_1) = \frac{p(a_2)\cdot p(b_1 \mid a_2)}{p(b_1)} = \lambda_2 \beta p(a_2)$$

$$= \frac{1}{(1+\beta)(1-\omega)}\cdot \beta \cdot (1-\omega) = \frac{\beta}{(1+\beta)} = D$$

$$p(a_2 \mid b_2) = \frac{p(a_2)\cdot p(b_2 \mid a_2)}{p(b_2)} = \lambda_2 p(a_2)$$

$$= \frac{1}{(1+\beta)(1-\omega)}\cdot (1-\omega) = \frac{1}{(1+\beta)} = 1-D$$

第 9 章 习题

1. 对(2, 1), (3, 1), (4, 1), (5, 1)，讨论其纠检错能力，对用完备译码、不完备译码以及不完备译码＋ARQ 等方法译码，求译码错误概率。

解：

对(2, 1)码，若 d=1，能纠检错 0 个；若 d=2,能检 1 个错，纠 0 个错

对(3, 1)码，若 d=1，能纠检错 0 个；若 d=2,能检 1 个错，纠 0 个错；若 d=3，能检 2 个错，纠 1 个错

对(4, 1)码，若 d=1，能纠检错 0 个；若 d=2,能检 1 个错，纠 0 个错；若 d=3，能检 2 个错，纠 1 个错，若 d=4,能检 3 个错，纠 1 个错

对(5, 1)码，若 d=1，能纠检错 0 个；若 d=2,能检 1 个错，纠 0 个错；若 d=3，能检 2 个错，纠 1 个错；若 d=4,能检 3 个错，纠 1 个错；若 d=5,能检 4 个错，纠 2 个错

2. 为什么 d =2 的(n, n–1)码能检测奇数个错误？

解:

d=2，能检 1 个错，又因为(n, n–1)码是奇偶校验码，即对于

奇校验码：$C_{n-1} \oplus C_{n-2} \cdots \oplus C_0 = 0$

偶校验码：$C_{n-1} \oplus C_{n-2} \cdots \oplus C_0 = 1$

当出现一个错或者奇数个错时，在接收端

奇校验码：$C_{n-1} \oplus C_{n-2} \cdots \oplus C_0 = 1$

偶校验码：$C_{n-1} \oplus C_{n-2} \cdots \oplus C_0 = 0$

都能检测到错误，故 d =2 的(n, n–1)码能检测奇数个错误。

3. 设 **C** = {11100, 01001, 10010, 00111}是一个二元码，求码 **C** 的最小距离 d。

解：

d(11100, 01001)=3 d(11100, 10010)=3 d(11100, 00111)=4

d(01001, 10010)=4 d(01001, 00111)=3 d(10010, 00111)=3

故码 **C** 的最小距离 *d=3*

4．设 **C** = {00000000, 00001111, 00110011, 00111100}是一个二元码。

（1） 计算码 **C** 中所有码字之间的距离及最小距离；

（2） 在一个二元码中，如果把某一个码字中的 0 和 1 互换，即 0 换为 1，1 换为 0，所得的字称为此码字的补。所有码字的补构成的集合称为此码的补码。求码 **C** 的补码以及补码中所有码字之间的距离和最小距离，它们与（1）中的结果有什么关系？

（3） 把（2）中的结果推广到一般的二元码。

解：

（1） d(00000000, 00001111)=4 d(00000000, 00110011)=4

d(00000000, 00111100)=4 d(00001111, 00110011)=4

d(00001111, 00111100)=4 d(00110011,00111100)=4

故码 **C** 的最小距离 *d=4*

（2） 码 **C** 的补码是 {11111111, 11110000, 11001100, 11000011}

d(11111111, 11110000)=4 d(11111111, 11001100)=4

d(11111111, 11000011)=4 d(11110000, 11001100)=4

d(11110000, 11000011)=4 d(11001100, 11000011)=4

故 **C** 补码的最小距离 *d=4*

（3）推广到一般的二元码也有以上的结论

设码 **C** 中任意两码字的距离为 d, 即两码字有 d 位不同，n-d 位相同。变补后，仍有 d 位不同，n-d 位相同，所以任意两码字的距离不变，最小距离当然不变。

1. 设 p 是一个素数，

（1） 在 GF(p)上把 x^p-1 分解成不可约因式的乘积；

（2） 在 GF(p)上把 $x^{p-1}-1$ 分解成不可约因式的乘积。

2. 在 GF(3)上把 x^4-1 分解成不可约多项式的乘积，确定所有码长是 4 的三元循环码，并写出每一个码的生成矩阵和校验矩阵。

解：因 $x^4-1=$

3. 设在 GF(q)上 x^n-1 可分解成 t 个不同的不可约多项式的乘积，试问有多少个码长为 n 的 q 元循环码？

4. 设 **C** 是一个二元循环码，证明分量全为 1 的向量$(1\ 1\ \cdots\ 1)\in$ **C** 的充分必要条件是 **C** 包含一个重量为奇数的码字。

证：用反证法

5. 在 GF(2)上 x^7-1 能分解成不可约因式的乘积：

$$x^7-1=(x-1)(x^3+x+1)(x^3+x^2+1)$$

确定所有码长为 7 的循环码，并且准确描述这些码的特性。

解：由题知 n=7,k=6,4

(1)当 k=6 时　　g (x)= x-1

(2)当k=4 时　　g (x)= x^3+x+1 或x^3+x^2+1

可进一步写出 G 和 H

6. 请对任意一个 21-bit 的数据，例如使用自己的学号化成 2 进制数，高位补“0”或某些随机数）

（1） 给出 BCH (31,21) 码的码多项式；

（2）假设传输过程中错了一位（可以任意设定），请译码；

（3）假设传输过程中错了两位（可以任意设定），请译码；

（4）假设传输过程中错了三位（可以任意设定），请译码。

解：（1）我们可以任选一个 21-bit 的数据，假设所选数据为 020321，其二进制数表示为：

0 0010 0000 0011 0010 0001　　21 位码

查表可知（31，21）码的本原多项式为：

$$g(x) = x^{17} + x^9 + x^8 + x^5 + 1$$

输入多项式为：

$$u(x) = x^{17} + x^9 + x^8 + x^5 + 1$$

所以输出码多项式为：

$v(x) = u(x)\,g(x)$

$=(x^{17} + x^9 + x^8 + x^5 + 1)(x^{10} + x^9 + x^8 + x^6 + x^5 + x^3 + 1)$

$= x^{27} + x^{26} + x^{25} + x^{23} + x^{22} + x^{20} + x^{19} + x^{17} + x^{16} + x^{14} + x^{12} + x^8 + x^6 + x^3 + 1$

(2)假设接收到的多项式为：

$r(x) = x^{27} + x^{25} + x^{23} + x^{22} + x^{20} + x^{19} + x^{17} + x^{16} + x^{14} + x^{12} + x^8 + x^6 + x^3 + 1$

则可得：σ（x）$=\alpha^{26}x + 1$　即错误位置为 26，可以纠正。

(3) 假设接收到的多项式为：

$r(x) = x^{27} + x^{26} + x^{23} + x^{22} + x^{20} + x^{19} + x^{17} + x^{16} + x^{14} + x^{12} + x^8 + x^6 + 1$

则可得：σ（x）=（$\alpha^{25}x + 1$）（$\alpha^3 x + 1$）

所以：$\beta_1=\alpha^{-25}$　　$\beta_2=\alpha^{-3}$

即错误位置为x^3和x^{25}，可以纠正。

(4) 假设接收到的多项式为：

$r(x) = x^{27} + x^{26} + x^{25} + x^{19} + x^{17} + x^{16} + x^{14} + x^{12} + x^8 + x^6 + x^3 + 1$

出现了 3 个错误，接收端能检出错误，但无法纠正。

7. 已知GF(2^5)中元素的几种表示如表 11.8 所示，有关元素的最小多项式如下：

$$\phi_1(x) = x^5 + x^2 + 1,\ \phi_3(x) = \phi_1(x) + x^4 + x^3,$$

$$\phi_5(x) = \phi_3(x) + x^3 + x,\quad \phi_7(x) = \phi_5(x) + x^4 + x^3,$$

$$\phi_{11}(x) = \phi_7(x) + x^4 + x^2,\ \phi_{15}(x) = \phi_{11}(x) + x^4 + x\text{。}$$

现欲对上题信源编码输出进行扩展的 BCH(32, 16)信道编码再传送。

（1）对于消息(10001 11111 101010) 给出信道编码的输出码字；

（2）若接收矢量为(10001 11111 101010 0110 1001 0011 1101)，试判断是否有错，如只有一个错请纠正之，如有两个或三个错请说明纠正的方法。

表 11.8　GF(2^5)域元素的两种表示（本原多项式$p(x) = x^5 + x^2 + 1$）

1	00001	α^8	01101 11110	α^{16}	11011	α^{24}
α	00010	α^9	11010 11001	α^{17}	10011	α^{25}

α^2	00100	α^{10}	10001	α^{18}	00011	α^{26}	10111
α^3	01000	α^{11}	00111	α^{19}	00110	α^{27}	01011
α^4	10000	α^{12}	01110	α^{20}	01100	α^{28}	10110
α^5	00101	α^{13}	11100	α^{21}	11000	α^{29}	01001
α^6	01010	α^{14}	11101	α^{22}	10101	α^{30}	10010
α^7	10100	α^{15}	11111	α^{23}	01111	α^{31}	00001

解：由题知：m=5，$n=2^5-1=31$

扩展的BCH(31+L, K)码，则L=1 (即加了1为奇偶校验位)，K=16

（1）若可以纠1个错，则$g(x) = p(x) = x^5+x^2+1$

则编码输出为：$u(x)\,g(x) =$

（2）

8.　令 $g(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$ 是 (15, 5)循环码的生成多项式，

（1）　求出该码的校验多项式；

（2）　写出该码的系统码形式的 **G** 和 **H** 矩阵；

（3）　构造 k 级编码器。

解：由题可得：

$x^{10}=g(x)+x^8+x^5+x^4+x^2+x+1$

$x^{11}=x\,g(x)+x^9+x^6+x^5+x^3+x^2+x$

$x^{12}=x^2\,g(x)+x^{10}+x^7+x^6+x^4+x^3+x^2$

$\quad=(x^2+1)\,g(x)+x^8+x^7+x^6+x^5+x^3+x+1$

$x^{13}=(x^3+x)\,g(x)+x^9+x^8+x^7+x^6+x^4+x^2+x$

$x^{14}=(x^4+x^2)\,g(x)+x^{10}+x^9+x^8+x^7+x^5+x^3+x^2$

$\quad=(x^4+x^2+1)\,g(x)+x^9+x^7+x^4+x^3+x+1$

所以可得：

$bo(x)= x^8+x^5+x^4+x^2+x+1$

$b_1(x)= x^9+x^6+x^5+x^3+x^2+x$

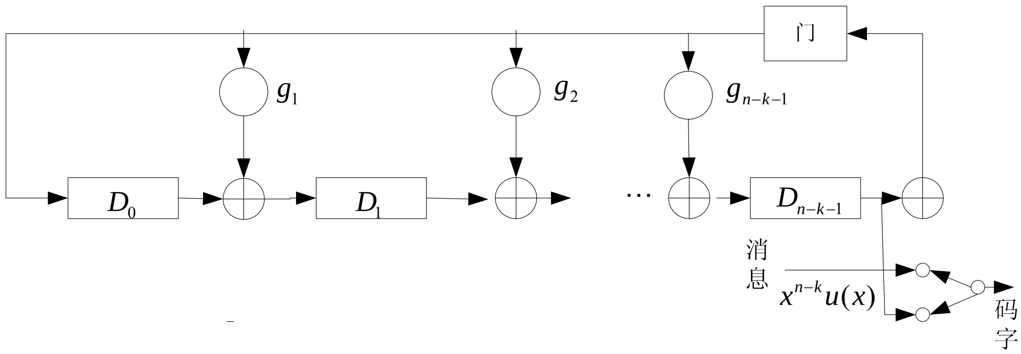
$b_2(x)= x^8+x^7+x^6+x^5+x^3+x+1$
$b_3(x)= x^9+x^8+x^7+x^6+x^4+x^2+x$
$b_4(x)= x^9+x^7+x^4+x^3+ x +1$

进而有：

$$G=\begin{bmatrix}100000100110111\\010001001101110\\001000111101011\\000101111010110\\000011010011011\end{bmatrix}$$

$$H=\begin{bmatrix}010111000000000\\101100100000000\\001110010000000\\011100001000000\\111000000100000\\100110000010000\\011010000001000\\110100000000100\\111110000000010\\101010000000001\\ \end{bmatrix}$$

K 级编码器为如下图：



9. 求GF(2^5)上以α, α^3为根的二进制循环码：

（1） 写出生成多项式 $g(x)$，确定码长 n 和信息位个数 k ；

（2） 写出该码系统码形式的 **G** 和 **H** 矩阵；

（3） 求出该码的 R 和最小距离。

解：（1）查表可得本原多项式为：$p(x)=x^5+x^2+1$

又$g(x)=LCM\{\Phi_1(x),\Phi_3(x)\}$

当$\beta_1=\alpha^-$ $\beta_2=\alpha^{-3}$

用 matlab 函数 gfminpol (1，5)和 gfminpol (3，5)

分别得：

$\Phi_1(x)=x^5+x^3+1$

$\Phi_3(x)=x^5+x^3+x^2+x+1$

所以$g(x)=\Phi_1(x)\,\Phi_3(x)=x^{10}+x^7+x^5+x^2+x+1$

所以$n=2^5-1=31$，$k=31-10=21$

（2）

同样由上题的方法可求出系统码形式的 G 和 H 矩阵

$x^{10}=g(x)+x^7+x^5+x^2+x+1$

$x^{11}=x\,g(x)+x^8+x^6+x^3+x^2+x$

……….

$X^{31}=$………

可进一步写出bo(x)……$b_{21}(x)$，从而写出G，H

G=

H=

（3）

10. 令n是$g(x)\,|\,(x^n-1)\,|$的最小正数。现用该$g(x)$生成位n的循环码，证明码的最小距离至少为 3。

11. 构造(15, 5, 7)码的译码器，它的生成多项式$g(x)=x^{10}+x^8+x^5+x^4+x^2+x+1$，该码能纠正 3 个错误。设用简单的捕错译码器译码。

（1）证明所有 2 个错误能被捕获；

（2）能捕获所有 3 个错误的图样吗？若不能，则有多少种 3 个错误图样不能被捕获；

（3）作出该码的简单捕获译码器。

12. 对 $m\ge 3, t<2^{m-1}$，存在有一个长为 2^m+1 纠 t 个错误的二进制本原 BCH 码吗？若有找出它的 $g(x)$。

习题

1．试画出 $k=3$，效率为 1/3，生成多项式如下所示的编码状态图、树状图和网格图：

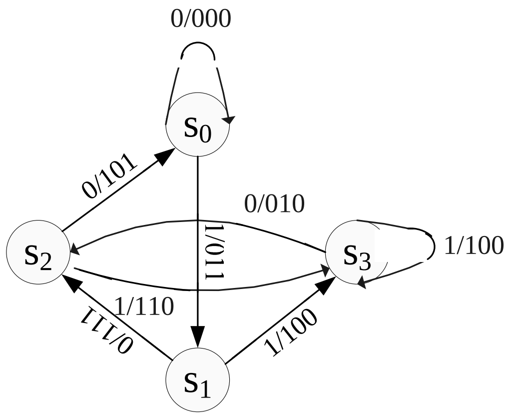
$$g_1(X)=X+X^2$$

$$g_2(X)=1+X$$

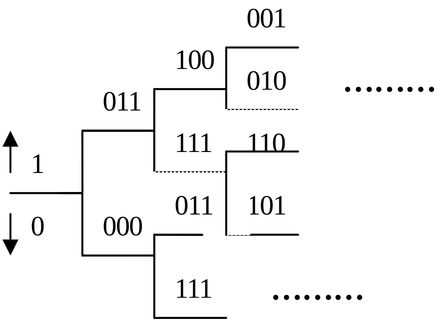
$$g_3(X)=1+X+X^2$$

解：$g_1(D)=D+D^2$，$g_2(D)=1+D$，$g_3(D)=1+D+D^2$

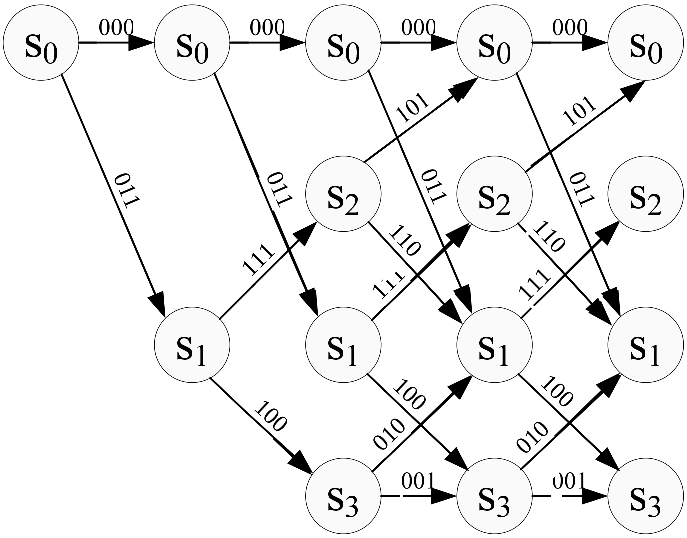
所以可得状态图如下：其中（s_0:00，s_1:01，s_2:10，s_3:11）



树状图如下：



网格图为：



2. 假定寻找从伦敦到维也纳坐船或坐火车的最快路径，图 12.25 给出了各种安排，各条分支上标注的是所需时间。采用维特比算法，找到从伦敦到维也纳的最快路线，解释如何应用该算法，需做哪些计算，以及该算法要求在存储器里保存什么信息。

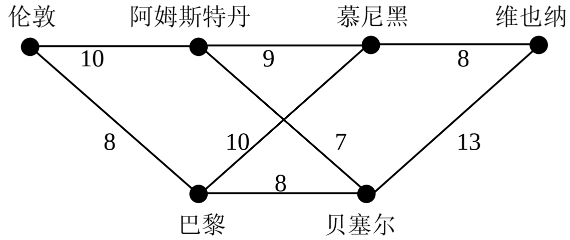


图 12.25

解：从伦敦到维也纳的最快路线为：

伦敦——巴黎——慕尼黑——维也纳

此算法需计算从伦敦到维也纳中间所可能经过的各节点离伦敦的时间，保留其中最短的，去除其它的。需要记录下各中间节点离伦敦的最短时间，其算法的实现就是 Dijkstra 算法。

3. 考虑图 12.26 中的卷积码。

（a）写出编码器的连接矢量和连接多项式。

（b）画出状态图、树状图和网格图。

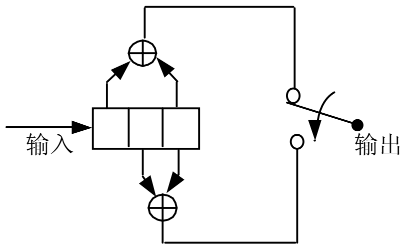
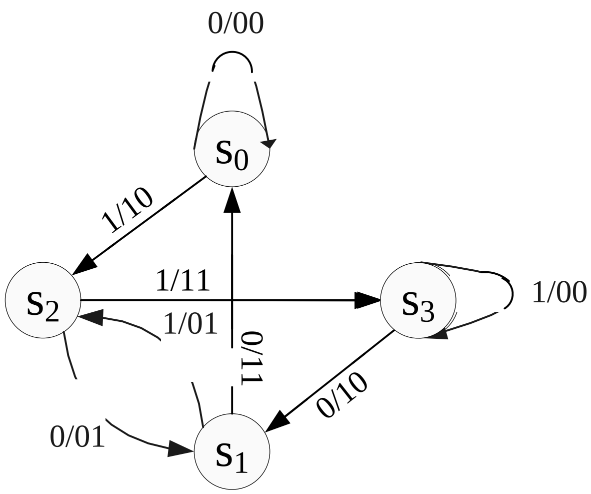


图 12.26

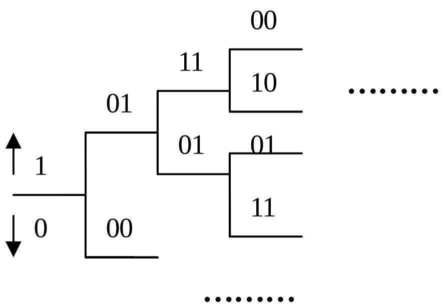
解：（1）由图可知：连接矢量为：$g^{(1)}=[1,0,1]$　　$g^{(2)}=[0,1,1]$

连接多项式为：$g^{(1)}$（D）= 1+D^2　　　$g^{(2)}$（D）=D+D^2

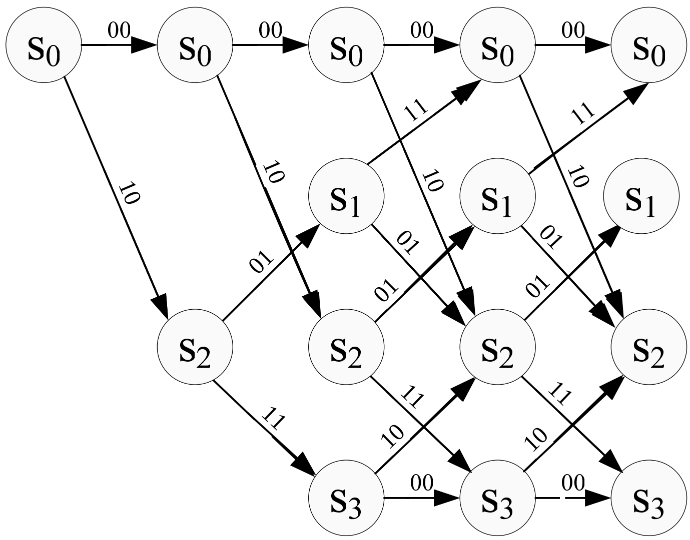
（2）状态图为：其中（s_0:00，s_1:01，s_2:10，s_3:11）


0/00
s_0
1/10
s_2
1/11
1/01
s_3
1/00
0/11
0/10
0/01
s_1

树状图为：


00
11
10
01
01
01
11
1
0
00
………
………

网格图为：



4.　下列码率为 1/2 的编码中哪些会引起灾难性错误传播？

（a）$g_1(X)=X^2$，　　$g_2(X)=1+X+X^3$

（b）$g_1(X)=1+X^2$，　　$g_2(X)=1+X^3$

（c）$g_1(X)=1+X+X^2$，　　$g_2(X)=1+X+X^3+X^4$

（d）$g_1(X)=1+X+X^3+X^4$，　　$g_2(X)=1+X^2+X^4$

（e）$g_1(X)=1+X^4+X^6+X^{10}$ ，$g_2(X)=1+X^3+X^4$

（f）$g_1(X)=1+X^3+X^4$，　　$g_2(X)=1+X+X^2+X^4$

解：会引起灾难性错误传播的有：

（b）有公因子（1＋x）

（c）有公因子（1＋x＋x^2）

（d）有公因子（1＋x＋x^2）

故此三个会引起会引起灾难性错误传播。

5.　不查表，使用功能强大的 PC 机，设计一个(2, 1, 2)卷积码。

6.　已知(2, 1, 3)码的子生成元$g^{(1,1)}=(1\ 1\ 0\ 1)$, $g^{(1,2)}=(1\ 1\ 1\ 0)$。

（1）　求出该码的$G(D)$和$H(D)$矩阵，以及G_∞和H_∞矩阵；

（2）　画出该码的编码器；

（3）　求出相应于信息序列 $M=(11001)$的码序列；

（4）　此码是否是系统码？

解：（１）因$g^{(1,1)}$（Ｄ）＝ １＋Ｄ＋Ｄ^3　　$g^{(1,2)}$（Ｄ）＝１＋Ｄ＋Ｄ^2
所以Ｇ（Ｄ）＝［１＋Ｄ＋Ｄ^3，１＋Ｄ＋Ｄ^2］
Ｈ（Ｄ）＝

（２）编码器如图：

（３）$v^{(1)}$＝（１１００１）＊（１１０１）
＝１０１１０１０１
$v^{(2)}$＝（１１００１）＊（１１１０）
＝１００１１１１０
交织得：ｖ＝（１１，００，１０，１１，０１，１１，０１，１０）
可知该码为非系统码。

7. 在图 12.16 所示的 Turbo 编码器中采用了两个 RSC 编码器。
（a）对此编码器进行扩展，使之包含有 M 个交织器。
（b）画出Turbo译码器的原理方框图，要求译码器采用由扩展生成的M组~~奇偶~~校验比特。

8. 设有一个 (3, 2, 3) 系统码的子生成元分别为：$g^{(1,3)}(D) = 1 + D^2 + D^3, g^{(2,3)}(D) = 1 + D + D^3$，问
（1）此码是恶性码吗？为什么？
（2）画出该码的编码器和对偶码的编码器；
（3）画出有 4 个分支长的树图；
（4）求出此码的最小距离d_m；
（5）求出此码的自由距离。

解：因$g^{(1,3)}(D) = 1 + D^2 + D^3$和$g^{(2,3)}(D) = 1 + D + D^3$

9. 已知有一个 (3, 1, 2) 码的子生成元是：$g^{(1,1)} = 1 + D, g^{(1,2)} = 1 + D^2$和 $g^{(1,3)} = 1 + D + D^2$。
（1）求出该码的 $G(D)$和 $H(D)$；

（2） 画出该码的编码电路；

（3） 该码是否是恶性码？找出有最小延迟前馈的逆矩阵$G^{-1}(D)$。

解：（１）$G(D)$＝［１＋D，１＋D ²，１＋D＋D ²］

H（D）＝

（２）该编码电路为：

（３）

10. Turbo 译码需要依靠外部信息的反馈。在 Turbo 译码器中采用的基本原则是避免反馈某一个译码段自身生成的译码段信息。试从概念上解释这个原则的正确性。

11. 设码率为 1/2 的 Turbo 码的生成矩阵分别为

4 状态编码器：

$$g(D)=\left[1,\frac{1+D+D^2}{1+D^2}\right]$$

8 状态编码器：

$$g(D)=\left[1,\frac{1+D+D^2+D^3}{1+D+D^2+D^3}\right]$$

16 状态编码器：

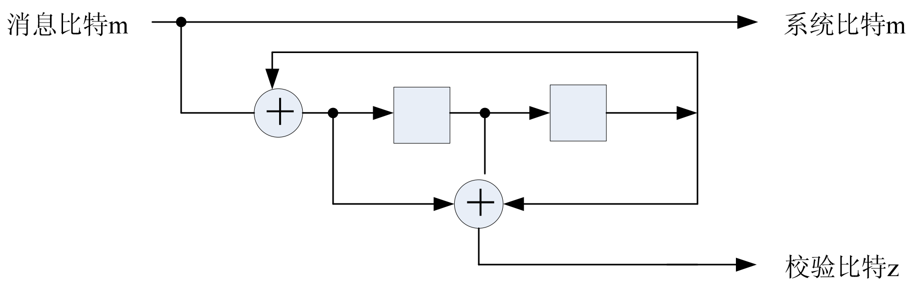
$$g(D)=\left[1,\frac{1+D^4}{1+D+D^2+D^3+D^4}\right]$$

（a） 试画出这些 RSC 编码器的方框图。

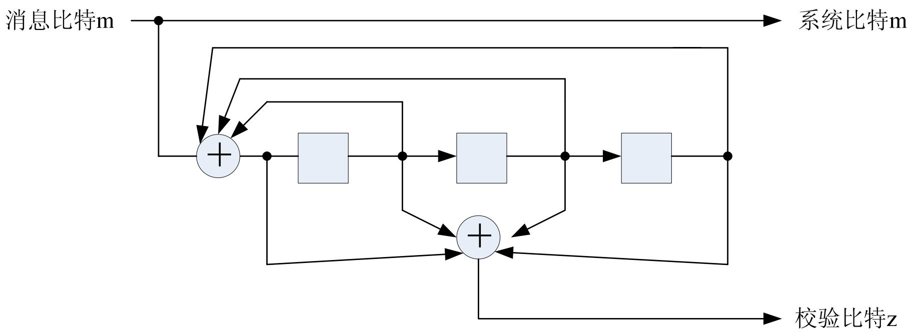
（b） 求出每个编码器对应的奇偶校等式。

解：RSC 编码器的方框图如下：

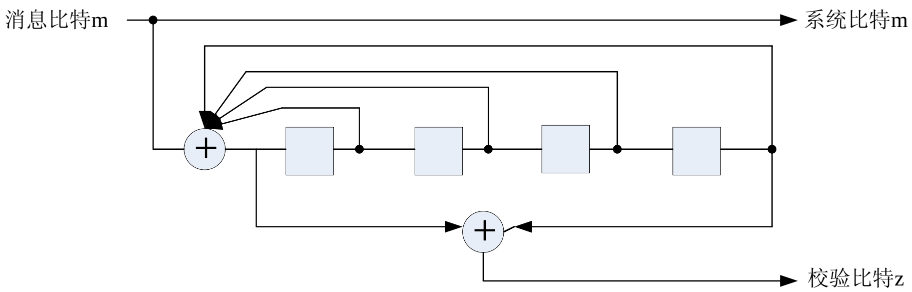
（1）



（2）



（3）



1. 若已知 DES 体制中 8 个 S 盒之一的 S 盒选择压缩函数如下：

列号 行号	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	5	12	8	2	4	9	1	7	5	11	2	14	10	0	6	13

假设输入S盒的输入矢量为$\mathbf{M} = (M_0 M_1 \ldots M_5)$。试求通过选择压缩函数S变换后的输出矢量。
解：M通过S盒时，代换表将选出一个相应的输出矢量。可以将矢量中的首尾两项$M_0\ M_5$看作是控制盒S中采用的不同行号，而将其余的四项看作是不同列号的一种。这样每个M就有唯一的Y相对应。如输入M＝（101100）则输出Y为第 2 行，第 6 列，结果为 2 即 0010

2. 试用公开密钥（e, n）=（5, 51）将报文 ABE，DEAD 用 A = 01, B = 02, …，进行加密。

解：用加密方程$\mathbf{C} = (\mathbf{M}^e \text{ 模 } n)$,　将 ABE，DEAD 分别代入可得结果为

1，32，14，4，14，1，4

3. 试用秘密密钥（d, n）=（13, 51）将报文 4, 1, 5, 1 解密。

解：用解密方程$\mathbf{M} = (\mathbf{C}^e \text{ 模 } n)$,　将 4, 1, 5, 1 分别代入可得结果为

4，1，20，1

4. 试用公开密钥（e, n）=（3, 55）将报文 BID HIGH 用 A = 01, B = 02, …，进行加密。

解：用加密方程$\mathbf{C} = (\mathbf{M}^e \text{ 模 } n)$,　将 BIG HIGH 分别代入可得结果为

8，14，9，17，14，13，17

5. 用秘密密钥（d, n）=（5, 51）将报文 4, 20, 1, 5, 20, 5, 4 解密。

解：用解密方程$\mathbf{M} = (\mathbf{C}^e \text{ 模 } n)$,　将 4, 20，1，5，20，5，4 分别代入可得结果为

4，5，1，4，5，14，4

6. 一个英文加密系统使用 10 个随机字母组成的密钥序列，计算其惟一性距离。
（1）每个密钥字符可以是 26 个字母中的任意一个，字母可以重复。
（2）密钥符号不能重复。
如果密钥序列由 0 ~ 999 整数中的 10 个随机整数组成，重新计算惟一性距离。

解：（1）密钥熵为H（K）$= \log_2 (26)^{10} = 47bit$

英语的绝对码率：$r' = \log_2 26 = 4.7$ 比特/字符
英语实际码率：$r = 1.5$ 比特/字符
冗余：$D = r' - r = 3.2$ 比特/字符
单一性距离：$N = H(K) / D = 47/ 3.2 \approx 15$ 字符

（2）密钥符号不能重复时

密钥熵为 $H（K）= \log_2 \binom{10}{26} = 44.13 bit$

单一性距离：$N = H(K)/D = 44.13/3.2 \approx 14$ 字符

（3）密钥熵为 $H（K）= \log_2 (1000)^{10} = 99.66 bit$

单一性距离：$N = H(K)/D = 99.66/3.2 \approx 32$ 字符

7. 使用 RSA 加密消息 $\mathbf{M} = 3$, 质数 $p = 5$, $q = 7$。解密密钥 d 选为 11，计算加密密钥 e 的值。

解：$\phi(n)$ = 4×6=24

解同余方程 $ed = (1 \text{ 模 } \phi(n))$ 可得 11×11=121=1（模 24）；

所以 e=11

8. 考虑以下 RSA 算法：

(a) 如果质数是 $p = 7$, $q = 11$，试举出 5 个允许的解密密钥 d。

(b) 如果质数是 $p = 13$, $q = 31$，解密密钥 $d = 37$，试求加密密钥 e，并加密单词“DIGITAL”。

解：

(a) 11×11 模 60=1，19×19 模 60=1，29×29 模 60=1，31×31 模 60=1，49×49 模 60=1，得 5 个允许的 d 为 11，18，29，31，49

(b) 37×251 模 360=1，所以 e 为 251

用加密方程 $\mathbf{C} = (\mathbf{M}^e \text{ 模 } n)$, 将 DIGTAL 分别代入可得结果为

9. 下面一段密文本来是连续的字符串，只是为了便于阅读将它分成每 5 个字符一组。明文是一般计算机教科书中的一段话，因此也许会有“COMPUTER”这个单词出现。加密采用的是 Polybius 方阵密码系统（参见 14.1.3 节）。明文中无安全可靠信道，无标点符号，试对此密文进行破译。

AAUAN CVIRE RURNN DLTME AEEPB YTUST ICEAT
NPMEY IICGO GORCH SRSOC NNTII IMIHA OOFPA
GSIVT TPSIT LBOLR OTOEX

10. 英文字母的替代密码的一般形式为

$$\mathbf{C} = \alpha\mathbf{M} + \beta \quad (\text{模 } 26)$$

其中这 $\mathbf{M}$ 为明文的字母，$\mathbf{C}$ 为密文的字母，α为与 26 互素的整数，β为 0~25 中的任意一个整数。试分析

（1）$\alpha = 1$，称为加法密码和

（2）$\beta = 0$，称为乘法密码

的特点及存在的问题。