通信系统的基本模型

信源 → 信源编码 → 加密编码 → 信道编码 → 信道 → 信道解码 → 解密 → 信源解码 → 信宿

概率空间
自信息，互信息
信源熵
马尔可夫极限熵
信息熵的性质

信源编码定理
克劳夫特不等式
香农，费诺，哈夫曼
平均码长，效率
算术编码

熵概念
RSA加密
RSA解密

信道编码定理
线性分组码
码集，最大纠检错距离
系统化，校验矩阵
伴随式（可纠）
汉明，伴随译码

信道矩阵（条件概率矩阵）
条件熵(噪声熵，疑义度）
信道容量（对称，准对称，一般）
香农公式

失真矩阵(函数）
平均失真
$d_{max}, d_{min}, R(d_{max}), R(d_{min})$,
对应假想信道矩阵

概率空间$(p_1, p_2, p_3, ...)$$p$是基本事件的概率。
一个事件y_j（不一定是基本事件）发生改变另一个事件x_i
不确定度的大小的度量：互信息

$$I(x_i; y_j) = \log\frac{1}{p(x_i)} - \log\frac{1}{p(x_i / y_j)}。$$

事件对自身的互信息：自信息

$$I(x_i) = I(x_i; x_i) = \log\frac{1}{p(x_i)}$$

信源（概率空间）中一个事件信息量的平均值 =
概率空间（信源）中所有事件自信息的统计平均：信源熵（信息熵）

$$H(X) = \sum_i p(x_i) I(x_i) = -\sum_i p(x_i)\log p(x_i)$$

两个信源各取一个事件互相给出的信息量的平均值 =
互信息的统计平均：平均互信息。

$$I(X;Y) == \sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i y_j)\log\frac{p(x_i / y_j)}{p(x_i)}$$

最大熵定理
离散信源，连续有界信源在信源各事件等概率出现时熵最大。
连续无界信源在信源概率分布为正态分布时熵最大。

如果你确定你朋友是6月生日，但不知道哪一天。那么你问你朋友你的生日是6月哪一天，答案中含有的信息量为_______.
互信息I(X;Y)是信源X的概率分布p(xi)和信道转移概率p(yj/xi）的函数。当p(xi)一定时，I是关于p(yj/xi)的____形凸函数。当p(yj/xi)一定时，I是关于p(xi)的___形凸函数。填（∪或∩）
随机事件的不确定度和自信息量的含义是一样的---()
连续信源的不确定度为无穷大，因此两个连续信源无法比较熵值大小-------（）
离散平稳有记忆信源符号序列的平均符号熵随着序列长度的增大而增大---------（）

对于无记忆离散信源X，其熵值为$H(X)$,由其生成的N次扩展信源X^N的熵为H（X^N），则H（X）与H（X^N）的关系为（H（X））^{N} = H（X^N）------()

联合熵：两个概率空间各发生一个事件构成概率空间的信息熵。
$H(XY)$ = 联合概率矩阵所有元素的统计平均。
条件熵：以另一个概率空间中事件为条件的条件概率空间信息熵关于条件空间中所有事件的统计平均。
$H(X/Y)$疑义度，$H(Y/X)$噪声熵。
条件概率矩阵行信息熵$H(Line)$的统计平均。
疑义度为0，由接收信息就可以确定发送信息。
噪声熵为0，由发送信息就可以确定接收信息。

$H(XY) = H(YX), H(Y/X) \neq H(X/Y)$
$H(XY) = H(X) + H(Y/X) = H(Y) + H(X/Y)$
$H(XYZ) = H(YZ) + H(X/YZ)$
$I(X;Y) = I(Y;X)$
$I(X;Y) = H(X) + H(Y) - H(XY) = H(X) - H(X/Y) = H(Y) - H(Y/X)$

一个旋转圆盘，被均匀的分成了38份，用1-38标示。其中2份涂绿，18涂红，18涂黑，停止旋转后，指针指向圆盘的某一份。若仅对颜色感兴趣则H（X）= ________。若颜色已知时，条件熵H（Y/X)=____。

设信道的转移概率矩阵为P= $\begin{matrix} 0.98 & 0.02 \\ 0.02 & 0.98 \end{matrix}$

(1)若$p(x0) = 0.6, p(x1) = 0.4$,
求$H(X), H(Y), H(X/Y), H(Y/X)$和$I(X;Y)$

有固定记忆长度的m阶马尔可夫信源：
输出与前m个输出有关。状态用前m个输出符号标记。
由概率转移矩阵描述。
部分马尔可夫信源在输出多次后达到稳态，其处于各个信源状态的概率不变。
稳态及极限熵的计算。
$p34$例$2-13$。三状态马尔可夫信源，转移概率矩阵为：

$$\mathbf{P_{ij}}=\begin{pmatrix} 0.1 & 0 & 0.9 \\ 0.5 & 0 & 0.5 \\ 0 & 0.2 & 0.8 \end{pmatrix}$$,求稳态分布，极限熵。

设：稳态概率分布为w_1, w_2, w_3

$$\begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix}^T = \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix}^T \begin{pmatrix} 0.1 & 0 & 0.9 \\ 0.5 & 0 & 0.5 \\ 0 & 0.2 & 0.8 \end{pmatrix}$$

同样三个方程任取2个，加上$w_1+w_2+w_3=1$
解出$w_1=5/59, w_2=9/59, w_3=45/59$。

极限熵，是稳态每个信源状态单符号平均自信息的统计平均
每个信源状态下一次输出单个符号的平均自信息
$H(1)=-0.1\log 0.1-0.9\log 0.9=0.469b/s$,
$H(2)=-0.5\log 0.5-0.5\log 0.5=1b/s$,
$H(3)=-0.2\log 0.2-0.8\log 0.8=0.722b/s$
$H_\infty=5/59\times H(1)+9/59\times H(2)+45/59\times H(3)=0.743b/s$

单个符号出现概率由各稳态输出该符号概率$\times$稳态概率w_1, w_2, w_3统计平均得到。

有一个由符号集（0,1）组成的二阶马尔可夫链，
状态变量S=（00,01,10,11），其符号条件转移概率
如下表所示：

	0	1
00	1/2	1/2
01	1/3	2/3
10	1/4	3/4
11	1/5	4/5

状态变化情形为：当在某一个状态时，如状态01时出现符号0，则将0加到状态01的后面，再将第一个符号0挤出，转移到状态10，其余状态的变化过程类似。
1，写出该信源的状态转移概率矩阵
2，画出该信源的状态转移图
3，计算该信源各状态的稳态分布概率
4，计算该信源稳定后的符号概率分布
5，计算该信源的极限熵

一阶齐次马尔可夫信源消息集X$\in$（a1, a2, a3）
状态集S$\in$（S1，S2，S3）。令$S_i=a_i, i=1,2,3.$

符号条件转移概率为$p(aj/si)=\begin{matrix} 1/3 & 1/3 & 1/3 \\ 1/4 & 1/2 & 1/4 \\ 1/4 & 1/4 & 1/2 \end{matrix}$

(1)画出该信源的状态转移图
（2）计算该信源极限熵。

信道：由信道矩阵描述。
信息传输率：信道中每传输一个符号，平均携带的信息量。
$R\equiv I(X;Y)=H(X)-H(X/Y)=H(Y)-H(Y/X)$
信道中R的最大值（以信源为变量）为信道容量C
对称：行元素置换＝行对称，列元素置换＝列对称。
行对称＋列对称＝对称。
只有行对称＝准对称。

对称：输入信源等概率分布时达到信道容量，此时输出也等概率。
$C=H(Y)-H(Y/X)=\log m-H(Line)$
准对称：输入等概率达到信道容量，输出不等概率。
划分成对称小矩阵后

$$C=\log n-H_{total}(Line)-\sum_{k=1}^{r} N_k \log M_k$$

N_k是第k个小对称矩阵的行概率和，任一行（因为对称）。
M_k是第k个小对称矩阵的列概率和，任一列（因为对称）

限时限频限功率高斯信道：香农公式

$$C_t=W\log(1+\frac{P_S}{N_0 W})$$

W带宽，P_s平均输入功率，N_0噪声功率谱密度。
$\frac{P_S}{N_0 W}$信噪比。

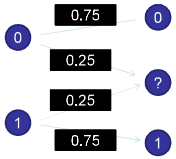
对于一个确定的信道，其信道容量不随信源概率分布的变化而变化——————（）

某信号在7MHZ带宽的某加性高斯信道上传输，若信道中的信号功率与噪声功率之比为3，则该信道的信道容量为_______。

若一个离散无干扰信道有n个输入，m个输出，并且有n>m,则信道容量C=_________。

设信道的转移概率矩阵为P=$\begin{matrix} 0.98 & 0.02 \\ 0.02 & 0.98 \end{matrix}$
(1)若$p(x0)=0.6, p(x1)=0.4$,
求$H(X), H(Y), H(X/Y), H(Y/X)$和$I(X;Y)$
(2)求信道的信道容量及其达到信道容量时输入符号的概率分布。

信道输入X（0,1），输出用Y表示，接受端
除了0,1外，还有不确定的符号用？表示
符号转移概率如图所示
（1）写出信道转移矩阵
（2）求这个信道的信道容量
(3）达到信道容量时，输入符号的概率分布



平均失真：失真矩阵元根据联合概率的统计平均。

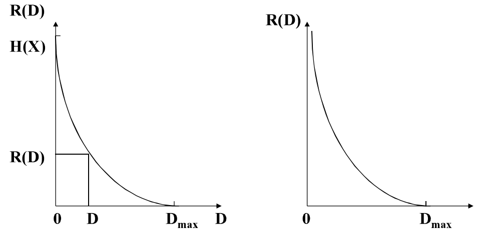
平均失真 = $\overline{D}$情况下，传输该信源所需要的最小信息传输率（以信道为泛函变量）：即率失真函数$R(\overline{D})$。

$D_{\min} = 0$, 对应信道是一一对应信道。

$D_{\max}$ = 使得$R(\overline{D})$为0的最小$\overline{D}$

率失真函数的性质

R(D)关于D，下凸，连续，单调递减



信息率失真曲线

$p76$, 例4.3，设输入输出符号表示为$X = Y = (0,1)$，输入概率分布为$p(x) = (1/3, 2/3)$，失真矩阵为$d = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

求$D_{\min}, R(D_{\min}), D_{\min}$对应的信道矩阵。

$D_{\max}, R(D_{\max}), D_{\max}$对应的信道矩阵。

$D_{\min} = 0, R(D_{\min}) = H(X) = 0.91 b/s$

对应信道矩阵选取一一对应矩阵即可

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

$D_{\max} = \min(\mathbf{p} \times \mathbf{D}) = \min(\sum_{i=1}^{n} p(x_i) d(x_i, y_j))$

$= \min(\left\langle \begin{array}{c|c} \frac{1}{3} \times 0 & \frac{1}{3} \times 1 \\ \frac{2}{3} \times 1 & \frac{2}{3} \times 0 \end{array} \right\rangle$列求和$) = \min(\frac{2}{3}, \frac{1}{3}) = \frac{1}{3}$

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

我们选的第二列的$C_2, q = 2$,因此对应信道矩阵为

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

设输入输出符号表示为$X = Y = (0,1)$，输入概率分布为$p(x) = (1/2, 1/2)$，失真函数为d (0, 0) =d (1, 1) =0
d (0, 1) =1, d (1, 0) =1. 5则

$D_{\min}$ = ______, $R(D_{\min})$ = ________,

相应的编码器转移概率矩阵p (Y/X) =________。

$D_{\max}$ = ______, $R(D_{\max})$ = ________,

相应的编码器转移概率矩阵p (Y/X) =________。

离散无记忆信源X的无失真编码压缩极限可以用____衡量，有失真信源编码的信息率失真函数$R(D)$表示给定的平均失真D下____________________。

编码方案中存在唯一可译码的充要条件

克劳夫特不等式:$\sum_{i=1}^{n} m^{-K_i} \le 1$

其中m是采用的编码进制，$m = 2$时表示编码用(0,1)

$m = 3$时用(0,1,2)......

i标示了等待编码的第i个信息。K_i是准备编给这第i个信息的码长。

n表示信源一共有n个信息等待编码。

不等式成立，则这种进制与码长的编码方案一定能编出唯一可译码。

定长编码定理：

定长编码携带最大熵为$K \log m$, K是码长，m是用几个符号编码，即几个码元，即码进制。

携带最大熵≥信源熵，可以使译码差错任意小。

携带最大熵≥信源最大可能熵，可以编成唯一可译码。

变长编码定理：

变长编码携带最大熵为$\overline{K} \log m$, $\overline{K}$是平均码长。

$\overline{K} = K_1 p(1) + K_2 p(2) + ...$, 码长的统计平均。

编码携带最大熵≥信源熵，可以编唯一可译码。

变长编码：香农码

二进制香农码

编码流程：

1.把信源信息按照概率从大到小排序。

2.求码长。排在第i个的信息对应码字的码长K_i满足

$-\log_2(p_i) \le K_i \le -\log_2(p_i) + 1$

可以发现这个码长完全符合变长编码定理。

3.编码字。

(1)求累加概率：即把排在第i位置前所有信息的概率求和$P_i = \sum_{k=1}^{i-1} p(k)$

(2)把累加概率用二进制写出

(3)二进制表达下P_i从小数点后第一位取码长K_i位作为码字

例5.4,7个符号的信源，二进制香农码的编码过程

信息	1.排序	2.求对数	3.定码长	4.求累加概率	5.二进制化	6.得码字
$a1$	0.2	2.34	3	0	0.000	000
$a2$	0.19	2.41	3	0.2	0.0011	001
$a3$	0.18	2.48	3	0.39	0.0110	011
$a4$	0.17	2.56	3	0.57	0.1000	100
$a5$	0.15	2.74	3	0.74	0.1011	101
$a6$	0.10	3.34	4	0.89	0.11100	1110
$a7$	0.01	6.66	7	0.99	0.11111100	1111110

可以求得平均码长$\overline{K}=\sum_{i=1}^{7}p_iK_i=3.14$

编码最大熵为$R=\overline{K}\log 2=3.14b/s$

编码效率$\eta=\frac{H(X)}{R}=0.831$

费诺码：二进制费诺码 编码流程：

1.把信源信息按照概率从 大到小排序。

2.找个位置分成上下两组，分组的原则每组的概 率和要最接近相等。对第一次分组就是概率 和接近0.5。

3.把上面一组给一个码字 0，下面一组给一个码字 1。

4.再把每个组再次分上下 两组，同样上组给 0，下组给1。

5.重复分组，编 0,1。直到每一组中都只有 一个信息。

6。把赋予一个信息所有 的码字按顺序写在一起 就是总的码字。

例5.4,7个符号的信源，费诺码的编码过程

信息	1.排序	2.第1次分组	3.第2次分组	4.第3次	5.第4次	6.码字
$a1$	0.2	0	0			00
$a2$	0.19	0	1	0		010
$a3$	0.18	0	1	1		011
$a4$	0.17	1	0			10
$a5$	0.15	1	1	0		110
$a6$	0.10	1	1	1	0	1110
$a7$	0.01	1	1	1	1	1111

可以求得平均码长$\overline{K}=\sum_{i=1}^{7}p_iK_i=2.74$

编码最大携带熵为$R=\overline{K}\log 2=2.74b/s$

编码效率$\eta=\frac{H(X)}{R}=0.953b/s$

费诺码的编码过程与码树构造即时码本质一样，因此费诺码是即时码

哈夫曼码：二进制哈夫 曼码编码流程：

1.把概率最小的两概率分 别赋予0和1。大的给0，小的给1。

2.把刚才赋予0,1的两信息概率求和作为 总概率赋予这两个信息 。用标记表明这两个信息 的概率是同一个东西。

3.再次把概率最小的两概 率赋予0和1。求和的概率虽然出现多 次但只是一个概率。

4.再次把最小两概率求和， 并赋予求总概率用到 的所有子概率。

5.重复以上步骤直到只有 两个不同的概率。

6。把赋予一个信息所有 的码字按倒序写好，就 是哈夫曼编码。

例5.4,7个符号的信源，哈夫曼码的编码过程

信息	排序	赋码	合并	赋码	合并	赋码	合并	赋码	合并	赋码	合并	赋码	码字
$a1$	0.2		0.2		0.2		0.2	0	$\underline{0.39}$		$\underline{0.39}$	1	10
$a2$	0.19		0.19		0.19		0.19	1	$\underline{0.39}$		$\underline{0.39}$	1	11
$a3$	0.18		0.18		0.18	0	$\underline{0.35}$		$\underline{0.35}$	0	$\underline{0.61}$	0	000
$a4$	0.17		0.17		0.17	1	$\underline{0.35}$		$\underline{0.35}$	0	$\underline{0.61}$	0	001
$a5$	0.15		0.15	0	$\underline{0.26}$		$\underline{0.26}$		$\underline{0.26}$	1	$\underline{0.61}$	0	010
$a6$	0.10	0	$\underline{0.11}$	1	$\underline{0.26}$		$\underline{0.26}$		$\underline{0.26}$	1	$\underline{0.61}$	0	0110
$a7$	0.01	1	$\underline{0.11}$	1	$\underline{0.26}$		$\underline{0.26}$		$\underline{0.26}$	1	$\underline{0.61}$	0	0111

可以求得平均码长$\overline{K}=\sum_{i=1}^{7}p_iK_i=2.72$

编码最大携带熵为$R=\overline{K}\log 2=2.72b/s$

编码效率$\eta=\frac{H(X)}{R}=0.96b/s$

哈夫曼码的编码过程与码树构造即时码本质也一样，也是即时码

两个概率相同时：

都没合并过则任意。

合并过则：合并的概率 看作比非合并概率略大 一点。

合并多的比合并少的看 作略大一点

编码效率 $\eta=\frac{H(X)}{\overline{K}\log m}$

算术码

1.把信源的符号排序好并计算积累概率(按概率排序)。

2.计算所给序列的积累概率$P(S)$和出现概率$p(S)$。

积累概率的算法：

给定初始序列为空，$P()=0,p()=1$

根据递推公式$P(S,r)=P(S)+p(S)P_r,p(S,r)=p(S)p_r$

一个个往空序列上加符号。每加一次计算出

P和p最后得出$P(S)$，$p(S)$。

3.根据$p(S)$定码长：$-\log_2(p(S))\le L<-\log_2(p(S))+1$

4.定码字，把$P(S)$二进制写出，把小数点后L位后的进位到L。

取这小数点后L位即为码字C。

例5.10信源符号概率分布：如表。要求序列$S=abda$的算术码。

信源符号	概率分布	计算积累概率
a	0.1	0
b	0.01	0.1
c	0.001	0.110
d	0.001	0.111

$P()=0,p()=1$

计算$P(,a)=P()+p()P_a=0+1\times 0=0,p(,a)=0.1$

计算$P(,a,b)=P(,a)+p(,a)P_b=0+0.1\times 0.1=0.01,p(,a,b)=0.1\times 0.01=0.001$

$P(,ab,d)=P(,ab)+p(,ab)P_d=0.01+0.001\times 0.111=0.010111$

$p(,ab,d)=p(,a,b)p(d)=0.001\times 0.001=0.000001$

$P(,abd,a)=P(,abd)+p(,abd)P_a=0.010111+0.000001\times 0=0.010111$

$p(,abd,a)=0.0000001$

码长$L=-\log_2 p(abda)=7$

取小数点后7位，码字为010111。

算术编码的译码流程：

以刚才的序列编码0101110为例。

译码需要信源概率分布，和信源排序规则。

信源符号	概率分布	计算积累概率
a	0.1	0
b	0.01	0.1
c	0.001	0.110
d	0.001	0.111

恢复码字为小数形式$C=0.010111$,看属于哪个积累概率范围。

发现$0\le C<0.1$则第一个符号为a。减去a的积累概率并除以p_a

$C_1=(0.0010111-0)\div 0.1=0.10111,$

发现$0.1\le C_1<0.110$则第二个符号为b。减去b的积累概率并除以p_b

$C_2=(0.10111-0.1)\div 0.01=0.111$

发现$0.111\le C_2$,则第三个符号为d。减去d的积累概率并除以p_d

$C_3=(0.111-0.111)\div 0.001=0$

则第四个符号为a。译码结束。译码结果为$abda$

冗余度来自两个方面，一是信源符号间的________，
另一方面是信源符号分布的________。

某信源包含6个消息符号，概率为
0.28,0.12,0.39,0.03,0.16,0.02
(1) 求该信源的熵
(2) 对信源做二进制哈夫曼编码，
写出相应码字，并求出平均码长，编码效率。
(3) 对此信源做二进制香农编码，写出相应码字
，并求出平均码长，编码效率。

某信源包含7个消息符号，概率为
0.3,0.2,0.15,0.12,0.1,0.07,0.06
(1) 求该信源的熵
(2) 对信源做二进制费诺编码，
写出相应码字，并求出平均码长，编码效率。
(3) 对此信源做二进制哈夫曼编码，写出相应码字
，并求出平均码长，编码效率。
（写出编码过程不然不得分）

信道编码的存在性：信道编码定理

当需要的信息传输率R小于信道容量C时，必定存在一种信道码
，可以使得信息通过信道后译码错误任意小。

当需要对信息传输率R大于信道容量C时，要使得信息通过信道
后译码错误任意小是不可能通过任何编码实现的。

信道译码：最优译码＝最大后验概率译码。
最大似然译码＝最大先验概率译码。
输入等概率时两者等同。

信道编码定理的内涵是：只要_________，总
存在一种信道编码可以以所要求的任意小差错
概率实现可靠通信。

已知输入码集为{c0, c1}，接收码字为c，若
译码方法是当p(c/c0)>p(c/c1)时，将c判为
c0，反之判为c1，则使用的译码方法为最大
后验概率译码。————————————（ ）

线性分组码由一个生成矩阵确定：
信息是2进制符号，长度为3。把其编成长度为6的线性分组码。
这是个(6,3)的线性分组码

给个生成矩阵为$\begin{pmatrix}1&1&1&0&1&0\\1&1&0&0&0&1\\0&1&1&1&0&1\end{pmatrix}$

其收码的正确性由对应的校验矩阵判断
$R\times H^T\neq 0$一定产生错误
生成矩阵(n,k),校验矩阵为$(n,n-k)$

线性分组编码码字＝信息码$m\otimes$生成矩阵G
其中加法满足$1+1=0$。

$$(0,0,0)\otimes\begin{pmatrix}1&1&1&0&1&0\\1&1&0&0&0&1\\0&1&1&1&0&1\end{pmatrix}=(0,0,0,0,0,0)=000000$$

$(0,0,1)\otimes G=011101,$
$010\otimes G=110001,$
$011\otimes G=(1,1,0,0,0,1)+(0,1,1,1,0,1)=(1,0,1,1,0,0)=101100$
$100\otimes G=111010, 101\otimes G=100111,$
$110\otimes G=001011, 111\otimes G=010110$

系统化生成矩阵,左边部分是单位矩阵。

$\begin{pmatrix}1&1&1&0&1&0\\1&1&0&0&0&1\\0&1&1&1&0&1\end{pmatrix}$,第一行上加第三行,

$\begin{pmatrix}1&0&0&1&1&1\\1&1&0&0&0&1\\0&1&1&1&0&1\end{pmatrix}$,第二行上加第一行,

$\begin{pmatrix}1&0&0&1&1&1\\0&1&0&1&1&0\\0&1&1&1&0&1\end{pmatrix}$,第三行上加第二行,

$\begin{pmatrix}1&0&0&1&1&1\\0&1&0&1&1&0\\0&0&1&0&1&1\end{pmatrix}$,生成矩阵系统化完成

求系统码的校验矩阵，并判断收吗$r=100110$的正确与否。

刚才的系统码生成矩阵为$\begin{pmatrix}1&0&0&1&1&1\\0&1&0&1&1&0\\0&0&1&0&1&1\end{pmatrix}$

生成矩阵是$(6,3)$校验矩阵为$(6,6-3)$

$P=\begin{pmatrix}1&1&1\\1&1&0\\0&1&1\end{pmatrix}$,$P^T=$第$n$行变第$n$列$=\begin{pmatrix}1&1&0\\1&1&1\\1&0&1\end{pmatrix}$

因此校验矩阵$H=\begin{pmatrix}1&1&0&1&0&0\\1&1&1&0&1&0\\1&0&1&0&0&1\end{pmatrix}$

$rH^T=(1,0,0,1,1,0)\begin{pmatrix}1&1&1\\1&1&0\\0&1&1\\1&0&0\\0&1&0\\0&0&1\end{pmatrix}=(0,0,1)\neq 0$,所以$r$在传输中一定出错了。

线性分组码译码：汉明译码
二进制码的汉明距离：$d=(R1-R2)$中1的个数。
汉明译码，收码译码为汉明距离最近的正确码。

伴随式译码：标准阵列译码。
伴随式$S=EH^T$长度为$n-k$,因此二进制下一共2^{n-k}个。
差错图样E,从重量为1开始遍历。直到每个伴随式
都有一个差错图样与之对应。

计算收码的伴随式$S=RH^T$,确定对应的差错图样。
$R+E=C$

线性分组码的dmin = 码集中码重最小的码字的码重
0码字不算。
检错能力t=dmin-1
纠错能力t=（dmin-1）/2 取整

伴随式与差错图案不是一一对应的，不同的差错图案可能有相同的伴随式————（）

设某二元码为C=11100,01001,10010,00111，则此码最小距离dmin=________。

已知(6,3)线性分组码的生成矩阵$G=\begin{pmatrix}1&0&1&1&0&1\\0&1&1&0&1&1\\1&0&0&0&1&1\end{pmatrix}$

(1)求该分组码的码集
（2）求系统形式的生成矩阵G和校验矩阵H
（3）计算该码的最小距离$d_{\min}$,及该码的纠错能力t
(4)列出可纠差错图案和对应的伴随式（针对系统码）
（5）若接收码字$R=111001$，求发码及信息位。

如果伴随式的个数与小于某个重量所有差错图样一一对应。
：完备码。汉明码（$2^m-1,2^m-1-m$），高莱码（23,12）。

同码长下纠错检错能力最强的码-极大最小距离码（MDC）。

对码字做循环操作跑不出码集，称为循环码。
要构造一个n,k的循环线性分组码
1.对多项式x^n+1做因式分解，找到其中一个最高次为$n-k$的多项式因子作为生成多项式。
2.把k重的信息码元按顺序作为$k-1$次方多项式的各个系数，构成$k-1$次的信息多项式。
3.把这两个多项式相乘，得到多项式的系数，就是该信息多项式对应的循环码码字。

信息多项式是$k-1$次的，而生成多项式是$n-k$次的。因此他们的乘积是$n-1$次的码多项式。对应的是长度为n的循环码码字。

构造一个长度为7,3的循环线性分组码：
1.要找x^7+1的$7-3=4$次方的因子。
把x^7+1因式分解。
$x^7+1=x^7-1=(x+1)(x^6+x^5+x^4+x^3+x^2+x+1)$
$=(x+1)(x^3+x^2+1)(x^3+x+1)$
找其中4次方因子
发现两个其一$(x+1)(x^3+x^2+1)=x^4+x^2+x+1$
其二$(x+1)(x^3+x+1)=x^4+x^3+x^2+1$
3重的信息空间一共8个码字，每个码字对应于一个信息多项式。
000对应0,001对应1,010对应x,011对应$x+1$
100对应x^2,101对应x^2+1,110对应x^2+x,111对应x^2+x+1。

用信息多项式乘以生成多项式就得到了码字多项式
我写出第一个码字多项式
$000\times g(x)=0=0000000$
$001\times g(x)=g(x)=x^4+x^2+x+1=0010111$
$010\times g(x)=x^5+x^3+x^2+x=0101110$
$011\times g(x)=(x+1)(x^4+x^2+x+1)=x^5+x^4+x^3+1=0111001$
$100\times g(x)=x^6+x^4+x^3+x^2=1011100$
$101\times g(x)=(x^2+1)(x^4+x^2+x+1)=x^6+x^3+x+1=1001011$
$110\times g(x)=(x^2+x)(x^4+x^2+x+1)=x^6+x^5+x^4+x=1110010$
$111\times g(x)=(x^2+x+1)(x^4+x^2+x+1)=x^6+x^5+x^2+1=1100101$

循环码是一种线性分组码，其主要特征在于一个码字的____仍然是一个码字。已知码长$n=7$的循环码生成多项式$g(x)=x^3+x^2+1$,则011将编码为____，校验多项式为：________；

循环码码集中任一个码字的循环移位可得到码集中的所有码字-------（）

加密编码
对称DES，非对称RSA

如果已知密文和密钥，则明文确定，加密已经没有信息量
$H(M/C,K)=0$

$H(K/C)\geq H(M/C)$
已知密文后密钥的疑义度大于等于明文的疑义度。
$I(M;C)\geq H(M)-H(K)$
密钥包含的信息量越少，密文含有的关于明文的信息量越大。

一个密码体制的安全性，既依赖于其密钥的保密性，有依赖于其加密，解密算法的保密性。------------------------（）

根据密钥的性质，密码体制可分为______和________.

RSA密码体制是一种____密钥体制，其基础是大数的素数分解难题，该难题具体可表示为______________。

RSA加密：

加密时：密文$y=\mathrm{mod}(x^e,n)$

解密时：明文$x=\mathrm{mod}(y^d,n)$

即加密时把明文自乘e次，然后对n求余数，余数即密文。

解密时把密文自乘d次，然后对n求余数。余数即明文。

其中e,n是公钥，n不是素数，而d是密钥。

RSA密钥的确定：

1.任选2个很大的素数$p,q,n=pq$

2.求$\Phi=(p-1)(q-1)$,从$[2,\Phi]$区间内任选一个整数作为e

3.由$\mathrm{mod}(ed,\Phi)=1$,求得d。

e,n是RSA的公钥，而d是私钥。基于n分解成pq的计算不可行，由e,n试图破解d是困难的。

例7.1,RSA密码中，$p=3,q=17$取$e=5$,试计算解密密钥d并加密$M=2$。

$\Phi=(p-1)(q-1)=2\times16=32$

$\mathrm{mod}(ed,\Phi)=1$

$5\times d=32\times u+1$--没啥技巧，自己看着猜吧，例如本题，

d一定不会是偶数。u要满足$2\times u=?4$(?9显然不可能)。

$u=2,d=13$是一个解。

对2加密,$n=pq=51$

$y=\mathrm{mod}(x^e,n)=\mathrm{mod}(2^5,51)=\mathrm{mod}(32,51)=32$

解密

$x=\mathrm{mod}(y^d,n)=\mathrm{mod}(32^{13},51)=2$

RSA密码用于数字签名，发送者Alice，接收者Bob

1.Alice签名，然后用自己私钥加密。

2.Alice再用Bob的公钥加密，确保安全性。发送给Bob

3.Bob用自己的私钥解密，密文恢复到1的状态。

4.Bob用Alice的公钥解密。恢复签名，如恢复的不对，则该密文系伪造。

已知用户A和B之间采用RSA算法进行签署报文的通信。

用户A选取p=5,q=11,e=27,B选取p=3，q=13，e=7

1分别计算A，B的公钥和私钥

2用户A发送报文2给用户B，需对此报文加密，问加密后的（即信道中传输的）密文为多少。

6，信道编码定理保证以任意小的差错概率实现传输速率小于信道容量的可靠通信，这要求编码码长可以任意长。————————————————————————（）

7，满足克劳夫特不等式的编码一定是唯一可译码。—（）

8，信息率失真函数是平均失真的上凸函数。————（）

9，唯一可译码一定是即时码，即时码也一定是唯一可译码————————————————————————（）

10，信源编码包括香农编码，费诺编码，哈夫曼编码，线性分组编码等。——————————————————（）

11,完备码的差错图案与伴随式一一对应。——————（）

1，有一个有符号集{0.1}组成的二阶马尔可夫链，状态变量为$S=\{00,01,10,11\}$,其符号条件转移概率如下表所示：

起始状态	0	1
00	1/2	1/2
01	1/3	2/3
10	1/4	3/4
11	1/5	4/5

状态变化的情形为：当在某一个状态时，如状态01时，出现符号0，则将0加到状态01的后面，再将第一个符号0挤出，转移到状态10，其余状态的变化过程类似。

（1），写出该信源的状态转移概率矩阵；

（2），画出该信源的状态转移图；

（3），计算该信源各状态的稳态分布概率；

（4），机选该信源稳定后的符号分布概率；

（5），计算该信源的极限熵。

所谓二阶马尔可夫链由前两个输出符号表示状态。

00输出0对应于状态由00—00

01输出0对应01—10

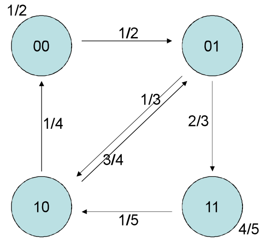
10输出1对应10—01，其它依次类推。

状态转移的概率由题表给出，写出状态转移矩阵

	00	01	10	11
00	1/2	1/2		
01			1/3	2/3
10	1/4	3/4		
11			1/5	4/5

其它的补上0，要注意的是，行求和一定为1。概率归一。

因此题目未必给全所有概率，可能每行留一个要算。



设各状态在稳态分布的概率为w_1, w_2, w_3, w_4

由稳态概念

$$(w_1, w_2, w_3, w_4)\times\begin{pmatrix}1/2 & 1/2 & 0 & 0\\ 0 & 0 & 1/3 & 2/3\\ 1/4 & 3/4 & 0 & 0\\ 0 & 0 & 1/5 & 4/5\end{pmatrix}=(w_1, w_2, w_3, w_4)$$

任选3个方程，加上$w_1+w_2+w_3+w_4=1$求解

可以解得

$w_1=3/35, w_2=6/35, w_3=6/35, w_4=4/7$

每个状态都有一定概率输出0或1

因此

$p(0)=w_1\times1/2+w_2\times1/3+w_3\times1/4+w_4\times1/5$

$=9/35$

$p(1)=w_1\times1/2+w_2\times2/3+w_3\times3/4+w_4\times4/5$

$=1-p(0)=26/35$

极限熵是各个状态熵的统计平均。

不是$H(9/35,26/35)$

而是

$H(w_1)=H(1/2,1/2)=1b/s$

$H(w_2)=H(1/3,2/3)=0.9183b/s$

$H(w_3)=H(1/4,3/4)=0.8113b/s$

$H(w_4)=H(1/5,4/5)=0.7219b/s$

$H_\infty=w_1\times H(w_1)+w_2\times H(w_2)+w_3\times H(w_3)+w_4\times H(w_4)$

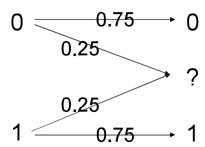
$=0.7947b/s$

信道输入X为符号集$\{0,1\}$,输出用Y表示，接收端除了0,1外还有不确定的符号用?表示。符号转移概率如右图所示：

(1) 写出信道转移矩阵；

(2) 求这个信道的信道容量；

(3) 达到信道容量时输入符号的概率分布。



	0	?	1
0	0.75	0.25	0
1	0	0.25	0.75

准对称信道，分块求信道容量。

$$\begin{pmatrix}0.75 & 0 & 0.25\\ 0 & 0.75 & 0.25\end{pmatrix}$$

$C=\log n-H(Line)-N_1\log M_1-N_2\log M_2$

$=1-(-0.75\log0.75-0.25\log0.25)$

$-(0.75+0)\log(0.75+0)-0.25\log(0.25+0.25)$

$=0.75b/s$

准对称信道在输入对称时达到信道容量

$p(0)=p(1)=0.5$

已知一信源包含6个消息符号，其出现概率如下表所示：

信源s	A	B	C	D	E	F
概率$p(s)$	0.028	0.12	0.39	0.03	0.16	0.02

(1)求该信源的熵

(2) 对此信源做二进制哈夫曼编码，写出相应码字，并求出平均码长，编码效率。

(3) 对此信源做二进制香农编码，写出相应码字，并求出平均码长，编码效率。

$H(X)=-p\log p=2.099b/s$

哈夫曼码

C	0.39									1	1
A	0.28							1	$\underline{0.61}$	0	01
E	0.16					1	$\underline{0.33}$	0	$\underline{0.61}$	0	001
B	0.12			0	$\underline{0.17}$	0	$\underline{0.33}$	0	$\underline{0.61}$	0	0000
D	0.03	0	$\underline{0.05}$	1	$\underline{0.17}$	0	$\underline{0.33}$	0	$\underline{0.61}$	0	00010
F	0.02	1	$\underline{0.05}$	1	$\underline{0.17}$	0	$\underline{0.33}$	0	$\underline{0.61}$	0	00011

$\overline{K}=0.39\times1+0.28\times2+0.16\times3+0.12\times4+0.03\times5+0.02\times5$

$=2.16$

$\eta=H(X)/2.16\log2=0.972$

香农码

符号	概率	概率对数	码长	积累概率	二进制化	码字
C	0.39	1.358	2	0	0.0000	00
A	0.28	1.8365	2	0.39	0.011	01
E	0.16	2.64	3	0.67	0.101	101
B	0.12	3.06	4	0.83	0.1101	1101
D	0.03	5.06	6	0.95	0.111100	111100
F	0.02	5.64	6	0.98	0.111110	111110

$\overline{K}=0.39\times2+0.28\times2+0.16\times3+0.12\times4+0.03\times6+0.02\times6$

$=2.6$

$\eta=H(X)/2.16\log2=0.8073$

已知(6,3)线性分组码的生成矩阵$G=\begin{pmatrix}1&0&1&1&0&1\\0&1&1&0&1&1\\1&0&0&0&1&1\end{pmatrix}$

(1)求该分组码的码集

（2）求系统形式的生成矩阵G和校验矩阵H

（3）计算该码的最小距离$d_{\min}$,及该码的纠错能力t

(4)列出可纠差错图案和对应的伴随式（针对系统码）

（5）若接收码字$R=111001$，求发码及信息位。

码集为$R=CG$

$C=000,001,010,011,100,101,110,111$

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

乘起来可得到对应码字。码集为

$$\begin{pmatrix}000&000000\\001&100011\\010&011011\\011&111000\\100&101101\\101&001110\\110&110110\\111&010101\end{pmatrix}$$

用行变换同矩阵对角化的方法系统化。

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

第一行加入第三行$G=\begin{pmatrix}1&0&1&1&0&1\\0&1&1&0&1&1\\0&0&1&1&1&0\end{pmatrix}$

第三行加入第二行$G=\begin{pmatrix}1&0&1&1&0&1\\0&1&0&1&0&1\\0&0&1&1&1&0\end{pmatrix}$

第三行加入第一行$G=\begin{pmatrix}1&0&0&0&1&1\\0&1&0&1&0&1\\0&0&1&1&1&0\end{pmatrix}$,系统化完成

系统生成矩阵的校验矩阵：

H是（$n,n-k$）$=(6,3)$的矩阵

去掉G中的单位矩阵

$\begin{pmatrix}&&&0&1&1\\&&&1&0&1\\&&&1&1&0\end{pmatrix}$,转置后放入$H$左边。

$\begin{pmatrix}0&1&1&&&\\1&0&1&&&\\1&1&0&&&\end{pmatrix}$，右边补单位矩阵。

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

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

写出码表后可得：

(001110,010101,011011,100011,101101,110110,111000)

码重最小为3因此

$d_{\min}=3,t=\dfrac{d_{\min}-1}{2}=1$

纠错能力为1，可纠的差错图案只能有一个错

$E=100000,010000,001000,000100,000010,000001$

共6个。

对应伴随式$S=EH^T$

000001	001
000010	010
000100	100
001000	110
010000	101
100000	011
000000	000000

$R=111001,$

$S=RH^T=001$

对应差错图案为000001

$C=R+E=111000$

方法二，算出码集，用最小距离（汉明译码）

信息位为111。

已知用户A和用户B之间采用RSA算法进行签署报文的通信

用户A选取$p=5,q=11,e=27,$用户B选取$p=3,q=13,e=7.$

(1)分别计算用户A，用户B的公钥和私钥。

（2）用户A发送报文2给用户B,需对此报文加密，问加密后的（即信道中传输的）密文是多少？

先算A

$\Phi=(p-1)(q-1)=40$

$\mathrm{mod}(ed,\Phi)=1$

$27d=40n+1$

最小解$3\times7=21$，$d=3$

A的公钥为（e,pq）=（27,55），私钥为(d,pq)=（3,55）

B

$\Phi=(p-1)(q-1)=24$

$\mathrm{mod}(ed,\Phi)=1$

$7d=24n+1$

$d=5$

B的公钥为（7,39),私钥为（5,39）

A签署报文

1用自己私钥加密：

$y = \mathrm{mod}(x^d, n) = \mathrm{mod}(2^3, 55) = 8$

2用B的公钥加密：

$y = \mathrm{mod}(8^7, 39) = 5$