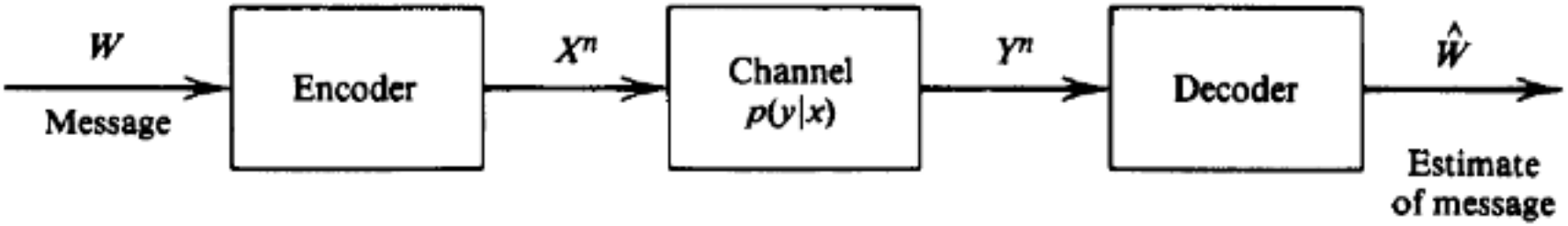
第七章 信道容量

- 通信：传递消息



- ✓ 输入序列、信道和输出序列都是随机的
- ✓ 接收者希望正确的解码结果，也就是误差概率尽可能的小
- ✓ 最理想情况：一个输出只对应一个输入

信源编码和信道编码

- **从提高信息传输效率的角度出发**，总是希望减少冗余度（压缩），用尽可能少的信道传输符号来传递信源消息，这是信源编码的作用
- **从提高信息抗干扰能力，增强通信可靠性的角度出发**，总是希望增加或保留剩余度，这是信道编码要达到的目的，一般是采用冗余编码法，赋予码字自身一定的纠错和检错能力。
- 提高抗干扰能力往往是以降低信息传输效率为代价的，而为了提高传输效率又往往削弱了其抗干扰能力。这样，设计者在取舍之间就要作均衡考虑。

信道容量的定义

- 定义 无记忆离散信道（Discrete Memoryless Channel, DMC）：由输入字母表 $\mathcal{X}$，输出字母表 $\mathcal{Y}$ 和概率转移矩阵$p(y|x)$构成，且输出的概率分布仅依赖于它对应的输入，而与先前信道的输入或输出条件独立。
- 定义 离散无记忆信道的“信息”信道容量（channel capacity）定义为

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

  - ✓ 固定$p(y|x)$，$I(X;Y)$是$p(x)$的凹函数

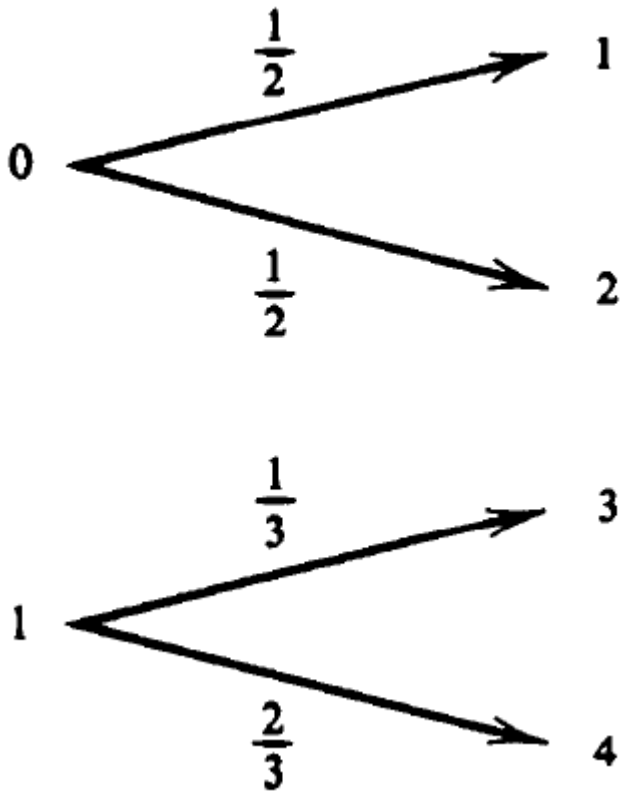
无噪声二元信道

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

$C = 1$比特/信道使用

$$p(x) = \left(\frac{1}{2}, \frac{1}{2}\right)$$

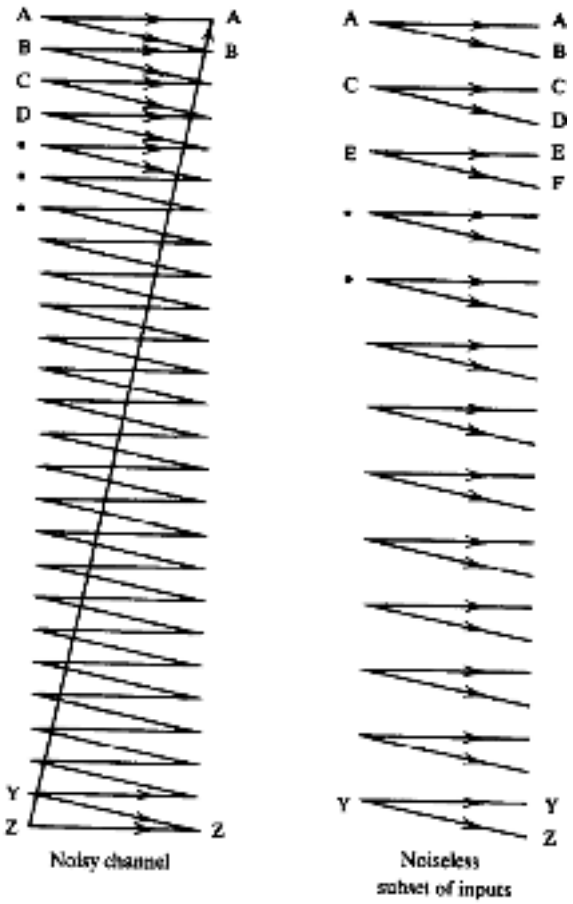
无重叠输出的有噪声信道



$C = 1$比特/信道使用

$$p(x) = \left(\frac{1}{2}, \frac{1}{2}\right)$$

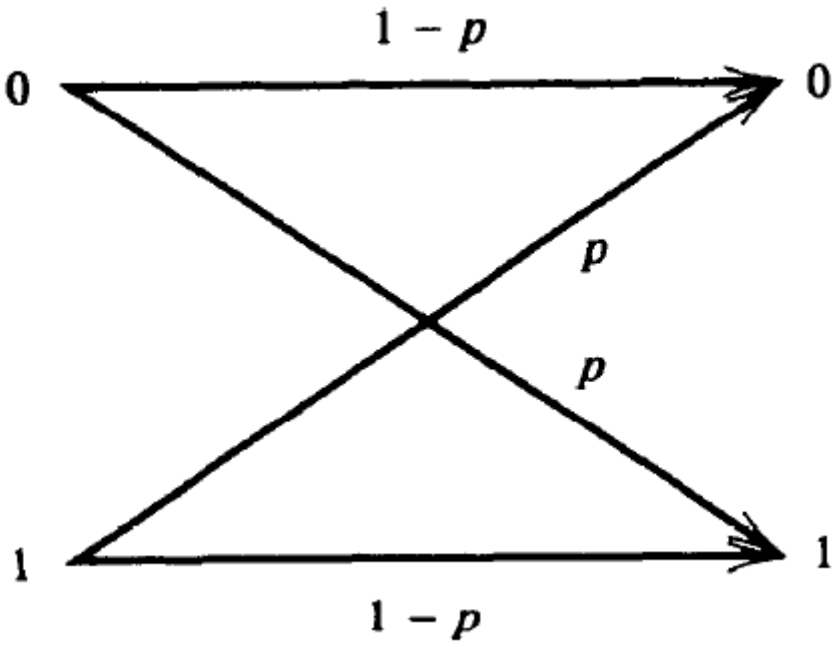
有噪声的打字机信道



$C = \log 13$比特/信道使用

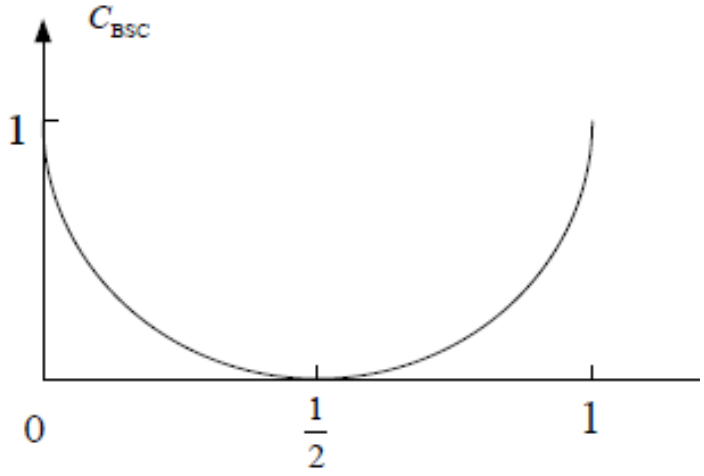
$p(x)$均匀分布

二元对称信道（Binary Symmetric Channel, BSC)

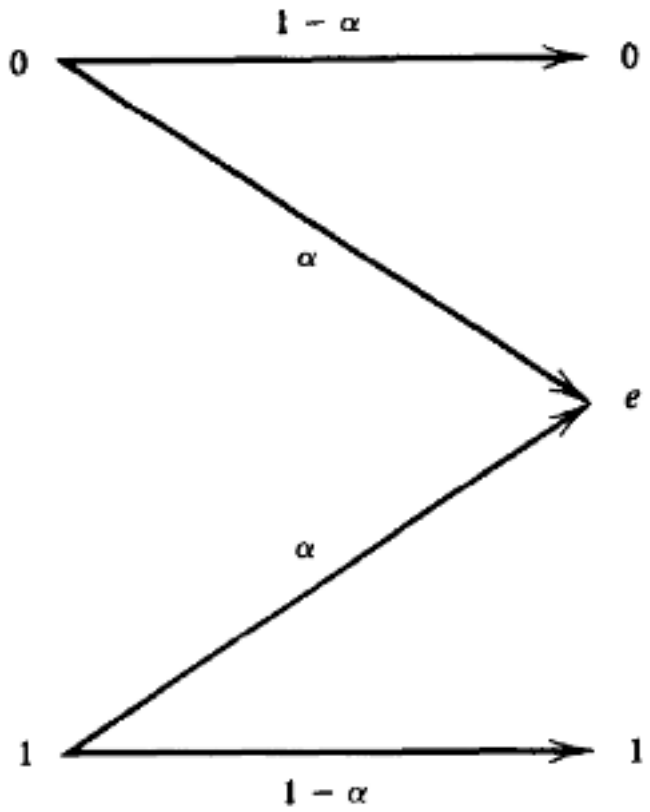


$C = 1 - H(p)$比特/信道使用

$p(x)$均匀分布



二元擦除信道（binary erasure channel）



$C = 1 - \alpha$比特/信道使用

$p(x)$均匀分布

对称信道

- 定义 对称信道：信道转移矩阵p(y|x)的任何两行互相置换；任何两列也互相置换
- 定义 弱对称（weakly symmetric）信道：信道转移矩阵p(y|x)的任何两行互相置换，而所有列的元素和 $\sum_x p(y|x)$ 相等

$$p(y|x)=\begin{bmatrix}0.3 & 0.2 & 0.5\\ 0.5 & 0.3 & 0.2\\ 0.2 & 0.5 & 0.3\end{bmatrix}$$

$$p(y|x)=\begin{pmatrix}\frac{1}{3} & \frac{1}{6} & \frac{1}{2}\\ \frac{1}{3} & \frac{1}{2} & \frac{1}{6}\end{pmatrix}$$

弱对称信道的信道容量

- **定理** 对于弱对称信道，

$$C = \log |\mathcal{Y}| - H(\text{转移矩阵的行})$$

当输入字母表上的分布为均匀分布时达到该容量。

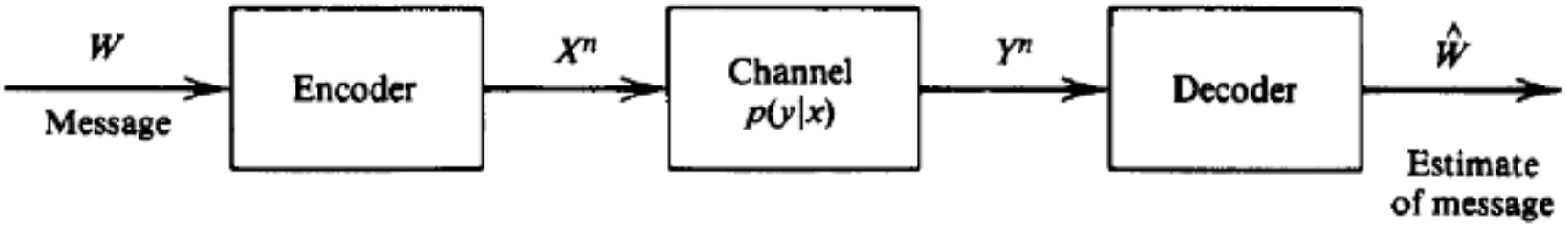
信道容量的性质

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

- 信道容量的非负性：$C \geq 0$
- 信道容量的极值性：$C \leq \log|\mathcal{X}|$

  $C \leq \log|\mathcal{Y}|$
- 信道容量的可达性：*I(X;Y)*是关于*p(x)*的一个凹函数

一些重要的定义

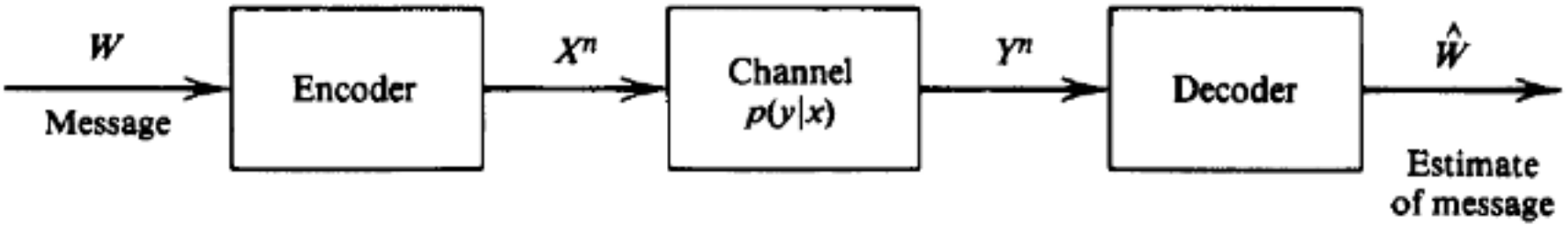


定义 离散信道：$(\mathcal{X}, p(y|x), \mathcal{Y})$ ，满足

$$p(y|x) \geq 0$$

$$\sum_y p(y|x) = 1$$

一些重要的定义

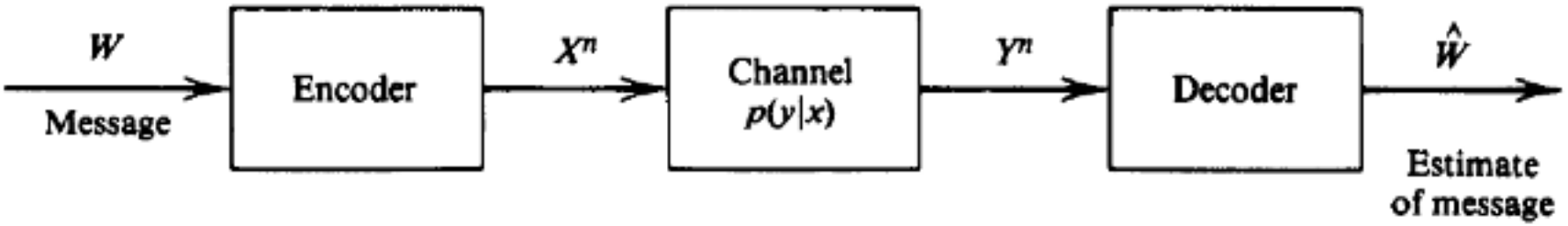


➢ 定义 离散无记忆信道的***n***次扩展是指信道 $(\mathcal{X}^n, p(y^n|x^n), \mathcal{Y}^n)$ ，其中

$$p(y_k|x^k, y^{k-1}) = p(y_k|x_k),\ k = 1, 2, \cdots, n$$

若无反馈，则 $$p(y^n|x^n) = \prod_{i=1}^{n} p(y_i|x_i)$$

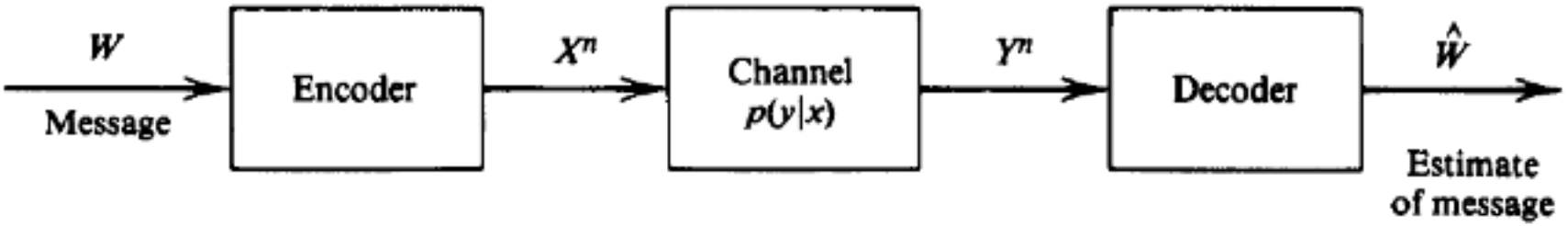
一些重要的定义



定义 信道 $(\mathcal{X}, p(y|x), \mathcal{Y})$ 的(*M,n*)码：

1. 下标集 $\{1, 2, \cdots, M\}$
2. 编码函数 $X^n : \{1, 2, \cdots, M\} \to \mathcal{X}^n$ 生成码字 $x^n(1), x^n(2), \cdots, x^n(M)$ 。所有码字的集合称作码簿(codebook)
3. 译码函数 $g : \mathcal{Y} \to \{1, 2, \cdots, M\}$

一些重要的定义



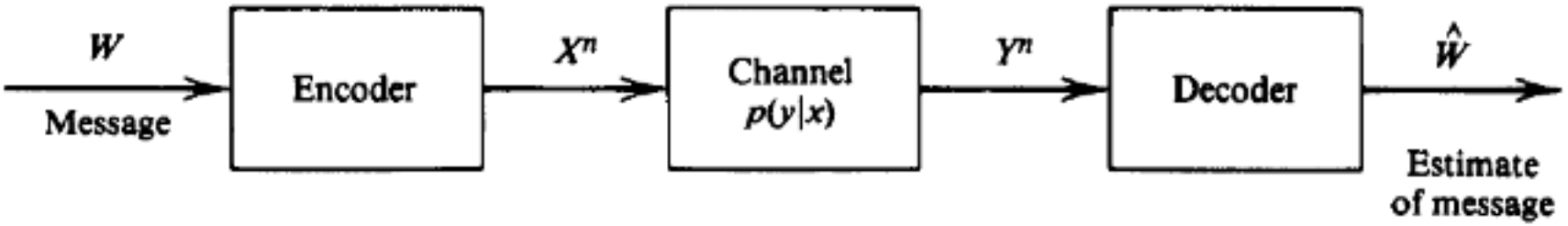
- 定义 条件误差概率：

$$\lambda_i = \Pr(g(Y^n) \neq i | X^n = x^n(i)) = \sum_{y^n} p(y^n|x^n(i))\delta(g(y^n) \neq i)$$

- 定义 (M,n)码的最大误差概率

$$\lambda^{(n)} = \max_{i \in (1,2,\cdots,M)} \lambda_i$$

一些重要的定义

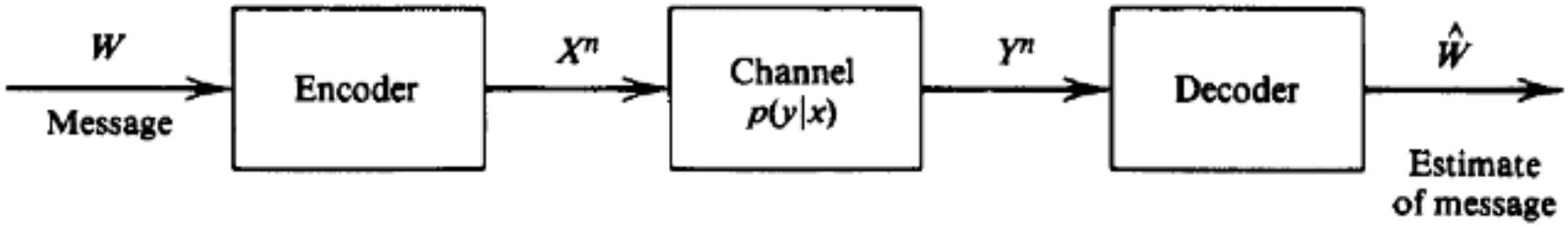


➢ 定义 (*M*,*n*)码的（算术）平均误差概率：

$$P_e^{(n)} = \frac{1}{M}\sum_{i=1}^{M}\lambda_i$$

✓ 若W是从集合$\{1, 2, \cdots, M\}$中的均匀分布选出的，以及$X^n = x^n(W)$，则 $P_e^{(n)} \triangleq \Pr(W \neq g(Y^n))$

一些重要的定义

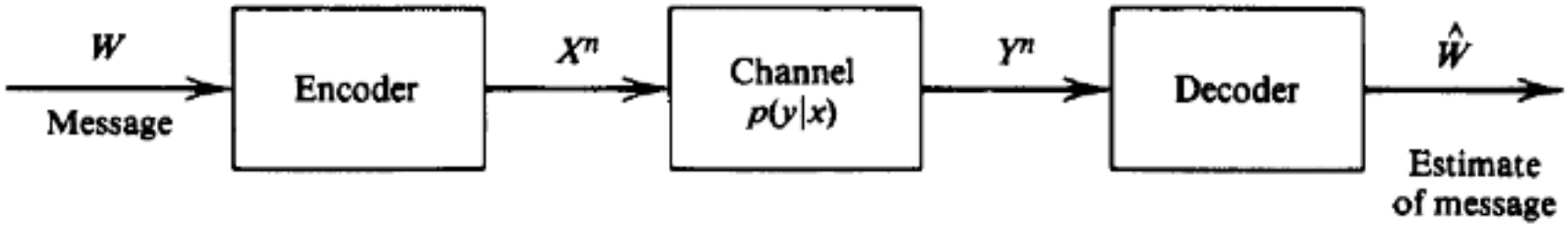


- 定义 (M,n)码的码率(rate)：

$$R = \frac{\log M}{n} \text{ 比特/传输}$$

- 定义 码率是可达的：存在$(\lceil 2^{nR} \rceil, n)$码序列，满足当$n \to \infty$时，$\lambda^{(n)} \to 0$
- 信道容量定义为所有可达码率的上界

一些重要的定义



- 定义 (*M*,*n*)码的码率(rate)：

$$R = \frac{\log M}{n} \text{ 比特/传输}$$

- 定义 码率是可达的：存在 $(2^{nR}, n)$ 码序列，满足当 $n \to \infty$ 时，$\lambda^{(n)} \to 0$
- 信道容量定义为所有可达码率的上界

联合典型序列(Jointly Typical Sequences)

- 定义 服从分布p(x,y)的联合典型序列 $\{x^n, y^n\}$ 所构成的集合 $A_\epsilon^{(n)}$ 满足

$$
\begin{aligned}
A_\epsilon^{(n)} = \{&(x^n, y^n) \in \mathcal{X}^n \times \mathcal{Y}^n : \\
&\left| -\frac{1}{n} \log p(x^n) - H(X) \right| < \epsilon \\
&\left| -\frac{1}{n} \log p(y^n) - H(Y) \right| < \epsilon \\
&\left| -\frac{1}{n} \log p(x^n, y^n) - H(X,Y) \right| < \epsilon \Big\}
\end{aligned}
$$

其中 $p(x^n, y^n) = \prod_{i=1}^{n} p(x_i, y_i)$

联合AEP（渐进均分性）

- **定理** 设 (X^n, Y^n) 为服从 $p(x^n, y^n) = \prod_{i=1}^{n} p(x_i, y_i)$ 的i.i.d.的*n*长序列，那么
  1. 当 $n \to \infty$ 时，$\Pr\left((X^n, Y^n) \in A_\epsilon^{(n)}\right) \to 1$
  2. $|A_\epsilon^{(n)}| \leq 2^{n(H(X,Y)+\epsilon)}$ 。
  3. 如果 $(\tilde{X}^n, \tilde{Y}^n) \sim p(x^n)p(y^n)$ ，即 $\tilde{X}^n$ 与 $\tilde{Y}^n$ 是独立的且与 $p(x^n, y^n)$ 有相同的边际分布，那么

$$\Pr\left((\tilde{X}^n, \tilde{Y}^n) \in A_\epsilon^{(n)}\right) \leq 2^{-n(I(X;Y)-3\epsilon)}$$

而且，对于充分大的*n*，

$$\Pr\left((\tilde{X}^n, \tilde{Y}^n) \in A_\epsilon^{(n)}\right) \geq (1-\epsilon)2^{-n(I(X;Y)+3\epsilon)}$$

信道编码定理

- 信道编码定理：只要码率小于信道容量，信息就可以通过该信道可靠的传输
- 信道编码定理使用的新思想：
  - ✓ 允许任意小的非0误差概率存在；
  - ✓ 连续使用信道许多次，以保证可以使用大数定理 ；
  - ✓ 在随机选择的码簿上计算平均误差概率，这样可以使概率对称，而且可以用来证明至少存在一个好的编码。

信道编码定理（香农第二定理）

- **定理** 对于离散无记忆信道，小于信道容量C的所有码率都是可达的。具体来说，对任意码率$R<C$，存在一个$(2^{nR}, n)$码序列，它的最大误差概率为$\lambda^{(n)} \to 0$。反之，任何满足$\lambda^{(n)} \to 0$的$(2^{nR}, n)$码序列必定有$R \leq C$。
- $W \to X^n(W) \to Y^n \to \hat{W}$

信道编码定理

- 与无失真信源编码定理类似，信道编码定理也是一个存在性定理，它指出信道容量是一个临界值，只要信息传输率不超过这个临界值，信道就可几乎无失真地把信息传送过去，否则就会产生失真。即在保证信息传输率低于(直至无限接近)信道容量的前提下，错误概率趋于“0”的编码是存在的。虽然定理设有具体说明如何构造这种码，但它对信道编码技术与实践仍然具有根本性的指导意义。

信道编码定理的证明

$$W \to X^n(W) \to Y^n \to \hat{W}$$

1. 生成服从分布p(x)的随机码。

$$\mathscr{C} = \begin{bmatrix} x_1(1) & x_2(1) & \cdots & x_n(1) \\ \vdots & \vdots & \ddots & \vdots \\ x_1(2^{nR}) & x_2(2^{nR}) & \cdots & x_n(2^{nR}) \end{bmatrix}$$

2. 将随机码通知发送者和接收者，并假定双方都知道信道转移矩阵
3. 依均匀分布选取一条消息W

$$\Pr(W = w) = 2^{-nR}, \quad w = 1, 2, \cdots, 2^{nR}$$

4. 通过信道发送 $X^n(w)$

信道编码定理的证明

$$W \to X^n(W) \to Y^n \to \hat{W}$$

5. 接收者收到的序列服从分布

$$P(y^n|x^n(w)) = \prod_{i=1}^{n} p(y_i|x_i(w))$$

6. 联合典型译码
   - ✓ $(X(\hat{W}), Y^n)$是联合典型的
   - ✓ 不存在其他的下标 $W' \neq \hat{W}$ 满足 $(X^n(W'), Y^n) \in A_\varepsilon^{(n)}$
7. 如果译码结果不等于W，则说明译码错误

信道编码定理的逆定理

$$1 + P_e \log |\mathcal{X}| \geq H(X|Y)$$

- $W \to X^n(W) \to Y^n \to \hat{W}$
- 设 Y^n 为 X^n 经过容量C的离散无记忆信道传输所得的信号，则

$$I(X^n; Y^n) \leq nC \text{ 对于任意的} p(x^n)$$

- 零误差码的情况下
- 费诺不等式：设离散无记忆信道的输入消息W服从 $\{1, 2, \cdots, 2^{nR}\}$ 上的均匀分布，则

$$H(W|\hat{W}) \leq 1 + P_e^{(n)} nR$$

重复码（Repetition Code）

- 信道编码的目的是通过增加冗余使得在一些信息损失或损坏的情况下，接受者仍可能恢复出信息。
- 简单的编码方案：重复所需传送的信息
  - 码率为1/n
  - 译码方案按多数原则
  - n趋向于无穷时，最大误差概率趋向于零
  - n趋向于无穷时，码率也趋向于零

奇偶校验码

- 采用某种巧妙的方法把所需传送的比特联合起来
- 奇偶校验码
  - 从n-1个信息比特的分组出发，选取第n个比特，使得整个分组的奇偶检验数为0；
  - 发现奇数次错误
  - 不能发现偶数次错误
  - 不能纠正错误

汉明码的例子

- 例 所有长度为3的非0二元向量的集合

$$H=\begin{bmatrix}0&0&0&1&1&1&1\\0&1&1&0&0&1&1\\1&0&1&0&1&0&1\end{bmatrix}$$

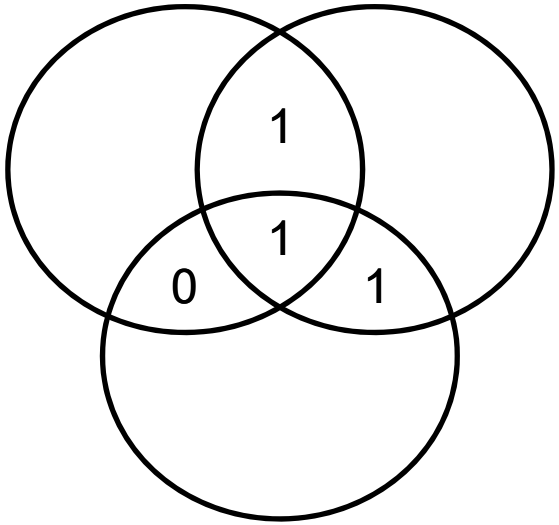
- 模2运算
- H的零空间（码字集合）

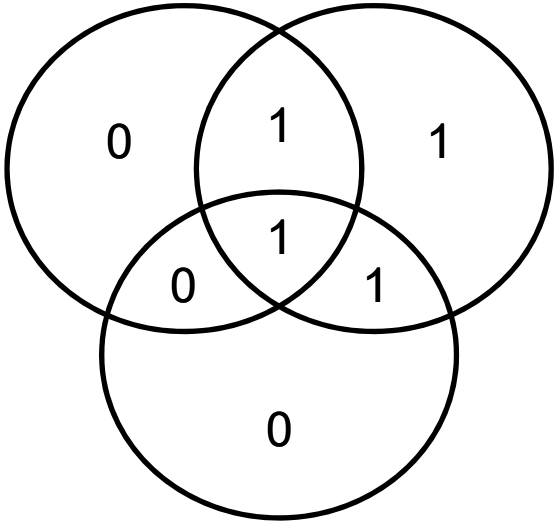
0000000	0100101	1000011	1100110
0001111	0101010	1001100	1101001
0010110	0110011	1010101	1110000
0011001	0111100	1011010	1111111

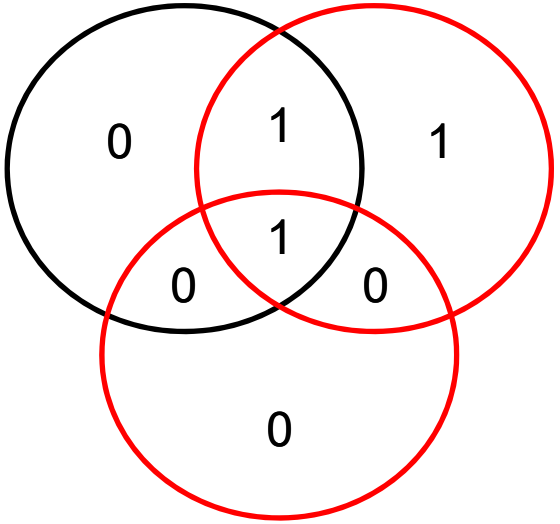
汉明码的码字集合

- H的零空间的性质
  - 4维线性子空间
  - 除全0码外，任何码字中1的最小数目为3，该最小数称为码的**最小重量**
  - 任意码字至少在3个位置上不同，不同的最小位置数称为码的**最小距离**
  - 对线性码来说，最小距离等于最小重量
  - 可以纠一个位置的错

汉明码纠错的文式图



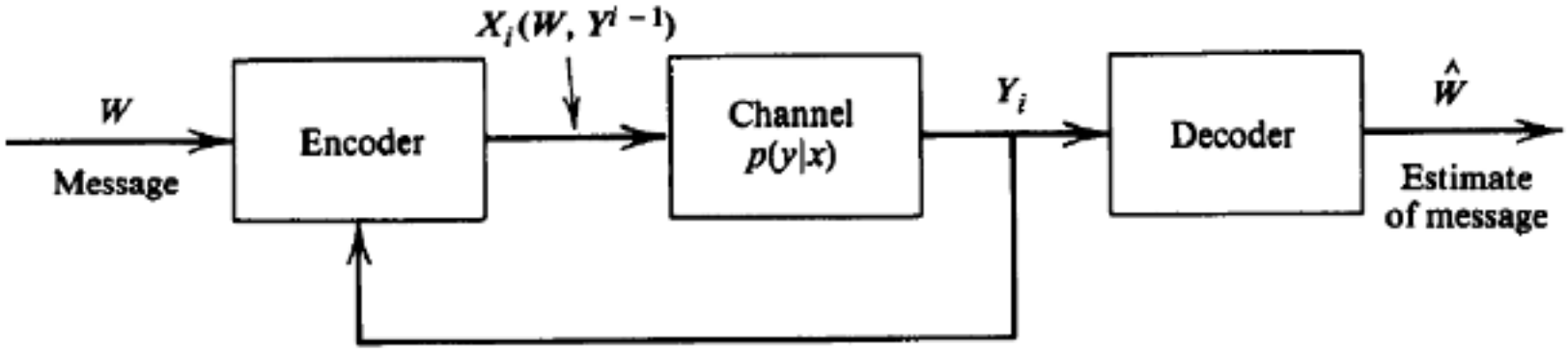




汉明码

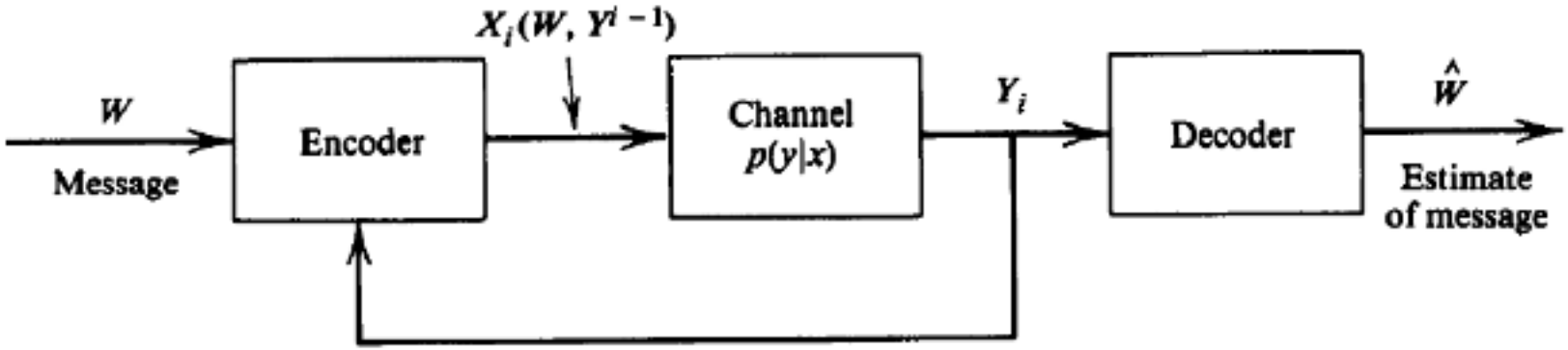
- 码字的前k个比特代表消息，后n-k个比特留作奇偶校验位;
- 汉明码的参数：分组长度n，信息比特数k，最小距离d;
- (n,k,d)汉明码
- 可纠错(d-1)/2;

反馈信道



- $(2^{nR}, n)$反馈码：一个映射序列 $X_i(W, Y^{i-1})$ 和一个译码函数序列 $g : \mathcal{Y}^n \to \{1, 2, \cdots, 2^{nR}\}$
- 离散无记忆信道的带反馈容量 C_{FB} ：反馈码可以达到的所有码率的上确界

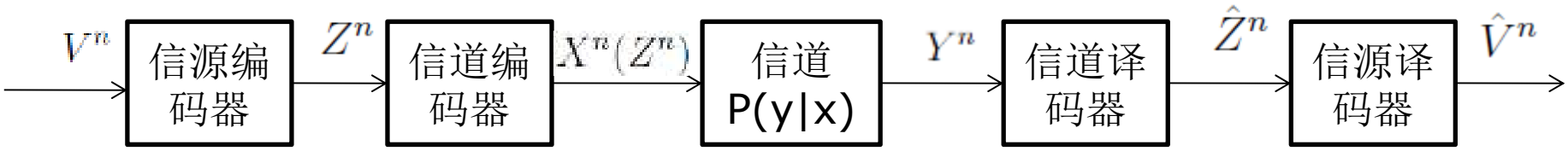
反馈容量



- $W \to Y^n \to \hat{W}$
- **定理** 反馈容量：

$$C_{FB} = C = \max_{p(x)} I(X;Y)$$

信源信道分离定理



- 两种传输方式一样有效
- 如果H<C，信源可以被可靠传输，如果H>C，则信源不能被可靠传输
- 理论上，可以独立地设计信源码和信道码