译码

- 编码是比较容易实现的，难点在于译码，一般线性码的译码问题是NP难问题。编码理论的一个中心任务就是设计有效的译码算法。译码方法在大体上分为两类：

(i) 可用于任意码的一般译码方法；

(ii) 用于特定的码或码类的专用译码方法。

二元对称信道

Definition 2.1.6 A *q-ary symmetric channel* is a memoryless channel which has a channel alphabet of size q such that

(i) each symbol transmitted has the same probability p ($<1/2$) of being received in error;
(ii) if a symbol is received in error, then each of the $q-1$ possible errors is equally likely.

In particular, the *binary symmetric channel* (*BSC*) is a memoryless channel which has channel alphabet $\{0, 1\}$ and channel probabilities

$$\mathcal{P}(1 \text{ received} \mid 0 \text{ sent}) = \mathcal{P}(0 \text{ received} \mid 1 \text{ sent}) = p,$$
$$\mathcal{P}(0 \text{ received} \mid 0 \text{ sent}) = \mathcal{P}(1 \text{ received} \mid 1 \text{ sent}) = 1 - p.$$

Thus, the probability of a bit error in a BSC is p. This is called the *crossover probability* of the BSC (see Fig. 2.2).

二元对称信道

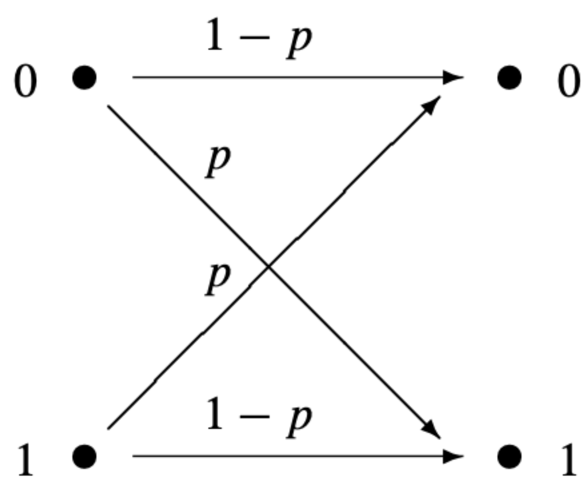

Fig. 2.2. Binary symmetric channel.

1 极大似然译码

Suppose that codewords from a code C are being sent over a communication channel. If a word $\mathbf{x}$ is received, we can compute the forward channel probabilities

$$\mathcal{P}(\mathbf{x} \text{ received} \mid \mathbf{c} \text{ sent})$$

for all the codewords $\mathbf{c} \in C$. The *maximum likelihood decoding* (*MLD*) *rule* will conclude that $\mathbf{c_x}$ is the most likely codeword transmitted if $\mathbf{c_x}$ maximizes the forward channel probabilities; i.e.,

$$\mathcal{P}(\mathbf{x} \text{ received} \mid \mathbf{c_x} \text{ sent}) = \max_{\mathbf{c} \in C} \mathcal{P}(\mathbf{x} \text{ received} \mid \mathbf{c} \text{ sent}).$$

1 极大似然译码

There are two kinds of MLD:

(i) *Complete maximum likelihood decoding* (*CMLD*). If a word **x** is received, find the most likely codeword transmitted. If there are more than one such codewords, select one of them arbitrarily.

(ii) *Incomplete maximum likelihood decoding* (*IMLD*). If a word **x** is received, find the most likely codeword transmitted. If there are more than one such codewords, request a retransmission.

2 极小距离译码

Definition. If a word $\mathbf{x}$ is received, the minimum distance decoding rule will decode $\mathbf{x}$ to $\mathbf{c_x}$ is minimal among all the codewords in C, i.e.,

$$d(\mathbf{x}, \mathbf{c_x}) = \min_{\mathbf{c} \in C} d(\mathbf{x}, \mathbf{c}).$$

Similarly, complete and incomplete minimum distance decoding rule.

3 校验子译码

- 假设Alice 发送给Bob的码字是 **c**, Bob接收到的字是 **r**, 我们有 **r**=**c**+**e**，其中 $e \in F_q^n$, **e** 表示传输中的发生的错误，称为错误向量。
- **定义 若** $C \subseteq F_q^n$ 是一个参数为[n,k]的线性码，H是C的一个校验矩阵，令 $r \in F_q^n$, 则

$$s = Hr^T = He^T \in F_q^{n-k}$$

称为 **r** 的校验子，也称为伴随式。

因此 **r**与 **e** 有相同的校验子 $\Leftrightarrow Hr^T = He^T$

$$\Leftrightarrow H(r-e)^T = 0 \Leftrightarrow r-e \in C.$$

定理

设$C \subseteq F_q^n$ 是一个线性码，则 $x, y \in F_q^n$有相同的校验子 $\Leftrightarrow x \in y+C.$

即 x,y 有相同的陪集。

陪集

- 定义　设 $C\subseteq F_q^n$是一个线性码， $x\in F_q^n$. 定义陪集 x+C 为

$$x+C=\{x+c\mid c\in C\}.$$

性质：

(i) 若 $x\in y+C$, 则 x+C=y+C.

(ii) 对每一对x, y, 或者 x+C=y+C 成立 或者

$$x+C\bigcap y+C=\phi$$

- 例　令 $C \subseteq F_2^4$ 定义为

C={(0000), (1100), (0011), (1111)}

写出它的所有陪集。

- 定义 在一个陪集中，具有最小重量的元素称为陪集首。
- 注： 对一个特定的陪集而言， 陪集首可能不唯一。

校验子译码算法：

(1) Bob 接收到字 **r.**
(2) 他计算 **r** 校验子$s = Hr^T$ 。
(3) 若 s=0, 则没有错误发生。
(4) 若 $s \neq 0,$ 则Bob观察所有的元素都有校验子s的陪集，找出陪集首并假定为 **e.**
(5) 他计算 c=r-e进行纠错。

这种方法的优点在于Bob能够在Alice 开始发送消息之前计算并储存一个校验子和陪集首的表，则当他收到消息之后，纠错是很快的。

- 例 参数为 [7 , 4] 的二元Hamming码的一个校验矩阵是

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

如果Alice 和Bob约定使用这个码， 则 Bob在Alice发送消息之前计算如下：

校验子	陪集首	校验子	陪集首
$\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$	$(0\ 0\ 0\ 0\ 0\ 0\ 0)$	$\begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$	$(0\ 0\ 0\ 1\ 0\ 0\ 0)$
$\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$	$(0\ 0\ 0\ 0\ 0\ 0\ 1)$	$\begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$	$(0\ 0\ 1\ 0\ 0\ 0\ 0)$
$\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$	$(0\ 0\ 0\ 0\ 0\ 1\ 0)$	$\begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$	$(0\ 0\ 1\ 0\ 0\ 0\ 0)$
$\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$	$(0\ 0\ 0\ 0\ 1\ 0\ 0)$	$\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$	$(0\ 1\ 0\ 0\ 0\ 0\ 0)$

假设Bob接收到 $r=(1011100)$,则计算 r 的校验子得到

$$s = Hr^T = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

他可以查表该向量的陪集首和校验子，因此计算(1011100)-(0000100)=(1011000)是一个有效的码字，因此 e=(0000100), Bob可以把(1011100)纠正为(1011000).