第十章 差错控制编码

10.1 差错控制编码的基本原理
10.2 常用的简单编码
10.3 线性分组码
10.4 循环码

10.1 差错控制编码的基本原理

西安交通大學

发生误码原因：

- 系统特性不理想（乘性干扰），数字信号通过系统时产生波形失真，在接收端判决时会产生判决错误。
- 信道中的噪声（加性干扰），这种干扰随机地与信号叠加，使信号波形产生失真，引起判决错误。

解决办法：

（1）适当增加发送信号功率

（2）选择抗噪声性能好的调制解调方式

（3）采用最佳接收

（4）采用差错控制编码

10.1 差错控制编码的基本原理

西安交通大學

信源编码目的：提高通信系统的有效性

差错控制编码（信道编码、抗干扰编码或纠错编码）

目的：提高通信的可靠性

差错控制编码方法：通过人为地加入多余度，使信号在一定的干扰条件下，具有检测或纠正错码的能力。

10.1 差错控制编码的基本原理

西安交通大學

信道分类：随机信道、突发信道、混合信道

（1）随机信道：错码出现互不相关、统计独立

如：高斯白噪声引起的错码

（2）突发信道：错码的出现前后相关。错码出现时，在短时间内有一连串的错码，而该时间过后又有较长的时间无错码。

如：随机的强突发脉冲干扰引起的错码。

（3）混合信道：产生的错码既有随机错码又有突发错码

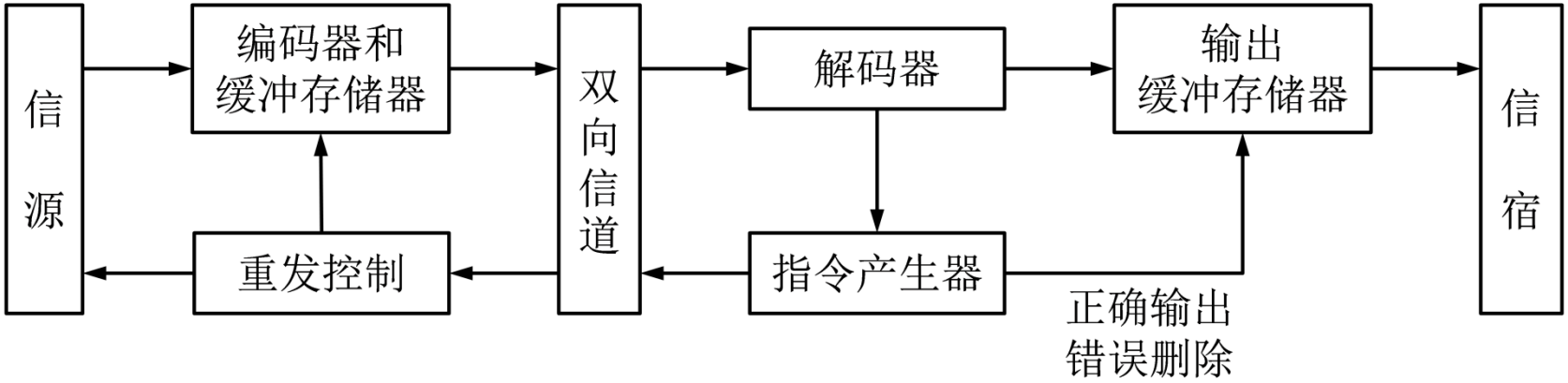
常用的差错控制方式

1. ARQ (Automatic Repeat Request)方式

(自动请求重发或检错重发)

发端发送出可以发现错误的码字。经过传输到接收端译码后，如果没有发现错误，则输出。如果发现错误，则自动请求发端重发，直到正确接收到码字为止。

10.1 差错控制编码的基本原理



ARQ系统组成

特点：设备简单、双向信道、传输效率低

2.反馈校验方式

接收端收到码字后，立即将接收到的码字返回发送端。发送端将返回的码字与发端缓冲存储器中相应的码字比较，若发现与发送码不同，即认为产生了错误，就重发上一次的码字。

特点：设备简单、双向信道、传输效率低

3. FEC（Forward Error Control，前向纠错）方式

发送端发出的码字不仅能够发现错误，而且能够纠正错误。在接收端译码后，若没有错误则直接输出。若有错误，则在接收端自动纠正后，再输出。

特点：不需要反向信道、实时性好、传输效率高。
但纠错编译码方法复杂。

4. HEC（Hybrid Error Control，混合纠错）方式

将ARQ方式和前向纠错方式结合使用。传输错码较少时，采用前向纠错方式，自动纠正错码。在错码较多时，采用ARQ方式自动请求重发。

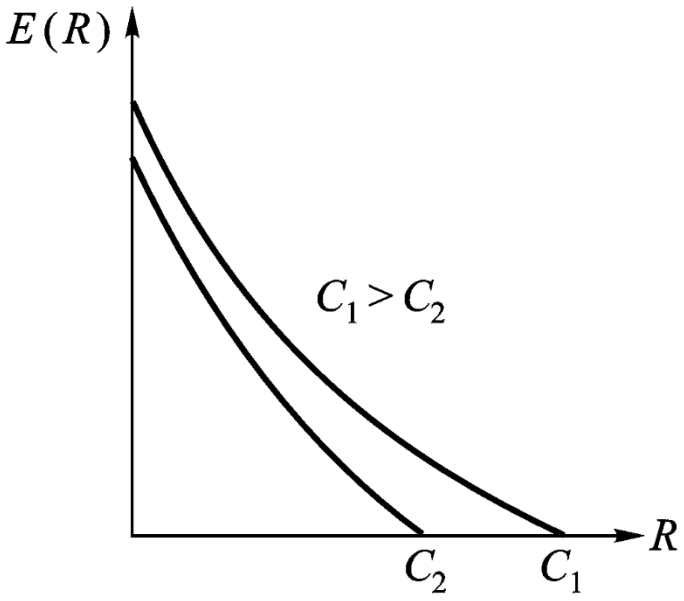
香农有扰信道编码定理：

在有扰信道中只要信息的传输速率R小于信道容量C，总可以找一种编码方法，使信息以任意小的差错概率通过信道传送到接收端，即误码率P_e可以任意小，而且传输速率R可以接近信道容量C。但若$R > C$，在传输过程中必定带来不可纠正错误，不存在使差错概率任意小的编码。

误码率：$$P_e = e^{-nE(R)}$$

式中，n为编码的码字长度(简称码长)；

$E(R)$为误码指数。



减小误码率P_e的两种途径：

（1）n及R一定时，增加信道容量C。

$E(R)$随C的增加而增大。

由信道容量公式知，增加C，可通过增加S和B来实现；

（2）在C及R一定的情况下，增加n可以使P_e指数减小

10.1 差错控制编码的基本原理

重复编码的例子：天气预报消息发布

	晴	雨	纠检错能力
第一种编码方法	1	0	无纠检错能力
第二种编码方法	11	00	可检1位错（01、10）、无纠错能力
第三种编码方法	111	000	可检2位错、可纠1位错（001、010、100 ⇒ 000；011、101、110 ⇒ 111）

许用码、禁用码、监督码元、最大似然准则

码间距离d及检错纠错能力

码字：由信息位和监督位组成的一组码元

用$\mathbf{C}=(c_{n-1}\ c_{n-2}\ \cdots\ c_0)$表示

（许用码、禁用码）

码元：组成码字的元素，用$\mathbf{C}_i$表示

码长：码字中码元的个数，用n表示

码组：由多个许用码组成的一组码字

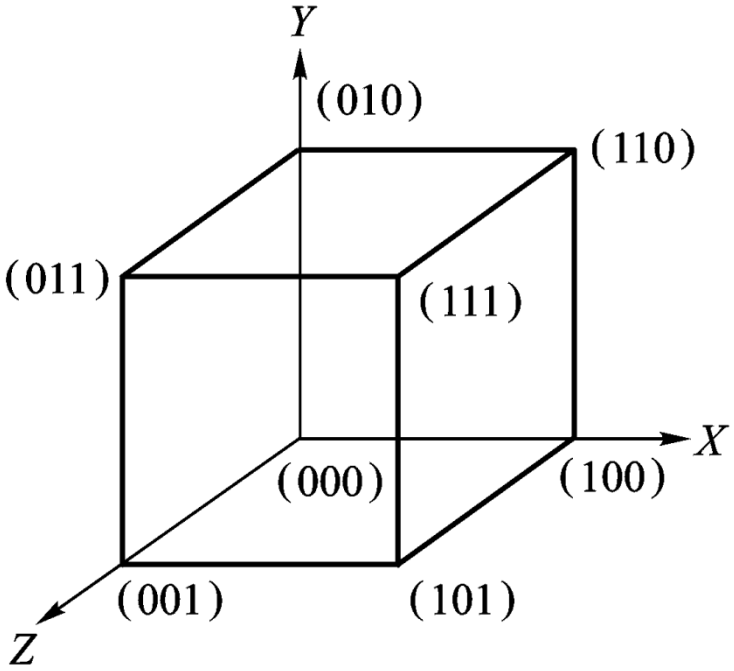
码间距离d（code distances）

简称码距，又称汉明距离，是码组中任意两个码字之间对应位上码元取值不同的个数。等于两个码字对应位模2相加后“1”的个数。

$$d(c_i, c_j) = \sum_{p=0}^{n-1} (c_{ip} \oplus c_{jp})$$

例：111 、000，d =3；11、00 ，d =2。

101110 、 101011 ，d =2 。

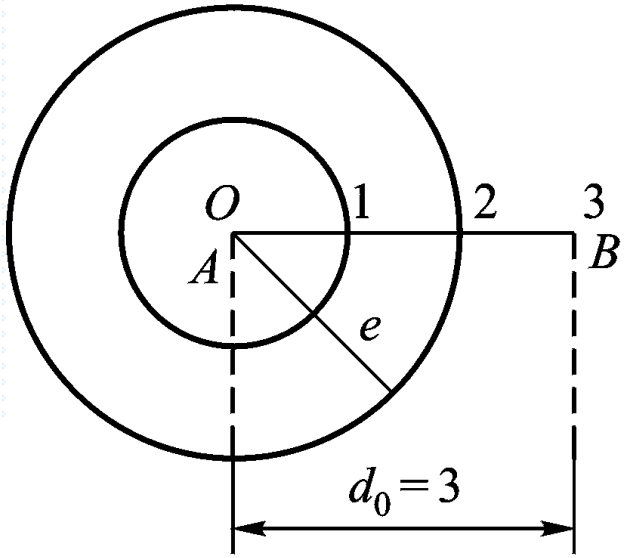


码间距离的几何意义

最小码间距离d_0：码组中各码字之间最小的码距

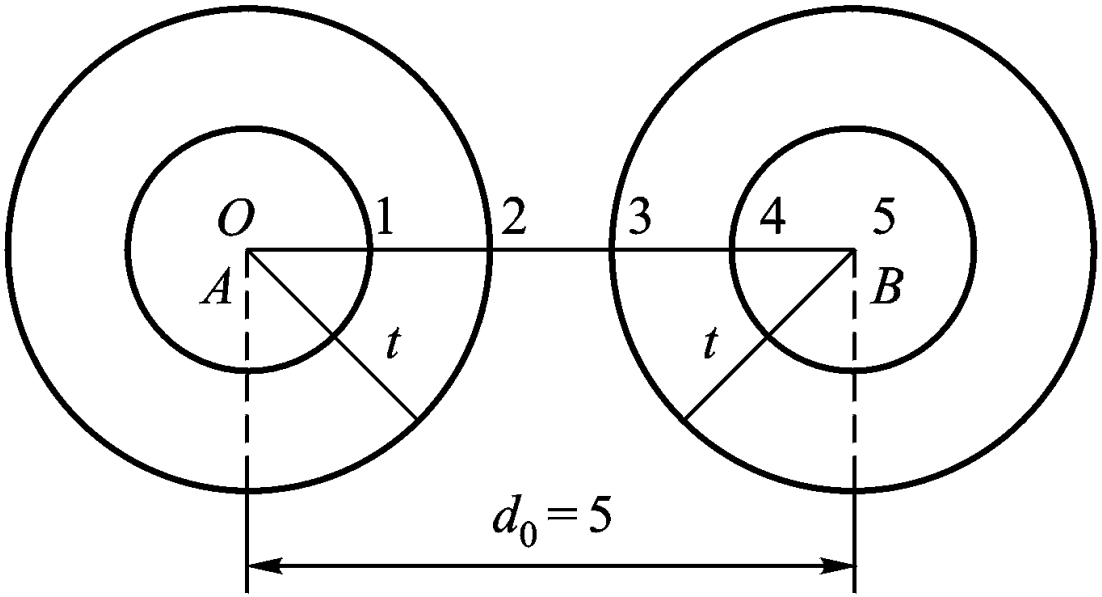
最小码间距离d_0与检错纠错能力的关系

(1) 当码组仅用于检测错误时，若要求检测e个错误，则最小码距为：$d_0 \geq e+1$



西安交通大学

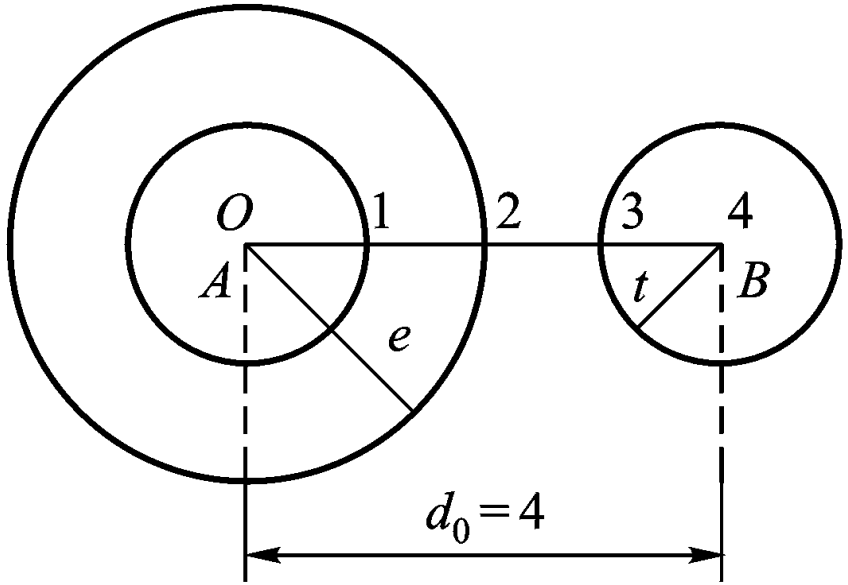
(2) 当码组仅用于纠正错误时，为纠正t个错误，要求最小码距为：$d_0 \geq 2t+1$



西安交通大學

(3) 当码组既要检错，又要纠错时，为纠正t个错误，同时检测e个错误，则要求的最小码距为

$$d_0 \geq e + t + 1 \quad (e > t)$$



差错控制编码的效果

在码长为n的码字中刚好发生r个错误的概率为：

$$P_n(r)=C_n^r P^r(1-P)^{n-r}$$

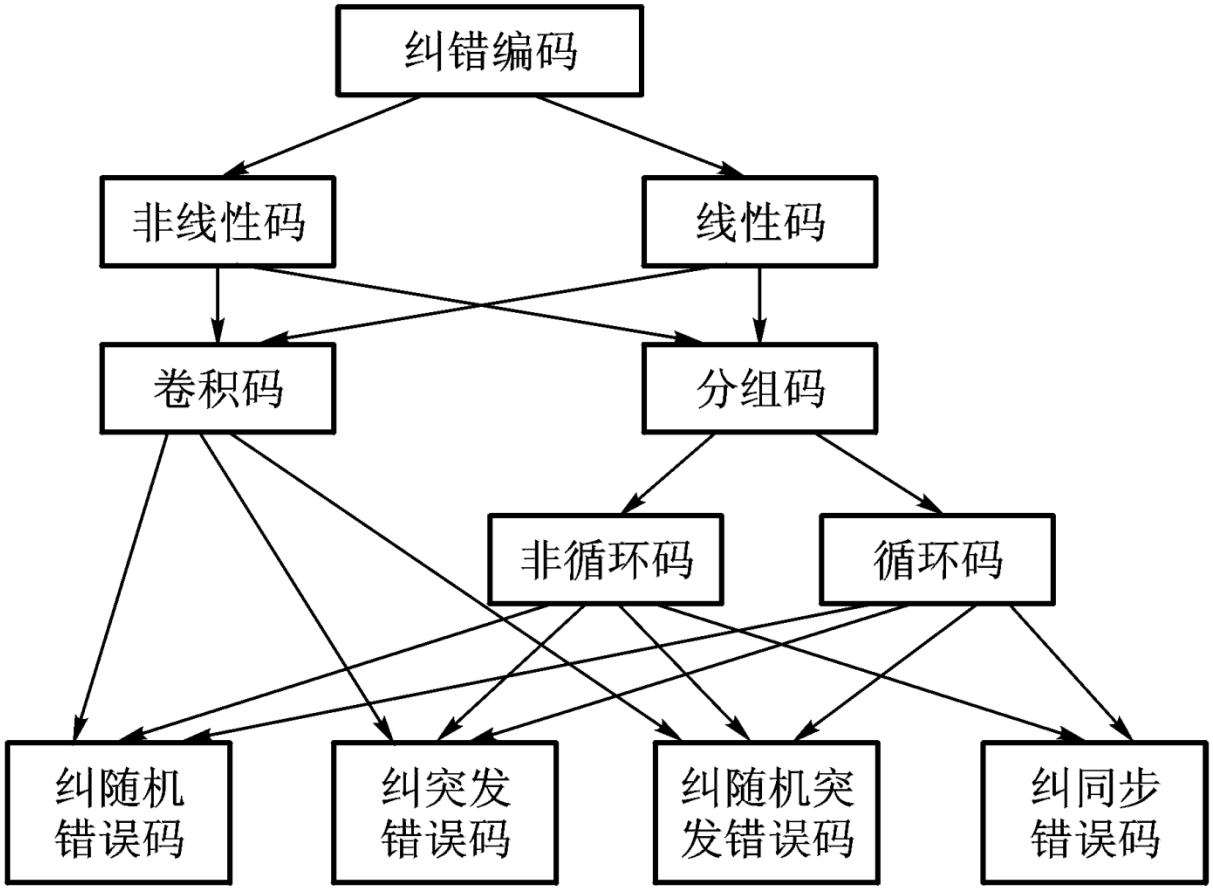
当$n=7$，$P=10^{-3}$时，有：

$$P_7(1)\approx 7\times 10^{-3}$$

$$P_7(2)\approx 2.1\times 10^{-5}$$

$$P_7(3)\approx 3.5\times 10^{-8}$$

纠错编码的分类


纠错编码
非线性码
线性码
卷积码
分组码
非循环码
循环码
纠随机
错误码
纠突发
错误码
纠随机突
发错误码
纠同步
错误码

编码效率

$$\eta = \frac{k}{n} = \frac{n-r}{n}$$

k：码字的信息码元个数

r：监督码元个数

n：码元总的个数（总码长）

$$n = k + r$$

10.2 常用的简单编码

西安交通大學

1. 奇偶监督码

2. 二维奇偶监督码

3. 恒比码（等重码）

西安交通大學

1.奇偶监督码（奇偶校验码）

广泛应用于计算机数据传输中。

编码规则：在每个分组的信息位后增加监督位，无论信息位有多少位，监督位只有一位。

偶监督码：给信息位后增加一位监督位，使码字中“1”的数目为偶数。

$$C_{n-1} \oplus C_{n-2} \oplus \cdots \oplus C_1 \oplus C_0 = 0$$

上式为偶监督码的监督关系，也称为校验方程

检测能力：检测奇数个错

10.2 常用的简单编码

奇监督码： 给信息位后增加一位监督位，使码字中“1”的数目为奇数。其校验方程为

$$C_{n-1} \oplus C_{n-2} \oplus \cdots \oplus C_1 \oplus C_0 \oplus 1 = 0$$

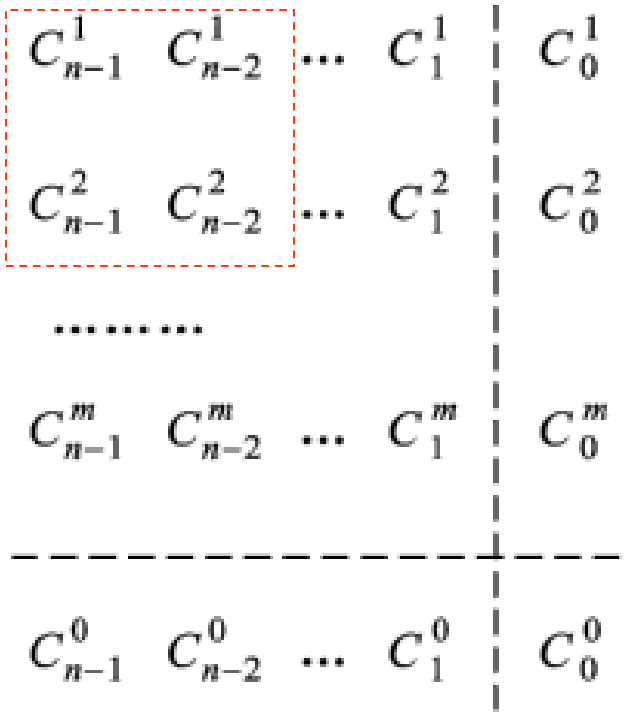
奇偶监督码的编码效率η较高，尤其是当码长n较大时，这一特点更为明显。

西安交通大学

2.二维奇偶监督码

（方阵码、行列监督码
或水平—垂直奇偶监督码）

编码方法：把m个信息码字排列成一个方阵，每个码字构成方阵的一行，在每一行的最后按奇偶监督规则增加一位水平监督位，再按列的方向每列增加一位垂直监督位（包括行监督位的列）



10.2 常用的简单编码

检测能力：

- ✓ 可以检测每行的奇数个错和每列的奇数个错；
- ✓ 行列交叉可以检测每行或每列的偶数个错；
- ✓ 但当发生的错误为刚好构成矩形的四个错码时，则不能检测出错误。

纠错能力：

只有一行出现奇数个错码时，按行检测可以判断出错在那一行，按列检测可以确定该行的那一列发生了错误，行列交叉可以判断错误的位置，即可纠错。此外，此种编码的效率较高。

3.恒比码（等重码）

每个许用码含有相同数目的“1”。码字中“1”与“0”的个数之比是恒定的，故称恒比码。码字中“1”的个数称为码重，因此恒比码又称等重码。

对于某种特定的恒比码，当码长确定后，其“1”的个数就确定了。所以在检测中只要计算“1”的个数就可以确定是否发生错误。恒比码多用于电传机中。

我国电传机传输汉字采用的是“5中取3”恒比码，其码长为5，码字中“1”的个数为3。这种码我国称为保护电码。码长为5的二进制数共有32种组合，选择其中含有3个“1”的组合作为许用码，为10个。

我国的保护电码与国际电码

阿拉伯数字	保护电码	国际电码	阿拉伯数字	保护电码	国际电码
0	01101	01101	5	00111	00001
1	01011	11101	6	10101	10101
2	11001	11001	7	11100	11100
3	10110	10000	8	01110	01100
4	11010	01010	9	10011	00011

西安交通大学

一、线性分组码概念

线性分组码是指信息位和监督位满足一组线性方程，即其编码规则可用一组线性方程来描述的分组码。

信息位k ⟶ 信息位k　监督位r　　记为(n, k)

n: 码元总的个数（总码长）

$$n = k + r$$

10.3 线性分组码

系统码： 码字的前一部分是连续 k 位信息码元，后一部分是连续 r 位监督码元，具有这种结构的线性分组码称为系统码。否则称为非系统码。

纠错原理

n 位长的二进制码共有 2^n 码字。

k 位长的二进制码共有 2^k 码字，故 2^k 个信息段仅构成 2^k 个 n 位长的码字，称为许用码字

而其他 2^n-2^k 个码字为禁用码字，当出现禁用码字时就可以发现或纠正错误。

西安交通大学

二、线性分组码的一致检验（监督矩阵）矩阵[H]

[H]矩阵是用来说明监督码元与信息码元之间关系的矩阵

以（7，3）码（k=3, r =4, n =7）为例：

码字矢量 $\mathbf{C}=[c_6c_5c_4c_3c_2c_1c_0]$

信息码元：$c_6c_5c_4$　　监督码元：$c_3c_2c_1c_0$

监督方程为：

r 行

$$\begin{cases} c_3 = c_6 \oplus c_4 \\ c_2 = c_6 \oplus c_5 \oplus c_4 \\ c_1 = c_6 \oplus c_5 \\ c_0 = c_5 \oplus c_4 \end{cases} \Rightarrow \begin{cases} c_6 \oplus c_4 \oplus c_3 = 0 \\ c_6 \oplus c_5 \oplus c_4 \oplus c_2 = 0 \\ c_6 \oplus c_5 \oplus c_1 = 0 \\ c_5 \oplus c_4 \oplus c_0 = 0 \end{cases}$$

将上方程系数写为矩阵形式

7×1

$4\times7\,(r\times n)$

$$\left[\begin{array}{ccc:cccc} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right] \begin{bmatrix} c_6 \\ c_5 \\ c_4 \\ c_3 \\ c_2 \\ c_1 \\ c_0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$4\times3\,[P]$ $(r\times k)$

$4\times4\,[I_4]$ $(r\times r)$

令 $[H]=\begin{bmatrix}1&0&1&1&0&0&0\\1&1&1&0&1&0&0\\1&1&0&0&0&1&0\\0&1&1&0&0&0&1\end{bmatrix}$ ⇒ $[H]=[P\ \ I_4]$

称[H]为线性分组码的一致检验矩阵（监督矩阵）

故有：$[H][C]^T=[0]^T$ ⇒ $[C][H]^T=[0]$

西安交通大学

[H]的性质：

（1）[H]是$(r\times n)$阶矩阵，即行数为监督码元个数，列数为码长。[H]中每行元素表明监督方程中线性相关的码元系数。

（2）[H]=[P I_4]，即[H]由两部分组成，前半部称为[P]矩阵$(r\times k)$，后半部称为[I]矩阵$(r\times r)$。此时，称[H]为典型矩阵，只有系统码才具有。

（3）[H]是接收端检错的依据。$[R][H]^T=[0]$

西安交通大学

三、线性分组码的生成矩阵[G]

[G]矩阵是在给定信息位的条件下，如何生成码字的矩阵。

仍以（7，3）码（k=3, r =4, n =7）为例：

码字矢量 $\mathbf{C}=[c_6c_5c_4c_3c_2c_1c_0]$ 信息码元：$c_6c_5c_4$；监督码元：$c_3c_2c_1c_0$

在监督方程基础上，加上信息码元方程。

监督方程

$$\begin{cases} c_3 = c_6 \oplus c_4 \\ c_2 = c_6 \oplus c_5 \oplus c_4 \\ c_1 = c_6 \oplus c_5 \\ c_0 = c_5 \oplus c_4 \end{cases}$$

$$\begin{cases} c_3 = c_6 \oplus c_4 \\ c_2 = c_6 \oplus c_5 \oplus c_4 \\ c_1 = c_6 \oplus c_5 \\ c_0 = c_5 \oplus c_4 \end{cases} \Rightarrow \begin{cases} c_6 = c_6 \\ c_5 = c_5 \\ c_4 = c_4 \\ c_3 = c_6 \oplus c_4 \\ c_2 = c_6 \oplus c_5 \oplus c_4 \\ c_1 = c_6 \oplus c_5 \\ c_0 = c_5 \oplus c_4 \end{cases} \Rightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} c_6 \\ c_5 \\ c_4 \end{bmatrix} = [C]^T$$

$$\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\\1&0&1\\1&1&1\\1&1&0\\0&1&1\end{bmatrix}\begin{bmatrix}c_6\\c_5\\c_4\end{bmatrix}=[C]^T$$

转置

$$[c_6c_5c_4]\begin{bmatrix}1&0&0&1&1&1&0\\0&1&0&0&1&1&1\\0&0&1&1&1&0&1\end{bmatrix}=[C]$$

生成矩阵[G]

码字矩阵

故有：$[c_6c_5c_4]\,[G]=[C]$

10.3 线性分组码

$3\times 7\ (k\times n)$

生成矩阵 $[G]=\left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{array}\right]=[I_k \quad Q]$

$3\times 3[I_k]$ $(k\times k)$ $\qquad$ $3\times 4[Q]$ $(k\times r)$

[G]的性质：

（1）[G]是 $(k \times n)$ 阶矩阵，即行数为信息码元个数，列数为码长。故若[G]给定，则在已知信息码元的情况下，就可得到码字（生成矩阵）。

（2）$[G]=[I_K \ Q]$ 为标准生成矩阵，[G]中每行是互相独立的（线性不相关）。实际上，[G]中每行就是一个许用码字。

推论：由K互相独立的码字可构成生成矩阵。

[G]的性质（二）

（3）[G]与[H]的关系

$$[G]=[I_K \quad Q] \qquad [H]=[P \; I_r]$$

可以证明：$[Q]=[P]^T$ 或 $[P]=[Q]^T$

如上例中：

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

[G]的性质（三）

（4）对偶码

将一码组（A）中的[H]当作另一码组（B）中的[G]，或反之，则称B为A的对偶码。

如：$[H]_{(7,3)} \rightarrow [G]_{(7,4)}$　　$[G]_{(7,3)} \rightarrow [H]_{(7,4)}$

则（7，4）为（7，3）的对偶码。

（5）封闭性

线性分组码组中，任意两个码字之和仍是此码组中的一个码字。

西安交通大學

四、线性分组码的译码及伴随式

1.译码

译码是判断接收码字是否为许用码，即根据

$$[C][H]^T=[0]$$

判断接收码字 $[R]=[r_{n-1},r_{n-2},\cdots,r_0]$ 是否满足

$$[R][H]^T=[0]$$

定义 $[E]=[C]\oplus[R]$ 为错误图样，当 $[E]=0$ 时，无误码。

$$[E]=[e_{n-1},\cdots,e_1,e_0]$$

当 $e_i=1$ 时，认为第 i 位发生了误码。

将 $[R]=[C]\oplus[E]$ 代入 $[R][H]^T=[0]$ 中，得：

$$[C][H]^T\oplus[E][H]^T=[E][H]^T=[S]_{1\times r}$$

称 $[S]=[s_{r-1},\cdots,s_1,s_0]$ 为伴随式，又称校验子。

当 $[E]=[0,\cdots,0]_{1\times n}$ 时，$[S]=[0,\cdots,0]_{1\times r}$ 无错误出现。

当 $e_i=1$ 时，认为第 i 位发生了误码。

此时，$[S]_{1\times r}=[E][H]^T$ 为 $[H]$ 中的第 i 列

故可用 $[H]$ 的列来表示误码位置。

由 $[S]=[s_{r-1},\cdots,s_1,s_0]$ 伴随式可检测 2^r-1 个错误。

要纠正小于或等于 t 个错，必须满足

$$2^r-1\geq C_n^1+C_n^2+\cdots+C_n^t$$

或

$$2^r\geq\sum_{i=0}^{t}C_n^i$$

汉明码

汉明码是一种可以纠正单个随机错误的线性分组码。它是一种完备码，编码效率很高。

$$2^r - 1 = n$$

$$(n, k) \rightarrow \left(2^r - 1\ ,\ 2^r - 1 - r\right)$$

编码效率

$$\eta = \frac{k}{n} = \frac{n-r}{n} = 1 - \frac{r}{n} = \frac{2^r - 1 - r}{2^r - 1} = 1 - \frac{r}{2^r - 1}$$

例：

$$r=3,\ n=2^r-1=7,\ k=n-r=4 \rightarrow (7,4)$$

$$\eta=\frac{k}{n}=\frac{4}{7}=57\%$$

$$r=7,\ n=2^r-1=127,\ k=n-r=120 \rightarrow (127,120)$$

$$\eta=\frac{k}{n}=\frac{120}{127}=94\%$$

汉明码特点

(1) 汉明码长 $n=2^r-1,\ r\geq 3$

(2) 信息位 $k=n-r=2^r-1-r$

(3) 最小码距 $d_0=3$，纠错能力为 $t=1$ 。

(4) 编码效率高。$n\uparrow\rightarrow\eta\uparrow$

10.4 循环码

西安交通大学

一、 循环码的基本概念及码多项式

定义：具有循环性的线性分组码。

循环性：码组中任一许用码字（全“0”码除外）循环左移（或循环右移）后所得到的码字仍为该循环码组中的另一许用码字。

$$[C]=[c_{n-1},c_{n-2},\cdots,c_1,c_0]\longrightarrow\begin{cases}c_{n-1},c_{n-2},\cdots,c_1,c_0\\ c_{n-2},c_{n-3},\cdots,c_0,c_{n-1}\\ \cdots\\ c_0,c_{n-1},\cdots,c_2,c_1\end{cases}$$

一种（7，3）循环码

序号	移位次数	信息位	监督位	序号	移位次数	信息位	监督位
0		000	0000	4	6	100	1110
1	0	001	1101	5	4	101	0011
2	5	010	0111	6	3	110	1001
3	1	011	1010	7	2	111	0100

西安交通大学

码多项式：把循环码中的码字用多项式来表示，码字中各码元的取值作为码多项式的系数。

$$[C]=[c_{n-1},c_{n-2},\cdots,c_1,c_0]$$

$$T(x)=c_{n-1}x^{n-1}+c_{n-2}x^{n-2}+\cdots+c_1x+c_0$$

例：对 $(7,3)$ 码

$$1001110\rightarrow T(x)=x^6+x^3+x^2+x$$

10.4 循环码

码多项式运算：

$$\frac{F(x)}{N(x)}=Q(x)+\frac{r(x)}{N(x)} \rightarrow F(x)=Q(x)N(x)+r(x) \quad (\text{模}N(x)\text{运算})$$

[定理10.4.1] 若$T(x)$是长为n的循环码中某个许用码字的码多项式，则$x^i \cdot T(x)$在按模x^n+1运算下，也是该循环码中一个许用码字的码多项式。

如：（7，3）循环码中许用码字**0011101**的码多项式为

$$T(x)=x^4+x^3+x^2+1$$

则

$$\frac{x^3T(x)}{x^7+1}=1+\frac{x^6+x^5+x^3+1}{x^7+1}$$

西安交通大學

$$x^3T(x) \equiv x^6 + x^5 + x^3 + 1 \quad (\text{模 } x^7 + 1 \text{ 运算})$$

$x^6 + x^5 + x^3 + 1$ 对应的码字为**1101001**，它是该（7，3）循环码中的一另一许用码字，它是循环码**0011101**左移3次后形成的。

西安交通大学

生成多项式及生成矩阵

[定理10.4.2] 在循环码（n，k）中，n-k 次幂的码多项式有一个，且仅有一个，用$g(x)$表示。称这唯一的n-k次多项式$g(x)$为循环码的生成多项式。$g(x)$的常数项不为零。

- ✓ 一旦$g(x)$确定，则该（n，k）循环码就被确定了。
- ✓ $g(x)$是循环码中幂次最低的码多项式。
- ✓ 由它左移就可产生其它码多项式。如$xg(x)$、$x^2g(x)$、$x^3g(x)$等。
- ✓ 用k个互相独立的码多项式$g(x)$、$xg(x)$、$x^2g(x)$… $x^{k-1}g(x)$可以构造出循环码的生成矩阵$\mathbf{G}(x)$

生成矩阵

$$G(x)=\begin{bmatrix} x^{k-1}g(x) \\ x^{k-2}g(x) \\ \cdot \\ x^{1}g(x) \\ g(x) \end{bmatrix}$$

例如，（7，3）循环码中最高次幂为$n-k$次的码字为**0010111**，其生成多项式$g(x)=x^4+x^2+x+1$。则利用上式可得其生成矩阵$\mathbf{G}(x)$为

$$G(x)=\begin{bmatrix} x^2g(x) \\ x^1g(x) \\ g(x) \end{bmatrix} \rightarrow G(x)=\begin{bmatrix} 1011100 \\ 0101110 \\ 0010111 \end{bmatrix}$$

上式不符合典型生成矩阵的形式，所以它不是典型生成矩阵，由它编出的码字不是系统码。但是对此矩阵作线性变化可以变换成典型生成矩阵的形式。

西安交通大学

[定理10.4.3] 循环码（n，k）的生成多项式$g(x)$是x^n+1的一个因式。

产生$g(x)$的方法：对（x^n+1）进行因式分解，从中找出一个最高次幂为（$n-k$）次且常数项不为零的因式，作为生成多项式$g(x)$。

例如：对于（7，3）循环码，$g(x)$的最高次幂为4。可从（x^7+1）中分解得到$g(x)$。

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

生成多项式可选为 $g_1(x)=(x+1)\ (x^3+x^2+1)=x^4+x^2+x+1$

或 $g_2(x)=(x+1)\ (x^3+x+1)=x^4+x^3+x^2+1$

循环码的编码及解码

1. 编码

设信息码多项式为$m(x)$

$$m(x)=m_{k-1}x^{k-1}+m_{k-2}x^{k-2}+\ldots+m_1x+m_0$$

$m(x)$的最高次幂为$k-1$。

将$m(x)$左移$n-k$位成为$x^{n-k}m(x)$，其最高次幂为$n-1$。$x^{n-k}m(x)$的前一部分为连续k位信息码，后一部分为$r=n-k$位的“0”。所以在它的后一部分添上监督码，就编出了相应的系统码。

西安交通大学

$$\frac{x^{n-k}m(x)}{g(x)}=q(x)+\frac{r(x)}{g(x)}\rightarrow$$

$$T(x)=x^{n-k}m(x)+r(x)=g(x)q(x)$$

$T(x)$能被$g(x)$整除，其最高次幂为n-1。$T(x)$ 的前一部分为连续k位信息码，后一部分为r=n-k位的监督码。$T(x)$为循环码的码多项式，而且是系统码。

例：（7，3）循环码编码过程。

选择生成多项式：$g(x)=x^4+x^3+x^2+1$，设信息码为111。

（1）信息位$m(x)$左移$n-k$位成为$x^{n-k}m(x)$。信息码111左移4位成为1110000。

$$m(x)=x^2+x+1 \rightarrow x^{n-k}m(x)=x^4(x^2+x+1)$$

（2）作除法，求出余式$r(x)$

$$\frac{x^6+x^5+x^4}{x^4+x^3+x^2+1}=x^2+\frac{x^2}{x^4+x^3+x^2+1} \quad \left(\frac{1110000}{11101}=100+\frac{0100}{11101}\right)$$

（3）构成系统码$T(x)=x^{n-k}m(x)+r(x)$

1110000+0100=1110100

2.解码：分检错和纠错两种情况

检错解码原理：它利用任何码多项式都可以被生成多项式$g(x)$整除原理实现。设发送码字为$T(x)$，接收码多项式为$R(x)$，做除法有

$$\frac{R(x)}{g(x)}=q'(x)+\frac{r'(x)}{g(x)}$$

判断余式是否为零，即可判断码字$R(x)$有无错码。

纠错解码原理

纠正错误，需要知道错误图样$E(x)$，以便纠正错误。原则上纠错解码可按以下步骤进行。

（1）用生成多项式$g(x)$除接收码字$R(x)=T(x)+E(x)$，得到余式；

（2）按余式用查表方法或通过某种运算得到错误图样$E(x)$；

（3）从$R(x)$中减去$E(x)$，得到纠错后的原发送码字$T(x)$。

本节习题：10-4、 10-5、10-8、
10-10、10-13、10-18