《信息论与编码》第七、第八章习题解答

7-2　设 E_n 是 n 维二元矢量空间中所有具备偶数重量的矢量集合。证明 E_n 是线性码，并确定 E_n 的参数（n, k, d），以及它的系统生成矩阵。

［证明］设 $\mathbf{c}_1$ 和 $\mathbf{c}_2$ 均属于 E_n，即均是重量为偶数的 n 维二元矢量。于是 $\mathbf{c}_1+\mathbf{c}_2$ 的重量为

$$w_H(\mathbf{c}_1+\mathbf{c}_2)=w_H(\mathbf{c}_1)+w_H(\mathbf{c}_2)-2w_H(\mathbf{c}_1\cdot\mathbf{c}_2)$$

是偶数，其中 $\mathbf{c}_1\cdot\mathbf{c}_2$ 表示 $\mathbf{c}_1$ 和 $\mathbf{c}_2$ 的交截。因此 $\mathbf{c}_1+\mathbf{c}_2\in E_n$，所以 E_n 是一个线性码。

由于对称性，在所有长度为 n 的二元矢量中，奇数重量与偶数重量的矢量数相等，所以 E_n 中码字数为 2^{n-1}，从而 $k=n-1$；又 E_n 中最小非零码字的重量为 2，所以 $d=2$，于是 E_n 的参数为 $(n,n-1,2)$。

7-4　设二元线性码 M 的生成矩阵为

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

求 M 的最小距离。

［解］由 G 生成的（5，3）码的八个码字为

（00000），（10011），（00101），（01111）

（10110），（01010），（11100），（11001）

所以非零码字最小重量为 2，从而最小 Hamming 矩离 $d_{\min}=2$。

7-5　设二元线性码 M 的生成矩阵为

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

建立码 M 的标准阵，并对码字 11111 和 10000 分别进行译码。

［解］由 G 生成的（5，2）码 M 的标准阵列为

（00000），（11010），（01010），（10000）

（00001），（11011），（01011），（10001）

（00010），（11000），（01000），（10010）

（00100），（11110），（01110），（10100）

（00011），（11001），（01001），（10011）

（00101），（11111），（01111），（10101）

（01100），（10110），（00110），（11100）

（00111），（11101），（01101），（10111）

接收到矢量（11111）**译成码字**（11010）

接收到矢量（10000）**译成码字**（10000）

7-7　**设二元线性码** M **的生成矩阵为**

$$G=\left[\begin{array}{c|cccc} & 1 & 1 & 0 & 0 \\ & 1 & 0 & 1 & 0 \\ & 0 & 1 & 1 & 0 \\ I_7 & 1 & 1 & 1 & 1 \\ & 1 & 1 & 0 & 1 \\ & 0 & 1 & 0 & 1 \\ & 1 & 0 & 0 & 1 \end{array}\right],$$

确定 M **的校验矩阵并求其最小距离。**

［解］ 与 G **相应的系统生成矩阵为**

$$G^{'}=\left[\begin{array}{cccc|c} 1 & 1 & 0 & 0 & \\ 1 & 0 & 1 & 0 & \\ 0 & 1 & 1 & 0 & \\ 1 & 1 & 1 & 1 & I_{7\times 7} \\ 1 & 1 & 0 & 1 & \\ 0 & 1 & 0 & 1 & \\ 1 & 0 & 0 & 1 & \end{array}\right]$$

相应的校验矩阵为

$$H'=\left[\begin{array}{c|ccccccc} & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ I_{4\times 4} & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right]$$

G **和** $G^{'}$ **的差别仅是列的置换，所以** H **和** H' **的差别也是同样的列置换，所以**

$$H=\left[\begin{array}{ccccccc|c} 1 & 1 & 0 & 1 & 1 & 0 & 1 & \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & I_{4\times 4} \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & \end{array}\right]$$

该码的校验矩阵任意二列线性独立，而第 1，2，3 **列之和为零矢量，所以存在着相关的三列，从而最小** Hamming **重量为** 3。

$d_{\min}=3$

7-8 **建立二元（7，4）**Hamming **码的包含陪集首项和伴随式的伴随表，并对收到的矢量** 0000011，1111111，1100110，1010101 **进行译码。**

[**解**]（7.4）Hamming **码的校验矩阵为**

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

错误形式和伴随矢量表为

e	**s**
（1000000）	（100）
（0100000）	（010）
（0010000）	（110）
（0001000）	（001）
（0000100）	（101）
（0000010）	（011）
（0000001）	（111）

接收矢量　伴随矢量　相应译出码字

（0000011）$\Rightarrow$（100）$\Rightarrow$（1000011）

（1111111）$\Rightarrow$（000）$\Rightarrow$（11111111）

（1100110）$\Rightarrow$（000）$\Rightarrow$（1100110）

（1010101）$\Rightarrow$（000）$\Rightarrow$（1010101）

7-9 **设二元（15，11）**Hamming **码的校验矩阵为**

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

试对收到的字 011011001111000，**和** 001100110011000 **进行译码。**

[**解**]

接收到矢量	**伴随式**	**错误形式**	**译出码字**
（011011001111000），	（0110），	（000001000000000），	（011010001111000）
（001100110011000），	（1111），	（000000000000001），	（001100110011001）

7-11 **研究系统码（8，4），其校验方程为**

$$c_0 = m_1 + m_2 + m_3$$

$$c_1 = m_0 + m_1 + m_2$$

$$c_2 = m_0 + m_1 + m_3$$

$$c_3 = m_0 + m_2 + m_3$$

其中 m_0, m_1, m_2, m_3 **是信息位，**c_0, c_2, c_3, c_4 **是校验位，求此码的生成矩阵和校验矩阵，并证明此码的最小距离为** 4**。**

［解］设系统码的校验矩阵为

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & g_{00} & g_{10} & g_{20} & g_{30} \\ 0 & 1 & 0 & 0 & g_{01} & g_{11} & g_{21} & g_{31} \\ 0 & 0 & 1 & 0 & g_{02} & g_{12} & g_{22} & g_{32} \\ 0 & 0 & 0 & 1 & g_{03} & g_{13} & g_{23} & g_{33} \end{bmatrix}$$

任何码字

$$\mathbf{c} = (c_0 c_1 c_2 c_3 m_0 m_1 m_2 m_3)$$

满足 $\mathbf{c} \cdot H^T = 0$

即

$$c_0 = g_{00}m_0 + g_{10}m_1 + g_{20}m_2 + g_{30}m_3$$

$$c_1 = g_{01}m_0 + g_{11}m_1 + g_{21}m_2 + g_{31}m_3$$

$$c_2 = g_{02}m_0 + g_{12}m_1 + g_{22}m_2 + g_{32}m_3$$

$$c_3 = g_{03}m_0 + g_{13}m_1 + g_{23}m_2 + g_{33}m_3$$

所以

$$g_{00} = 0\text{，}\ g_{10} = g_{20} = g_{30} = 1$$

$$g_{31} = 0\text{，}\ g_{01} = g_{11} = g_{21} = 1$$

$$g_{22} = 0\text{，}\ g_{02} = g_{12} = g_{32} = 1$$

$$g_{13} = 0\text{，}\ g_{03} = g_{23} = g_{33} = 1$$

因此

$$H = \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{array}\right]$$

所以

$$G = \left[\begin{array}{cccc|cccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right]$$

因为在 H **矩阵中没有任何** 3 **列线性相关，同时** 1，2，3，6 **列是线性相关的，所以最**

小重量为 4，也就是最小 Hamming 重量为 4。

7-12 证明 Hamming 距离的三角不等式，即若 c_1, c_2, c_3 是 $GF(2)$ 上三个长度为 n 的矢量，则

$$d(c_1, c_2) + d(c_2, c_3) \geq d(c_1, c_3)$$

［**证明**］ 设 $c_1 = (c_{10}, c_{11}, \cdots, c_{1,n-1})$

$c_2 = (c_{20}, c_{21}, \cdots, c_{2,n-1})$

$c_3 = (c_{30}, c_{31}, \cdots, c_{3,n-1})$

考虑第 i 位分量，如果 c_{1i} 和 c_{3i} 取相同符号，即

$$d(c_{1i}, c_{3i}) = 0$$

则显然 $d(c_{1i}, c_{2i}) + d(c_{2i}, c_{3i}) \geq d(c_{1i}, c_{3i}) = 0$

如果 c_{1i} 和 c_{3i} 取相异符号，即

$$d(c_{1i}, c_{3i}) = 1$$

则不管 c_{2i} 取什么符号，至少它与 c_{1i} 和 c_{3i} 中一个符号相反，所以

$$d(c_{1i}, c_{2i}) + d(c_{2i}, c_{3i}) \geq d(c_{1i}, c_{3i}) = 1$$

所以 $d(c_1, c_2) + d(c_2, c_3) \geq d(c_1, c_3)$

8-2 另 m 是一个正整数，若 m 不是质数，证明集合 $\{1,\ 2, \cdots,\ m\}$ 在模 m 加法和乘法下不是域。

［**证明**］

∵ m 不是质数 可设 $m = k \cdot t$，设 $1 < k \leq t < m$，则 $t \geq \sqrt{m}$

考虑 k 和集合中其它非零元的模 m 乘法：

$$\begin{array}{llcll}
k \cdot 1 & \bmod & m & = & k > 1 \\
k \cdot 2 & \bmod & m & = & 2k > 1 \\
\vdots & & & & \vdots \\
k \cdot \sqrt{m} & \bmod & m & = & \sqrt{m}\ k > 1 \\
k \cdot t & \bmod & m & = & 0 \\
k \cdot (t+1) & \bmod & m & = & k > 1
\end{array}$$

$$k\cdot(t+2) \mod m = 2k>1$$
$$\vdots \qquad\qquad \vdots$$
$$k\cdot(t+\sqrt{m}) \mod m = \sqrt{m}k>1$$
$$\vdots \qquad\qquad \vdots$$

∴ k 和集合中其它非零元的模 m 乘法在集合 $\{0,k,\ k+1,\cdots,\ \sqrt{m}\cdot k\}$ 中取值，其中不包括“1”，即 k 不存在逆元。

∴ 集合 $\{1,\ 2,\cdots,\ m\}$ 在模 m 加法和乘法下不是域。

8-4 根据本原多项式 $P(X)=1+X+X^3$ 构造 $GF(2^3)$ 表；列出每个元素的幂，多项式和矢量表示，决定每一元素的阶。

[解]：

$GF(2^3)$ 的 8 个元素：

(000)	0	(110)	$1+a$
(100)	1	(101)	$1+a^2$
(010)	a	(011)	$a+a^2$
(001)	a^2	(111)	$1+a+a^2$

∵ 由定理 8.1.4 可得， $GF(2^3)$ 中非零元素可能的阶数是 1 或 7

∴ 1 的阶数为 1，其余非零元素的阶数为 7

8-7 考虑由 $g(X)=1+X+X^4$ 生成的(15,11)循环 Hamming 码。

(a) 确定此码的校验多项式。
(b) 确定它对偶码的生成多项式。
(c) 找出此码的系统生成矩阵和一致校验矩阵。

[解] (a) 校验多项式

$$\begin{aligned} h(X) &= (X^{15}+1)/g(X) \\ &= X^{11}+X^8+X^7+X^5+X^3+X^2+X+1 \end{aligned}$$

(b) 对偶码生成多项式为 $h(X)$ 的倒易多项式，即

$$\begin{aligned} G^1(X) &= X^{11}\cdot h(\frac{1}{X}) \\ &= 1+X^3+X^4+X^6+X^8+X^9+X^{10}+X^{11} \end{aligned}$$

(c) 此码的一个非系统生成矩阵为

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

系统生成矩阵为：

$$G=\left(\begin{array}{cccc|c}1&1&0&0&\\0&1&1&0&\\0&0&1&1&\\1&1&0&1&\\1&0&1&0&\\0&1&0&1&I_{11\times 11}\\1&1&1&0&\\0&1&1&1&\\1&1&1&1&\\1&0&1&1&\\1&0&0&1&\end{array}\right)$$

$$H=\left(\begin{array}{c|ccccccccccc}&1&0&0&1&1&0&1&0&1&1&1\\I_{4\times 4}&1&1&0&1&0&1&1&1&1&0&0\\&0&1&1&0&1&0&1&1&1&1&0\\&0&0&1&1&0&1&0&1&1&1&1\end{array}\right)$$

8-8 设计由 $g(X)=1+X+X^4$ 生成的(15,11)循环 Hamming 码的编码器。

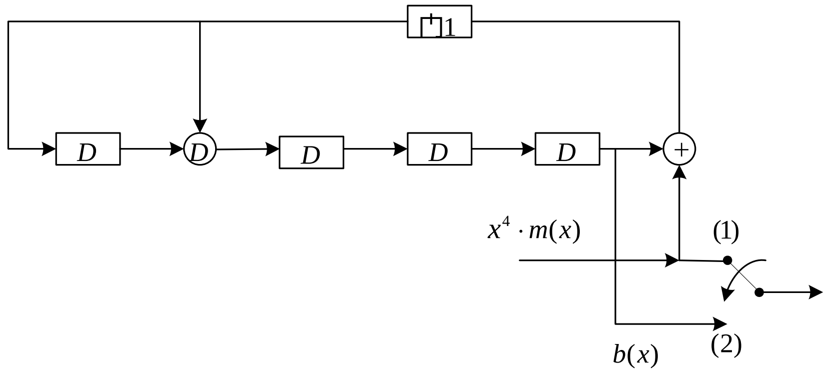
[解]：

设计一个(15,11)的系统循环码的编码过程由三步组成：

1、用 x^4 乘以消息多项式 $m(x)$

2、用 $g(x)$ 除 $x^4\cdot m(x)$ 得到余式 $b(x)$

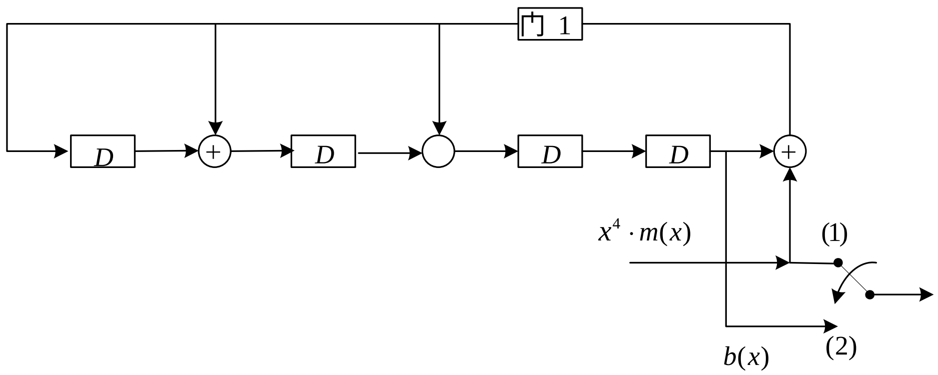
3、码字多项式 $c(x)=x^4\cdot m(x)+b(x)$



8-12 对于由生成多项式 $g(X)=1+X+X^2+X^4$ 所生成的(7,3)码，画出系统编码器。同样画出由 $g(X)=1+X^2+X^3$ 所生成的（7,4）码系统编码器。

[解]：

1、$g(X)=1+X+X^2+X^4$ 所生成的(7,3)码系统编码器：



2、$g(X)=1+X^2+X^3$ 所生成的（7,4）码系统编码器：