# 密码学与信息安全第四次作业

郭嘉　17345019　数学与应用数学

2020 年 5 月 23 日

1.（第四章第 1 题）

对 $x^4-1$ 分解得 $x^4-1=(x+1)^4$

故下面容易对三种不同情况直接写出结果

(1) 当生成多项式 $g(x)=x+1$

故生成矩阵

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

进而得到 C$=\{xG|x\in\Pi_2^3\}=\{(0000),(1100),(0110),(0011),(1001),(1010),(0101),(1111)\}$

也可以得到校验多项式 $h(x)=(x^4-1)/g(x)=x^3+x^2+x+1$

故校验矩阵为

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

(2) 当生成多项式 $g(x)=(x+1)^2=x^2+1$

故生成矩阵

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

进而得到 C$=\{xG|x\in\Pi_2^2\}=\{(0000),(1010),(0101),(1111)\}$

也可以得到校验多项式 $h(x)=(x^4-1)/g(x)=x^2+1$

故校验矩阵为

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

(3) 当生成多项式 $g(x)=(x+1)^3=x^3+x^2+x+1$

故生成矩阵

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

进而得到 C= $\{xG|x \in \Pi_2^1\} = \{(0000), (1111)\}$

也可以得到校验多项式 $h(x) = (x^4 - 1)/g(x) = x + 1$

故校验矩阵为

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

2.（第四章第 2 题）

必要性：如果 $C_2 \subset C_1$，那么由于 $g_2(x) \in C_2$, 那么 $g_2(x) \in C_1$，但由于 $g_1(x)$ 是 $C_1$ 的生成多项式, 故其整除 $C_1$ 中所有的码字，特别的，有 $g_1(x)|g_2(x)$

充分性：如果 $g_1(x)|g_2(x)$，那么 $\forall c(x) \in C_2$ 有 $g_2(x)|c(x)$ ，又由于 $g_1(x)|g_2(x)$ 因此 $g_1(x)|c(x)$, 这说明 $c(x) \in C_1$

得证

3.（第四章第 6 题）

由第 2 题结论 $C' \subset C$, 因此 C' 的最小距离 $\geq$C 的最小距离, 即 C' 的最小距离 $\geq$d

下面只需要说明 C' 的最小距离不可能为 d，由于 d 为奇数，我们只需要说明 C' 的最小距离不可能为奇数。又由于 C' 为线性码，故其最小距离等于最小重量，因此我们只需要说明 C' 码字的最小重量不可能为奇数

我们注意到 $\forall c(x) \in C'$ 都有 $g(x)(x-1)|c(x)$。特别地，有 $(x-1)|c(x)$ 即 c(1)=0 即 c(x) 的系数和为 0，这就意味着 c(x) 的重量为偶数，特别地 C' 码字的最小重量为偶数，再结合上面的讨论就完成了证明。

得证

4.（第四章第 7 题）

非系统: $a(x) = x + x^3$

$c(x) = a(x)g(x) = x + x^2 + x^3 + x^6$ 即 (0111001)

系统: $\overline{a(x)} = x^6 + x^4 = (x^3 + 1)(x^3 + x + 1) + (x + 1)$

即 $r(x) = x + 1$ ,$c(x) = \overline{a(x)} - r(x) = x^6 + x^4 + x + 1$ 即 (1100101)