密码学与信息安全第五次作业

郭嘉　17345019　数学与应用数学

2020 年 5 月 23 日

1.（第四章第 5 题）

为了得到 C 的校验矩阵，我们用 p(x) 的根来刻画循环码 C=(p(x))

设 p(x) 在 $\mathbb{F}_{2^r}$ 的一个根为 β

那么其它的 r-1 个根为 β^2,β^{2^2}...$\beta^{2^{r-1}}$

则容易验证 $C=\left\{c(x)=\sum_{i=0}^{2^r-2}c_ix^i\in\Pi_2^{(2^r-1)}|c(\beta)=c(\beta^2)=c(\beta^{2^2})=...=c(\beta^{2^{r-1}})=0\right\}$

也容易说明 C 的校验矩阵为

$$H_C=\begin{bmatrix}1 & \beta & ... & \beta^{n-1}\\ 1 & \beta^2 & ... & \beta^{2(n-1)}\\ ... & ... & ... & ...\\ 1 & \beta^{2^{r-2}} & ... & \beta^{2^{r-2}(n-1)}\\ 1 & \beta^{2^{r-1}} & ... & \beta^{2^{r-1}(n-1)}\end{bmatrix}$$

而 Ham(r,2) 的校验矩阵 H_{Ham} 以 Π_2^r 中除了零向量以外的向量为列向量

可以说明对于 $\forall c\in\Pi_2^{(2^r-1)}$ $H_{Ham}c^T=0$ 当且仅当 $H_Cc^T=0$(我在这里的说明遇到了困难，不过这个论断应该是正确的，而且应该可以通过某些技巧验证)

因此这两个码等价

2.（第五章第 3 题）

容易直接写出

$B_2(15,9,\beta)=\left\{c(x)=\sum_{i=0}^{14}c_ix^i\in\Pi_2^{(15)}|c(\beta)=c(\beta^3)=c(\beta^5)=c(\beta^7)=0\right\}$

其中 β 为 x^4+x+1 的一个根

为求生成多项式，只需要求 $\beta,\beta^2,\beta^3,\beta^4,\beta^5,\beta^6,\beta^7,\beta^8$ 在 Π_2 上的极小多项式。

由于书中例题已经求出其中一些，我们只需要求 β^7 在 Π_2 上的极小多项式, 容易得到 $m_7(x) = (x-\beta^7)(x-\beta^{14})(x-\beta^{28})(x-\beta^{56}) = x^4+x^3+1$

故生成多项式 $g(x) = m_1(x)m_3(x)m_5(x)m_7(x) = (x^4+x+1)(x^4+x^3+x^2+x+1)(x^2+x+1)(x^4+x^3+1) = x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$

3.（第五章第 5 题）

(1) 计算校验子

$v(\beta) = \epsilon(\beta) = \beta^{11}$

$v(\beta^2) = \epsilon(\beta^2) = \beta^7$

$v(\beta^3) = \epsilon(\beta^3) = \beta^{13}$

$v(\beta^4) = \epsilon(\beta^4) = \beta^{14}$

$v(\beta^5) = \epsilon(\beta^5) = 1$

$v(\beta^6) = \epsilon(\beta^6) = \beta^{11}$

(2) 解非齐次线性方程组

$\epsilon(\beta^3)\sigma_1 + \epsilon(\beta^2)\sigma_2 + \epsilon(\beta)\sigma_3 = \epsilon(\beta^4)$

$\epsilon(\beta^4)\sigma_1 + \epsilon(\beta^3)\sigma_2 + \epsilon(\beta^2)\sigma_3 = \epsilon(\beta^5)$

$\epsilon(\beta^5)\sigma_1 + \epsilon(\beta^4)\sigma_2 + \epsilon(\beta^3)\sigma_3 = \epsilon(\beta^6)$

把 (1) 中所得结果带入上述方程组，并求解

得到 $\sigma_1 = \beta^1 1$ $\sigma_2 = \beta^2$ $\sigma_3 = \beta^3$

故差错位置多项式为 $\sigma(z) = 1+\sigma_1 z+\sigma_2 z^2+\sigma_3 z^3$

得到其三个根分别为 $\beta^{-3}, \beta^{-6}, \beta^{-9}$

故差错位置为 3，6，9

差错多项式为 $\epsilon(x) = x^3+x^6+x^9$

原码字多项式 $c(x) = v(x)-\epsilon(x) = 1+x^2+x^3+x^6+x^8+x^{13}+x^{14}$

4.（第五章第 6 题）

容易直接写出

$S(7,3,\beta) =$

$\{c_f = (f(1), f(\beta), f(\beta^2), f(\beta^3), f(\beta^4), f(\beta^5), f(\beta^6)) \in \mathbb{F}_8^7 | \forall f(x) \in \mathbb{F}_8[x], deg(f(x)) \leq k-1\}$

其中 k=n-δ+1=7-3+1=5

生成矩阵为

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 \\ 1 & \beta^2 & \beta^4 & \beta^6 & \beta^1 & \beta^3 & \beta^5 \\ 1 & \beta^3 & \beta^6 & \beta^2 & \beta^5 & \beta^1 & \beta^4 \\ 1 & \beta^4 & \beta^1 & \beta^5 & \beta^2 & \beta^6 & \beta^3 \end{bmatrix}$$