密码学与信息安全第三次作业

郭嘉　17345019　数学与应用数学

2020 年 4 月 25 日

1.（第三章第 1 题）

该码若为线性码，必须为 $\mathbb{F}_2^8$ 的 k 维子空间，然而 K=20 并不是 2 的幂次，故该码不可能为线性码。

2.（第三章第 4 题）

分两个方向证明。

若该码为等距码，则对于 $\forall c_1,c_2 \in$C, 有 w(c_1)=d(c_1,0)=d(c_2,0)=w(c_2), 故为等重码

若该码为等重码，则对于 $\forall c_1,c_2,c_1',c_2' \in$C, 有 d($c_1$,$c_2$)=w($c_1$-$c_2$)=w($c_1'$-$c_2'$)=d($c_1'$,$c_2'$), 故为等距码

得证

3.（第三章第 7 题）

前两问在课上讲过相同的例题，这里仅作简略说明

(1)n=$\frac{3^2-1}{3-1}$=4

k=4-2=2

d=3

(2)

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{bmatrix}$$

这里容易验证这四个列向量任意两个线性无关

写出校验矩阵 H 后容易写出生成矩阵 G：

$$G = \begin{bmatrix} 2 & 2 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{bmatrix}$$

$(3)\alpha^T = Hv^T = \begin{bmatrix} 2 \\ 2 \end{bmatrix} = 2\begin{bmatrix} 1 \\ 1 \end{bmatrix}$

即 $\epsilon = \begin{bmatrix} 0 & 0 & 2 & 0 \end{bmatrix}$

故 $u = v - \epsilon = \begin{bmatrix} 2 & 0 & 2 & 2 \end{bmatrix}$

4.（第三章第 8 题）

根据本章习题 4，我们只需要证明重量部分。

根据定义，Ham(r,2) 对偶码的生成矩阵 G 是 $r \times (2^r - 1)$ 的矩阵, 且它的列向量是 $\mathbb{F}_2^r$ 中除了 0 向量外其它的所有元素, 注意到这点之后我们就知道 G 的每个行向量，都有 $2^r/2 = 2^{r-1}$ 个 1 和 $2^r/2 - 1 = 2^{r-1} - 1$ 个 0. 故 $\forall x \in \{\ x | x \in \mathbb{F}_2^r, x$ 仅有一个分量为 1，剩余分量都为 0 $\}$ 有 xG 为 G 中其中一个行向量，故 xG 重量为 2^{r-1}。但现在我们需要证明的是对 $\forall x \in \{x | x \in \mathbb{F}_2^r, x \neq 0\}$ 都有 xG 重量为 2^{r-1}, 即若干个 G 中的行向量之和的重量为 2^{r-1}。

下面采用计数的方法说明 G 中两个行向量之和重量为 2^{r-1}，考虑这两个行向量对应分量元素只能为 $\begin{bmatrix} 0 \\ 0 \end{bmatrix}$ $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ 这四种情况出现的次数分别为 $2^r/4 - 1$，$2^r/4$，$2^r/4$，$2^r/4$

故和为 1 的中间两种情况加起来共出现 2^{r-1} 次，这就说明了论断。

对于 G 中 m 个行向量之和,m<=r, 利用同样的计数方法，重量为 $2^{r-m}\sum_{i=0}^{\lfloor m/2 \rfloor}\binom{r}{2i+1} = 2^{r-1}$

得证