

Q27: By induction, we only need to prove that

$$\text{If } e(x) = e_0 + e_1x + \dots + e_{n-1}x^{n-1}$$

is not a codeword of C , then

$$e'(x) = e_{n-1} + e_0x + \dots + e_{n-2}x^{n-1}$$

is not a codeword of C .

Suppose $e'(x)$ is a codeword of

C . Because C is cyclic,

$e(x)$ must be a codeword of

C , which leads to a contradiction.

Q.E.D.

Q28 Suppose l_0 is the smallest such l . Then $n = a \cdot l_0 + r$

for some $0 < r < l_0$.

$$\begin{aligned}\Rightarrow \vec{v} &= \vec{v}^{(n)} = \vec{v}^{(a \cdot l_0 + r)} = \left(\vec{v}^{(a \cdot l_0)} \right)^r \\ &= \vec{v}^{(r)}\end{aligned}$$

which contradicts that l_0 is the smallest such l . Q.E.D.

Q29: For any codeword $\vec{c}_3 \in \mathcal{C}_3$

$$\vec{c}_3^{(+1)} \in \mathcal{C}_2 \quad \& \quad \vec{c}_3^{(+1)} \in \mathcal{C}_1.$$

$$\Rightarrow \vec{c}_3^{(+1)} \in \mathcal{C}_3 \quad \Rightarrow \quad \mathcal{C}_3 \text{ is cyclic.}$$

Suppose $g_1(x)$ generates \mathcal{C}_1 .

$g_2(x)$ generates \mathcal{C}_2

Claim: $g_3(x) \triangleq \text{L.C.M.}(g_1(x), g_2(x))$
generates \mathcal{C}_3 .

generates C_3 .

Proof: " \Rightarrow " $\begin{cases} g_1(x) \mid m_3(x)g_3(x) \\ g_2(x) \mid m_3(x)g_3(x) \end{cases}$

therefore any codeword

$m_3(x)g_3(x)$ belongs to C_3

" \Leftarrow "

suppose $C_3(x) \in C_3$

$$\Rightarrow \begin{cases} g_1(x) \mid C_3(x) \\ g_2(x) \mid C_3(x) \end{cases}$$

$$\Rightarrow \text{LCM}(g_1(x), g_2(x)) \mid C_3(x)$$

$\Rightarrow C_3(x)$ can be written as

$$m_3(x) \cdot g_3(x) \quad \text{Q.E.D.}$$

Q30: $d_{\min} = 2^{m-r} = 2^3 = 8$

$\underbrace{m}_{m-r} \dots 0 \quad 1 \dots 1 \dots m \quad \underbrace{m-r}_{m-r} \dots h \dots h \dots 1$

$$M_{\{0\}} = 0$$

$$\begin{aligned} b_0 + b_1 &= 0 \\ b_2 + b_3 &= 0 \\ b_4 + b_5 &= 0 \\ b_6 + b_7 &= 1 \\ b_8 + b_9 &= 1 \\ b_{10} + b_{11} &= 0 \\ b_{12} + b_{13} &= 0 \\ b_{14} + b_{15} &= 0 \end{aligned}$$

$$M_{\{1\}} = 1$$

$$\begin{aligned} b_0 + b_2 &= 1 \\ b_1 + b_3 &= 1 \\ b_4 + b_6 &= 1 \\ b_5 + b_7 &= 0 \\ b_8 + b_{10} &= 1 \\ b_9 + b_{11} &= 0 \\ b_{12} + b_{14} &= 1 \\ b_{13} + b_{15} &= 1 \end{aligned}$$

$$M_{\{2\}} = 0$$

$$\begin{aligned} b_0 + b_4 &= 0 \\ b_1 + b_5 &= 0 \\ b_2 + b_6 &= 0 \\ b_3 + b_9 &= 1 \\ b_8 + b_{12} &= 0 \\ b_9 + b_{13} &= 1 \\ b_{10} + b_{14} &= 0 \\ b_{11} + b_{15} &= 0 \end{aligned}$$

$$M_{\{3\}} = 0$$

$$\begin{aligned} b_0 + b_8 &= 0 \\ b_1 + b_9 &= 1 \\ b_2 + b_{10} &= 0 \\ b_3 + b_{11} &= 0 \\ b_4 + b_{12} &= 0 \\ b_5 + b_{13} &= 0 \\ b_6 + b_{14} &= 0 \\ b_7 + b_{15} &= 1 \end{aligned}$$

$$M_{\{1\}} \cdot G_{\{1\}} =$$



$$\begin{array}{|c|c|c|c|} \hline 0011 & 0011 & 0011 & 0011 \\ \hline \end{array}$$

$$\Rightarrow y' = \begin{array}{|c|c|c|c|} \hline 10000 & 0001 & 0(00 & 0000 \\ \hline \end{array}$$

$$\Rightarrow m_{\phi} = 0.$$

Q3/ $G_1 = RM(m-r-1, m)$

$$G_2 = RM(r, m).$$

Prove that

$$g_1(s_1) \cdot g_2(s_2) = 0,$$

for all $|s_1| \leq m-r-1$ and $|s_2| \leq r$.

Since $g_1(s_1) \cdot g_2(s_2)$

$$= \sum_{\substack{\vec{b} \in \{0,1\}^m \\ \text{mod } 2}} \mathbb{1}_{\{b_i = 1 \text{ for all } i \in S_1 \cup S_2\}}$$

$$= 2^{m - |S_1 \cup S_2|} \text{ mod } 2$$

since $|S_1 \cup S_2| \leq m-1$

$$\Rightarrow g_1(S_1) \cdot g_2(S_2) = 0.$$