Q1) dual of $C^\perp$ of a $[n, k]$ linear code C over $\mathbb{F}_q$

is : $C^\perp = \{ v \in \mathbb{F}^n : c \cdot v^T = 0 \}$

$C^\perp$ is linear.

If c is an MDS code, so is $C^\perp$

Ans) A code is an MDS code if it meets the singleton bound with equality : $d = n - k + 1$

Suppose C is a code with a generator matrix G

$$G = \begin{bmatrix} c_1 & | & c_2 & | & \cdots & c_n \end{bmatrix}_{k \times n} \text{ matrix.}$$

In an MDS code, $d = n - k + 1$ (Hamming weight)

$\downarrow$

or d_{min}

Let G be the generator matrix for C, and H be a parity check matrix for C, then G^T will be parity check for $C^\perp$ & H^T will be a generator matrix.

$C \rightarrow k \times n$

$C^T \rightarrow n \times k$

$C = [n, k, n-k+1]$ code

H

$C^{\perp} = [n, n-k+1, k+1]$ code

Every subset of k columns of G is Linearly Independent

Suppose some k columns are dependent, they can be written as

$$\alpha_1 C_1 + \alpha_2 C_2 + \cdots \alpha_k C_k = 0$$

where $\alpha_1 \neq \alpha_2 \neq \alpha_3 = \cdots \neq \alpha_k = 0$

We can use these linear combinations in generator matrix G

This will get the Hamming weight $\leq n-k$

Contradiction because $H.W = n-k+1$ for an MDS code

dual of $(n, k, n-k+1)$ code is $(n, n-k+1, k+1)$ code which is also MDS.

Q2) [4, 2] Reed Solomon code over $\mathbb{F}_4$

message vector $(1, \alpha)$ $\alpha \in \mathbb{F}_4$

Error position is 3.

Ans)

$[4,2] \Rightarrow n=4 \quad k=2$

$m = (1, \alpha)_{1\times k} = (m_0 \; m_1)$

$$G = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \cdots & \\ \vdots & & & & \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & & \alpha_n^{k-1} \end{bmatrix}_{k\times n}$$

$$\Rightarrow G = \begin{bmatrix} 1 & 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \end{bmatrix}_{2\times 4} \text{ matrix.}$$

error bit.

$y \rightarrow$ Rx vector $\quad y_1 \; y_2 \; y_3 \; y_4$

$$E(x) = \prod_{i : y_i \neq m(\alpha_i)} (x - \alpha_i) = (x - \alpha_3)$$

$$\text{Codeword} = \left(m(X)\Big|_{X=\alpha_1},\ m(X)\Big|_{X=\alpha_2},\ m(X)_{X=\alpha_3}\ M(X)_{X=\alpha_4} \right)$$

$$\begin{aligned} y_i\, E(\alpha_i) &= E(\alpha_i)\, m(\alpha_i) \\ &= N(\alpha_i) \end{aligned}$$

$$m \cdot G = \Big((1+\alpha\alpha_1),\ (1+\alpha\alpha_2),\ (1+\alpha\alpha_3)\ (1+\alpha\alpha_4) \Big)_{1\times 4}$$

$$\left.\begin{aligned} y_1(x-\alpha_3) &= (x-\alpha_3)(1+\alpha\alpha_1) \\ y_2(x-\alpha_3) &= (x-\alpha_3)(1+\alpha\alpha_2) \\ y_3(x-\alpha_3) &= (x-\alpha_3)(1+\alpha\alpha_3) \\ y_4(x-\alpha_3) &= (x-\alpha_3)(1+\alpha\alpha_4) \end{aligned}\right\} \underline{4\ \text{Eq}}$$

$$y_1(x-\alpha_3) = x + x\alpha\alpha_1 - \alpha_3 - \alpha\alpha_1\alpha_3$$

$$y_2(x-\alpha_3) = x + x\alpha\alpha_2 - \alpha_3 - \alpha\alpha_3\alpha_2$$

$$y_3(x-\alpha_3) =$$