Assignment #4 4.14, 4.31, A, B, C, D

A Let $\vec{v} \in \mathbb{F}_2^n$. Prove that $\vec{v}\cdot\vec{v}=0$ if and only if $wt(\vec{v})$ is even.

B Let $\vec{v} \in \mathbb{F}_3^n$. Prove that $\vec{v}\cdot\vec{v}=0$ if and only if $wt(\vec{v})$ is a multiple of 3.

C Let C be the $[6,3,3]_2$-linear code with generator matrix

$$G = \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right)$$

1. How many cosets does C have?
2. Find a parity-check matrix H and calculate the syndromes for these cosets using as coset leaders vectors of smallest possible weight.
3. Decode the error words

   011110, 101110, 111100

   using syndromes.

D Is the following matrix the generator matrix for a self-dual code? Explain.

$$G = \left[\; I_7 \;\; \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix} \;\right]$$

4.14 Determine which are linear codes (i.e., subspaces over $\mathbb{F}_q$)

(a) $q=2$, $\mathcal{C} = \{1101, 1110, 1011, 1111\}$

Not a linear code $1101 - 1101 = 0000 \notin \mathcal{C}$

So $\mathcal{C}$ is not closed under addition and scalar multiplication.

(b) $q=3$, $\mathcal{C} = \{0000, 1001, 0110, 2002, 0220, 1111, 1221, 2112, 2222\}$

Yes, $\mathcal{C} = \text{Row}\left(\begin{bmatrix} 1001 \\ 0110 \end{bmatrix}\right)$

(c) $q=2$, $\mathcal{C} = \{00000, 11110, 01111, 10001\}$

Yes, $\mathcal{C} = \text{Row}\left(\begin{bmatrix} 11110 \\ 01111 \end{bmatrix}\right)$

4.31

(a) $G = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$ Generates a linear code $\mathcal{C}$ in $\mathbb{F}_2^4$

Find $[n,k,d]_2$ for this code and a parity check matrix.

$$\begin{matrix} 1&0&0&0 \\ 0&1&1&0 \\ 0&0&1&0 \\ 0&0&0&1 \\ \cancel{1}&\cancel{0}&\cancel{0}&\cancel{1} \end{matrix} \longrightarrow \begin{matrix} 1&0&0&0 \\ 0&1&1&0 \\ 0&0&1&0 \\ 0&0&0&1 \end{matrix} \xrightarrow{R_2+R_3} \begin{bmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \end{bmatrix}$$

so $\mathcal{C}$ is a $[4,4,1]_2$-linear code.

So $\dim(\mathcal{C}^{\perp}) = 4-4=0$ so $\mathcal{C}^{\perp}=\{0000\}$

So $H=[0000]$

(b) $\mathcal{C}$ is a linear code in $\mathbb{F}_3^6$

with $G = \begin{bmatrix} 1&1&0&0&0&0 \\ 0&1&1&0&0&0 \\ 0&0&1&1&0&0 \\ 0&0&0&1&1&0 \\ 0&0&0&0&1&1 \end{bmatrix}$ Find $[n,k,d]_3$ for $\mathcal{C}$ and find a parity-check matrix.

$$\begin{matrix} 1&1&0&0&0&0 \\ 0&1&1&0&0&0 \\ 0&0&1&1&0&0 \\ 0&0&0&1&1&0 \\ 0&0&0&0&1&1 \end{matrix} \xrightarrow[R_4-R_5]{} \begin{matrix} 1&1&0&0&0&0 \\ 0&1&1&0&0&0 \\ 0&0&1&1&0&0 \\ 0&0&0&1&0&2 \\ 0&0&0&0&1&1 \end{matrix} \xrightarrow[R_3-R_4]{} \begin{matrix} 1&1&0&0&0&0 \\ 0&1&1&0&0&0 \\ 0&0&1&0&0&1 \\ 0&0&0&1&0&2 \\ 0&0&0&0&1&1 \end{matrix} \xrightarrow[R_2-R_3]{}$$

$$\begin{matrix} 1&1&0&0&0&0 \\ 0&1&0&0&0&2 \\ 0&0&1&0&0&1 \\ 0&0&0&1&0&2 \\ 0&0&0&0&1&1 \end{matrix} \xrightarrow[R_1-R_2]{} \left[\begin{array}{ccccc:c} 1&0&0&0&0&1 \\ 0&1&0&0&0&2 \\ 0&0&1&0&0&1 \\ 0&0&0&1&0&2 \\ 0&0&0&0&1&1 \end{array}\right] = [I_5 | A] \text{ in standard form}$$

So $H=[-A^T \mid I_{6-5}] = [-A^T \mid I_1]$ is a parity-check matrix

$\boxed{H=[2\,1\,2\,1\,2 \mid 1]}$

$\mathcal{C}$ is a $[6,5,2]_3$-linear code.

* A linear combo of one row has wt ≥ 2
* A linear combination of $k \geq 2$ rows has wt $\geq k$.

c)

$$\begin{matrix} 1&0&1&0&1&0&1&0 \\ 1&1&0&0&1&1&0&0 \\ 1&1&1&1&0&0&0&0 \\ 0&1&1&0&0&1&1&0 \\ 0&0&1&1&1&1&0&0 \end{matrix} \xrightarrow[R_3+R_1]{R_2+R_1} \begin{matrix} 1&0&1&0&1&0&1&0 \\ 0&1&1&0&0&1&1&0 \\ 0&1&0&1&1&0&1&0 \\ 0&1&1&0&0&1&1&0 \\ 0&0&1&1&1&1&0&0 \end{matrix} \xrightarrow[\substack{R_3+R_2 \\ R_4+R_2}]{}$$

$$\begin{matrix} 1&0&1&0&1&0&1&0 \\ 0&1&1&0&0&1&1&0 \\ 0&0&1&1&1&1&0&0 \\ \cancel{0}&\cancel{0}&\cancel{0}&\cancel{0}&\cancel{0}&\cancel{0}&\cancel{0}&\cancel{0} \\ 0&0&1&1&1&1&0&0 \end{matrix} \xrightarrow[R_4+R_2]{} \begin{matrix} 1&0&1&0&1&0&1&0 \\ 0&1&1&0&0&1&1&0 \\ 0&0&1&1&1&1&0&0 \\ \cancel{0}&\cancel{0}&\cancel{0}&\cancel{0}&\cancel{0}&\cancel{0}&\cancel{0}&\cancel{0} \\ \cancel{0}&\cancel{0}&\cancel{0}&\cancel{0}&\cancel{0}&\cancel{0}&\cancel{0}&\cancel{0} \end{matrix} \xrightarrow[\substack{R_1+R_3 \\ R_2+R_3}]{}$$

$$\left[\begin{array}{ccc|ccccc} 1&0&0&1&0&1&1&0 \\ 0&1&0&1&1&0&1&0 \\ 0&0&1&1&1&1&0&0 \end{array}\right]$$

is a generator matrix in standard form $[I_3|A]$. This is an $[8,3,4]_2$-linear code with parity-check matrix

$$\left[\begin{array}{ccc|c} 1&1&1& \\ 0&1&1& \\ 1&0&1& I_5 \\ 1&1&0& \\ 0&0&0& \end{array}\right]$$

$\boxed{D}$

$$G = \left[\begin{array}{c|ccccccc} & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ I_7 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ & 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{array}\right] \quad \text{over } \mathbb{F}_2$$

Generates a $[14, 7, d]_2$-linear code $\mathcal{C}$.

The dual code has length $= 14$, $\dim = 14 - 7 = 7$

So C is self dual as long as the rows of G are orthogonal to each other and themselves.

But they are not $wt(R_7) = 5$ so $R_7 \cdot R_7 = 1 \neq 0$.

also $R_5 \cdot R_7 = 1 \neq 0$, ... etc....