Class no: 13

Quiz 1: Solns:

TP: If A, then B.
Proof by contradiction: Suppose $\bar{B}$ - Then we show $\bar{A}$. Then proof is complete.

1. $\mathcal{C}^{\perp} = \{ \underline{v} \in \mathbb{F}_q^n : \underline{c}\,\underline{v}^T = 0 \}$

$\forall \underline{c} \in \mathcal{C} \rightarrow [n, k]$.

$\dim(\mathcal{C}^{\perp}) = n-k$. $\mathcal{C}^{\perp}$ is linear.

Suppose $\mathcal{C}$ is MDS then show that $\mathcal{C}^{\perp}$ is also MDS.

A B

Soln: Let $G_{k \times n}$ be a gen matrix of $\mathcal{C}$.

We know from Singleton bound that $d_{min}(\mathcal{C}^{\perp}) \leq k+1$

Suppose $\boxed{d_{min}(\mathcal{C}^{\perp}) \leq k+1}$ $\Rightarrow$ "$\mathcal{C}^{\perp}$ is not MDS" is our assumption. $(\bar{B})$

Say $d_{min}(\mathcal{C}^{\perp}) = k' \leq k$.

Let $\underset{1\times n}{v} \in \mathbb{F}_2^n$ be a non-zero codeword of wt k'.

Then $G v^T = \underset{k\times n \; n\times 1}{0}$ $\Rightarrow$ There are k' cols of G which are linearly dependent.

$$(1\,1\,0\,0\,0)\cdot\begin{pmatrix}1\\1\\0\\0\\0\end{pmatrix} = 0 \text{ (over } \mathbb{F}_2)$$

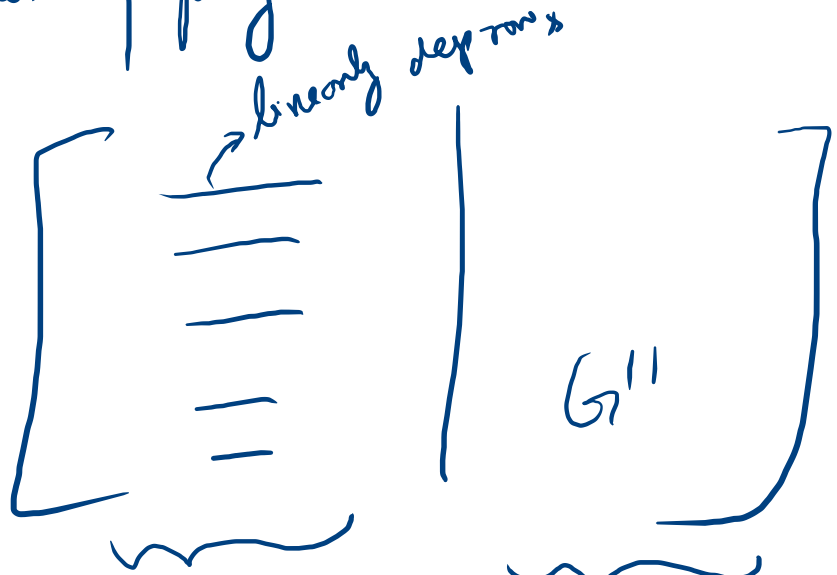
$\rightarrow$ Suppose these are the first k'-cols

$$G = \left[\; \underbrace{G_1\; G_2 \ldots G_{k'}}_{\text{linearly dependent}}\; G_{k'+1} \ldots G_k\; G_{k+1} \ldots G_n \;\right]$$

Thus the first k cols are Linearly dependent.

$\Rightarrow$ the 'leading' $k\times k$ submatrix of G has rank $< k$ $\Rightarrow$ In the 'leading' $k\times k$ submatrix of G, the k rows are linearly dep.

Can we use this property to show a nonzero codeword in G with wt $< n-k+1$



. There exists some $\underset{1\times k}{m} \neq 0$ such that

$\underset{}{m}\, G_1' = \underset{}{0}$ ⟼ non-trivial linear comb of rows of G_1' $= \underset{}{0}$

Now consider that $\underset{}{m}$

$$\underset{1\times k}{m}\ \underset{k\times n}{G_1} = \left(\underset{1\times k}{mG_1' = 0} \;\middle|\; \underset{}{m\, G_1''}\right)$$

Is this a nonzero codeword in G_1?
Ans: Yes, because $\underset{}{m} \neq \underset{}{0}$ & G_1 has k l.i. rows

↘ wt $(\underset{}{m}\, G_1) \leq n-k$ clearly

Thus we have shown a codeword in G of wt $\leq n-k$ ⇒ G is not MDS (contradiction)

Q.E.D.