E2 205 Error-Control Coding
Lecture 7

Naveenkumar M

September 4, 2019

1 More on Linear Codes

- $\mathbb{C}^{\perp} = \{ \underline{y} \ | \ \underline{x}^t \ \underline{y} = 0, all \ \underline{x} \in \mathbb{C} \}$
- $\mathbb{C}^{\perp} = \eta(G)_{(k \times n)}$
- Define H = generator matrix of $\mathbb{C}^{\perp}$ and a parity check matrix for $\mathbb{C}$
- $\mathbb{C} = \eta(H) \quad \therefore \mathbb{C} = (\mathbb{C}^{\perp})^{\perp}$
- If H is of size $(n - k \times n)$ and $\eta(H) = \mathbb{C}$, then H is a parity check matrix for $\mathbb{C}$.
- If H has a rank $(n - k)$ and $GH^{\top} = [0]$, then H is a parity check matrix for $\mathbb{C}$.

1.1 Theorem 1

Let H be of size $(n - k \times n)$ and $\eta(H) = \mathbb{C}$, then H is a parity check matrix for $\mathbb{C}$.

Proof: We need to show that $Row(\,H) = \mathbb{C}^{\perp}$

$$\begin{bmatrix} \underline{h}_1^t \\ \underline{h}_2^t \\ \\ \cdot \\ \cdot \\ \cdot \\ \underline{h}_{(\,n-k)}^t \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ \\ \cdot \\ \cdot \\ \cdot \\ c_n \end{bmatrix} = \begin{bmatrix} 0 \end{bmatrix}, all\ \underline{c}\ \in\ \mathbb{C}. \tag{1}$$

$\therefore\ \ \underline{h}_i \in \mathbb{C}^{\perp}$, all i

$\therefore\ \ Row(\,H) \subseteq R^{\perp}$

$\therefore\ \ Row(\,H) = R^{\perp}$, since both have dimension $= (n-k)$.

(Since $\mathbb{C}^{\perp} = \eta(\,G)$, it follows that if $\mathbb{C}$ is an $[\,n,k]$ code, $\mathbb{C}^{\perp}$ is an $[\,n,n-k]$ code.)

Note: $Rank(\,H) = n-k.$

1.2 Theorem 2

Suppose G is the generator matrix of an $[\,n,k]$ code and H is an $(\,n-k\times n)$ matrix of rank $(\,n-k)$, such that

$$GH^{\top} = [\,0]$$
$$(\,k\times n)\,(\,n\times n-k) = (\,k\times n-k)$$

Then H is a parity check matrix for $\mathbb{C}$.

Proof:

$$\begin{bmatrix} \underline{g}_1^t \\ \underline{g}_2^t \\ \\ \cdot \\ \cdot \\ \cdot \\ \underline{g}_k^t \end{bmatrix}_{k\times n} \begin{bmatrix} \underline{h}_1 & \underline{h}_2 & \cdot & \cdot & \cdot & \underline{h}_{(n-k)} \end{bmatrix}_{n\times n-k} = \begin{bmatrix} 0 \end{bmatrix}_{k\times n-k} \tag{2}$$

G $\qquad\qquad\qquad\qquad$ $H^{\top}$

$$\therefore \quad \underline{g}_i^t \cdot \underline{h}_j = 0, \ all \ i, \ j$$

$$\therefore \quad \underline{c}^t \cdot h_j = 0, \ all \ \underline{c} \in \mathbb{C}$$

$\therefore \quad \underline{h}_j \ \in \ \mathbb{C}^{\perp}$

$\therefore \quad Rowspace(H) \ \subseteq \ \mathbb{C}^{\perp}$

$\therefore \quad Rowspace(H) \ = \ \mathbb{C}^{\perp}$ (By comparing dimensions)

1.2.1 Example-1

$\mathbb{C}$ is the $[7, 6]$ single parity check code, then

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}_{1\times 7}$$

1.2.2 Example-2

$\mathbb{C}$ is the repetition code, then

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}_{6\times 7} = \begin{bmatrix} I_6 \mid \ \underline{1} \end{bmatrix}$$

H is not unique.

Definition 1 *A $(k \times n)$ matrix G is said to be a systematic generator matrix for the $[n, k]$ code $\mathbb{C}$, if G is of the form:*

$$G = \begin{bmatrix} I_k \mid \ P \end{bmatrix}_{k\times n},$$

where $P_{k\times n-k}$ is the parity matrix.

2 Encoding in a Linear Code

$$\begin{array}{cc} \underline{u} \longrightarrow & \underline{c} \\ \in \mathbb{F}_2^k & \in \mathbb{F}_2^n \\ \text{Message Vector} & \text{Code word} \end{array}$$

$$\underline{c}^t = \underline{u}^t G$$

If G is systematic, then

$$\underline{c}^t = \underline{u}^t \cdot \begin{bmatrix} I_k \mid & P \end{bmatrix} = \begin{bmatrix} \underline{u}^t \mid & \underline{u}^t \cdot P \end{bmatrix}$$

Thus the 1^{st} k code symbols are precisely the message symbols.

<u>*Note*</u> : Let G be a systematic generator matrix.

$$G = \begin{bmatrix} I_k \mid & P \end{bmatrix}_{k \times n}$$

for a linear code $\mathbb{C}$, Then

$$H = \begin{bmatrix} P^\top \mid & I_{n-k} \end{bmatrix}_{n-k \times n}$$

is a valid parity check matrix for the code $\mathbb{C}$.

Proof: H is of size $(n - k \times n)$, $Rank(H) = n - k$.

$$GH^\top = \begin{bmatrix} I_k \mid & P \end{bmatrix}_{k \times n} \begin{bmatrix} P \\ -- \\ I_{n-k} \end{bmatrix}_{n \times n-k}$$

$$= I_k \ P + P \ I_{n-k} = P + P = \begin{bmatrix} 0 \end{bmatrix}.$$

2.0.1 Example

Let

$$G = \begin{bmatrix} I_6 \mid & P \end{bmatrix}$$

be the generator matrix for Single Parity check code, Then

$$H = \begin{bmatrix} P^\top \mid I_1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & \mid 1 \end{bmatrix}$$

is a valid parity check matrix for the single parity check code.

2.0.2 Question

Does every $[n, k]$ linear code have a systematic generator matrix?

$$G = [\underline{g}_1 \quad \underline{g}_2 \quad \underline{g}_1 \quad \cdot \quad \cdot \quad \underline{g}_k \quad \cdot \quad \cdot \quad \underline{g}_n]$$

<u>*Ans*</u>:Not necessarily as this depends upon the rank of the sub-matrix associated to the 1^{st} k columns of G.

Definition 2 *Two codes $\mathbb{C}_1$, $\mathbb{C}_2$ are said to be equivalent if one can be obtained from the other by permuting code symbols.*

Example:
$(c_1, c_2, c_3, c_4, c_5, c_6, c_7) \in \mathbb{C}_1$

$(c_1, c_3, c_5, c_7, c_2, c_4, c_6) \in \mathbb{C}_2$

$\Longrightarrow$ $\mathbb{C}_1$ and $\mathbb{C}_2$ are equivalent

It follows that every code $\mathbb{C}$ is equivalent to a second code $\mathbb{C}^{`}$ that has a systematic generator matrix.

3 Minimum Distance of a Linear Block Code

3.1 Theorem

The minimum distance d_{min} of a linear block code $\mathbb{C}$ is the minimum Hamming weight W_{min} of a non zero codeword.

Proof: Let $\underline{c}_1, \ \underline{c}_2 \in \mathbb{C}$ such that $d_H(\underline{c}_1, \underline{c}_2) = d_{min}$.

Then $W_H(\underline{c}_1 + \underline{c}_2) = d_{min}$

$\therefore W_{min} \leq d_{min}$ (*Since* $\underline{c}_1 + \underline{c}_2 \in \mathbb{C}$)

Next , let $W_H(\underline{c}) = W_{min}, \quad \underline{c} \neq 0$

Then $W_H(\underline{0}, \underline{c}) = W_{min} \Longrightarrow d_H(\underline{0}, \underline{c}) = W_{min} \Longrightarrow d_{min} \leq W_{min}$

$\therefore \quad d_{min} = W_{min}$

Example-1 $\mathbb{C}$ is the Single Parity check code, then $d_{min} = 2$.

Example-2 $\mathbb{C}$ is the repetition code with $n = 7$, then $d_{min} = 7$.

Definition 3 *Given a linear code $\mathbb{C}$, let s be the largest integer, such that any s columns of parity check matrix H are linearly independent.*

Theorem: $d_{min}(\mathbb{C}) = s + 1$

Proof: Let

$$H = \begin{bmatrix} \underline{\mathrm{h}}_1 & \underline{\mathrm{h}}_2 & \underline{\mathrm{h}}_3 & \cdot & \cdot & \underline{\mathrm{h}}_n \end{bmatrix}.$$

Note that $\underline{\mathrm{h}}_1 + \underline{\mathrm{h}}_2 + \underline{\mathrm{h}}_3 = \underline{0}$ iff $\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & \cdots & 0 \end{bmatrix}^\top \in \mathbb{C}$.
Thus the presence of a non zero code word of Hamming weight W in $\mathbb{C}$ implies that the parity check matrix H of $\mathbb{C}$ contains a set of W dependent columns.
It follows that,

$$s = W_{min} - 1$$

$$\therefore \quad W_{min} = d_{min} = s + 1$$

Example Hamming code: $[7, 4, 3]$

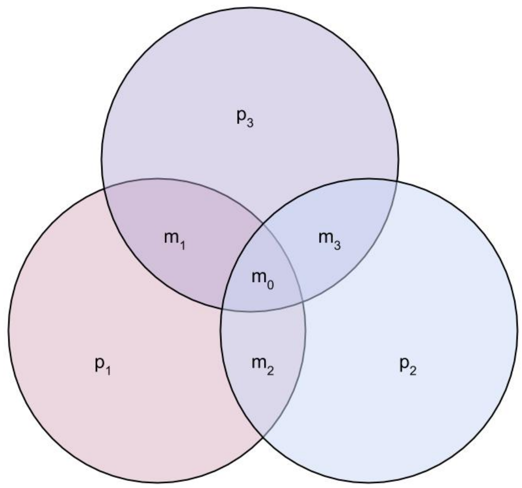

Figure 1: Hamming Code $[7, 4, 3]$

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} m_0 \\ m_1 \\ m_2 \\ m_3 \\ p_1 \\ p_2 \\ p_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

s=2

$\therefore \quad d_{min} = 3$

3.2 Parameters of a Hamming code

Definition 4 *Let $r \geq 2$ be an integer and set $n = 2^r - 1$. Then the Hamming code of length n is any code that has an $(r \times 2^r - 1)$ parity check matrix whose $2^r - 1$ columns are precisely the set of all non-zero r-tuples.*

$$[\, n = 2^r - 1, \; 2^r - 1 - r, \; 3]$$
$$n \qquad\qquad k \qquad\qquad d_{min}$$

4 Singleton Bound

4.1 Theorem

Let $\mathbb{C}$ be an [n, k] linear code, Then $d_{min} \leq (n-k+1)$

Proof:

$$s \leq n-k$$

$$\therefore \quad d_{min} \leq (n-k+1)$$

Example: For $[n, n-1, 2]$ single parity check code, $d_{min} = n-k+1 = 2$.

Definition 5 *Codes that achieve the Singleton bound with equality are called Maximum Distance Separable (MDS) codes.*

Example: For $[n, 1, n]$ repetition code

$$d_{min} = n$$

$\therefore$ The code is Maximum Distance Separable.

Exercise: Show that these are the only possible MDS binary codes.

5 Bounds on code size (Hamming Bound)

5.1 Theorem

Let $\mathbb{C}$ be an (n, M, d_{min}) code, then

$$M \leq \frac{2^n}{\sum_{i=0}^{t} \binom{n}{i}},$$

where $t = \lfloor \frac{d_{min}-1}{2} \rfloor$.

Proof:

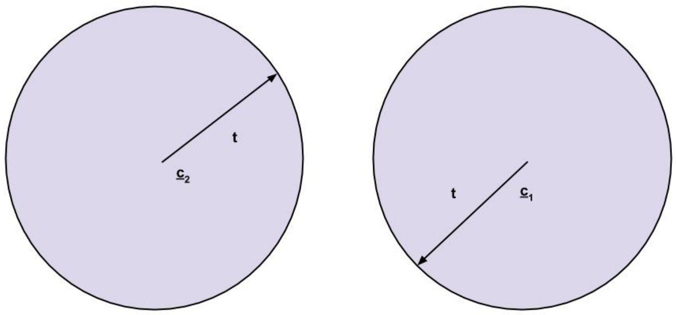

Figure 2: Hamming Bound

Note that in $\mathbb{C}$, $B(\underline{c}_1, t) \cap B(\underline{c}_2, t) = \phi$

$\therefore \quad M \mid B(\underline{c}, t) \mid \ \leq \ 2^n$

$\therefore \quad M \quad \leq \frac{2^n}{|B(\underline{C},t)|} = \frac{2^n}{\sum_{i=0}^{t}\binom{n}{i}}$

Example: $[2^r - 1, 2^r - 1 - r, 3]$ Hamming Code , $t = 1$

$M \leq \frac{2^n}{1+n} \leq \frac{2^{2^r-1}}{2^r} = 2^{2^r-1-r}$

Codes achieving the Hamming bound with equality are called perfect codes.

Thus Hamming codes are perfect.