22|1|2020 

# Lecture 5 (Generator Matrix, Dual Code, Parity check matrix)

Linear block Code is a subspace of $\mathbb{F}^n$ (or $\mathbb{F}_2^n$).

The dimension of a linear block code is its dimension as a subspace of $\mathbb{F}^n$.

Minimum distance of a linear Code is equal to the minimum Hamming weight of a non zero Code.

## Generator Matrix of a Code

Any $k \times n$ matrix $G$ with entries from the field $\mathbb{F}$ which form a basis for Code $\mathbb{C}$.

$(n, k, d)$ Code $\mathbb{C}$.

- A Code can have more than one generator matrix.

# Examples of generator matrices of Codes

① $(n, 1, n)$ – Repetition Code.

$$\begin{bmatrix} 1 & \cdots & 1 \end{bmatrix}_{1\times n}.$$

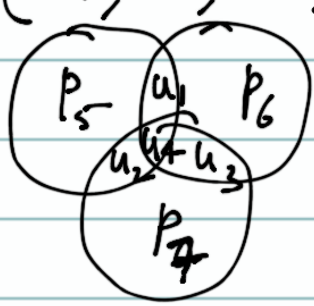
② $(n, n-1, 2)$ – simple parity check Code

$(n-1)\times n$ matrix which forms a basis for all even weight codewords

$$\left[\begin{array}{c|c} I_{(n-1)\times(n-1)} & \begin{matrix}1\\1\\1\\1\\\vdots\\1\end{matrix} \end{array}\right]_{(n-1)\times n} \rightarrow \text{linearly independent}$$

Rows of $G$ are all linearly independent is the same as saying that $\text{rank}(G) = K$

③ $(7, 4, 3) \rightarrow$ Hamming Code




$P_5 = u_1 \oplus u_2 \oplus u_4$

$P_6 = u_1 \oplus u_4 \oplus u_3$

$P_7 = u_2 \oplus u_3 \oplus u_4$.

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

$$G = \left[\begin{array}{c|ccc} & 1 & 1 & 0 \\ I_4 & 1 & 0 & 1 \\ & 0 & 1 & 1 \\ & 1 & 1 & 1 \end{array}\right]$$

$\underline{c} = [u_1\ u_2\ u_3\ u_4\ P_5\ P_6\ P_7]$.

## Systematic Generator Matrix

A $(k \times n)$ generator matrix $G$ is said to systematic if it is of the following form.

$$G_{k\times n} = \left[ I_k \;\middle|\; P_{k\times(n-k)} \right]$$

If the generator matrix is systematic, then the message vector $\underline{u}$ will be part of the codeword, which it is mapping to.

$$\underset{\sim}{\underline{c}} = \underline{u}\,G = \underline{u}\left[ I_k \mid P \right]$$
$$= \left[ \underset{\sim}{\underline{u}} \mid \underline{u}P \right]$$

<u>Claim</u>:- Every linear code $\mathbb{C}$ is equivalent (upto permutation of coordinates) to another linear code $\mathbb{C}'$ which has a systematic generator matrix.

<u>Proof</u>:- If the first $k$ columns of $G$ are linearly independent.

$$G = \left[ \underset{k\times k}{G_1} \;\middle|\; \underset{k\times(n-k)}{G_2} \right].$$

where $G_1$ is full rank.

$G_1$ is full rank & of size $(k \times k)$.

$G_1^{-1}$ exists.

$G' = G_1^{-1}\left[\, G_1 \mid G_2 \,\right] \rightarrow$ also forms a basis for code $\mathbb{C}$.

Rows of generator matrix form a basis for $\mathbb{C}'$.

$$G' = \left[\, G_1^{-1} G_1 \mid G_1^{-1} G_2 \,\right]$$

$$= \left[\, I_k \mid P \,\right] \qquad P = G_1^{-1} G_2 .$$

This means that $\mathbb{C}$ has a systematic generator matrix.

Let $G$ be generator matrix of an $(n, k)$ code. There exists a set of $k$ columns indexed by set $S$ $(S \subseteq \{1, 2, \ldots, n\})$; such that $G|_S$ is full rank. $S = \{s_1, s_2, \ldots, s_k\}$.

Apply a permutation $\pi$ on these coordinates such that $\pi(s_i) = i$.

$n = 8 \quad k = 3$

$s_1 = 2, \; s_2 = 4$

$s_3 = 5$

$\boxed{\pi(2) = 1, \; \pi(4) = 2, \; \pi(5) = 3}$

After column permutations, the rowspace of new $G$ is not the same as the code that we started off with.

The span of the new generator matrix is another code $\mathbb{C}'$.

$\mathbb{C}$ is said to be equivalent to $\mathbb{C}'$ (under column permutations).

$$\begin{array}{ccc} \mathbb{C}. & & \mathbb{C}' \\ 0000 & \text{permute cols} & 0000 \\ 0011 & \xleftrightarrow{2\,\&\,3} & 0101 \\ 1100 & & 1010 \\ 1111 & & 1111 \end{array}$$

$G = \begin{bmatrix} 1100 \\ 0011 \end{bmatrix}$ $\qquad$ $G' = \begin{bmatrix} 1010 \\ 0101 \end{bmatrix}$

$G$ is not in systematic form $\qquad$ $G'$ is in systematic form

$C$ is equivalent to $\mathbb{C}'$.

Suppose there do not exist $k$ columns s.t. they are linearly independent, then col rank$(G) < k$.
$\Rightarrow$ row rank$(G) < k$.

## Dual Code

Let $\mathbb{C}$ be an $(n,k)$ code. Then, the dual of the code $\mathbb{C}$, denoted by $\mathbb{C}^{\perp}$

$$\mathbb{C}^{\perp} = \left\{ \underline{y} \in \mathbb{F}_2^n \,\middle|\, \underline{x}^t \underline{y} = 0 \ \forall \ \underline{x} \in \mathbb{C} \right\}$$

Set of all vectors in $\mathbb{F}_2^n$ which are <u>orthogonal</u> to every vector in the code $\mathbb{C}$.

Is $\mathbb{C}^{\perp}$ a linear code?

$$\underline{x}^t \underline{y}$$

$$\begin{bmatrix} x_1 & \dots & x_n \end{bmatrix} \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = 0. \qquad \sum_{i=1}^{n} x_i y_i = 0. \quad \forall \ \underline{x} \in \mathbb{C}.$$

<u>closure</u> If $\underline{y} \in \mathbb{C}^{\perp}$ & $\underline{z} \in \mathbb{C}^{\perp}$, then $\underline{y} + \underline{z} \in \mathbb{C}^{\perp}$.

$$\underline{x}^t \underline{y} = 0 \ \forall \ x \in \mathbb{C}$$

$$\underline{x}^t \underline{z} = 0 \ \forall \ x \in \mathbb{C}.$$

$$\Rightarrow \underline{x}^t (\underline{y} + \underline{z}) = 0 \ \forall \ x \in \mathbb{C}.$$

$$\Rightarrow \underline{y} + \underline{z} \in \mathbb{C}^{\perp}$$

$\mathbb{C}^\perp$ will have a basis & a dimension too.

<u>claim</u>:- $\mathbb{C}^\perp = \text{nullspace}(G)$
where $G$ is the generator matrix of $(n, k)$ code.

$\{\underline{y} \in \mathbb{F}_2^n \mid G\underline{y} = \underline{0}\} = \text{nullspace}(G)$

$\mathbb{C}^\perp = \{\underline{y} \in \mathbb{F}_2^n \mid \underline{x}^t \underline{y} = 0 \ \forall x \in \mathbb{C}\}$.

$\text{nullspace}(G) = \{\underline{y} \in \mathbb{F}_2^n \mid G\underline{y} = 0\}$. $\begin{bmatrix} \underline{g}_1^t \\ \underline{g}_2^t \\ \vdots \\ \underline{g}_k^t \end{bmatrix} \underline{y} = 0$

$\mathbb{C}^\perp \subseteq \text{nullspace}(G)$

If $\underline{y} \in \mathbb{C}^\perp$, then $\underline{x}^t \underline{y} = 0 \ \forall \ x \in \mathbb{C}$.
In particular, $\underline{g}_i^t \underline{y} = 0 \ \forall i$ $\qquad$ $\underline{g}_1^t$ is the first row of $G$.
because $\underline{g}_i \in \mathbb{C}$.
$\Rightarrow G\underline{y} = 0 \Rightarrow \underline{y} \in \text{nullspace}(G)$.

If $\underline{y} \in \text{nullspace}(G)$, $G\underline{y} = \underline{0}$.
$\Rightarrow \underline{u}^t G \underline{y} = 0 \Rightarrow \underline{x}^t \underline{y} = 0 \ \forall \ \underline{x} \in \mathbb{C}$.

$\boxed{\underline{x}^t = \underline{u}^t G}$

$\Rightarrow y \in \mathbb{C}^\perp$.

$\text{nullspace}(G) \subseteq \mathbb{C}^\perp$.

**Prop:-** The dimension of $\mathbb{C}^{\perp} = n-k$.

**Proof:** Follows from rank nullity theorem

$G$ is the generator matrix of $(n,k)$ code $\mathbb{C}$.

$$\text{rank}(G) + \text{nullity}(G) = n.$$

$$k + \text{nullity}(G) = n.$$

$\text{nullity}(G) =$ dimension of null space of $G = n-k$.

Because $\mathbb{C}^{\perp} = \text{null space}(G)$;

$$\dim(\mathbb{C}^{\perp}) = n-k.$$

**Defn:-** Any $(n-k)\times k$ matrix which is a basis for the dual code $\mathbb{C}^{\perp}$ is known as the parity check matrix for code $\mathbb{C}$.

Parity check matrix is denoted by $H$.

$$H_{(n-k)\times n}.$$

**Claim:-** $\boxed{G H^T = 0}$

$$\boxed{G_{k\times n} H^T_{n\times(n-k)} = 0_{k\times(n-k)}}$$

$$GH^t = 0$$

$$(GH^t)^t = 0.$$

$$HG^t = 0$$

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

$$G^t \underline{u} = \underline{x}.$$

$$H \underbrace{G^t \underline{u}} = 0$$

$$\boxed{H \underline{x} = 0} \leftarrow$$ H is specifying a set of linear equations which codewords have to satisfy.

$\forall x \in \mathbb{C}.$

<u>Examples</u>

$(n, 1, n)$ – repetition code $\mathbb{C}$.

$(n, n-1, 2)$ Simple parity check code $\mathbb{C}^\perp$

Simple parity check code is the dual code of repetition code.

$$\left\{ \underline{y} \in \mathbb{F}_2^n \;\middle|\; \underline{x}^t \underline{y} = 0 \;\forall\, x \in \mathbb{C} \right\}$$

$$\mathbb{C} = \{(0, \ldots 0), (1 \ldots 1)\}$$

$$\left\{ \underline{y} \in \mathbb{F}_2^n \;\middle|\; [1 \ldots 1]\, \underline{y} = 0 \right\}$$

$$\Rightarrow \sum_{i=1}^{n} y_i = 0 \leftarrow$$ <u>Even weight code</u>

**Lemma:** $(\mathbb{C}^{\perp})^{\perp} = \mathbb{C}$.

**Proof:**

$$\underline{\mathbb{C} \subseteq (\mathbb{C}^{\perp})^{\perp}}.$$

$$(\mathbb{C}^{\perp})^{\perp} = \left\{ \underline{z} \in \mathbb{F}_2^n \;\middle|\; \underline{y}^t \underline{z} = 0 \ \forall\, \underline{y} \in \mathbb{C}^{\perp} \right\}.$$

If $\underline{z} \in \mathbb{C}$, then $\underline{z} \in (\mathbb{C}^{\perp})^{\perp}$.

$$\dim\left((\mathbb{C}^{\perp})^{\perp}\right) = n - \dim(\mathbb{C}^{\perp})$$

$$= n - (n - \dim(\mathbb{C}))$$

$$= \dim(\mathbb{C})$$

$$\Rightarrow (\mathbb{C}^{\perp})^{\perp} = \mathbb{C}.$$

Dual of dual of a code is the original code itself.