27/1/2021

Lecture 6 (Decoding of linear block codes)

Recap

→ Generator matrix of size $k \times n$.

→ Every code is equivalent to another code with a systematic generator matrix.

→ Dual of a code, parity check matrix

→ $\dim(\mathbb{C}^{\perp}) = n-k$, $GH^T = 0$, $(\mathbb{C}^{\perp})^{\perp} = \mathbb{C}$.

Lemma:- Let s denote the largest number such that any s columns of H are linearly independent, then $\boxed{s = d_{min} - 1.}$

Proof:- $H\underline{c} = \underline{0} \quad \forall\, \underline{c} \in \mathbb{C}$.

(Because rows of H form a basis for the dual code)

$$\underline{c} = (c_1, \ldots, c_n) \in \mathbb{F}^n.$$

$$H \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} = \underline{0} \qquad H = \left[\underline{h}_1\ \underline{h}_2\ \ldots\ \underline{h}_n\right]_{(n-k)\times n}.$$

$$\underline{h}_i \in \mathbb{F}^{n-k}.$$

$\boxed{H\underline{c} = \underline{0}}$ if and only if $\underline{c} \in \mathbb{C}$.

$$c_1 \underline{h}_1 + c_2 \underline{h}_2 + \dots + c_n \underline{h}_n = \underline{0}.$$

s is the largest number s.t. any s columns of H are linearly independent.

To prove that $s = d_{min} - 1$

ⓐ · Any $d_{min}-1$ columns of H are linearly independent

ⓑ There exist a set of d_{min} columns of H which are linearly dependent.

Proof of part ⓐ Suppose there exists a set of $(d_{min}-1)$ columns of H which are linearly dependent.

Let S denote that set. $(S \subseteq \{1, \dots, n\})$

$$\sum_{i \in S} a_i \underline{h}_i = \underline{0}. \quad \text{where all } a_i\text{s are not zero.}$$

$\Rightarrow \underline{a} = (0 \cdot a_1\ 0\ a_2 \cdots 0 \cdot a_{|S|}) \in \mathbb{C}$.

$w_H(\underline{a}) \leq d_{min} - 1. \Rightarrow$ Contradiction to the definition of d_{min}.

Proof of part (b)

By the defn of minimum distance of a code; there exists a nonzero codeword in $\mathbb{C}$. s.t. $w_H(\underline{c}) = d_{min}$

Let $\underline{c}$ be that codeword and let $\underline{S}$ denote the $supp(\underline{c})$.

$supp(\underline{c})$ = Coordinates which are nonzero in $\underline{c}$.

$\underline{c} = (1\ 0\ 1\ 0\ 1\ 1)$. $supp(\underline{c}) = \{1, 3, 5, 6\}$.

$\underline{c} \in \mathbb{C} \Rightarrow H\underline{c} = 0$.

$$\sum_{i \in S} c_i \underline{h}_i = 0. \quad |S| = d_{min}$$

$\Rightarrow$ There exists a set of d_{min} columns of H which are linearly dependent.

Lemma follows by putting together (a) & (b)

Example: Hamming Code $(7,4) \rightarrow$ Parity check matrix.

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}_{3 \times 7}$$

All nonzero vectors of length 3 & fill the columns.

$\rightarrow$ First determine s.

$\rightarrow$ Then $d_{min} = s + 1$

$\underline{\underline{s = 2}}$

Any 2 columns are linearly independent because any 2 columns are distinct

$\exists$ a set of 3 columns which are linearly dependent

$$\begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

This implies that $s = 2$ and $d_{min} = s+1 = 3$.

Decoding of Linear block Codes

Minimum Distance decoding (MDD).

$\hookrightarrow$ was ML decoding for the case of binary Symmetric channel.

Given a received vector $\underline{y} \in \mathbb{F}^n$; decode to a codeword $\underline{c} \in \mathbb{C}$ that minimizes $d_H(\underline{y}, \underline{c})$

$$\hat{\underline{c}} = \underset{\underline{c} \in \mathbb{C}}{\arg\min}\, d_H(\underline{y}, \underline{c}).$$

In addition, we are saying these are linear codes.

$$d_H(\underline{y}, \underline{c}) = w_H(\underline{y} - \underline{c}).$$

$$\underline{y} - \underline{c} = \underline{e} \text{ (error vector)}.$$

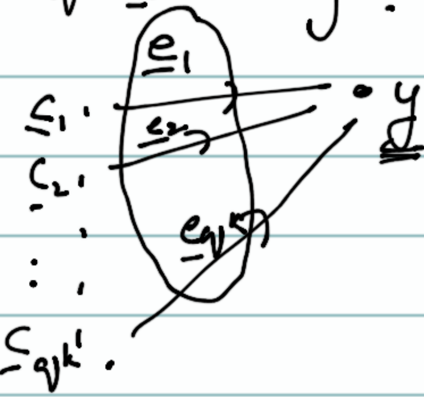
$$\hat{c} = \arg\min_{\underline{c} \in \mathbb{C}} d_H(\underline{y}, \underline{c})$$

$$\boxed{\hat{c} = \arg\min_{\underline{c} \in \mathbb{C}} w_H(\underline{y} - \underline{c})}.$$

Given $\underline{y}$ and varying $\underline{c}$, you will get a set of error vectors.

$$E(\underline{y}) = \{\underline{e} \mid \underline{e} = \underline{y} - \underline{c} \ \forall\, \underline{c} \in \mathbb{C}\}.$$

$$E(\underline{y}) = \{\underline{e} \mid \underline{e} = \underline{y} + \underline{c} \ \forall\, \underline{c} \in \mathbb{C}\}$$



$$\boxed{E(\underline{y}) = \underline{y} + \mathbb{C}.}$$

$E(\underline{y})$ is said to be a coset of $\mathbb{C}$.

↳ Group theory

$\mathbb{C} \rightarrow$ Abelian group under addition

Quick Review of Cosets

Defn: A coset of $\mathbb{C}$ in $\mathbb{F}^n$ is a set of the form
$$\underline{b} + \mathbb{C} = \{\underline{b} + \underline{c}, \ \forall\, c \in \mathbb{C}\} \text{ for some } \underline{b} \in \mathbb{F}^n.$$

(**Note:-** You will not get any new set/coset if $\underline{b} \in \mathbb{C}$).

Facts about Cosets

① $|\underline{b} + \mathbb{C}| = |\mathbb{C}| = q^k$.

Proof:- $f : \mathbb{C} \to \underline{b} + \mathbb{C}$ which is a bijection
$\underline{c} \to \underline{b} + \underline{c}$ (one-one & onto).

② Every vector $\underline{b} \in \mathbb{F}^n$ lies in some coset of $\mathbb{C}$.

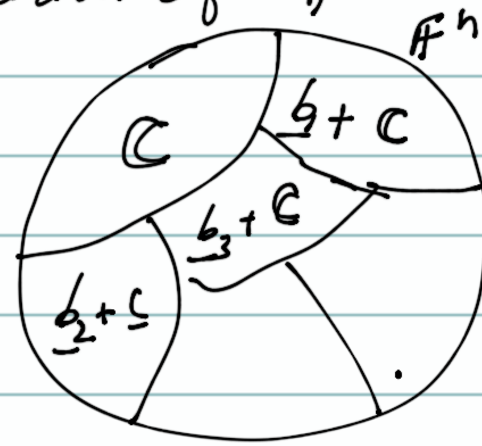
Proof:- $\underline{b} + \mathbb{C}$. $\underline{b} \in \underline{b} + \mathbb{C}$ since $\underline{0} \in \mathbb{C}$.

③ $\underline{a}$ and $\underline{b}$ are in the same coset of $\mathbb{C}$ if and only if $a - b \in \mathbb{C}$.

Proof. If $\underline{a} - \underline{b} \in \mathbb{C}$, then $\underline{b} \in \underline{a} + \mathbb{C}$
then $\underline{b} - \underline{a} \in \mathbb{C}$. & $\underline{a} \in \underline{b} + \mathbb{C}$.

$\underline{a} = \underline{b} + \underline{c} \Leftrightarrow \underline{a} - \underline{b} \in \mathbb{C}$.

Theorem: The distinct cosets of a linear code $\mathbb{C} \subseteq \mathbb{F}^n$ form a partition of $\mathbb{F}^n$.



Proof:

Equivalence relation

$\underline{a} \sim \underline{b}$ if $\underline{a}-\underline{b} \in \mathbb{C}$.

$\sim$ = Equivalence relation (Reflexive, symmetry, transitivity)

(i) $\underline{a} \sim \underline{a}$ (because $\underline{0} \in \mathbb{C}$)

(ii) $\underline{a} \sim \underline{b} \Leftrightarrow \underline{b} \sim \underline{a}$ ($\underline{a}-\underline{b} \in \mathbb{C} \Rightarrow \underline{b}-\underline{a} \in \mathbb{C}$)

(iii) $\underline{a} \sim \underline{b}$, $\underline{b} \sim \underline{c}$, then $\underline{a} \sim \underline{c}$.
($\underline{a}-\underline{b} \in \mathbb{C}$, $\underline{b}-\underline{c} \in \mathbb{C}$, $\underline{a}-\underline{c} \in \mathbb{C}$).

$\Rightarrow$ Equivalence classes under $\sim$ form a partition of $\mathbb{F}^n$.

$\hookrightarrow$ Precisely the distinct cosets of $\mathbb{C}$ in $\mathbb{F}^n$.

Corollary: Assuming $|\mathbb{F}| = q$; $|\mathbb{C}| = q^k$;
then no. of distinct cosets is q^{n-k}.

$$\boxed{\frac{|\mathbb{F}^n|}{q^k} = q^{n-k}.}$$

Going back to minimum distance decoding of linear codes

$$\hat{c} = \arg\min_{\underline{c} \in \mathbb{C}} d_H(\underline{y}, \underline{c})$$

$$= \arg\min_{\underline{c} \in \mathbb{C}} \omega_H(\underline{y} - \underline{c}).$$

$$= \arg\min_{\underline{c} \in \mathbb{C}} \omega_H(\underline{y} + \underline{c}).$$

Given a received vector $\underline{y} \in \mathbb{F}^n$

1. Find the coset of $\mathbb{C}$ to which $\underline{y}$ belongs to $(\underline{y} + \mathbb{C})$.

2. Find an element $\underline{e}$ in the coset which has min Hamming weight $\omega_H(\underline{e})$

3. Decode $\hat{c} = \underline{y} - \underline{e}$. (Element $\underline{e}$ in the coset which has the min. Hamming weight is known as the "coset leader").

If there is unique element like this coset leader is clear.

If there is more than element in the coset, then we pick one of them & call it a coset leader.

<u>Example</u>: Let $\mathbb{C}$ be a $[6,3]$ binary code generated by

$$G = \left[I_k \mid P \right]$$

$$= \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right]. \qquad |\mathbb{C}| = 8 = q^k.$$

No. of cosets $= q^{n-k} = 2^{6-3} = 8$.

$d_{min}(\mathbb{C}) = 3$ $\rightarrow$ Total no. of vectors in $\mathbb{F}_2^6 = 64$.

<u>Standard Array</u>

A standard array of a linear code is a listing of the code and all of its cosets in the form of an array.

It is a listing of all vectors in $\mathbb{F}^n$.