L13

Thursday, September 22, 2022 11:18 AM

Recall for linear codes in $\mathbb{F}$

$$\vec{x} = G \cdot \vec{m}$$

and $\vec{0} = H \cdot \vec{x}$

$$d_{min} = \min_{1 \le i \le |F|^k - 1} \text{weight}(\vec{c_i})$$

Theorem: $\mathcal{C}$ has a parity check matrix H. The $d_{min}(\mathcal{C})$ is the minimum number of columns that are <u>linearly dependent</u>.

I.e.

$$H = \begin{bmatrix} | & | & | & \cdots & | \end{bmatrix}$$

$$\sum_{i=1}^{d_{min}} c_i \cdot \begin{bmatrix} | \end{bmatrix} = \vec{0}$$ for some coeff $c_i \in \mathbb{F}$

Eg. binary (7,4) Hamming

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$\Rightarrow d_{min} = 3$

proof: ① Any 1 column cannot be linearly independent

② Any 2 columns cannot be linearly indep

③ $\exists$ 3 columns that are L.I.

the minimal weight codeword is $(1, 1, 0, 1, 0, 0, 0)$

Corollary: The Singleton bound.

$$d_{min} \leq n - k + 1$$

$d_{min} \le n-k+1$

$\because$ the rank of $H = n-k$

So any $n-k+1$ columns must be independent.

* Binary Hamming Codes (Not just (7,4) codes)

for any $l \geq 3$, the corresponding Hamming code is an $(2^l-1, 2^l-1-l)$ code such that its parity check matrix

$$H = l\left[\ \overbrace{\qquad\qquad\qquad\qquad}^{2^l-1}\ \right]$$

contains all the non-zero columns of $\{0,1\}^l$

E.g. $l=3$ Hamming Code $= (7,4)$