An introduction to coding theory

Adrish Banerjee

Department of Electrical Engineering
Indian Institute of Technology Kanpur
Kanpur, Uttar Pradesh
India

Jan. 30, 2017

Lecture #5A: Distance Properties of Linear Block Codes-I

Distance properties of block codes

- Let $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1})$ be a binary n-tuple. The *Hamming weight* of $\mathbf{v}$, denoted by d($\mathbf{v}$) is defined as number of nonzero components of $\mathbf{v}$.

Distance properties of block codes

- Let $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1})$ be a binary n-tuple. The *Hamming weight* of $\mathbf{v}$, denoted by d($\mathbf{v}$) is defined as number of nonzero components of $\mathbf{v}$.
- Let $\mathbf{v}$, and $\mathbf{w}$ be two n-tuples. The *Hamming distance* between $\mathbf{v}$ and $\mathbf{w}$, denoted by d($\mathbf{v}$,$\mathbf{w}$) is defined as the number of places where they differ.

Distance properties of block codes

- Let $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1})$ be a binary n-tuple. The *Hamming weight* of $\mathbf{v}$, denoted by d($\mathbf{v}$) is defined as number of nonzero components of $\mathbf{v}$.
- Let $\mathbf{v}$, and $\mathbf{w}$ be two n-tuples. The *Hamming distance* between $\mathbf{v}$ and $\mathbf{w}$, denoted by d($\mathbf{v}$,$\mathbf{w}$) is defined as the number of places where they differ.
- Example 3.1: The Hamming distance between $\mathbf{v}$= (1 0 0 1 0 1 1) and $\mathbf{w}$= (0 1 0 0 0 1 1) is 3.

Distance properties of block codes

- Let $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1})$ be a binary n-tuple. The *Hamming weight* of $\mathbf{v}$, denoted by d($\mathbf{v}$) is defined as number of nonzero components of $\mathbf{v}$.
- Let $\mathbf{v}$, and $\mathbf{w}$ be two n-tuples. The *Hamming distance* between $\mathbf{v}$ and $\mathbf{w}$, denoted by d($\mathbf{v}$,$\mathbf{w}$) is defined as the number of places where they differ.
- Example 3.1: The Hamming distance between $\mathbf{v}$= (1 0 0 1 0 1 1) and $\mathbf{w}$= (0 1 0 0 0 1 1) is 3.
- Let $\mathbf{v}$, $\mathbf{w}$, and $\mathbf{x}$ be three binary n-tuples. Then

$$d(\mathbf{v}, \mathbf{w}) + d(\mathbf{w}, \mathbf{x}) \geq d(\mathbf{v}, \mathbf{x}) \quad \text{(Triangle inequality)}$$

Distance properties of block codes

- Proof: Let $\mathbf{v}$, $\mathbf{w}$, and $\mathbf{x}$ be three binary n-tuples, we can write

$$\begin{aligned} d(\mathbf{v},\mathbf{w}) &= w(\mathbf{v}+\mathbf{w}) \\ d(\mathbf{w},\mathbf{x}) &= w(\mathbf{w}+\mathbf{x}) \\ d(\mathbf{v},\mathbf{x}) &= w(\mathbf{v}+\mathbf{x}) \end{aligned}$$

Distance properties of block codes

- Proof: Let $\mathbf{v}$, $\mathbf{w}$, and $\mathbf{x}$ be three binary n-tuples, we can write

$$\begin{aligned} d(\mathbf{v},\mathbf{w}) &= w(\mathbf{v}+\mathbf{w}) \\ d(\mathbf{w},\mathbf{x}) &= w(\mathbf{w}+\mathbf{x}) \\ d(\mathbf{v},\mathbf{x}) &= w(\mathbf{v}+\mathbf{x}) \end{aligned}$$

- - For any two code vectors $\mathbf{a}$ and $\mathbf{b}$,

$$w(\mathbf{a}) + w(\mathbf{b}) \geq w(\mathbf{a}+\mathbf{b})$$

Distance properties of block codes

- Proof: Let $\mathbf{v}$, $\mathbf{w}$, and $\mathbf{x}$ be three binary n-tuples, we can write

$$\begin{aligned} d(\mathbf{v},\mathbf{w}) &= w(\mathbf{v}+\mathbf{w}) \\ d(\mathbf{w},\mathbf{x}) &= w(\mathbf{w}+\mathbf{x}) \\ d(\mathbf{v},\mathbf{x}) &= w(\mathbf{v}+\mathbf{x}) \end{aligned}$$

- - For any two code vectors $\mathbf{a}$ and $\mathbf{b}$,

$$w(\mathbf{a}) + w(\mathbf{b}) \geq w(\mathbf{a}+\mathbf{b})$$

- - Let $\mathbf{a}$= $\mathbf{v}$+$\mathbf{w}$ and $\mathbf{b}$= $\mathbf{w}$+$\mathbf{x}$, we get

$$w(\mathbf{v}+\mathbf{w}) + w(\mathbf{w}+\mathbf{x}) \geq w(\mathbf{v}+\mathbf{w}+\mathbf{w}+\mathbf{x}) = w(\mathbf{v}+\mathbf{x})$$

Distance properties of block codes

- Proof: Let $\mathbf{v}$, $\mathbf{w}$, and $\mathbf{x}$ be three binary n-tuples, we can write

$$\begin{aligned} d(\mathbf{v},\mathbf{w}) &= w(\mathbf{v}+\mathbf{w}) \\ d(\mathbf{w},\mathbf{x}) &= w(\mathbf{w}+\mathbf{x}) \\ d(\mathbf{v},\mathbf{x}) &= w(\mathbf{v}+\mathbf{x}) \end{aligned}$$

- - For any two code vectors $\mathbf{a}$ and $\mathbf{b}$,

$$w(\mathbf{a}) + w(\mathbf{b}) \geq w(\mathbf{a}+\mathbf{b})$$

- - Let $\mathbf{a}$= $\mathbf{v}$+$\mathbf{w}$ and $\mathbf{b}$= $\mathbf{w}$+$\mathbf{x}$, we get

$$w(\mathbf{v}+\mathbf{w}) + w(\mathbf{w}+\mathbf{x}) \geq w(\mathbf{v}+\mathbf{w}+\mathbf{w}+\mathbf{x}) = w(\mathbf{v}+\mathbf{x})$$

- Thus,

$$d(\mathbf{v},\mathbf{w}) + d(\mathbf{w},\mathbf{x}) \geq d(\mathbf{v},\mathbf{x})$$

Distance properties of block codes

- The *minimum distance*, $d_{\min}$ of a linear block code C is defined as

$$d_{\min} \stackrel{\Delta}{=} \min \{d(\mathbf{v}, \mathbf{w}) : \mathbf{v}, \mathbf{w} \in C, \mathbf{v} \neq \mathbf{w}\}.$$

Distance properties of block codes

- The *minimum distance*, $d_{\min}$ of a linear block code C is defined as

$$d_{\min} \stackrel{\Delta}{=} \min \{d(\mathbf{v}, \mathbf{w}) : \mathbf{v}, \mathbf{w} \in C, \mathbf{v} \neq \mathbf{w}\}.$$

- The *minimum weight*, $w_{\min}$ of C is defined as

$$w_{\min} \stackrel{\Delta}{=} \min \{w(\mathbf{v}) : \mathbf{v} \in C, v \neq \mathbf{0}\}$$

Distance properties of block codes

- The *minimum distance*, $d_{\min}$ of a linear block code C is defined as

$$d_{\min} \stackrel{\Delta}{=} \min\{d(\mathbf{v},\mathbf{w}) : \mathbf{v},\mathbf{w} \in C, \mathbf{v} \neq \mathbf{w}\}.$$

- The *minimum weight*, $w_{\min}$ of C is defined as

$$w_{\min} \stackrel{\Delta}{=} \min\{w(\mathbf{v}) : \mathbf{v} \in C, v \neq \mathbf{0}\}$$

- Note:

$$\begin{aligned} d_{\min} &= \min\{d(\mathbf{v},\mathbf{w}) : \mathbf{v},\mathbf{w} \in C, \mathbf{v} \neq \mathbf{w}\} \\ &= \min\{w(\mathbf{v}+\mathbf{w}) : \mathbf{v},\mathbf{w} \in C, \mathbf{v} \neq \mathbf{w}\} \\ &= \min\{w(\mathbf{x}) : \mathbf{x} \in C, \mathbf{x} \neq \mathbf{0}\} \\ &= w_{\min}. \end{aligned}$$

Distance properties of block codes

Theorem:

- Let C be an (n,k) linear code with parity check matrix **H**. For each codeword of Hamming weight l, there exist l columns of **H** such that the vector sum of these l columns is equal to the zero vector.

Proof:

Distance properties of block codes

Theorem:

- Let C be an (n,k) linear code with parity check matrix $\mathbf{H}$. For each codeword of Hamming weight l, there exist l columns of $\mathbf{H}$ such that the vector sum of these l columns is equal to the zero vector.

Proof:

- Let's represent the parity check matrix, $\mathbf{H}$ as

$$\mathbf{H} = [\mathbf{h}_0, \mathbf{h}_1, \cdots, \mathbf{h}_{n-1}],$$

where $\mathbf{h}_i$ represents the i^{th} column of $\mathbf{H}$.

Distance properties of block codes

Theorem:

- Let C be an (n,k) linear code with parity check matrix $\mathbf{H}$. For each codeword of Hamming weight l, there exist l columns of $\mathbf{H}$ such that the vector sum of these l columns is equal to the zero vector.

Proof:

- Let's represent the parity check matrix, $\mathbf{H}$ as

$$\mathbf{H} = [\mathbf{h}_0, \mathbf{h}_1, \cdots, \mathbf{h}_{n-1}],$$

where $\mathbf{h}_i$ represents the i^{th} column of $\mathbf{H}$.

- Let $v_{i_1}, v_{i_2}, \cdots, v_{i_l}$ be the l nonzero components of the codeword $\mathbf{v}$, where $0 \leq i_1 \leq i_2 \leq \cdots < i_l \leq n-1$, then $v_{i_1} = v_{i_2} = \cdots = v_{i_l} = 1$.

Distance properties of block codes

Proof (contd.):

- Since $\mathbf{v}$ is a codeword, we must have

$$\begin{aligned} \mathbf{0} &= \mathbf{v} \cdot \mathbf{H}^{\mathsf{T}} \\ &= v_0\mathbf{h}_0 + v_1\mathbf{h}_1 + \cdots + v_{n-1}\mathbf{h}_{n-1} \\ &= v_{i_1}\mathbf{h}_{i_1} + v_{i_2}\mathbf{h}_{i_2} + \cdots + v_{i_l}\mathbf{h}_{i_l} \\ &= \mathbf{h}_{i_1} + \mathbf{h}_{i_2} + \cdots + \mathbf{h}_{i_l} \end{aligned}$$

Distance properties of block codes

Theorem:

- If there exists l columns of H whose vector sum is zero vector, there exists a codeword of Hamming weight l in C.

Proof:

Distance properties of block codes

Theorem:

- If there exists l columns of H whose vector sum is zero vector, there exists a codeword of Hamming weight l in C.

Proof:

- Suppose $\mathbf{h}_{i_1}, \mathbf{h}_{i_2}, \cdots, \mathbf{h}_{i_l}$ are the l columns of $\mathbf{H}$ such that

$$\mathbf{h}_{i_1} + \mathbf{h}_{i_2} + \cdots + \mathbf{h}_{i_l} = \mathbf{0}$$

Distance properties of block codes

Theorem:

- If there exists l columns of H whose vector sum is zero vector, there exists a codeword of Hamming weight l in C.

Proof:

- Suppose $\mathbf{h}_{i_1}, \mathbf{h}_{i_2}, \cdots, \mathbf{h}_{i_l}$ are the l columns of $\mathbf{H}$ such that

$$\mathbf{h}_{i_1} + \mathbf{h}_{i_2} + \cdots + \mathbf{h}_{i_l} = \mathbf{0}$$

- Let's form a binary n-tuple $\mathbf{x} = (x_1, x_2, \cdots, x_{n-1})$ whose nonzero components are $x_{i_1}, x_{i_2}, \cdots, x_{i_l}$. The Hamming weight of $\mathbf{x}$ is l.

Distance properties of block codes

Proof (contd.):

- Consider the product

$$\begin{aligned}\mathbf{x}\cdot\mathbf{H}^{\mathbf{T}} &= x_0\mathbf{h}_0 + x_1\mathbf{h}_1 + \cdots + x_{n-1}\mathbf{h}_{n-1}\\ &= x_{i_1}\mathbf{h}_{i_1} + x_{i_2}\mathbf{h}_{i_2} + \cdots + x_{i_l}\mathbf{h}_{i_l}\\ &= \mathbf{h}_{i_1} + \mathbf{h}_{i_2} + \cdots + \mathbf{h}_{i_l}\\ &= 0\end{aligned}$$

Distance properties of block codes

Proof (contd.):

- Consider the product

$$\begin{aligned}\mathbf{x}\cdot\mathbf{H}^{\mathbf{T}} &= x_0\mathbf{h}_0 + x_1\mathbf{h}_1 + \cdots + x_{n-1}\mathbf{h}_{n-1}\\ &= x_{i_1}\mathbf{h}_{i_1} + x_{i_2}\mathbf{h}_{i_2} + \cdots + x_{i_l}\mathbf{h}_{i_l}\\ &= \mathbf{h}_{i_1} + \mathbf{h}_{i_2} + \cdots + \mathbf{h}_{i_l}\\ &= 0\end{aligned}$$

- Thus, $\mathbf{x}$ is a codeword of weight l in C.

Distance properties of block codes

- Let C be a linear block code with parity check matrix $\mathbf{H}$. If no $d-1$ or fewer columns of $\mathbf{H}$ add to $\mathbf{0}$, the code has minimum weight at least d.

Distance properties of block codes

- Let C be a linear block code with parity check matrix $\mathbf{H}$. If no $d-1$ or fewer columns of $\mathbf{H}$ add to $\mathbf{0}$, the code has minimum weight at least d.
- Let C be a linear block code with parity check matrix $\mathbf{H}$. The minimum weight of C, d_{min} is equal to the fewest number of columns of $\mathbf{H}$ (rows of $\mathbf{H}^{\mathbf{T}}$) that add to $\mathbf{0}$.