# An introduction to coding theory

Adrish Banerjee

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

Jan. 30, 2017

## Lecture #5B: Distance Properties of Linear Block Codes-II

## Distance properties of block codes

Example 3.2: Let $k = 3$ and $n = 6$. The table gives a $(6, 3)$ linear block code.

| Message $(u_0, u_1, u_2)$ | Codewords $(v_0, v_1, v_2, v_3, v_4, v_5)$ |
|---|---|
| (0 0 0) | (0 0 0 0 0 0) |
| (1 0 0) | (0 1 1 1 0 0) |
| (0 1 0) | (1 0 1 0 1 0) |
| (1 1 0) | (1 1 0 1 1 0) |
| (0 0 1) | (1 1 0 0 0 1) |
| (1 0 1) | (1 0 1 1 0 1) |
| (0 1 1) | (0 1 1 0 1 1) |
| (1 1 1) | (0 0 0 1 1 1) |



## Distance properties of block codes

- Let $A_i$ be the number of codewords in C with Hamming weight $i$.

## Distance properties of block codes

- Let $A_i$ be the number of codewords in C with Hamming weight $i$.
- The set $\{A_0, A_1, \cdots, A_n\}$ is called the *weight distribution* of C.



## Distance properties of block codes

- Let $A_i$ be the number of codewords in C with Hamming weight $i$.
- The set $\{A_0, A_1, \cdots, A_n\}$ is called the *weight distribution* of C.
- Note that $A_0 = 1$, and $\sum_{i=0}^{n} A_i = 2^k$.

## Distance properties of block codes

- Let $A_i$ be the number of codewords in C with Hamming weight $i$.
- The set $\{A_0, A_1, \cdots, A_n\}$ is called the *weight distribution* of C.
- Note that $A_0 = 1$, and $\sum_{i=0}^{n} A_i = 2^k$.
- Example 3.3: For the (6,3) code in example 3.2

$$A_0 = 1, A_1 = 0, A_2 = 0, A_3 = 4, A_4 = 3, A_5 = 0, A_6 = 0.$$



## Distance properties of block codes

- Let $A_i$ be the number of codewords in C with Hamming weight $i$.
- The set $\{A_0, A_1, \cdots, A_n\}$ is called the *weight distribution* of C.
- Note that $A_0 = 1$, and $\sum_{i=0}^{n} A_i = 2^k$.
- Example 3.3: For the (6,3) code in example 3.2

$$A_0 = 1, A_1 = 0, A_2 = 0, A_3 = 4, A_4 = 3, A_5 = 0, A_6 = 0.$$

- $d_{\min}$ in the above example is 3.

## Error detecting properties of block codes

- The probability of undetected error on a BSC is given by

$$P_u(E) = \sum_{i=1}^{n} A_i p^i (1-p)^{n-i}$$



## Error detecting properties of block codes

- The probability of undetected error on a BSC is given by

$$P_u(E) = \sum_{i=1}^{n} A_i p^i (1-p)^{n-i}$$

- Example 3.4: For the $(6, 3)$ code in example 3.2,

$$P_u(E) = 4p^3(1-p)^3 + 3p^4(1-p)^2 \approx 4p^3 \quad \text{(for small p)}$$

## Error detecting properties of block codes

- There exist (n,k) linear block codes for which

$$P_u(E) \leq 2^{-(n-k)} \quad \text{for all p} \leq 1/2$$

on a BSC.



## Error detecting properties of block codes

- There exist (n,k) linear block codes for which

$$P_u(E) \leq 2^{-(n-k)} \quad \text{for all p} \leq 1/2$$

on a BSC.

- The above bound shows that the undetected error probability can be made to decrease exponentially with the number of parity check bits $n - k$ in a linear code.

## Error detecting properties of block codes

- There exist (n,k) linear block codes for which

$$P_u(E) \leq 2^{-(n-k)} \quad \text{for all p} \leq 1/2$$

  on a BSC.
- The above bound shows that the undetected error probability can be made to decrease exponentially with the number of parity check bits $n-k$ in a linear code.
- For a codeword with minimum distance $d_{\min}$, no error pattern with weight $d_{\min}-1$ or less can change a transmitted codeword into another codeword.



## Error detecting properties of block codes

- There exist (n,k) linear block codes for which

$$P_u(E) \leq 2^{-(n-k)} \quad \text{for all p} \leq 1/2$$

  on a BSC.
- The above bound shows that the undetected error probability can be made to decrease exponentially with the number of parity check bits $n-k$ in a linear code.
- For a codeword with minimum distance $d_{\min}$, no error pattern with weight $d_{\min}-1$ or less can change a transmitted codeword into another codeword.
- Therefore, all error patterns with $d_{\min}-1$ or fewer errors are detectable, and $d_{\min}-1$ is called the *random error detecting capability* of a block code.

## Error correcting properties of block codes

Theorem:

- A block code C with minimum distance $d_{\min}$ is capable of correcting all error patterns of weight t or less, where t is an integer such that $2t + 1 \leq d_{\min} \leq 2t + 2$.

Proof:



## Error correcting properties of block codes

Theorem:

- A block code C with minimum distance $d_{\min}$ is capable of correcting all error patterns of weight t or less, where t is an integer such that $2t + 1 \leq d_{\min} \leq 2t + 2$.

Proof:

- Assuming codeword $\mathbf{v}$ is transmitted and $\mathbf{r}$ is the received sequence. Let $\mathbf{w} \neq \mathbf{v}$ be any other codeword. Then $d(\mathbf{v}, \mathbf{w}) \leq d(\mathbf{v}, \mathbf{r}) + d(\mathbf{r}, \mathbf{w})$ (triangle inequality).

## Error correcting properties of block codes

Theorem:

- A block code C with minimum distance $d_{\min}$ is capable of correcting all error patterns of weight t or less, where t is an integer such that $2t + 1 \leq d_{\min} \leq 2t + 2$.

Proof:

- Assuming codeword $\mathbf{v}$ is transmitted and $\mathbf{r}$ is the received sequence. Let $\mathbf{w} \neq \mathbf{v}$ be any other codeword. Then $d(\mathbf{v}, \mathbf{w}) \leq d(\mathbf{v}, \mathbf{r}) + d(\mathbf{r}, \mathbf{w})$ (triangle inequality).
- If the error pattern has weight t', then d($\mathbf{v}$,$\mathbf{r}$) = t'.



## Error correcting properties of block codes

Proof (contd):

- Since $\mathbf{v}$, and $\mathbf{w}$ are codewords,

$$d(\mathbf{v}, \mathbf{w}) \geq d_{\min} \geq 2t + 1$$

Therefore,

$$d(\mathbf{r}, \mathbf{w}) \geq d(\mathbf{v}, \mathbf{w}) - d(\mathbf{v}, \mathbf{r}) \geq 2t + 1 - t'.$$

## Error correcting properties of block codes

Proof (contd):

- Since $\mathbf{v}$, and $\mathbf{w}$ are codewords,

$$d(\mathbf{v}, \mathbf{w}) \geq d_{\min} \geq 2t + 1$$

Therefore,

$$d(\mathbf{r}, \mathbf{w}) \geq d(\mathbf{v}, \mathbf{w}) - d(\mathbf{v}, \mathbf{r}) \geq 2t + 1 - t'.$$

- If t' $\leq$ t, then

$$d(\mathbf{r}, \mathbf{w}) \geq t + 1 > t \quad \text{and} \quad d(\mathbf{v}, \mathbf{r}) = t' \leq t.$$



## Error correcting properties of block codes

Proof (contd):

- Since $\mathbf{v}$, and $\mathbf{w}$ are codewords,

$$d(\mathbf{v}, \mathbf{w}) \geq d_{\min} \geq 2t + 1$$

Therefore,

$$d(\mathbf{r}, \mathbf{w}) \geq d(\mathbf{v}, \mathbf{w}) - d(\mathbf{v}, \mathbf{r}) \geq 2t + 1 - t'.$$

- If t' $\leq$ t, then

$$d(\mathbf{r}, \mathbf{w}) \geq t + 1 > t \quad \text{and} \quad d(\mathbf{v}, \mathbf{r}) = t' \leq t.$$

- Hence $\mathbf{r}$ is closer to $\mathbf{v}$ than any other codeword $\mathbf{w}$, and an ML decoder will decode correctly.

## Error correcting properties of block codes

Theorem:

- For all $l \geq t+1$, there is atleast one error pattern of weight $l$ that may not be correctly decoded by an ML decoder.

Proof:

- Let $\mathbf{v}$ and $\mathbf{w}$ be two codewords such that d($\mathbf{v}$,$\mathbf{w}$) $= d_{\min}$. Let $\mathbf{e}_1$, and $\mathbf{e}_2$ be two error patterns such that

  (i) $\mathbf{e}_1 + \mathbf{e}_2 = \mathbf{v} + \mathbf{w}$
  (ii) $w(\mathbf{e}_1 + \mathbf{e}_2) = w(\mathbf{e}_1) + w(\mathbf{e}_2)$ (nonoverlapping 1's)
  (iii) $w(\mathbf{e}_1) = l \geq t+1$

  Then,

$$w(\mathbf{e}_1) + w(\mathbf{e}_2) = w(\mathbf{e}_1 + \mathbf{e}_2) = w(\mathbf{v} + \mathbf{w}) = d(\mathbf{v} + \mathbf{w}) = d_{\min}.$$



## Error correcting properties of block codes

- Assuming $\mathbf{v}$ is transmitted and $\mathbf{r} = \mathbf{v} + \mathbf{e}_1$ is received. Then

$$\begin{aligned} d(\mathbf{w}, \mathbf{r}) &= w(\mathbf{w} + \mathbf{r}) = w(\mathbf{w} + \mathbf{v} + \mathbf{e}_1) = w(\mathbf{e}_2) = d_{\min} - w(\mathbf{e}_1) \\ &< 2t + 2 - (t+1) = t+1 \end{aligned}$$

## Error correcting properties of block codes

- Assuming $\mathbf{v}$ is transmitted and $\mathbf{r} = \mathbf{v} + \mathbf{e}_1$ is received. Then

$$\begin{aligned} d(\mathbf{w}, \mathbf{r}) &= w(\mathbf{w} + \mathbf{r}) = w(\mathbf{w} + \mathbf{v} + \mathbf{e}_1) = w(\mathbf{e}_2) = d_{\min} - w(\mathbf{e}_1) \\ &< 2t + 2 - (t + 1) = t + 1 \end{aligned}$$

- Therefore $d(\mathbf{w}, \mathbf{r}) \leq d(\mathbf{v}, \mathbf{r})$ and an ML decoder may decode incorrectly.



## Error correcting properties of block codes

- Assuming $\mathbf{v}$ is transmitted and $\mathbf{r} = \mathbf{v} + \mathbf{e}_1$ is received. Then

$$\begin{aligned} d(\mathbf{w}, \mathbf{r}) &= w(\mathbf{w} + \mathbf{r}) = w(\mathbf{w} + \mathbf{v} + \mathbf{e}_1) = w(\mathbf{e}_2) = d_{\min} - w(\mathbf{e}_1) \\ &< 2t + 2 - (t + 1) = t + 1 \end{aligned}$$

- Therefore $d(\mathbf{w}, \mathbf{r}) \leq d(\mathbf{v}, \mathbf{r})$ and an ML decoder may decode incorrectly.
- Hence for a block code with minimum distance $d_{\min}$, an ML decoder will correctly decode any error pattern of weight t $\stackrel{\Delta}{=} \lfloor \frac{d_{\min}-1}{2} \rfloor$ or less.

## Error correcting properties of block codes

- Assuming $\mathbf{v}$ is transmitted and $\mathbf{r} = \mathbf{v} + \mathbf{e}_1$ is received. Then

$$\begin{aligned} d(\mathbf{w}, \mathbf{r}) &= w(\mathbf{w} + \mathbf{r}) = w(\mathbf{w} + \mathbf{v} + \mathbf{e}_1) = w(\mathbf{e}_2) = d_{\min} - w(\mathbf{e}_1) \\ &< 2t + 2 - (t + 1) = t + 1 \end{aligned}$$

- Therefore $d(\mathbf{w}, \mathbf{r}) \leq d(\mathbf{v}, \mathbf{r})$ and an ML decoder may decode incorrectly.
- Hence for a block code with minimum distance $d_{\min}$, an ML decoder will correctly decode any error pattern of weight t $\stackrel{\Delta}{=} \lfloor \frac{d_{\min}-1}{2} \rfloor$ or less.
- $t$ is called the random error correcting capability of the code.



## Error correcting properties of block codes

Theorem:

- For an $(n, k)$ linear code C with minimum distance $d_{\min}$, all the n-tuples of weight $t = \lfloor (d_{\min} - 1)/2 \rfloor$ or less can be used as coset leaders of a standard array of C.

Proof

## Error correcting properties of block codes

Theorem:

- For an $(n, k)$ linear code C with minimum distance $d_{\min}$, all the n-tuples of weight $t = \lfloor (d_{\min} - 1)/2 \rfloor$ or less can be used as coset leaders of a standard array of C.

Proof

- Since minimum distance of C is $d_{\min}$, minimum weight of C is also $d_{\min}$.



## Error correcting properties of block codes

Theorem:

- For an $(n, k)$ linear code C with minimum distance $d_{\min}$, all the n-tuples of weight $t = \lfloor (d_{\min} - 1)/2 \rfloor$ or less can be used as coset leaders of a standard array of C.

Proof

- Since minimum distance of C is $d_{\min}$, minimum weight of C is also $d_{\min}$.
- Let $\mathbf{x}$ and $\mathbf{y}$ be two $n-$tuples of weight $t$ or less.

## Error correcting properties of block codes

Theorem:

- For an $(n, k)$ linear code C with minimum distance $d_{\min}$, all the n-tuples of weight $t = \lfloor (d_{\min} - 1)/2 \rfloor$ or less can be used as coset leaders of a standard array of C.

Proof

- Since minimum distance of C is $d_{\min}$, minimum weight of C is also $d_{\min}$.
- Let $\mathbf{x}$ and $\mathbf{y}$ be two $n-$tuples of weight $t$ or less.
- $w(\mathbf{x} + \mathbf{y}) \leq w(\mathbf{x}) + w(\mathbf{y}) \leq 2t < d_{\min}$



## Error correcting properties of block codes

Theorem:

- For an $(n, k)$ linear code C with minimum distance $d_{\min}$, all the n-tuples of weight $t = \lfloor (d_{\min} - 1)/2 \rfloor$ or less can be used as coset leaders of a standard array of C.

Proof

- Since minimum distance of C is $d_{\min}$, minimum weight of C is also $d_{\min}$.
- Let $\mathbf{x}$ and $\mathbf{y}$ be two $n-$tuples of weight $t$ or less.
- $w(\mathbf{x} + \mathbf{y}) \leq w(\mathbf{x}) + w(\mathbf{y}) \leq 2t < d_{\min}$
- Suppose $\mathbf{x}$ and $\mathbf{y}$ are in the same coset, then $\mathbf{x} + \mathbf{y}$ must be a nonzero codeword in C.

## Error correcting properties of block codes

Theorem:

- For an $(n, k)$ linear code C with minimum distance $d_{\min}$, all the n-tuples of weight $t = \lfloor (d_{\min} - 1)/2 \rfloor$ or less can be used as coset leaders of a standard array of C.

Proof

- Since minimum distance of C is $d_{\min}$, minimum weight of C is also $d_{\min}$.
- Let $\mathbf{x}$ and $\mathbf{y}$ be two $n-$tuples of weight $t$ or less.
- $w(\mathbf{x} + \mathbf{y}) \leq w(\mathbf{x}) + w(\mathbf{y}) \leq 2t < d_{\min}$
- Suppose $\mathbf{x}$ and $\mathbf{y}$ are in the same coset, then $\mathbf{x} + \mathbf{y}$ must be a nonzero codeword in C.
- This is impossible as weight of $\mathbf{x} + \mathbf{y} < d_{\min}$.



## Error correcting properties of block codes

Theorem:

- For an $(n, k)$ linear code C with minimum distance $d_{\min}$, if all the n-tuples of weight $t = \lfloor (d_{\min} - 1)/2 \rfloor$ or less are used as coset leaders of a standard array of C, then there is at least one n-tuple of weight $t + 1$ that cannot be used as coset leader.

Proof:

- Let $\mathbf{v}$ be the minimum weight codeword of C

## Error correcting properties of block codes

Theorem:

- For an $(n, k)$ linear code C with minimum distance $d_{\min}$, if all the n-tuples of weight $t = \lfloor (d_{\min} - 1)/2 \rfloor$ or less are used as coset leaders of a standard array of C, then there is at least one n-tuple of weight $t + 1$ that cannot be used as coset leader.

Proof:

- Let $\mathbf{v}$ be the minimum weight codeword of C
- Let $\mathbf{x}$ and $\mathbf{y}$ be two n-tuples that satisfies the following conditions:



## Error correcting properties of block codes

Theorem:

- For an $(n, k)$ linear code C with minimum distance $d_{\min}$, if all the n-tuples of weight $t = \lfloor (d_{\min} - 1)/2 \rfloor$ or less are used as coset leaders of a standard array of C, then there is at least one n-tuple of weight $t + 1$ that cannot be used as coset leader.

Proof:

- Let $\mathbf{v}$ be the minimum weight codeword of C
- Let $\mathbf{x}$ and $\mathbf{y}$ be two n-tuples that satisfies the following conditions:
  - $\mathbf{x} + \mathbf{y} = \mathbf{v}$.

## Error correcting properties of block codes

Theorem:

- For an $(n, k)$ linear code C with minimum distance $d_{\min}$, if all the n-tuples of weight $t = \lfloor (d_{\min} - 1)/2 \rfloor$ or less are used as coset leaders of a standard array of C, then there is at least one n-tuple of weight $t + 1$ that cannot be used as coset leader.

Proof:

- Let $\mathbf{v}$ be the minimum weight codeword of C
- Let $\mathbf{x}$ and $\mathbf{y}$ be two n-tuples that satisfies the following conditions:
  - $\mathbf{x} + \mathbf{y} = \mathbf{v}$.
  - $\mathbf{x}$ and $\mathbf{y}$ do not have nonzero component in common places.



## Error correcting properties of block codes

Proof (contd.)

- From definition, $\mathbf{x}$ and $\mathbf{y}$ must be in the same coset, and

$$w(\mathbf{x}) + w(\mathbf{y}) = w(\mathbf{v}) = d_{\min}.$$

## Error correcting properties of block codes

Proof (contd.)

- From definition, $\mathbf{x}$ and $\mathbf{y}$ must be in the same coset, and

$$w(\mathbf{x}) + w(\mathbf{y}) = w(\mathbf{v}) = d_{\min}.$$

- If we choose $w(\mathbf{y}) = t + 1$, then $w(\mathbf{x}) = t$ or $t + 1$ (since $2t + 1 \leq d_{\min} \leq 2t + 2$).



## Error correcting properties of block codes

Proof (contd.)

- From definition, $\mathbf{x}$ and $\mathbf{y}$ must be in the same coset, and

$$w(\mathbf{x}) + w(\mathbf{y}) = w(\mathbf{v}) = d_{\min}.$$

- If we choose $w(\mathbf{y}) = t + 1$, then $w(\mathbf{x}) = t$ or $t + 1$ (since $2t + 1 \leq d_{\min} \leq 2t + 2$).
- Therefore if $\mathbf{x}$ is chosen as coset leader, $\mathbf{y}$ cannot be coset leader.