Information and Coding Theory

MA41024/ MA60020/ MA60262

Bibhas Adhikari

Spring 2022-23, IIT Kharagpur

Lecture 13
March 6, 2023

Linear block code

Correction of error Let C be an (n, k) linear code with minimum distance $d_{\min}$. Then

$$2t + 1 \leq d_{\min} \leq 2t + 2$$

for some positive integer t.

Linear block code

Correction of error Let C be an (n, k) linear code with minimum distance $d_{\min}$. Then

$$2t + 1 \leq d_{\min} \leq 2t + 2$$

for some positive integer t. Suppose now that there are error patterns with l errors, $l > t$.

Linear block code

Correction of error Let C be an (n, k) linear code with minimum distance $d_{\min}$. Then

$$2t + 1 \leq d_{\min} \leq 2t + 2$$

for some positive integer t. Suppose now that there are error patterns with l errors, $l > t$.

Claim C is NOT capable of correcting all the error patterns of l errors.

$\rightarrow$ Suppose $\mathbf{v}$ and $\mathbf{w}$ are codewords such that $d(\mathbf{v}, \mathbf{w}) = d_{\min}$

Linear block code

Correction of error Let C be an (n, k) linear code with minimum distance $d_{\min}$. Then

$$2t + 1 \leq d_{\min} \leq 2t + 2$$

for some positive integer t. Suppose now that there are error patterns with l errors, $l > t$.

Claim C is NOT capable of correcting all the error patterns of l errors.

→ Suppose $\mathbf{v}$ and $\mathbf{w}$ are codewords such that $d(\mathbf{v}, \mathbf{w}) = d_{\min}$

→ Let $\mathbf{e}_1$ and $\mathbf{e}_2$ be two error patterns such that

$$\mathbf{e}_1 + \mathbf{e}_2 = \mathbf{v} + \mathbf{w}$$

Linear block code

Correction of error Let C be an (n, k) linear code with minimum distance $d_{\min}$. Then

$$2t + 1 \leq d_{\min} \leq 2t + 2$$

for some positive integer t. Suppose now that there are error patterns with l errors, $l > t$.

Claim C is NOT capable of correcting all the error patterns of l errors.

$\rightarrow$ Suppose $\mathbf{v}$ and $\mathbf{w}$ are codewords such that $d(\mathbf{v}, \mathbf{w}) = d_{\min}$

$\rightarrow$ Let $\mathbf{e}_1$ and $\mathbf{e}_2$ be two error patterns such that

$\mathbf{e}_1 + \mathbf{e}_2 = \mathbf{v} + \mathbf{w}$

$\mathbf{e}_1$ and $\mathbf{e}_2$ do not have nonzero entries in common positions

Linear block code

Correction of error Let C be an (n, k) linear code with minimum distance $d_{\min}$. Then

$$2t + 1 \leq d_{\min} \leq 2t + 2$$

for some positive integer t. Suppose now that there are error patterns with l errors, $l > t$.

Claim C is NOT capable of correcting all the error patterns of l errors.

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

  $\mathbf{e}_1 + \mathbf{e}_2 = \mathbf{v} + \mathbf{w}$

  $\mathbf{e}_1$ and $\mathbf{e}_2$ do not have nonzero entries in common positions
- $\rightarrow$ Then

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

Linear block code

Suppose $\mathbf{v}$ is transmitted and is corrupted by error $\mathbf{e}_1$. Then

$$\mathbf{r} = \mathbf{v} + \mathbf{e}_1$$

Linear block code

Suppose $\mathbf{v}$ is transmitted and is corrupted by error $\mathbf{e}_1$. Then

$$\mathbf{r} = \mathbf{v} + \mathbf{e}_1$$

$$d(\mathbf{v}, \mathbf{r}) = w(\mathbf{v} + \mathbf{r}) = w(\mathbf{e}_1)$$

Linear block code

Suppose $\mathbf{v}$ is transmitted and is corrupted by error $\mathbf{e}_1$. Then

$$\mathbf{r} = \mathbf{v} + \mathbf{e}_1$$
$$d(\mathbf{v}, \mathbf{r}) = w(\mathbf{v} + \mathbf{r}) = w(\mathbf{e}_1)$$
$$d(\mathbf{w}, \mathbf{r}) = w(\mathbf{w} + \mathbf{r}) = w(\mathbf{w} + \mathbf{v} + \mathbf{e}_1) = w(\mathbf{e}_2)$$

Linear block code

Suppose $\mathbf{v}$ is transmitted and is corrupted by error $\mathbf{e}_1$. Then

$$\mathbf{r} = \mathbf{v} + \mathbf{e}_1$$
$$d(\mathbf{v}, \mathbf{r}) = w(\mathbf{v} + \mathbf{r}) = w(\mathbf{e}_1)$$
$$d(\mathbf{w}, \mathbf{r}) = w(\mathbf{w} + \mathbf{r}) = w(\mathbf{w} + \mathbf{v} + \mathbf{e}_1) = w(\mathbf{e}_2)$$

If $\mathbf{e}_1$ contains more than t errors with $w(\mathbf{e}_1) > t$. Then

$$w(\mathbf{e}_2) \leq t + 1$$

since $w(\mathbf{e}_1) + w(\mathbf{e}_2) = d_{\text{min}}$ and $2t + 1 \leq d_{\text{min}} \leq 2t + 2$

Linear block code

Suppose $\mathbf{v}$ is transmitted and is corrupted by error $\mathbf{e}_1$. Then

$$\mathbf{r} = \mathbf{v} + \mathbf{e}_1$$
$$d(\mathbf{v}, \mathbf{r}) = w(\mathbf{v} + \mathbf{r}) = w(\mathbf{e}_1)$$
$$d(\mathbf{w}, \mathbf{r}) = w(\mathbf{w} + \mathbf{r}) = w(\mathbf{w} + \mathbf{v} + \mathbf{e}_1) = w(\mathbf{e}_2)$$

If $\mathbf{e}_1$ contains more than t errors with $w(\mathbf{e}_1) > t$. Then

$$w(\mathbf{e}_2) \leq t + 1$$

since $w(\mathbf{e}_1) + w(\mathbf{e}_2) = d_{\text{min}}$ and $2t + 1 \leq d_{\text{min}} \leq 2t + 2$
Thus $d(\mathbf{v}, \mathbf{r}) = w(\mathbf{e}_1) > t$ and $d(\mathbf{w}, \mathbf{r}) = w(\mathbf{e}_2) \leq t + 1$, which implies

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

This implies there exists an error pattern of $l > t$ errors that results in a received vector that is closer to an incorrect codeword than the transmitted codeword

Linear block code

Based on maximum likelihood decoding scheme, an incorrect decoding would be performed.

Linear block code

Based on maximum likelihood decoding scheme, an incorrect decoding would be performed.

Conclusion A linear block code with minimum distance d_{min} guarantees correction of all the error patterns of $t = \lfloor (d_{\text{min}} - 1)/2 \rfloor$ or fewer errors. This parameter is called *random-error-correcting capability* of a code

Linear block code

Syndrome decoding through standard array

- Let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{2^k}$ be the codewords of C, and $\mathbf{r}$ be a received codeword
- Partition 2^n possible received codewords into 2^k disjoint subsets $D_1, D_2, \ldots, D_{2^k}$ such that the codeword $\mathbf{v}_i \in D_i$, $1 \leq i \leq 2^k$

Linear block code

Syndrome decoding through standard array

- $\rightarrow$ Let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{2^k}$ be the codewords of C, and $\mathbf{r}$ be a received codeword
- $\rightarrow$ Partition 2^n possible received codewords into 2^k disjoint subsets $D_1, D_2, \ldots, D_{2^k}$ such that the codeword $\mathbf{v}_i \in D_i$, $1 \leq i \leq 2^k$
- $\rightarrow$ If $\mathbf{r} \in D_i$ then $\mathbf{r}$ is decoded as $\mathbf{v}_i$

Linear block code

Syndrome decoding through standard array

- $\rightarrow$ Let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{2^k}$ be the codewords of C, and $\mathbf{r}$ be a received codeword
- $\rightarrow$ Partition 2^n possible received codewords into 2^k disjoint subsets $D_1, D_2, \ldots, D_{2^k}$ such that the codeword $\mathbf{v}_i \in D_i$, $1 \leq i \leq 2^k$
- $\rightarrow$ If $\mathbf{r} \in D_i$ then $\mathbf{r}$ is decoded as $\mathbf{v}_i$

Partition method - standard array

- $\rightarrow$ Place the 2^k codewords of C in a row with the zero vector codeword $\mathbf{v}_1$ as the first (leftmost)

Linear block code

Syntax decoding through standard array

- $\rightarrow$ Let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{2^k}$ be the codewords of C, and $\mathbf{r}$ be a received codeword
- $\rightarrow$ Partition 2^n possible received codewords into 2^k disjoint subsets $D_1, D_2, \ldots, D_{2^k}$ such that the codeword $\mathbf{v}_i \in D_i$, $1 \leq i \leq 2^k$
- $\rightarrow$ If $\mathbf{r} \in D_i$ then $\mathbf{r}$ is decoded as $\mathbf{v}_i$

Partition method - standard array

- $\rightarrow$ Place the 2^k codewords of C in a row with the zero vector codeword $\mathbf{v}_1$ as the first (leftmost)
- $\rightarrow$ Denote the set of $2^{n-k} - 1$ error vectors of length n as $\mathbf{e}_2, \ldots, \mathbf{e}_{2^{n-k}}$

Linear block code

Syndrome decoding through standard array

- $\rightarrow$ Let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{2^k}$ be the codewords of C, and $\mathbf{r}$ be a received codeword
- $\rightarrow$ Partition 2^n possible received codewords into 2^k disjoint subsets $D_1, D_2, \ldots, D_{2^k}$ such that the codeword $\mathbf{v}_i \in D_i$, $1 \leq i \leq 2^k$
- $\rightarrow$ If $\mathbf{r} \in D_i$ then $\mathbf{r}$ is decoded as $\mathbf{v}_i$

Partition method - standard array

- $\rightarrow$ Place the 2^k codewords of C in a row with the zero vector codeword $\mathbf{v}_1$ as the first (leftmost)
- $\rightarrow$ Denote the set of $2^{n-k} - 1$ error vectors of length n as $\mathbf{e}_2, \ldots, \mathbf{e}_{2^{n-k}}$
- $\rightarrow$ Form the second row by adding $\mathbf{e}_2$ to each codeword $\mathbf{v}_i$ in the first row and placing the sum $\mathbf{e}_2 + \mathbf{v}_i$ under $\mathbf{v}_i$
- $\rightarrow$ Continue the process until all the error vectors are used

Linear block code

Observation

1. The sum of any two vectors in the same row is a codeword in C

Linear block code

Observation

1. The sum of any two vectors in the same row is a codeword in C
2. No two n-tuples in the same row of a standard array are identical. Every n-tuple appears in one and only one row.

Linear block code

Observation

1. The sum of any two vectors in the same row is a codeword in C
2. No two n-tuples in the same row of a standard array are identical. Every n-tuple appears in one and only one row.

More on standard array

$\rightarrow$ The 2^{n-k} rows are called the *cosets* of the code C

Linear block code

Observation

1. The sum of any two vectors in the same row is a codeword in C
2. No two n-tuples in the same row of a standard array are identical. Every n-tuple appears in one and only one row.

More on standard array

- $\rightarrow$ The 2^{n-k} rows are called the *cosets* of the code C
- $\rightarrow$ The first n-tuple $\mathbf{e}_j$ of each coset is called a *coset leader*

Linear block code

Observation

1. The sum of any two vectors in the same row is a codeword in C
2. No two n-tuples in the same row of a standard array are identical. Every n-tuple appears in one and only one row.

More on standard array

- $\rightarrow$ The 2^{n-k} rows are called the *cosets* of the code C
- $\rightarrow$ The first n-tuple $\mathbf{e}_j$ of each coset is called a *coset leader*
- $\rightarrow$ There are 2^k columns and each column consists of 2^{n-k} vectors

Linear block code

Observation

1. The sum of any two vectors in the same row is a codeword in C
2. No two n-tuples in the same row of a standard array are identical. Every n-tuple appears in one and only one row.

More on standard array

- $\rightarrow$ The 2^{n-k} rows are called the *cosets* of the code C
- $\rightarrow$ The first n-tuple $\mathbf{e}_j$ of each coset is called a *coset leader*
- $\rightarrow$ There are 2^k columns and each column consists of 2^{n-k} vectors
- $\rightarrow$ Let D_j denote the jth column and define

$$D_j = \{\mathbf{v}_j, \mathbf{e}_2 + \mathbf{v}_j, \ldots, \mathbf{e}_{2^{n-k}} + \mathbf{v}_j\}, 1 \leq j \leq 2^k$$

Linear block code

Observation

1. The sum of any two vectors in the same row is a codeword in C
2. No two n-tuples in the same row of a standard array are identical. Every n-tuple appears in one and only one row.

More on standard array

- $\rightarrow$ The 2^{n-k} rows are called the *cosets* of the code C
- $\rightarrow$ The first n-tuple $\mathbf{e}_j$ of each coset is called a *coset leader*
- $\rightarrow$ There are 2^k columns and each column consists of 2^{n-k} vectors
- $\rightarrow$ Let D_j denote the jth column and define

$$D_j = \{\mathbf{v}_j, \mathbf{e}_2 + \mathbf{v}_j, \ldots, \mathbf{e}_{2^{n-k}} + \mathbf{v}_j\}, 1 \leq j \leq 2^k$$

- $\rightarrow$ If $r \in D_j$ then declare the codeword as $\mathbf{v}_j$ and it will be decoded correctly if and only if the error vector is a corresponding coset leader

Linear block code

Conclusion Every (n, k) block code is capable of correcting 2^{n-k} error patterns.

Linear block code

Conclusion Every (n, k) block code is capable of correcting 2^{n-k} error patterns.

We have already seen that the code is capable of detecting $2^n - 2^k$ error patterns. Thus for large n, 2^{n-k} is a small fraction of $2^n - 2^k$.

Linear block code

Conclusion Every (n, k) block code is capable of correcting 2^{n-k} error patterns.

We have already seen that the code is capable of detecting $2^n - 2^k$ error patterns. Thus for large n, 2^{n-k} is a small fraction of $2^n - 2^k$.

Theorem All the 2^k n-tuples of a coset have the same syndrome. The syndromes for different cosets are different

Linear block code

Conclusion Every (n, k) block code is capable of correcting 2^{n-k} error patterns.

We have already seen that the code is capable of detecting $2^n - 2^k$ error patterns. Thus for large n, 2^{n-k} is a small fraction of $2^n - 2^k$.

Theorem All the 2^k n-tuples of a coset have the same syndrome. The syndromes for different cosets are different

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 let $\mathbf{x}$ and $\mathbf{y}$ be two n-tuples of weight t or less. Then

$$w(\mathbf{x} + \mathbf{y}) \leq w(\mathbf{x}) + w(\mathbf{y}) \leq 2t < d_{\min}$$

If $\mathbf{x}$ and $\mathbf{y}$ are in the same coset then $\mathbf{x} + \mathbf{y}$ must be a codeword, which is impossile since $w(\mathbf{x} + \mathbf{y}) < d_{\min}$

Linear block code

Decoding algorithm

1. Compute the syndrome $\mathbf{r}H^T$

Linear block code

Decoding algorithm

1. Compute the syndrome $\mathbf{r}H^T$
2. Locate the coset leader $\mathbf{e}_i$ whose syndrome is $\mathbf{r}H^T$. Then $\mathbf{e}_i$ is assumed to be the error pattern caused by the channel

Linear block code

Decoding algorithm

1. Compute the syndrome $\mathbf{r}H^T$
2. Locate the coset leader $\mathbf{e}_i$ whose syndrome is $\mathbf{r}H^T$. Then $\mathbf{e}_i$ is assumed to be the error pattern caused by the channel
3. Decode the received vector $\mathbf{r}$ into the codeword $\mathbf{v}^* = \mathbf{r} + \mathbf{e}_i$