# Information and Coding Theory

## MA41024/ MA60020/ MA60262

Bibhas Adhikari

Spring 2022-23, IIT Kharagpur

Lecture 12
February 28, 2023

# Linear block code

Syndrome decoding Consider an $(n, k)$ linear code corresponding to generator matrix $\mathbf{G}$ and parity-check matrix $\mathbf{H}$. Let $\mathbf{r} = (r_0, r_1, \ldots, r_{n-1})$ be the received vector at the output of a noisy channel corresponding to a codeword $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$.

# Linear block code

Syndrome decoding Consider an $(n, k)$ linear code corresponding to generator matrix $\mathbf{G}$ and parity-check matrix $\mathbf{H}$. Let $\mathbf{r} = (r_0, r_1, \ldots, r_{n-1})$ be the received vector at the output of a noisy channel corresponding to a codeword $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$.

Then

$$\mathbf{r} = \mathbf{v} + \mathbf{e} \Rightarrow \mathbf{e} = \mathbf{r} + \mathbf{v} = (e_0, e_1, \ldots, e_{n-1})$$

is the *error vector*, where $e_i = 1$ for $r_i \neq v_i$, and $e_i = 0$ for $r_i = v_i$.

# Linear block code

Syndrome decoding Consider an $(n, k)$ linear code corresponding to generator matrix $\mathbf{G}$ and parity-check matrix $\mathbf{H}$. Let $\mathbf{r} = (r_0, r_1, \ldots, r_{n-1})$ be the received vector at the output of a noisy channel corresponding to a codeword $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$.

Then

$$\mathbf{r} = \mathbf{v} + \mathbf{e} \Rightarrow \mathbf{e} = \mathbf{r} + \mathbf{v} = (e_0, e_1, \ldots, e_{n-1})$$

is the *error vector*, where $e_i = 1$ for $r_i \neq v_i$, and $e_i = 0$ for $r_i = v_i$.
Thus the 1's in $\mathbf{e}$ are the transmission errors caused by the channel noise.

# Linear block code

Syndrome decoding Consider an $(n, k)$ linear code corresponding to generator matrix $\mathbf{G}$ and parity-check matrix $\mathbf{H}$. Let $\mathbf{r} = (r_0, r_1, \ldots, r_{n-1})$ be the received vector at the output of a noisy channel corresponding to a codeword $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$.

Then

$$\mathbf{r} = \mathbf{v} + \mathbf{e} \Rightarrow \mathbf{e} = \mathbf{r} + \mathbf{v} = (e_0, e_1, \ldots, e_{n-1})$$

is the *error vector*, where $e_i = 1$ for $r_i \neq v_i$, and $e_i = 0$ for $r_i = v_i$. Thus the 1's in $\mathbf{e}$ are the transmission errors caused by the channel noise.

Note The receiver does not know both $\mathbf{v}$ and $\mathbf{e}$

# Linear block code

Syndrome decoding Consider an $(n, k)$ linear code corresponding to generator matrix $\mathbf{G}$ and parity-check matrix $\mathbf{H}$. Let $\mathbf{r} = (r_0, r_1, \ldots, r_{n-1})$ be the received vector at the output of a noisy channel corresponding to a codeword $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$.

Then

$$\mathbf{r} = \mathbf{v} + \mathbf{e} \Rightarrow \mathbf{e} = \mathbf{r} + \mathbf{v} = (e_0, e_1, \ldots, e_{n-1})$$

is the *error vector*, where $e_i = 1$ for $r_i \neq v_i$, and $e_i = 0$ for $r_i = v_i$. Thus the 1's in $\mathbf{e}$ are the transmission errors caused by the channel noise.

Note The receiver does not know both $\mathbf{v}$ and $\mathbf{e}$

Question How does the receiver detect, locate and correct the error?

# Linear block code

On receiving **r**, the decoder must first determine whether **r** contains transmission errors. Thus the decoder computes

$$\mathbf{s} = \mathbf{r} \cdot \mathbf{H}^T = (s_0, s_1, \ldots, s_{n-k-1})$$

which is called the *syndrome* of **r**.

# Linear block code

On receiving $\mathbf{r}$, the decoder must first determine whether $\mathbf{r}$ contains transmission errors. Thus the decoder computes

$$\mathbf{s} = \mathbf{r} \cdot \mathbf{H}^T = (s_0, s_1, \ldots, s_{n-k-1})$$

which is called the *syndrome* of $\mathbf{r}$.

Then $\mathbf{s} = \mathbf{0}$ if and only if $\mathbf{r}$ is a codeword, and $\mathbf{s} \neq \mathbf{0}$ if and only if $\mathbf{r}$ is not a codeword. Thus when $\mathbf{s} = 0$, $\mathbf{r}$ is a codeword, and the receiver accepts $\mathbf{r}$ as the transmitted codeword.

# Linear block code

On receiving $\mathbf{r}$, the decoder must first determine whether $\mathbf{r}$ contains transmission errors. Thus the decoder computes

$$\mathbf{s} = \mathbf{r} \cdot \mathbf{H}^T = (s_0, s_1, \ldots, s_{n-k-1})$$

which is called the *syndrome* of $\mathbf{r}$.

Then $\mathbf{s} = \mathbf{0}$ if and only if $\mathbf{r}$ is a codeword, and $\mathbf{s} \neq \mathbf{0}$ if and only if $\mathbf{r}$ is not a codeword. Thus when $\mathbf{s} = 0$, $\mathbf{r}$ is a codeword, and the receiver accepts $\mathbf{r}$ as the transmitted codeword.

Caution It is possible that the errors in certain error vectors are not detectable. For instance, if $\mathbf{e}$ is identical to a nonzero codeword. This kind of error patterns are called *undetectable* error patterns. There are $2^k - 1$ undetectable errors

# Linear block code

However, note that

$$\mathbf{s} = \mathbf{r} \cdot \mathbf{H}^T = (\mathbf{v} + \mathbf{e}) \cdot \mathbf{H}^T = \mathbf{v} \cdot \mathbf{H}^T + \mathbf{e} \cdot \mathbf{H}^T = \mathbf{e} \cdot \mathbf{H}^T$$

# Linear block code

However, note that

$$\mathbf{s} = \mathbf{r} \cdot \mathbf{H}^T = (\mathbf{v} + \mathbf{e}) \cdot \mathbf{H}^T = \mathbf{v} \cdot \mathbf{H}^T + \mathbf{e} \cdot \mathbf{H}^T = \mathbf{e} \cdot \mathbf{H}^T$$

Thus the syndrome bits give information about error bits.

# Linear block code

However, note that

$$\mathbf{s} = \mathbf{r} \cdot \mathbf{H}^T = (\mathbf{v} + \mathbf{e}) \cdot \mathbf{H}^T = \mathbf{v} \cdot \mathbf{H}^T + \mathbf{e} \cdot \mathbf{H}^T = \mathbf{e} \cdot \mathbf{H}^T$$

Thus the syndrome bits give information about error bits.

Question Can we solve the linear system and obtain $\mathbf{e}$?

# Linear block code

However, note that

$$\mathbf{s} = \mathbf{r} \cdot \mathbf{H}^T = (\mathbf{v} + \mathbf{e}) \cdot \mathbf{H}^T = \mathbf{v} \cdot \mathbf{H}^T + \mathbf{e} \cdot \mathbf{H}^T = \mathbf{e} \cdot \mathbf{H}^T$$

Thus the syndrome bits give information about error bits.

Question Can we solve the linear system and obtain $\mathbf{e}$?

Note that there are $n - k$ linear equations and the system does not have a unique solution but can have $2^k$ solutions!!

# Linear block code

Minimum distance of a block code Let $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ be an $n$-tuple. Then the *Hamming weight* of $\mathbf{v}$, denotes as $w(\mathbf{v})$ is the number of nonzero entries of $\mathbf{v}$.

# Linear block code

Minimum distance of a block code Let $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ be an $n$-tuple. Then the *Hamming weight* of $\mathbf{v}$, denotes as $w(\mathbf{v})$ is the number of nonzero entries of $\mathbf{v}$.

The *Hamming distance* between two vectors $\mathbf{v}$ and $\mathbf{w}$, denotes as $d_h(\mathbf{v}, \mathbf{w})$ is the number of places where $\mathbf{v}$ and $\mathbf{w}$ differ.

# Linear block code

Minimum distance of a block code Let $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ be an $n$-tuple. Then the *Hamming weight* of $\mathbf{v}$, denotes as $w(\mathbf{v})$ is the number of nonzero entries of $\mathbf{v}$.

The *Hamming distance* between two vectors $\mathbf{v}$ and $\mathbf{w}$, denotes as $d_h(\mathbf{v}, \mathbf{w})$ is the number of places where $\mathbf{v}$ and $\mathbf{w}$ differ.

Question Show that Hamming distance is a metric.

# Linear block code

Minimum distance of a block code Let $\mathbf{v} = (v_0, v_1, \ldots, v_{n-1})$ be an $n$-tuple. Then the *Hamming weight* of $\mathbf{v}$, denotes as $w(\mathbf{v})$ is the number of nonzero entries of $\mathbf{v}$.

The *Hamming distance* between two vectors $\mathbf{v}$ and $\mathbf{w}$, denotes as $d_h(\mathbf{v}, \mathbf{w})$ is the number of places where $\mathbf{v}$ and $\mathbf{w}$ differ.

Question Show that Hamming distance is a metric.

The minimum distance of a code $C$ is defined by

$$d_{\min} = \min\{d_h(\mathbf{v}, \mathbf{w}) : \mathbf{v}, \mathbf{w} \in C, \mathbf{v} \neq \mathbf{w}\}$$

# Linear block code

Note that

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

Thus minimum distance of a linear code is the minimum weight of the code.

# Linear block code

Theorem Let $C$ be an $(n, k)$ linear code with parity-check matrix $\mathbf{H}$. Then for each codeword of Hamming weight $l$, there exists $l$ columns of $\mathbf{H}$ such that the sum of these $l$ columns is equal to the zero vector. Conversely, if there exist $l$ columns of $\mathbf{H}$ whose sum is the zero vector then there exists a codeword of Hamming weight $l$ in $C$.

# Linear block code

Theorem Let $C$ be an $(n, k)$ linear code with parity-check matrix $\mathbf{H}$. Then for each codeword of Hamming weight $l$, there exists $l$ columns of $\mathbf{H}$ such that the sum of these $l$ columns is equal to the zero vector. Conversely, if there exist $l$ columns of $\mathbf{H}$ whose sum is the zero vector then there exists a codeword of Hamming weight $l$ in $C$.

Corollary Let $C$ be a linear block code with parity-check matrix $\mathbf{H}$. Then

(a) If no $d - 1$ or fewer columns of $\mathbf{H}$ add to $\mathbf{0}$, the code has minimum weight at least $d$

# Linear block code

Theorem Let $C$ be an $(n, k)$ linear code with parity-check matrix $\mathbf{H}$. Then for each codeword of Hamming weight $l$, there exists $l$ columns of $\mathbf{H}$ such that the sum of these $l$ columns is equal to the zero vector. Conversely, if there exist $l$ columns of $\mathbf{H}$ whose sum is the zero vector then there exists a codeword of Hamming weight $l$ in $C$.

Corollary Let $C$ be a linear block code with parity-check matrix $\mathbf{H}$. Then

(a) If no $d - 1$ or fewer columns of $\mathbf{H}$ add to $\mathbf{0}$, the code has minimum weight at least $d$

(b) The minimum distance of $C$ is equal to the smallest number of columns of $\mathbf{H}$ that sum to $\mathbf{0}$.

# Linear block code

Error detection and error correction Suppose a codeword $\mathbf{v}$ is transmitted over a noisy channel. Then a block code with minimum distance $d_{\min}$ is capable of detecting all the error patterns of $d_{\min} - 1$ or fewer errors:

$\rightarrow$ If there are $l$ errors in the corresponding received vector $\mathbf{r}$, then $d(\mathbf{v}, \mathbf{r}) = l$

# Linear block code

Error detection and error correction Suppose a codeword $\mathbf{v}$ is transmitted over a noisy channel. Then a block code with minimum distance $d_{\min}$ is capable of detecting all the error patterns of $d_{\min} - 1$ or fewer errors:

- $\rightarrow$ If there are $l$ errors in the corresponding received vector $\mathbf{r}$, then $d(\mathbf{v}, \mathbf{r}) = l$
- $\rightarrow$ If the minimum distance of a block code $C$ is $d_{\min}$, then any two distinct codewords in $C$ differ at least in $d_{\min}$ places

# Linear block code

Error detection and error correction Suppose a codeword $\mathbf{v}$ is transmitted over a noisy channel. Then a block code with minimum distance $d_{\min}$ is capable of detecting all the error patterns of $d_{\min} - 1$ or fewer errors:

$\rightarrow$ If there are $l$ errors in the corresponding received vector $\mathbf{r}$, then $d(\mathbf{v}, \mathbf{r}) = l$

$\rightarrow$ If the minimum distance of a block code $C$ is $d_{\min}$, then any two distinct codewords in $C$ differ at least in $d_{\min}$ places

$\rightarrow$ Then for this code, no error pattern of $d_{\min} - 1$ or fewer errors can change one codeword into another, hence any error pattern of $d_{\min} - 1$ or few errors will result in a received vector $\mathbf{r}$ that is not a codeword in $C$

# Linear block code

Error detection and error correction Suppose a codeword $\mathbf{v}$ is transmitted over a noisy channel. Then a block code with minimum distance $d_{\min}$ is capable of detecting all the error patterns of $d_{\min} - 1$ or fewer errors:

- $\rightarrow$ If there are $l$ errors in the corresponding received vector $\mathbf{r}$, then $d(\mathbf{v}, \mathbf{r}) = l$
- $\rightarrow$ If the minimum distance of a block code $C$ is $d_{\min}$, then any two distinct codewords in $C$ differ at least in $d_{\min}$ places
- $\rightarrow$ Then for this code, no error pattern of $d_{\min} - 1$ or fewer errors can change one codeword into another, hence any error pattern of $d_{\min} - 1$ or few errors will result in a received vector $\mathbf{r}$ that is not a codeword in $C$

Question Can it detect all the error patterns of $d_{\min}$ errors?

# Linear block code

Observation $(n, k)$ linear block code can detect $2^n - 2^k$ error patterns of length $n$

$\rightarrow$ The number of nonzero error patterns is equal to $2^n - 1$, among which $2^k - 1$ error patterns are the $2^k - 1$ nonzero codewords.

# Linear block code

Observation $(n,k)$ linear block code can detect $2^n - 2^k$ error patterns of length $n$

- $\rightarrow$ The number of nonzero error patterns is equal to $2^n - 1$, among which $2^k - 1$ error patterns are the $2^k - 1$ nonzero codewords.
- $\rightarrow$ If any of these $2^k - 1$ error patterns occurs, it alters $\mathbf{v}$ into another codeword $\mathbf{w}$, and its syndrome is zero. Thus the decoder performs an incorrect decoding. Therefore there are $2^k - 1$ undetectable error patterns

# Linear block code

Observation $(n, k)$ linear block code can detect $2^n - 2^k$ error patterns of length $n$

- $\rightarrow$ The number of nonzero error patterns is equal to $2^n - 1$, among which $2^k - 1$ error patterns are the $2^k - 1$ nonzero codewords.
- $\rightarrow$ If any of these $2^k - 1$ error patterns occurs, it alters $\mathbf{v}$ into another codeword $\mathbf{w}$, and its syndrome is zero. Thus the decoder performs an incorrect decoding. Therefore there are $2^k - 1$ undetectable error patterns
- $\rightarrow$ Note that there are exactly $2^n - 2^k$ error patterns that are not identical to the codewords of the $(n, k)$ block code, which are detectable

# Linear block code

Observation $(n, k)$ linear block code can detect $2^n - 2^k$ error patterns of length $n$

- $\rightarrow$ The number of nonzero error patterns is equal to $2^n - 1$, among which $2^k - 1$ error patterns are the $2^k - 1$ nonzero codewords.
- $\rightarrow$ If any of these $2^k - 1$ error patterns occurs, it alters $\mathbf{v}$ into another codeword $\mathbf{w}$, and its syndrome is zero. Thus the decoder performs an incorrect decoding. Therefore there are $2^k - 1$ undetectable error patterns
- $\rightarrow$ Note that there are exactly $2^n - 2^k$ error patterns that are not identical to the codewords of the $(n, k)$ block code, which are detectable
- $\rightarrow$ For large $n$, $2^k - 1 \ll 2^n$ in general, hence only a small fraction of error patterns pass through the decoder without being detected

# Linear block code

## Maximum-Likelihood (ML) decoding

$\rightarrow$ A decoder must determine $\mathbf{w}$ to minimize

$$P(E|\,\mathbf{r}) = P(\mathbf{w} \neq \mathbf{v}|\,\mathbf{r})$$

$\rightarrow$ The probability of error is

$$P(E) = \sum_{\mathbf{r}} P(E|\,\mathbf{r})P(\mathbf{r})$$

# Linear block code

## Maximum-Likelihood (ML) decoding

→ A decoder must determine $\mathbf{w}$ to minimize

$$P(E|\,\mathbf{r}) = P(\mathbf{w} \neq \mathbf{v}|\,\mathbf{r})$$

→ The probability of error is

$$P(E) = \sum_{\mathbf{r}} P(E|\,\mathbf{r})P(\mathbf{r})$$

→ Memoryless channel: ML decoder

△ Maximize $P(\mathbf{r}|\,\mathbf{v}) = \prod_j P(r_j|\,v_j)$

# Linear block code

## Maximum-Likelihood (ML) decoding

→ A decoder must determine $\mathbf{w}$ to minimize

$$P(E|\,\mathbf{r}) = P(\mathbf{w} \neq \mathbf{v}|\,\mathbf{r})$$

→ The probability of error is

$$P(E) = \sum_{\mathbf{r}} P(E|\,\mathbf{r})P(\mathbf{r})$$

→ Memoryless channel: ML decoder

- △ Maximize $P(\mathbf{r}|\,\mathbf{v}) = \prod_j P(r_j|\,v_j)$
- △ Alternatively, choose $\mathbf{v}$ to maximize $\log P(\mathbf{r}|\,\mathbf{v}) = \sum_j \log P(r_j|\,v_j)$

# Linear block code

## Maximum-Likelihood (ML) decoding

→ A decoder must determine $\mathbf{w}$ to minimize

$$P(E|\,\mathbf{r}) = P(\mathbf{w} \neq \mathbf{v}|\,\mathbf{r})$$

→ The probability of error is

$$P(E) = \sum_{\mathbf{r}} P(E|\,\mathbf{r})P(\mathbf{r})$$

→ Memoryless channel: ML decoder

- △ Maximize $P(\mathbf{r}|\,\mathbf{v}) = \prod_j P(r_j|\,v_j)$
- △ Alternatively, choose $\mathbf{v}$ to maximize $\log P(\mathbf{r}|\,\mathbf{v}) = \sum_j \log P(r_j|\,v_j)$
- △ The ML decoder is optimal if and only if all $\mathbf{v}$ are equally likely as input vectors, otherwise $P(\mathbf{r}|\,\mathbf{v})$ must be weighted by the codeword probabilities $P(\mathbf{v})$

# Linear block code

ML decoding on the BSC Suppose the noisy channel is BSC with bit-flip probability $\epsilon$. Then

$\rightarrow$ $P(r_j | v_j) = 1 - \epsilon$ if $r_j = v_j$ and $\epsilon$ otherwise

# Linear block code

ML decoding on the BSC Suppose the noisy channel is BSC with bit-flip probability $\epsilon$. Then

$\rightarrow$ $P(r_j|\, v_j) = 1 - \epsilon$ if $r_j = v_j$ and $\epsilon$ otherwise

$\rightarrow$

$$\begin{aligned}
\log P(\mathbf{r}|\,\mathbf{v}) &= \sum_j \log P(r_j|\, v_j) \\
&= d(\mathbf{r},\mathbf{v}) \log \epsilon + (n - d(\mathbf{r},\mathbf{v})) \log(1-\epsilon) \\
&= d(\mathbf{r},\mathbf{v}) \log \frac{\epsilon}{1-\epsilon} + n \log(1-\epsilon)
\end{aligned}$$

# Linear block code

ML decoding on the BSC Suppose the noisy channel is BSC with bit-flip probability $\epsilon$. Then

- $\rightarrow$ $P(r_j | v_j) = 1 - \epsilon$ if $r_j = v_j$ and $\epsilon$ otherwise
- $\rightarrow$

$$\begin{aligned}\log P(\mathbf{r}|\mathbf{v}) &= \sum_j \log P(r_j|v_j) \\ &= d(\mathbf{r},\mathbf{v})\log\epsilon + (n - d(\mathbf{r},\mathbf{v}))\log(1-\epsilon) \\ &= d(\mathbf{r},\mathbf{v})\log\frac{\epsilon}{1-\epsilon} + n\log(1-\epsilon)\end{aligned}$$

- $\rightarrow$ $\log\frac{\epsilon}{1-\epsilon} < 0$ for $\epsilon < 0.5$, so an ML decoder for a BSC must choose $\mathbf{v}$ to minimize $d(\mathbf{r},\mathbf{v})$

# Linear block code

Then for a linear block code, an ML decoder takes $n$ received bits as input and returns the most likely $k$-bit message among the $2^k$ possible messages.

# Linear block code

Then for a linear block code, an ML decoder takes $n$ received bits as input and returns the most likely $k$-bit message among the $2^k$ possible messages. Implementing ML decoder

$\rightarrow$ Enumerate all $2^k$ valid codewords, each $n$ bit in length

# Linear block code

Then for a linear block code, an ML decoder takes $n$ received bits as input and returns the most likely $k$-bit message among the $2^k$ possible messages. Implementing ML decoder

$\rightarrow$ Enumerate all $2^k$ valid codewords, each $n$ bit in length

$\rightarrow$ Compare the received word $\mathbf{r}$ to each of these valid codewords and find the one with smallest Hamming distance to $\mathbf{r}$

# Linear block code

Then for a linear block code, an ML decoder takes $n$ received bits as input and returns the most likely $k$-bit message among the $2^k$ possible messages. Implementing ML decoder

- → Enumerate all $2^k$ valid codewords, each $n$ bit in length
- → Compare the received word $\mathbf{r}$ to each of these valid codewords and find the one with smallest Hamming distance to $\mathbf{r}$
- → However, it has exponential time complexity. What we would like is something a lot faster. Note that this comparing to all valid codewords method does not take advantage of the linearity of the code.

# Linear block code

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

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

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 $t$.

Claim $C$ is capable of correcting all the error patterns of $t$ or fewer errors.

$\rightarrow$ Let $\mathbf{v}$ and $\mathbf{r}$ denote the transmitted codeword and the received vector respectively.

# Linear block code

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

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

for some positive integer $t$.

Claim $C$ is capable of correcting all the error patterns of $t$ or fewer errors.

- → Let $\mathbf{v}$ and $\mathbf{r}$ denote the transmitted codeword and the received vector respectively.
- → Let $\mathbf{w}$ be any other codeword of $C$. Then

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

# 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 $t$.
Claim $C$ is capable of correcting all the error patterns of $t$ or fewer errors.

$\rightarrow$ Let $\mathbf{v}$ and $\mathbf{r}$ denote the transmitted codeword and the received vector respectively.

$\rightarrow$ Let $\mathbf{w}$ be any other codeword of $C$. Then

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

$\rightarrow$ Suppose an error pattern of $t'$ errors occurs i.e. $d(\mathbf{v}, \mathbf{r}) = t'$

# 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 $t$.

Claim $C$ is capable of correcting all the error patterns of $t$ or fewer errors.

→ Let $\mathbf{v}$ and $\mathbf{r}$ denote the transmitted codeword and the received vector respectively.

→ Let $\mathbf{w}$ be any other codeword of $C$. Then

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

→ Suppose an error pattern of $t'$ errors occurs i.e. $d(\mathbf{v}, \mathbf{r}) = t'$

→ Obviously, $d(\mathbf{v}, \mathbf{w}) \geq d_{\min} \geq 2t + 1$, and hence $d(\mathbf{w}, \mathbf{r}) \geq 2t + 1 - t'$

# Linear block code

- $\rightarrow$ If $t' < t$ then $d(\mathbf{w}, \mathbf{r}) > t$
- $\rightarrow$ Thus if an error pattern of $t$ or fewer errors occurs, the received vector $\mathbf{r}$ is closer in Hamming distance to the transmitted codeword $\mathbf{v}$ than any other codeword $\mathbf{w}$ in $C$

# Linear block code

→ If $t' < t$ then $d(\mathbf{w}, \mathbf{r}) > t$

→ Thus if an error pattern of $t$ or fewer errors occurs, the received vector $\mathbf{r}$ is closer in Hamming distance to the transmitted codeword $\mathbf{v}$ than any other codeword $\mathbf{w}$ in $C$

→ According to ML decoding scheme, it is a correct transmitted codeword, thus the errors are corrected.