An introduction to coding theory

Adrish Banerjee

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

Jan. 30, 2017

Lecture #5C: Problem solving session-II
Problem # 1: Let $C$ be a linear code with both even and odd weight codewords. Show that the number of even weight codewords is equal to the number of odd-weight codewords.

Solutions: Let $C_e$ be the set of code words in $C$ with even weight and let $C_o$ be the set of code words in $C$ with odd weight.
Problem # 1: Let C be a linear code with both even and odd weight codewords. Show that the number of even weight codewords is equal to the number of odd-weight codewords.

Solutions: Let \( C_e \) be the set of code words in C with even weight and let \( C_o \) be the set of code words in C with odd weight.

Let \( x \) be any odd-weight code vector from \( C_o \). Adding \( x \) to each vector in \( C_o \), we obtain a set of \( C_e' \) of even weight vector.

The number of vectors in \( C_e' \) is equal to the number of vectors in \( C_o \), i.e. \( |C_e'| = |C_o| \). Also \( |C_e'| \leq |C_e| \). Thus \( |C_o| \leq |C_e| \).
Problem # 1: Let $C$ be a linear code with both even and odd weight codewords. Show that the number of even weight codewords is equal to the number of odd-weight codewords.

Solutions: Let $C_e$ be the set of code words in $C$ with even weight and let $C_o$ be the set of code words in $C$ with odd weight.

Let $x$ be any odd-weight code vector from $C_o$. Adding $x$ to each vector in $C_o$, we obtain a set of $C_o'$ of even weight vector.

The number of vectors in $C_o'$ is equal to the number of vectors in $C_o$, i.e. $|C_o'| = |C_o|$. Also $|C_o'| \leq |C_e|$. Thus $|C_o| \leq |C_e|$. 

Now adding $x$ to each vector in $C_e$, we obtain a set $C_o'$ of odd weight code words.

The number of vectors in $C_o'$ is equal to the number of vectors in $C_e$ and $|C_o'| \leq |C_o|$. Hence $|C_e| \leq |C_o|$.
**Linear block code**

- **Problem # 1:** Let $C$ be a linear code with both even and odd weight codewords. Show that the number of even weight codewords is equal to the number of odd-weight codewords.

  **Solutions:** Let $C_e$ be the set of code words in $C$ with even weight and let $C_o$ be the set of code words in $C$ with odd weight.

  - Let $x$ be any odd-weight code vector from $C_o$. Adding $x$ to each vector in $C_o$, we obtain a set of $C'_e$ of even weight vector.
  - The number of vectors in $C'_e$ is equal to the number of vectors in $C_o$, i.e. $|C'_e| = |C_o|$. Also $|C'_e| \leq |C_e|$. Thus $|C_o| \leq |C_e|$.
  - Now adding $x$ to each vector in $C_e$, we obtain a set $C'_o$ of odd weight code words.
  - The number of vectors in $C'_o$ is equal to the number of vectors in $C_e$ and $|C'_o| \leq |C_o|$. Hence $|C_e| \leq |C_o|$.
  - Both these conditions are true only when $|C_e| = |C_o|$.

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

An introduction to coding theory

---

**Linear block code**

- **Problem # 2:** Consider an $(n, k)$ linear code $C$ whose generator matrix $G$ contains no zero column. Arrange all the codewords of $C$ as rows of a $2^k$ by $n$ array.
Problem # 2: Consider an \((n, k)\) linear code \(C\) whose generator matrix \(G\) contains no zero column. Arrange all the codewords of \(C\) as rows of a \(2^k\) by \(n\) array.

a) Show that no column of the array contains only zeros.

Solution: From the given condition on \(G\), we see that, for any digit position, there is a row in \(G\) with a nonzero component at that position.
Problem # 2: Consider an \((n, k)\) linear code \(C\) whose generator matrix \(G\) contains no zero column. Arrange all the codewords of \(C\) as rows of a \(2^k \times n\) array

a) Show that no column of the array contains only zeros.

Solution: From the given condition on \(G\), we see that, for any digit position, there is a row in \(G\) with a nonzero component at that position.

This row is a code word in \(C\). Hence in the code array, each column contains at least one nonzero entry.

Therefore no column in the code array contains only zeros.
Problem 2 (contd.): Consider an \((n, k)\) linear code \(C\) whose generator matrix \(G\) contains no zero column. Arrange all the codewords of \(C\) as rows of a \(2^k\) by \(n\) array.

b) Show that each column of the array consists of \(2^{k-1}\) zeros and \(2^{k-1}\) ones.
Problem 2 (contd.): Consider an \((n, k)\) linear code \(C\) whose generator matrix \(G\) contains no zero column. Arrange all the codewords of \(C\) as rows of a \(2^k\) by \(n\) array.

b) Show that each column of the array consists of \(2^{k-1}\) zeros and \(2^{k-1}\) ones.

Solution: To prove that each column of this array has \(2^{k-1}\) zeros and \(2^{k-1}\) ones, we will show that the number of codewords that “1” at the \(l\)-th position is same as number of codewords that have “0” at the \(l\)-th position.

In the code array, each column contains at least one nonzero entry. Consider the \(l\)-th column of the code array.
Problem 2 (contd.): Consider an \((n, k)\) linear code \(C\) whose generator matrix \(G\) contains no zero column. Arrange all the codewords of \(C\) as rows of a \(2^k\) by \(n\) array.

b) Show that each column of the array consists of \(2^{k-1}\) zeros and \(2^{k-1}\) ones.

Solution: To prove that each column of this array has \(2^{k-1}\) zeros and \(2^{k-1}\) ones, we will show that the number of codewords that “1” at the \(l\)-th position is same as number of codewords that have “0” at the \(l\)-th position.

In the code array, each column contains at least one nonzero entry. Consider the \(l\)-th column of the code array.

Let \(S_0\) be the codewords with a “0” at the \(l\)-th position and \(S_1\) be the codewords with a “1” at the \(l\)-th position.

Let \(x\) be a codeword from \(S_1\). Adding \(x\) to each vector in \(S_0\), we obtain a set \(S'_1\) of codewords with a “1” at the \(l\)-th position.

\[|S'_1| = |S_0| \quad \text{and} \quad S'_1 \subseteq S_1\]
**Problem 2 (contd.):** The above condition implies that

$$|S_0| \leq |S_1|$$

(1)

Adding $\mathbf{x}$ to each vector in $S_1$, we obtain a set $S'_0$ of codewords with a “0” at the $l$–th position.

$$|S'_0| = |S_1| \quad \text{and} \quad S'_0 \subseteq S_0$$
Problem 2 (contd.): The above condition implies that

\[ |S_0| \leq |S_1| \]  \hspace{1cm} (1)

Adding \( \mathbf{x} \) to each vector in \( S_1 \), we obtain a set \( S'_0 \) of codewords with a “0” at the \( l \)-th position.

\[ |S'_0| = |S_1| \quad \text{and} \quad S'_0 \subseteq S_0 \]

The above condition implies that

\[ |S_1| \leq |S_0| \]  \hspace{1cm} (2)

From (1) and (2), we get \( |S_0| = |S_1| \). Therefore \( l \)-th column contains \( 2^{k-1} \) zeros and \( 2^{k-1} \) ones.
c) **Problem 2 (contd.):** Show that the minimum distance $d_{\text{min}}$ of $C$ satisfies the following inequality

$$d_{\text{min}} \leq \frac{n \cdot 2^{k-1}}{2^k - 1}$$

**Solution:** The total number of ones in the array is $n \cdot 2^{k-1}$. Each nonzero codeword has weight at least $d_{\text{min}}$. Hence,

$$(2^k - 1) \cdot d_{\text{min}} \leq n \cdot 2^{k-1}$$
c) **Problem 2 (contd.):** Show that the minimum distance $d_{\text{min}}$ of $C$ satisfies the following inequality

$$d_{\text{min}} \leq \frac{n \cdot 2^{k-1}}{2^k - 1}$$

**Solution:** The total number of ones in the array is $n \cdot 2^{k-1}$. Each nonzero codeword has weight at least $d_{\text{min}}$. Hence,

$$(2^k - 1) \cdot d_{\text{min}} \leq n \cdot 2^{k-1}$$

This implies that

$$d_{\text{min}} \leq \frac{n \cdot 2^{k-1}}{2^k - 1}$$

---

**Minimum distance of a code**

**Problem # 3** What should be the minimum distance of a linear block code $C$ so that it can simultaneously correct $\nu$ errors and $e$ erasures. Prove your result.
Minimum distance of a code

Problem # 3 What should be the minimum distance of a linear block code $C$ so that it can simultaneously correct $\nu$ errors and $e$ erasures. Prove your result.

Solution: The minimum distance $d_{\text{min}}$ should be

$$d_{\text{min}} \geq 2\nu + e + 1$$

Delete from all the codewords the $e$ components where the receiver has declared erasures.
Problem # 3 What should be the minimum distance of a linear block code $C$ so that it can simultaneously correct $\nu$ errors and $e$ erasures. Prove your result.

Solution: The minimum distance $d_{\text{min}}$ should be

$$d_{\text{min}} \geq 2\nu + e + 1$$

Delete from all the codewords the $e$ components where the receiver has declared erasures.

This deletion results in a shortened code of length $n - e$. 

The minimum distance of this shortened code should be at least

$$d_{\text{min}} - e \geq 2\nu + 1.$$
Problem # 3 What should be the minimum distance of a linear block code $C$ so that it can simultaneously correct $\nu$ errors and $e$ erasures. Prove your result.

Solution: The minimum distance $d_{\text{min}}$ should be

$$d_{\text{min}} \geq 2\nu + e + 1$$

Delete from all the codewords the $e$ components where the receiver has declared erasures.

This deletion results in a shortened code of length $n - e$.

The minimum distance of this shortened code should be atleast

$$d_{\text{min}} - e \geq 2\nu + 1.$$ 

Hence, the $\nu$ errors in the unerased positions can be corrected. As a result the shortened code with $e$ components erased can be recovered.
**Problem # 4** Prove that a linear code is capable of correcting $\lambda$ or fewer errors and simultaneously detecting $l (l > \lambda)$ or fewer errors if its minimum distance $d_{\text{min}} \geq \lambda + l + 1$.

**Solutions:** From the given condition, we see that $\lambda < \left\lfloor \frac{d_{\text{min}} - 1}{2} \right\rfloor$. 
Problem # 4 Prove that a linear code is capable of correcting \( \lambda \) or fewer errors and simultaneously detecting \( l(l > \lambda) \) or fewer errors if its minimum distance \( d_{\text{min}} \geq \lambda + l + 1 \).

Solutions: From the given condition, we see that \( \lambda < \left\lfloor \frac{d_{\text{min}} - 1}{2} \right\rfloor \).

It means that all the error patterns of \( \lambda \) or fewer errors can be used as coset leaders in a standard array. Hence, they are correctable.

In order to show that any error pattern of \( l \) or fewer errors is detectable, we need to show that no error pattern \( x \) of \( l \) or fewer errors can be in the same coset as an error pattern \( y \) of \( \lambda \) or fewer errors.
**Problem # 4** Prove that a linear code is capable of correcting \( \lambda \) or fewer errors and simultaneously detecting \( l(l > \lambda) \) or fewer errors if its minimum distance \( d_{\text{min}} \geq \lambda + l + 1 \).

**Solutions:** From the given condition, we see that \( \lambda < \left\lfloor \frac{d_{\text{min}} - 1}{2} \right\rfloor \).

It means that all the error patterns of \( \lambda \) or fewer errors can be used as coset leaders in a standard array. Hence, they are correctable.

In order to show that any error pattern of \( l \) or fewer errors is detectable, we need to show that no error pattern \( x \) of \( l \) or fewer errors can be in the same coset as an error pattern \( y \) of \( \lambda \) or fewer errors.

Suppose that \( x \) and \( y \) are in the same coset. Then \( x + y \) is a nonzero code word. The weight of this code word satisfies

\[
wt(x + y) \leq wt(x) + wt(y) \leq l + \lambda \leq d_{\text{min}}
\]

This is impossible since the minimum weight of the code is \( d_{\text{min}} \). Hence \( x \) and \( y \) are in different cosets. As a result, when \( x \) occurs, it will not be mistaken as \( y \). Therefore \( x \) is detectable.
Problem # 5 Let $C_i$ be the binary $(n, k_i)$ linear code with generator matrix $G_i$ and minimum distance $d_i$, respectively. Let $C$ be the binary $(2n, k_1 + k_2)$ linear code with generator matrix

$$G = \begin{bmatrix} G_1 & G_1 \\ 0 & G_2 \end{bmatrix}$$

where $0$ is a $k_2 \times n$ zero matrix. Calculate the minimum distance of $C$. Prove your result.

Solution: Let $u = (u_0, u_1, \ldots, u_{n-1})$ and $v = (v_0, v_1, \ldots, v_{n-1})$ be two binary n-tuples. We form $2n$-tuple from $u$ and $v$ as follows

$$|u|u + v| = (u_0, u_1, \ldots, u_{n-1}, u_0 + v_0, u_1 + v_1, \ldots, u_{n-1} + v_{n-1})$$
Problem # 5 Let $C_i$ be the binary $(n, k_i)$ linear code with generator matrix $G_i$ and minimum distance $d_i$, respectively. Let $C$ be the binary $(2n, k_1 + k_2)$ linear code with generator matrix

$$G = \begin{bmatrix} G_1 & G_1 \\ 0 & G_2 \end{bmatrix}$$

where $0$ is a $k_2 \times n$ zero matrix. Calculate the minimum distance of $C$. Prove your result.

Solution: Let $u = (u_0, u_1, \cdots, u_{n-1})$ and $v = (v_0, v_1, \cdots, v_{n-1})$ be two binary $n$-tuples. We form $2n$-tuple from $u$ and $v$ as follows

$$|u|u + v| = (u_0, u_1, \cdots, u_{n-1}, u_0 + v_0, u_1 + v_1, \cdots, u_{n-1} + v_{n-1})$$

The linear block code $C$ is

$$C = |C_1|C_1 + C_2|$$

$$= \{ |u|u + v| : u \in C_1, \text{ and } v \in C_2 \}$$

Problem #5 (contd.): The minimum distance of $C$ is

$$d_{\text{min}} = \min\{2d_1, d_2\}$$
Minimum distance of a code

- **Problem #5 (contd.):** The minimum distance of $C$ is
  \[ d_{\text{min}} = \min\{2d_1, d_2\} \]

- Let $x = |u|u + v|$ and $y = |u'|u' + v'|$ be two distinct codewords in $C$.
  \[ d(x, y) = w(u + u') + w(u + u' + v + v') \]
  where $w(z)$ is the Hamming weight of $z$.

Consider two cases $v = v'$ and $v \neq v'$. If $v = v'$, since $x \neq y$, we must have $u \neq u'$. In this case
\[ d(x, y) = w(u + u') + w(u + u') \]
Minimum distance of a code

- **Problem #5 (contd.):** The minimum distance of $C$ is
  \[ d_{\text{min}} = \min\{2d_1, d_2\} \]

- Let $x = |u|u + v|$ and $y = |u'|u' + v'|$ be two distinct codewords in $C$.
  \[ d(x, y) = w(u + u') + w(u + u' + v + v') \]
  where $w(z)$ is the Hamming weight of $z$.

- Consider two cases $v = v'$ and $v \neq v'$. If $v = v'$, since $x \neq y$, we must have $u \neq u'$. In this case
  \[ d(x, y) = w(u + u') + w(u + u') \]

- Since $u + u'$ is a nonzero codeword in $C_1$, $w(u + u') \geq d_1$. Therefore
  \[ d(x, y) \geq 2d_1 \quad (3) \]

From triangle inequality, we have
\[
\begin{align*}
    d(x, y) &\geq d(x, z) - d(y, z) \\
    w(x + y) &\geq wt(x + z) - wt(y + z)
\end{align*}
\]
Minimum distance of a code

Problem #5 (contd.): Let \( x + z = v + v' \) and \( y + z = u + u' \), then we get

\[
w(u + u' + v + v') \geq w(v + v') - w(u + u')
\]

If \( v \neq v' \), we have

\[
d(x, y) \geq w(u + u') + w(v + v') - w(u + u') = w(v + v')
\]
Minimum distance of a code

Problem #5 (contd.): Let $x + z = v + v'$ and $y + z = u + u'$, then we get

$$w(u + u' + v + v') \geq w(v + v') - w(u + u')$$

- If $v \neq v'$, we have

$$d(x, y) \geq w(u + u') + w(v + v') - w(u + u')$$
$$= w(v + v')$$

- Since $v + v'$ is a nonzero codeword in $C_2$, $w(v + v') \geq d_2$, we have

$$d(x, y) \geq d_2$$

(4)

From (3) and (4) we have

$$d(x, y) \geq \min\{2d_1, d_2\}$$
Problem #5 (contd.): Let $u_0$ and $v_0$ be two minimum-weight codewords in $C_1$ and $C_2$ respectively.

The vector $|u_0|u_0|$ is a codeword in $C$ with weight $2d_1$. 
Problem #5 (contd.): Let $u_0$ and $v_0$ be two minimum-weight codewords in $C_1$ and $C_2$ respectively.

- The vector $|u_0|u_0|$ is a codeword in $C$ with weight $2d_1$.
- Similarly the vector $|0|v_0|$ is a codeword in $C$ with weight $d_2$.

Therefore

$$d(x, y) = \min \{2d_1, d_2\}$$