An introduction to coding theory

Adrish Banerjee

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

Jan. 23, 2017

Lecture #3B: Problem solving session-I

Linear block code

- **Problem # 1:** Consider a linear block code, C with parity check matrix given by

$$\mathbf{H} = \begin{bmatrix} 1\,0\,0\,1\,0\,1\,1 \\ 0\,1\,0\,1\,1\,1\,0 \\ 0\,0\,1\,0\,1\,1\,1 \\ 1\,1\,1\,0\,0\,1\,0 \end{bmatrix}$$

What is (n, k) of C?

Linear block code

- **Problem # 1:** Consider a linear block code, C with parity check matrix given by

$$\mathbf{H} = \begin{bmatrix} 1\,0\,0\,1\,0\,1\,1 \\ 0\,1\,0\,1\,1\,1\,0 \\ 0\,0\,1\,0\,1\,1\,1 \\ 1\,1\,1\,0\,0\,1\,0 \end{bmatrix}$$

What is (n, k) of C?

- **Solutions:** Rank of **H** matrix is 3. So, $n = 7$, $k = 7 - 3 = 4$.

Linear block code

- **Problem # 2:** Consider the following binary block code, C,

$$C = \{000000, 110011, 011101, 111111\}$$

Is C a linear block code? Justify your answer.

Linear block code

- **Problem # 2:** Consider the following binary block code, C,

$$C = \{000000, 110011, 011101, 111111\}$$

Is C a linear block code? Justify your answer.

- **Solutions:** No.

Linear block code

- **Problem # 2:** Consider the following binary block code, C,

$$C = \{000000, 110011, 011101, 111111\}$$

  Is C a linear block code? Justify your answer.
- **Solutions:** No.
- Sum of two codewords for a linear block code is a valid codeword.

Linear block code

- **Problem # 2:** Consider the following binary block code, C,

$$C = \{000000, 110011, 011101, 111111\}$$

  Is C a linear block code? Justify your answer.
- **Solutions:** No.
- Sum of two codewords for a linear block code is a valid codeword.
- Let $v_0 = 000000$, $v_1 = 110011$, $v_2 = 011101$, and $v_3 = 111111$, then $v_1 + v_2$, $v_1 + v_3$, $v_2 + v_3$, and $v_1 + v_2 + v_3$ must also be a valid codeword.

$$\begin{aligned} v_1 + v_2 &= 101110 \\ v_1 + v_3 &= 001100 \\ v_2 + v_3 &= 100010 \\ v_1 + v_2 + v_3 &= 010001 \end{aligned}$$

Problem # 2 (contd.)

- Thus a linear block code should have the following codewords

$$C = \{000000, 110011, 011101, 111111, 101110, 001100, 100010, 010001\}$$

Problem # 2 (contd.)

- Thus a linear block code should have the following codewords

$$C = \{000000, 110011, 011101, 111111, 101110, 001100, 100010, 010001\}$$

- This is a (6,3) linear binary code.

Problem # 2 (contd.)

- Thus a linear block code should have the following codewords

$$C = \{000000, 110011, 011101, 111111, 101110, 001100, 100010, 010001\}$$

- This is a (6,3) linear binary code.
- One example of generator matrix for this code

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Problem # 2 (contd.): Generator matrix in systematic form

- How to write the generator matrix in systematic form?

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Problem # 2 (contd.): Generator matrix in systematic form

- How to write the generator matrix in systematic form?

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

- Row 3 $\rightarrow$ Row 3 + Row 1

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

Problem # 2 (contd.): Generator matrix in systematic form

- How to write the generator matrix in systematic form?

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

- Row 3 $\rightarrow$ Row 3 + Row 1

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

- Row 2 $\rightarrow$ Row 3 + Row 2

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

Problem # 2 (contd.): Generator matrix in systematic form

- Row 1 $\rightarrow$ Row 1 + Row 2

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

Problem # 2 (contd.): Generator matrix in systematic form

- Row 1 $\rightarrow$ Row 1 + Row 2

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

- Similarly parity check matrix in systematic form can be written as

$$\mathbf{H} = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Linear block code

- **Problem # 3:** Let **H** be the parity check matrix of an (n,k) linear code C that has both odd and even-weight codewords. Construct a new linear code C_1 with the following parity-check matrix

$$\mathbf{H_1} = \left[\begin{array}{c|c} 0 & \\ 0 & \\ \vdots & \mathbf{H} \\ 0 & \\ \cdots & \cdots \\ 1 & 11\cdots 1 \end{array}\right]$$

Linear block code

- **Problem # 3:** Let **H** be the parity check matrix of an (n,k) linear code C that has both odd and even-weight codewords. Construct a new linear code C_1 with the following parity-check matrix

$$\mathbf{H_1} = \left[\begin{array}{c|c} 0 & \\ 0 & \\ \vdots & \mathbf{H} \\ 0 & \\ \cdots & \cdots \\ 1 & 11\cdots 1 \end{array}\right]$$

1. Show that C_1 is an $(n+1, k)$ linear code.

Linear block code

- **Problem # 3:** Let **H** be the parity check matrix of an (n,k) linear code C that has both odd and even-weight codewords. Construct a new linear code C_1 with the following parity-check matrix

$$\mathbf{H_1} = \left[\begin{array}{c|c} 0 & \\ 0 & \\ \vdots & \mathbf{H} \\ 0 & \\ \cdots & \cdots \\ 1 & 11\cdots1 \end{array}\right]$$

1. Show that C_1 is an $(n+1,k)$ linear code.
2. Show that every codeword of C_1 has even weight.

Linear block code

- **Problem # 3:** Let **H** be the parity check matrix of an (n,k) linear code C that has both odd and even-weight codewords. Construct a new linear code C_1 with the following parity-check matrix

$$\mathbf{H_1} = \left[\begin{array}{c|c} 0 & \\ 0 & \\ \vdots & \mathbf{H} \\ 0 & \\ \cdots & \cdots \\ 1 & 11\cdots1 \end{array}\right]$$

1. Show that C_1 is an $(n+1,k)$ linear code.
2. Show that every codeword of C_1 has even weight.
3. Show that C_1 can be obtained from C by adding an extra parity check digit, denoted by v_∞ to the left of each codeword **v** as follows

Linear block code

- **Problem # 3:** Let $\mathbf{H}$ be the parity check matrix of an (n,k) linear code C that has both odd and even-weight codewords. Construct a new linear code C_1 with the following parity-check matrix

$$\mathbf{H_1} = \left[\begin{array}{c|c} 0 & \\ 0 & \\ \vdots & \mathbf{H} \\ 0 & \\ \cdots & \cdots \\ 1 & 11\cdots1 \end{array}\right]$$

1. Show that C_1 is an $(n+1, k)$ linear code.
2. Show that every codeword of C_1 has even weight.
3. Show that C_1 can be obtained from C by adding an extra parity check digit, denoted by v_∞ to the left of each codeword $\mathbf{v}$ as follows
   1) if $\mathbf{v}$ has odd weight, then $v_\infty = 1$, and

Linear block code

- **Problem # 3:** Let $\mathbf{H}$ be the parity check matrix of an (n,k) linear code C that has both odd and even-weight codewords. Construct a new linear code C_1 with the following parity-check matrix

$$\mathbf{H_1} = \left[\begin{array}{c|c} 0 & \\ 0 & \\ \vdots & \mathbf{H} \\ 0 & \\ \cdots & \cdots \\ 1 & 11\cdots1 \end{array}\right]$$

1. Show that C_1 is an $(n+1, k)$ linear code.
2. Show that every codeword of C_1 has even weight.
3. Show that C_1 can be obtained from C by adding an extra parity check digit, denoted by v_∞ to the left of each codeword $\mathbf{v}$ as follows
   1) if $\mathbf{v}$ has odd weight, then $v_\infty = 1$, and
   2) if $\mathbf{v}$ has even weight, then $v_\infty = 0$

Problem # 3 (contd.)

- The matrix $\mathbf{H_1}$ is an $(n-k+1) \times (n+1)$ matrix.

Problem # 3 (contd.)

- The matrix $\mathbf{H_1}$ is an $(n-k+1) \times (n+1)$ matrix.
- First we note that the $n-k$ rows of $\mathbf{H}$ are linearly independent. It is clear that the first $(n-k)$ rows of $\mathbf{H_1}$ are also linearly independent.

Problem # 3 (contd.)

- The matrix $\mathbf{H_1}$ is an $(n-k+1) \times (n+1)$ matrix.
- First we note that the $n-k$ rows of $\mathbf{H}$ are linearly independent. It is clear that the first $(n-k)$ rows of $\mathbf{H_1}$ are also linearly independent.
- The last row of $\mathbf{H_1}$ has a "1" at its first position but other rows of $\mathbf{H_1}$ have a "0" at their first position. Any linear combination including the last row of $\mathbf{H_1}$ will never yield a zero vector.

Problem # 3 (contd.)

- The matrix $\mathbf{H_1}$ is an $(n-k+1) \times (n+1)$ matrix.
- First we note that the $n-k$ rows of $\mathbf{H}$ are linearly independent. It is clear that the first $(n-k)$ rows of $\mathbf{H_1}$ are also linearly independent.
- The last row of $\mathbf{H_1}$ has a "1" at its first position but other rows of $\mathbf{H_1}$ have a "0" at their first position. Any linear combination including the last row of $\mathbf{H_1}$ will never yield a zero vector.
- Thus all the rows of $\mathbf{H_1}$ are linearly independent. Hence the row space of $\mathbf{H_1}$ has dimension n-k+1.

Problem # 3 (contd.)

- The matrix $\mathbf{H_1}$ is an $(n-k+1) \times (n+1)$ matrix.
- First we note that the $n-k$ rows of $\mathbf{H}$ are linearly independent. It is clear that the first $(n-k)$ rows of $\mathbf{H_1}$ are also linearly independent.
- The last row of $\mathbf{H_1}$ has a "1" at its first position but other rows of $\mathbf{H_1}$ have a "0" at their first position. Any linear combination including the last row of $\mathbf{H_1}$ will never yield a zero vector.
- Thus all the rows of $\mathbf{H_1}$ are linearly independent. Hence the row space of $\mathbf{H_1}$ has dimension n-k+1.
- The dimension of its null space, C_1 , is then equal to

$$\dim(C_1) = (n+1) - (n-k+1) = k$$

Problem # 3 (contd.)

- The matrix $\mathbf{H_1}$ is an $(n-k+1) \times (n+1)$ matrix.
- First we note that the $n-k$ rows of $\mathbf{H}$ are linearly independent. It is clear that the first $(n-k)$ rows of $\mathbf{H_1}$ are also linearly independent.
- The last row of $\mathbf{H_1}$ has a "1" at its first position but other rows of $\mathbf{H_1}$ have a "0" at their first position. Any linear combination including the last row of $\mathbf{H_1}$ will never yield a zero vector.
- Thus all the rows of $\mathbf{H_1}$ are linearly independent. Hence the row space of $\mathbf{H_1}$ has dimension n-k+1.
- The dimension of its null space, C_1 , is then equal to

$$\dim(C_1) = (n+1) - (n-k+1) = k$$

- Hence C_1 is an $(n+1, k)$ linear code.

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to coding theory

Problem # 3 (contd.)

- Show that every codeword of C_1 has even weight.

Problem # 3 (contd.)

- Show that every codeword of C_1 has even weight.
- **Solution:** The last row of $\mathbf{H}_1$ is an all-one vector.

Problem # 3 (contd.)

- Show that every codeword of C_1 has even weight.
- **Solution:** The last row of $\mathbf{H_1}$ is an all-one vector.
- The inner product of a vector with odd weight and the all-one vector is "1" . Hence, for any odd weight vector $\mathbf{v}$,

$$\mathbf{v}H_1^T \neq 0$$

and $\mathbf{v}$ cannot be a code word in C_1.

Problem # 3 (contd.)

- Show that every codeword of C_1 has even weight.
- **Solution:** The last row of $\mathbf{H_1}$ is an all-one vector.
- The inner product of a vector with odd weight and the all-one vector is "1" . Hence, for any odd weight vector $\mathbf{v}$,

$$\mathbf{v}H_1^T \neq 0$$

and $\mathbf{v}$ cannot be a code word in C_1.
- Therefore, C_1 consists of only even-weight code words.

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to coding theory

Problem # 3 (contd.)

- Show that C_1 can be obtained from C by adding an extra parity check digit, denoted by v_∞ to the left of each codeword $\mathbf{v}$ as follows

Problem # 3 (contd.)

- Show that C_1 can be obtained from C by adding an extra parity check digit, denoted by v_∞ to the left of each codeword $\mathbf{v}$ as follows
  1) if $\mathbf{v}$ has odd weight, then $v_\infty = 1$, and

Problem # 3 (contd.)

- Show that C_1 can be obtained from C by adding an extra parity check digit, denoted by v_∞ to the left of each codeword $\mathbf{v}$ as follows
  1) if $\mathbf{v}$ has odd weight, then $v_\infty = 1$, and
  2) if $\mathbf{v}$ has even weight, then $v_\infty = 0$

Problem # 3 (contd.)

- Show that C_1 can be obtained from C by adding an extra parity check digit, denoted by v_∞ to the left of each codeword $\mathbf{v}$ as follows
  1) if $\mathbf{v}$ has odd weight, then $v_\infty = 1$, and
  2) if $\mathbf{v}$ has even weight, then $v_\infty = 0$
- **Solution:** Let $\mathbf{v}$ be a code word in C. Then $\mathbf{v}H^T = 0$. Extend $\mathbf{v}$ by adding a digit v_∞ to its left.

Problem # 3 (contd.)

- Show that C_1 can be obtained from C by adding an extra parity check digit, denoted by v_∞ to the left of each codeword $\mathbf{v}$ as follows
  1) if $\mathbf{v}$ has odd weight, then $v_\infty = 1$, and
  2) if $\mathbf{v}$ has even weight, then $v_\infty = 0$
- **Solution:** Let $\mathbf{v}$ be a code word in C. Then $\mathbf{v}H^T = 0$. Extend $\mathbf{v}$ by adding a digit v_∞ to its left.
- This results in a vector of n+1 digits,

$$\mathbf{v_1} = (v_\infty, \mathbf{v}) = (v_\infty, v_0, v_1, \cdots, v_{n-1}).$$

Problem # 3 (contd.)

- Show that C_1 can be obtained from C by adding an extra parity check digit, denoted by v_∞ to the left of each codeword $\mathbf{v}$ as follows
  1) if $\mathbf{v}$ has odd weight, then $v_\infty = 1$, and
  2) if $\mathbf{v}$ has even weight, then $v_\infty = 0$
- **Solution:** Let $\mathbf{v}$ be a code word in C. Then $\mathbf{v}H^T = 0$. Extend $\mathbf{v}$ by adding a digit v_∞ to its left.
- This results in a vector of n+1 digits,

$$\mathbf{v_1} = (v_\infty, \mathbf{v}) = (v_\infty, v_0, v_1, \cdots, v_{n-1}).$$

- For $\mathbf{v_1}$ to be a vector in C_1 , we must require that

$$\mathbf{v_1 H_1^T = 0}$$

Problem # 3 (contd.)

- Note that the inner product of v_1 with any of the first n-k rows of $\mathbf{H_1}$ is 0.

Problem # 3 (contd.)

- Note that the inner product of v_1 with any of the first n-k rows of $\mathbf{H_1}$ is 0.
- The inner product of $\mathbf{v_1}$ with the last row of $\mathbf{H_1}$ is

$$v_\infty + v_0 + v_1 + \cdots + v_{n-1}$$

Problem # 3 (contd.)

- Note that the inner product of v_1 with any of the first n-k rows of $\mathbf{H_1}$ is 0.
- The inner product of $\mathbf{v_1}$ with the last row of $\mathbf{H_1}$ is

$$v_\infty + v_0 + v_1 + \cdots + v_{n-1}$$

- For this sum to be zero, we must require that $v_\infty = 1$ if the vector $\mathbf{v}$ has odd weight and $v_\infty = 0$ if the vector $\mathbf{v}$ has even weight.

Problem # 3 (contd.)

- Note that the inner product of v_1 with any of the first n-k rows of $\mathbf{H_1}$ is 0.
- The inner product of $\mathbf{v_1}$ with the last row of $\mathbf{H_1}$ is

$$v_\infty + v_0 + v_1 + \cdots + v_{n-1}$$

- For this sum to be zero, we must require that $v_\infty = 1$ if the vector $\mathbf{v}$ has odd weight and $v_\infty = 0$ if the vector $\mathbf{v}$ has even weight.
- Therefore, any vector v_1 formed as above is a codeword in C_1, there are 2^k such codewords.

Adrish Banerjee Department of Electrical Engineering Indian Institute of Technology Kanpur Kanpur, Uttar Pradesh India
An introduction to coding theory

Problem # 3 (contd.)

- Note that the inner product of v_1 with any of the first n-k rows of $\mathbf{H_1}$ is 0.
- The inner product of $\mathbf{v_1}$ with the last row of $\mathbf{H_1}$ is

$$v_\infty + v_0 + v_1 + \cdots + v_{n-1}$$

- For this sum to be zero, we must require that $v_\infty = 1$ if the vector $\mathbf{v}$ has odd weight and $v_\infty = 0$ if the vector $\mathbf{v}$ has even weight.
- Therefore, any vector v_1 formed as above is a codeword in C_1, there are 2^k such codewords.
- The dimension of C_1 is k, these 2^k codewords are all the code words of C_1 .