An introduction to coding theory

Adrish Banerjee

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

Jan. 23, 2017

Lecture #2: Introduction to linear block codes, generator matrix and parity check matrix

Linear block codes

- An (n,k) linear block code can be defined by a k $\times$ n *generator matrix*.

$$\mathbf{G} = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_{k-1} \end{bmatrix} = \begin{bmatrix} g_{0,0} & g_{0,1} & g_{0,2} & \cdots & g_{0,n-1} \\ g_{1,0} & g_{1,1} & g_{1,2} & \cdots & g_{1,n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ g_{k-1,0} & g_{k-1,1} & g_{k-1,2} & \cdots & g_{k-1,n-1} \end{bmatrix}$$

Linear block codes

- An (n,k) linear block code can be defined by a k $\times$ n *generator matrix*.

$$\mathbf{G} = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_{k-1} \end{bmatrix} = \begin{bmatrix} g_{0,0} & g_{0,1} & g_{0,2} & \cdots & g_{0,n-1} \\ g_{1,0} & g_{1,1} & g_{1,2} & \cdots & g_{1,n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ g_{k-1,0} & g_{k-1,1} & g_{k-1,2} & \cdots & g_{k-1,n-1} \end{bmatrix}$$

- The set of 2^k binary codewords is formed by taking the *linear combinations* of the rows of G.

Linear block codes

- An (n,k) linear block code can be defined by a k $\times$ n *generator matrix*.

$$\mathbf{G} = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_{k-1} \end{bmatrix} = \begin{bmatrix} g_{0,0} & g_{0,1} & g_{0,2} & \cdots & g_{0,n-1} \\ g_{1,0} & g_{1,1} & g_{1,2} & \cdots & g_{1,n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ g_{k-1,0} & g_{k-1,1} & g_{k-1,2} & \cdots & g_{k-1,n-1} \end{bmatrix}$$

- The set of 2^k binary codewords is formed by taking the *linear combinations* of the rows of G.
- For the binary information sequence $\mathbf{u}= (u_0, u_1, \cdots, u_{k-1})$, the corresponding binary codeword sequence is given by

$$\mathbf{v} = \mathbf{uG} = u_0\mathbf{g}_0 + u_1\mathbf{g}_1 + \cdots + u_{k-1}\mathbf{g}_{k-1} \quad \text{(modulo-2)}$$

Linear block codes

- The sum of any two codewords in a linear code is also a codeword, i.e., if $\mathbf{v_1}$ and $\mathbf{v_2}$ are codewords, then $\mathbf{v_1} + \mathbf{v_2}$ is a codeword.

Linear block codes

- The sum of any two codewords in a linear code is also a codeword, i.e., if $\mathbf{v_1}$ and $\mathbf{v_2}$ are codewords, then $\mathbf{v_1} + \mathbf{v_2}$ is a codeword.
- The all zero vector $\mathbf{0}$= (0, 0, $\cdots$, 0) is a codeword in every linear code.

Linear block codes

- The sum of any two codewords in a linear code is also a codeword, i.e., if $\mathbf{v_1}$ and $\mathbf{v_2}$ are codewords, then $\mathbf{v_1} + \mathbf{v_2}$ is a codeword.
- The all zero vector $\mathbf{0}$= (0, 0, $\cdots$, 0) is a codeword in every linear code.
- An (n, k) linear block code is a k-dimensional subspace of the vector space V_n of all binary n-tuples.

Linear block codes

Example 2.1: 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)

Linear block codes

Example 2.1 (contd.): We can write the coded bits in terms of information bits as follows

$$\begin{aligned} v_0 &= u_1 + u_2 \\ v_1 &= u_0 + u_2 \\ v_2 &= u_0 + u_1 \\ v_3 &= u_0 \\ v_4 &= u_1 \\ v_5 &= u_2 \end{aligned}$$

$$[v_0 \;\; v_1 \;\; v_2 \;\; v_3 \;\; v_4 \;\; v_5] = [u_0 \;\; u_1 \;\; u_2] \begin{bmatrix} g_{0,0} & g_{0,1} & g_{0,2} & g_{0,3} & g_{0,4} & g_{0,5} \\ g_{1,0} & g_{1,1} & g_{1,2} & g_{1,3} & g_{1,4} & g_{1,5} \\ g_{2,0} & g_{2,1} & g_{2,2} & g_{2,3} & g_{2,4} & g_{2,5} \end{bmatrix}$$

Linear block codes

A generator matrix for this code is

$$\mathbf{G} = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \mathbf{g}_2 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

The codeword for the message $\mathbf{u} = (1\ 0\ 1)$ is

$$\begin{aligned} \mathbf{v} &= \mathbf{u} \cdot \mathbf{G} \\ &= 1 \cdot (0\ 1\ 1\ 1\ 0\ 0) + 0 \cdot (1\ 0\ 1\ 0\ 1\ 0) + 1 \cdot (1\ 1\ 0\ 0\ 0\ 1) \\ &= (0\ 1\ 1\ 1\ 0\ 0) + (0\ 0\ 0\ 0\ 0\ 0) + (1\ 1\ 0\ 0\ 0\ 1) \\ &= (1\ 0\ 1\ 1\ 0\ 1) \end{aligned}$$

Linear block codes

- An (n,k) linear block code is in *systematic form*, if its generator matrix is in the following form:

$$\begin{aligned} \mathbf{G} &= [\mathbf{P} : \mathbf{I}_k] \\ &= \left[\begin{array}{cccc|ccccc} p_{0,0} & p_{0,1} & \cdots & p_{0,n-k-1} & 1 & 0 & 0 & \cdots & 0 \\ p_{1,0} & p_{1,1} & \cdots & p_{1,n-k-1} & 0 & 1 & 0 & \cdots & 0 \\ p_{2,0} & p_{2,1} & \cdots & p_{2,n-k-1} & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ p_{k-1,0} & p_{k-1,1} & \cdots & p_{k-1,n-k-1} & 0 & 0 & 0 & \cdots & 1 \end{array}\right] \end{aligned}$$

Linear block codes

- An (n,k) linear block code is in *systematic form*, if its generator matrix is in the following form:

$$\mathbf{G} = [\mathbf{P} : \mathbf{I}_k] = \left[\begin{array}{cccc|ccccc} p_{0,0} & p_{0,1} & \cdots & p_{0,n-k-1} & 1 & 0 & 0 & \cdots & 0 \\ p_{1,0} & p_{1,1} & \cdots & p_{1,n-k-1} & 0 & 1 & 0 & \cdots & 0 \\ p_{2,0} & p_{2,1} & \cdots & p_{2,n-k-1} & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ p_{k-1,0} & p_{k-1,1} & \cdots & p_{k-1,n-k-1} & 0 & 0 & 0 & \cdots & 1 \end{array}\right]$$

- Every codeword consists of two parts: a message part and a parity check part.

Linear block codes

- For systematic linear block code, the message part consists of the k unaltered message bits, and the parity check part consists of $n-k$ parity check bits.

Linear block codes

- For systematic linear block code, the message part consists of the k unaltered message bits, and the parity check part consists of $n-k$ parity check bits.
- The encoding equations for a systematic code are given by (parity check equations:)

$$v_j = u_0 p_{0,j} + u_1 p_{1,j} + \cdots + u_{k-1} p_{k-1,j}, \quad 0 \leq j \leq n-k-1$$

(message bits:)

$$v_{n-k+i} = u_i, 0 \leq i \leq k-1$$

Linear block codes

- For systematic linear block code, the message part consists of the k unaltered message bits, and the parity check part consists of $n-k$ parity check bits.
- The encoding equations for a systematic code are given by (parity check equations:)

$$v_j = u_0 p_{0,j} + u_1 p_{1,j} + \cdots + u_{k-1} p_{k-1,j}, \quad 0 \leq j \leq n-k-1$$

(message bits:)

$$v_{n-k+i} = u_i, 0 \leq i \leq k-1$$

- Each parity bit $v_j, 0 \leq j \leq n-k-1$, is a (modulo-2) sum of certain message bits.

Linear block codes

- Linear (n,k) block can also be specified by an (n-k) $\times$ n *parity check matrix* $\mathbf{H}$.

Linear block codes

- Linear (n,k) block can also be specified by an (n-k) $\times$ n *parity check matrix* $\mathbf{H}$.
- If $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1})$ is a binary n-tuple, then $\mathbf{v}$ is a codeword if and only if

$$\mathbf{v}\mathbf{H}^{\mathbf{T}} = (0, 0, \cdots, 0),$$

Linear block codes

- Linear (n,k) block can also be specified by an (n-k) $\times$ n *parity check matrix* $\mathbf{H}$.
- If $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1})$ is a binary n-tuple, then $\mathbf{v}$ is a codeword if and only if
$$\mathbf{v}\mathbf{H}^{\mathbf{T}} = (0, 0, \cdots, 0),$$
- Example 2.3: Consider a $(7, 4)$ linear systematic code with generator matrix
$$\mathbf{G} = \left[\begin{array}{ccc|cccc} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right]$$

Linear block codes

- The encoding equations can be written as
$$[v_0\ v_1\ v_2\ v_3\ v_4\ v_5\ v_6] = [u_0\ u_1\ u_2\ u_3] \left[\begin{array}{ccccccc} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right]$$

Linear block codes

- The encoding equations can be written as

$$[v_0\ v_1\ v_2\ v_3\ v_4\ v_5\ v_6] = [u_0\ u_1\ u_2\ u_3] \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

- We can write this as

$$\begin{aligned} v_0 &= u_0 + u_1 + u_3 \\ v_1 &= u_0 + u_1 + u_2 \\ v_2 &= u_1 + u_2 + u_3 \\ v_3 &= u_0 \\ v_4 &= u_1 \\ v_5 &= u_2 \\ v_6 &= u_3 \end{aligned}$$

Linear block codes

- Equivalently, we can write the encoding equations as

$$\begin{aligned} v_0 + v_3 + v_5 + v_6 &= 0 \\ v_1 + v_3 + v_4 + v_5 &= 0 \\ v_2 + v_4 + v_5 + v_6 &= 0 \end{aligned}$$

Linear block codes

- Equivalently, we can write the encoding equations as

$$\begin{aligned} v_0 + v_3 + v_5 + v_6 &= 0 \\ v_1 + v_3 + v_4 + v_5 &= 0 \\ v_2 + v_4 + v_5 + v_6 &= 0 \end{aligned}$$

- In matrix form,

$$[v_0\ v_1\ v_2\ v_3\ v_4\ v_5\ v_6] \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Linear block codes

- For a systematic code with generator matrix $\mathbf{G} = [\mathbf{P} : \mathbf{I}_k]$, the parity check matrix can be written as,

$$\begin{aligned} \mathbf{H} &= \left[\mathbf{I}_{n-k} : \mathbf{P}^{\mathbf{T}}\right] \\ &= \left[\begin{array}{ccccc|cccc} 1 & 0 & 0 & \cdots & 0 & p_{0,0} & p_{1,0} & \cdots & p_{k-1,0} \\ 0 & 1 & 0 & \cdots & 0 & p_{0,1} & p_{1,1} & \cdots & p_{k-1,1} \\ 0 & 0 & 1 & \cdots & 0 & p_{0,2} & p_{1,2} & \cdots & p_{k-1,2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & p_{0,n-k-1} & p_{1,n-k-1} & \cdots & p_{k-1,n-k-1} \end{array}\right] \end{aligned}$$

Linear block codes

Example 2.3: Consider a $(7, 4)$ linear systematic code with generator matrix

$$\mathbf{G} = \left[\begin{array}{cccc|cccc} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right]$$

Then the parity-check matrix in systematic form is

$$\mathbf{H} = \left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right]$$