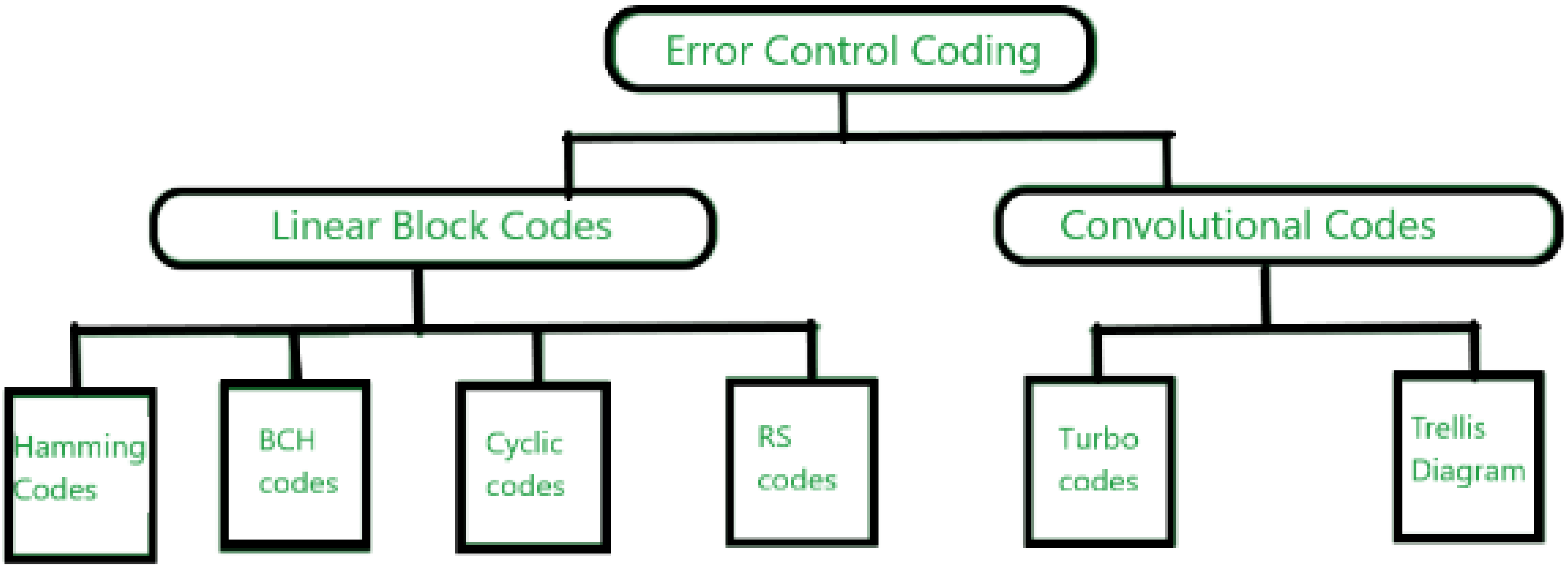
Module-7

Introduction to Information Theory

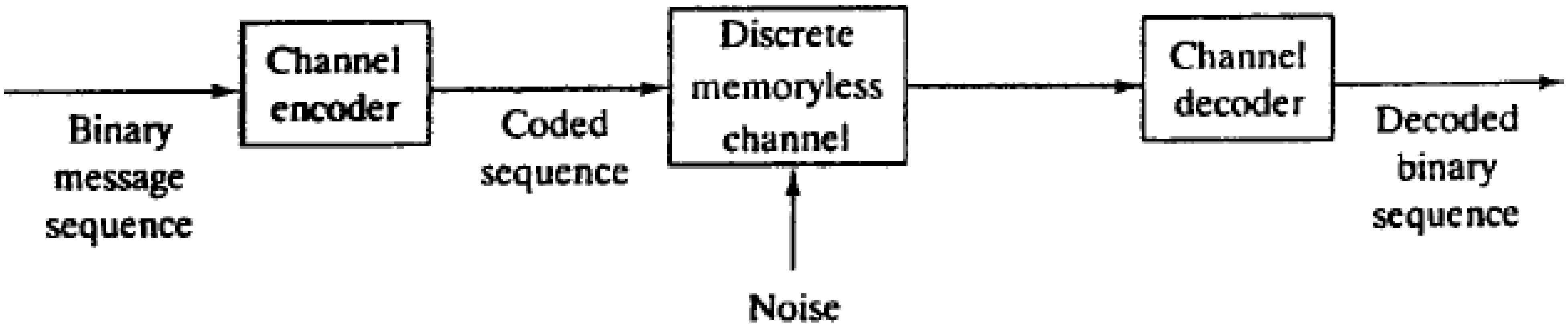
Error Control codes

- Noise or Error is the main problem in the signal, which disturbs the reliability of the communication system.
- Codes that can correct or merely detect errors depends on the amount of redundancy present in the code.
- Codes that can only detect errors are called as error detection codes
- Codes that can correct errors are called ass error correction codes
- Error control codes are broadly classified into Block codes and Convolutional codes

Error Control codes



Channel coding



Channel coding theorem

The channel coding theorem for a DMC is stated as follows:

Given a DMS X with entropy $H(X)$ bits/symbol and a DMC with capacity C_s bits/symbol, if $H(X) \leqslant C_s$, there exists a coding scheme for which the source output can be transmitted over the channel with an arbitrarily small probability of error.

Conversely, if $H(X) > C_s$, it is not possible to transmit information over the channel with an arbitrarily small probability of error.

Linear block codes

- It is a simple error control coding technique used for error detection and correction.
- Information data is partitioned into blocks of length k pieces called Information word.
- Every information word is then coded into a block of length n bits called a codeword
- The resultant block code is called (n , k) linear block code where n>k
- Also, n = k + r, where 'r ' denotes the parity bits or check bits added to every information word.
- Vector documentation is utilized for the Data word and Codeword: message m = (m_1, m_2 m_n), Codeword c = (c_1, c_2, c_n).
- The ratio k/n is called code rate.

Binary field

The set $K = \{0, 1\}$ is a *binary field*. The binary field has two operations, addition and multiplication such that the results of all operations are in K. The rules of addition and multiplication are as follows:

Addition:

$$0 \oplus 0 = 0 \quad 1 \oplus 1 = 0 \quad 0 \oplus 1 = 1 \oplus 0 = 1$$

Multiplication:

$$0 \cdot 0 = 0 \quad 1 \cdot 1 = 1 \quad 0 \cdot 1 = 1 \cdot 0 = 0$$

Linear codes

Let $\mathbf{a} = (a_1,a_2,\ldots,a_n)$, and $\mathbf{b} = (b_1,b_2,\ldots,b_n)$ be two code words in a code C. The sum of $\mathbf{a}$ and $\mathbf{b}$, denoted by $\mathbf{a} \oplus \mathbf{b}$, is defined by $(a_1 \oplus b_1,\ a_2 \oplus b_2,\ldots,a_n \oplus b_n)$. A code C is called *linear* if the sum of two code words is also a code word in C. A linear code C must contain the zero code word $\mathbf{0} = (0,0,\ldots,0)$, since $\mathbf{a} \oplus \mathbf{a} = \mathbf{0}$.

Hamming weight and distance

Let $\mathbf{c}$ be a code word of length n. The *Hamming weight* of $\mathbf{c}$, denoted by $w(\mathbf{c})$, is the number of 1's in $\mathbf{c}$.

Let $\mathbf{a}$ and $\mathbf{b}$ be code words of length n. The *Hamming distance* between $\mathbf{a}$ and $\mathbf{b}$, denoted by $d(\mathbf{a}, \mathbf{b})$, is the number of positions in which $\mathbf{a}$ and $\mathbf{b}$ differ. Thus, the Hamming weight of a code word $\mathbf{c}$ is the Hamming distance between $\mathbf{c}$ and $\mathbf{0}$, that is

$$w(\mathbf{c}) = d(\mathbf{c}, \mathbf{0})$$

Similarly, the Hamming distance can be written in terms of Hamming weight as

$$d(\mathbf{a}, \mathbf{b}) = w(\mathbf{a} \oplus \mathbf{b})$$

Minimum distance

The minimum distance $d_{\min}$ of a linear code C is defined as the smallest Hamming distance between any pair of code words in C.

- The minimum hamming distance of the codeword is equal to the smallest weight of any non zero code vector

Error detection and correction capabilities

The minimum distance d_{min} of a linear code C is an important parameter of C. It determines the error detection and correction capabilities of C. This is stated in the following theorems.

A linear code C of minimum distance d_{min} can detect up to t errors if and only if

$$d_{min} \geqslant t + 1$$

A linear code C of minimum distance d_{min} can correct up to t errors if and only if

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

Generator matrix

In an (n, k) linear block code C, we define a code vector **c** and a data (or message) vector **d** as follows:

$$\mathbf{c} = [c_1, c_2, \ldots, c_n]$$
$$\mathbf{d} = [d_1, d_2, \ldots, d_k]$$

If the data bits appear in specified location of **c**, then the code C is called *systematic*. Otherwise, it is called nonsystematic. Here we assume that the first k bits of **c** are the data bits and the last $(n-k)$ bits are the parity-check bits formed by linear combination of data bits, that is,

$$\begin{aligned}
c_1 &= d_1 \\
c_2 &= d_2 \\
&\vdots \\
c_{k+1} &= p_{11}d_1 \oplus p_{12}d_2 \oplus \cdots \oplus p_{1k}d_k \\
c_{k+2} &= p_{21}d_1 \oplus p_{22}d_2 \oplus \cdots \oplus p_{2k}d_k \\
&\vdots \\
c_{k+m} &= p_{m1}d_1 \oplus p_{m2}d_2 \oplus \cdots \oplus p_{mk}d_k
\end{aligned}$$

where $m = n - k$.

Generator matrix

$$
\mathbf{c} = \mathbf{d}G = [d_1 \quad d_2 \quad \cdots \quad d_k]\begin{bmatrix} 1 & 0 & \cdots & 0 & p_{11} & p_{12} & \cdots & p_{1k} \\ 0 & 1 & \cdots & 0 & p_{21} & p_{22} & \cdots & p_{2k} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & p_{m1} & p_{m2} & \cdots & p_{mk} \end{bmatrix}
$$

where

$$
G = [I_k \, P \;]
$$

- I_k is the k^{th} order identity matrix and P is the parity matrix
- The n x k matrix G is called Generator matrix which contains n rows and k columns

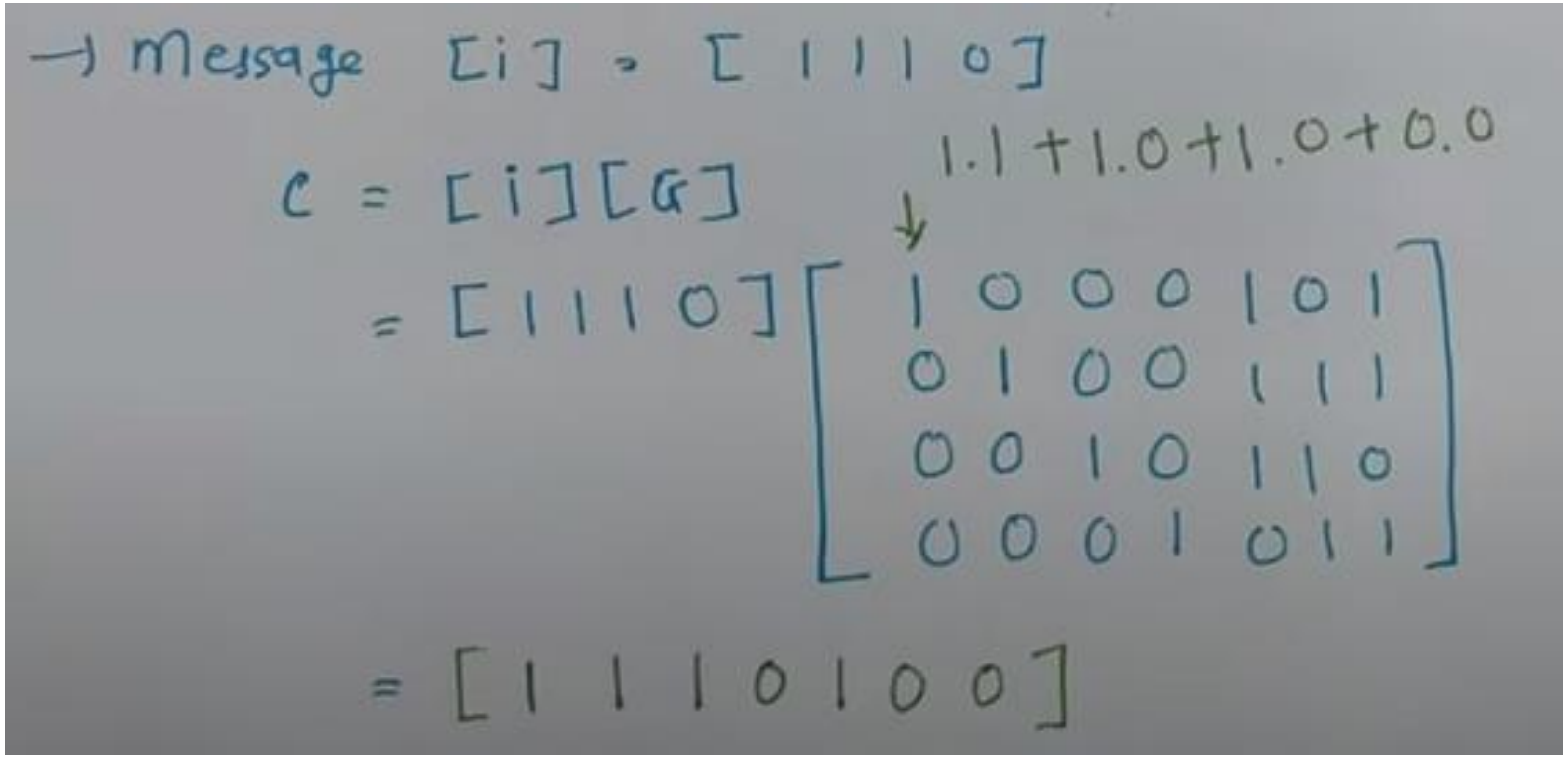
Generator matrix

- Generate codeword for d=(1 1 1 0) with (7,4) G matrix

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

Generator matrix

- Generate codeword for d=(1 1 1 0) with (7,4) G matrix



Generator matrix

- Determine the set of codewords for the (6,3) LBC with generator matrix

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

Generator matrix

- Determine the set of codewords for the (6,3) LBC with generator matrix

	m_0	m_1	m_2	P_0	P_1	P_2
c_0	0	0	0	0	0	0
c_1	0	0	1	1	1	0
c_2	0	1	0	1	0	1
c_3	0	1	1	0	1	1
c_4	1	0	0	0	1	1
c_5	1	0	1	1	0	1
c_6	1	1	0	1	1	0
c_7	1	1	1	0	0	0

Parity check matrix

- Let H denote the n x m matrix defined by

$$H = [P^T \quad I_m]$$

where $m = n - k$ and I_m is the mth-order identity matrix. Then

$$H^T = \begin{bmatrix} P \\ I_m \end{bmatrix}$$

$$GH^T = [I_k \quad P]\begin{bmatrix} P \\ I_m \end{bmatrix} = P \oplus P = O$$

where O denotes the $k \times m$ zero matrix.

$$\mathbf{c}H^T = \mathbf{d}GH^T = \mathbf{0}$$

where $\mathbf{0}$ denotes the $1 \times m$ zero vector.

Parity check matrix

The minimum distance $d_{\min}$ of a linear block code C is equal to the minimum number of rows of H^T that sum to $\mathbf{0}$, where H^T is the transpose of the parity-check matrix H of C.

Parity check matrix

- Generate the parity check matrix from the given G matrix

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

Parity check matrix

- Generate the parity check matrix from the given G matrix

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

$$P = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \Rightarrow P^T = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}$$

Parity check matrix

- Generate the parity check matrix from the given G matrix

$$\Rightarrow I_{n-k} = I_{7-4} = I_3$$

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

$$[H] = [P^T : I_{n-k}]$$

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

Syndrome decoding

Let $\mathbf{r}$ denote the received word of length n when code word $\mathbf{c}$ of length n was sent over a noisy channel. Then $\mathbf{r} = \mathbf{c} \oplus \mathbf{e}$, where $\mathbf{e}$ is called the error pattern. Note that $\mathbf{e} = \mathbf{r} + \mathbf{c}$.

Consider first the case of a single error in the ith position. Then we can represent $\mathbf{e}$ by

$$\mathbf{e} = [0 \cdots 0\underset{\substack{\uparrow \\ i\text{th position}}}{1}0 \cdots 0]$$

Next, we evaluate $\mathbf{r}H^T$ and obtain

$$\mathbf{r}H^T = (\mathbf{c} \oplus \mathbf{e})H^T = \mathbf{c}H^T \oplus \mathbf{e}H^T = \mathbf{e}H^T = \mathbf{s}$$

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

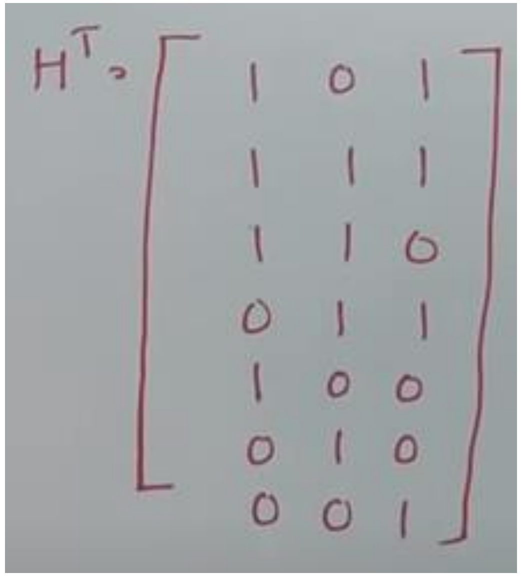
Thus, using $\mathbf{s}$ and noting that $\mathbf{e}H^T$ is the ith row of H^T, we can identify the error position by comparing $\mathbf{s}$ to the rows of H^T. Decoding by this simple comparison method is called *syndrome decoding*. Note that not all error patterns can be correctly decoded by syndrome decoding. The zero syndrome indicates that $\mathbf{r}$ is a code word and is presumably correct.

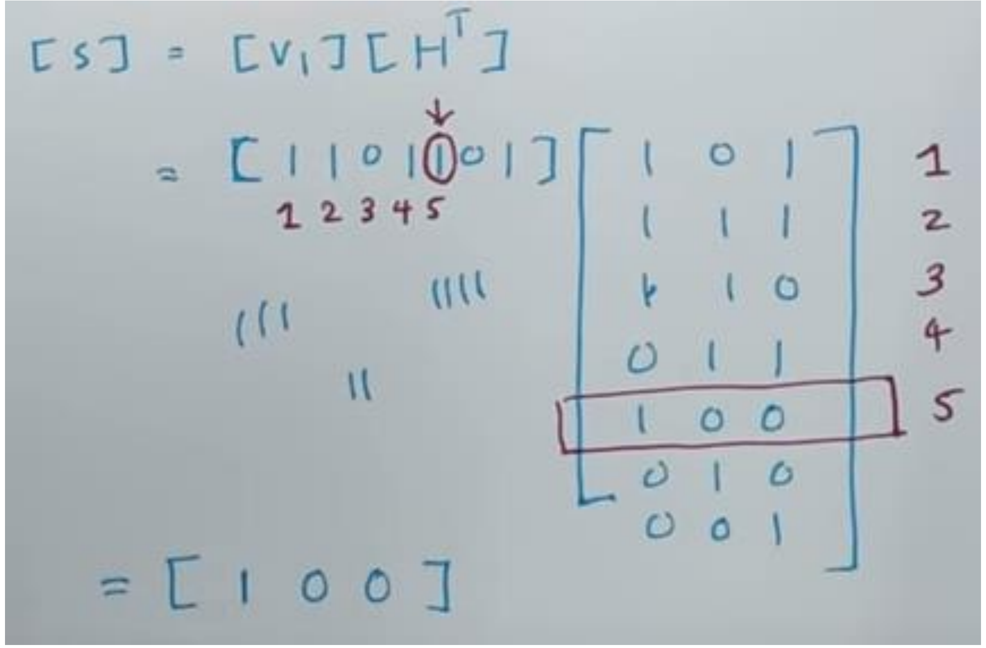
Syndrome decoding

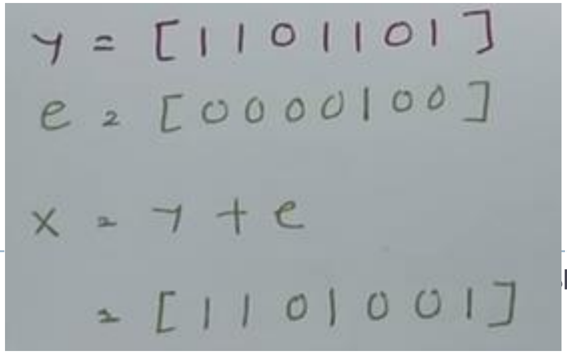
- Find the error syndrome of the received word Y=[1 1 0 1 1 0 1]. Take the H^T from the previous problem.

Syndrome decoding

- Find the error syndrome of the received word Y=[1 1 0 1 1 0 1]. Take the H^T from the previous problem.







Problems

- The parity check matrix of the (7,4) LBC is given below.

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

- Find the G matrix and the set of codewords.
- Draw the encoder diagram.

Problems

$$H = \left[\underbrace{\begin{matrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{matrix}}_{P^T} \;\; \underbrace{\begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix}}_{I} \right]$$

$$(P^T)^T = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}^T$$

$$P = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

Problems

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

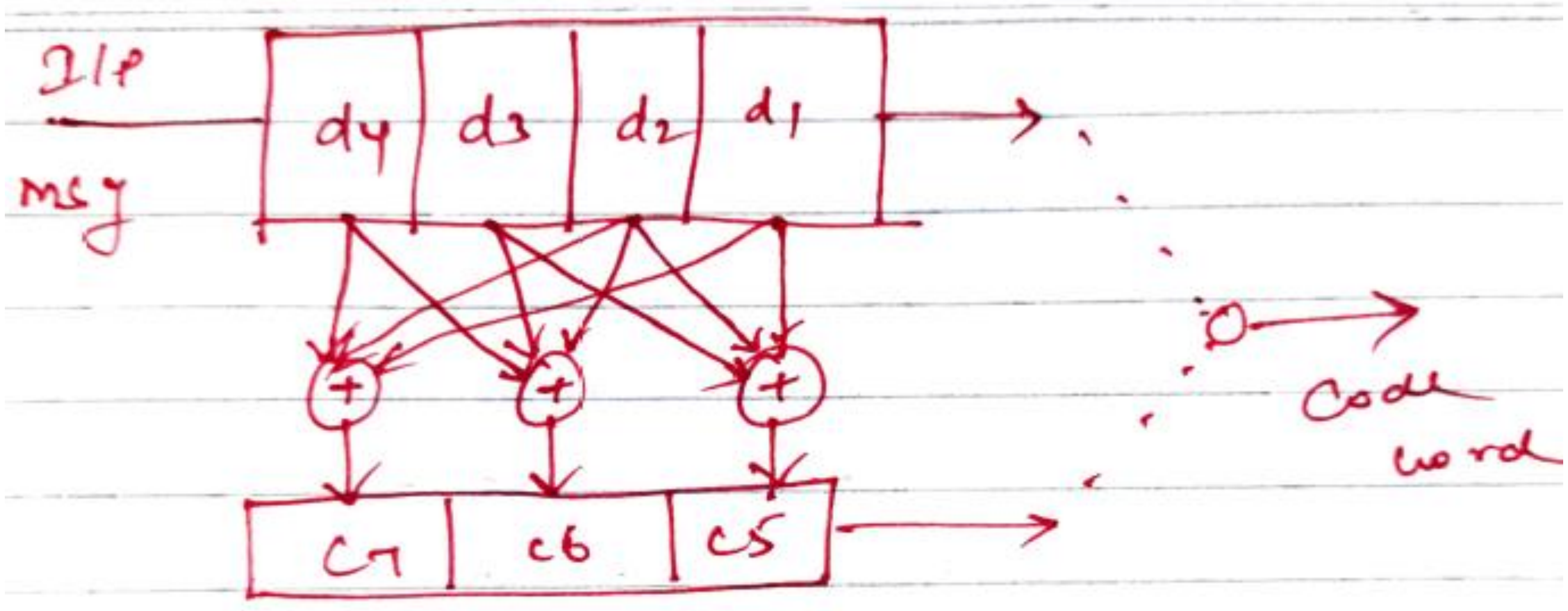
$$C = dP$$

$$\begin{bmatrix} c_5 & c_6 & c_7 \end{bmatrix} = \begin{bmatrix} d_1 & d_2 & d_3 & d_4 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

Problems

d_1	d_2	d_3	d_4	c_5	c_6	c_7	$w(c)$
0	0	0	0				
0	0	0	1				
0	0	1	0				
		⋮					
1	1	1	1				

Problems



Problems

- In a LBC, the syndrome digits are given as

$$S_1 = r_1 + r_2 + r_3 + r_5$$

$$S_2 = r_2 + r_3 + r_4 + r_6$$

$$S_3 = r_1 + r_2 + r_4 + r_7$$

- Find the H matrix and the set of codewords.
- Draw the encoder diagram.
- Determine the error detection and correction capability of the LBC.
- Calculate the syndrome for the received data 1100101.

Problems

$$S_1 = r_1 + r_2 + r_3 + r_5$$

$$S_2 = r_2 + r_3 + r_4 + r_6$$

$$S_3 = r_1 + r_2 + r_4 + r_7$$

$$S = [\,s_0 \quad s_1 \quad s_2\,] = r H^T$$

$$= (r_0, r_1, r_2, r_3, r_4, r_5, r_6)\, H^T$$

Problems

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

$$[H] = [P^T : I_{n-k}]$$

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

Problems

$$P^T = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}$$

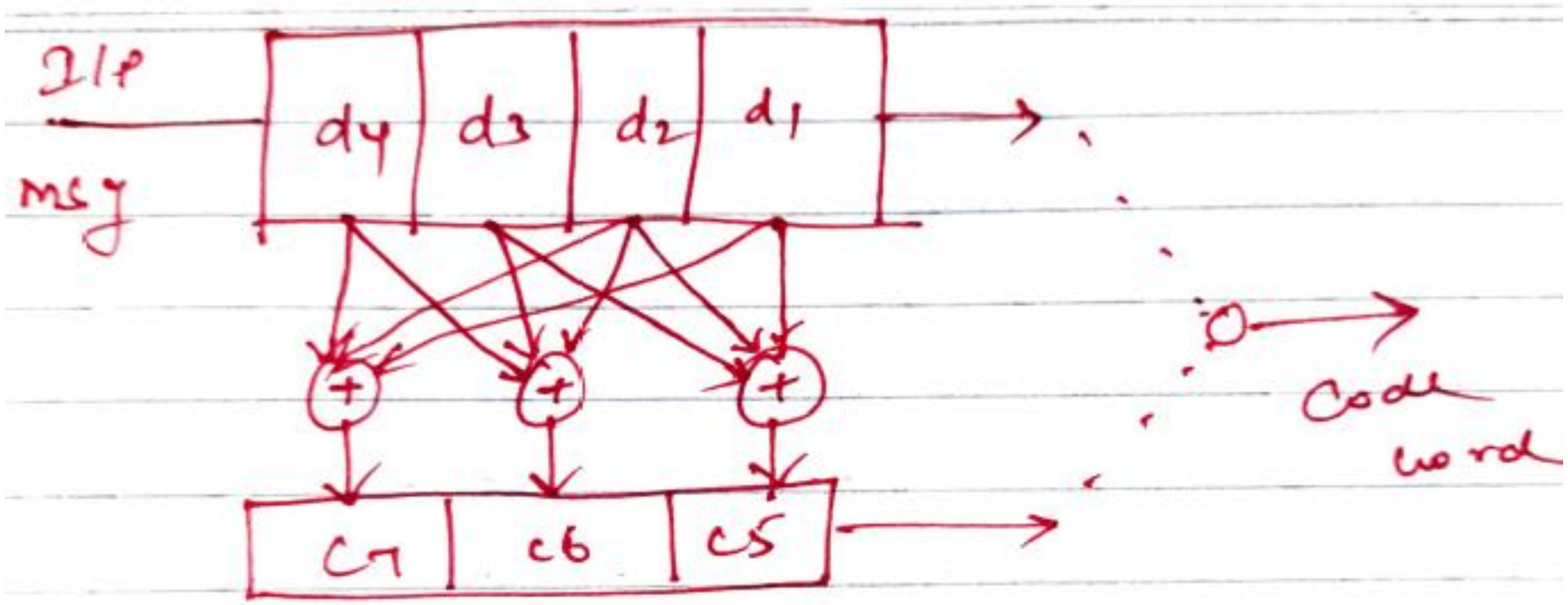
$$P = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

Problems

$$c = [d_1 \; d_2 \; d_3 \; d_4] \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

d_1	d_2	d_3	d_4	c_5	c_6	c_7	$w(c)$
0	0	0	0				
0	0	0	1				
0	0	1	0				
		⋮					
1	1	1	1				

Problems



Problems

$$s = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$$

Problems

Error is in 2^{nd} bit.

$$E = [\,0\ 1\ 0\ 0\ 0\ 0\ 0\,]$$

$$\oplus$$

$$Y = [\,1\ 1\ 0\ 0\ 1\ 0\ 1\,]$$

corrected $cw = [\,1\ 0\ 0\ 0\ 1\ 0\ 1\,]$