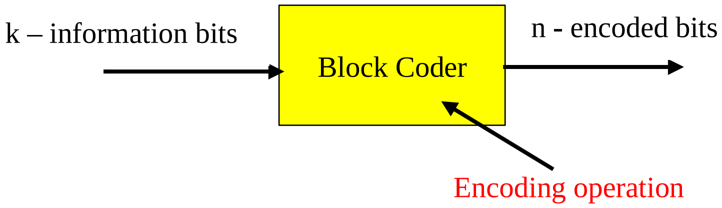
Linear Block codes

(n, k) Block codes



n-digit codeword made up of k-information digits and (n-k) redundant parity check digits. The rate or efficiency for this code is k/n.

$$Code\ efficiency\ r = \frac{k}{n} = \frac{Number\ of\ information\ bits}{Total\ number\ of\ bits\ in\ codeword}$$

Note: unlike source coding, in which data is compressed, here redundancy is deliberately added, to achieve error detection.

SYSTEMATIC BLOCK CODES

A systematic block code consists of vectors whose 1st k elements (or last k-elements) are identical to the message bits, the remaining (n-k) elements being check bits. A code vector then takes the form:

$$X = (m_0, m_1, m_2, \ldots\ldots m_{k-1}, c_0, c_1, c_2, \ldots\ldots c_{n-k})$$

Or

$$X = (c_0, c_1, c_2, \ldots\ldots c_{n-k}, m_0, m_1, m_2, \ldots\ldots m_{k-1})$$

Systematic code: information digits are explicitly transmitted together with the parity check bits. For the code to be systematic, the k-information bits must be transmitted contiguously as a block, with the parity check bits making up the code word as another contiguous block.

Information bits	Parity bits

A systematic linear block code will have a generator matrix of the form:

$$G = [P \mid I_k]$$

Systematic codewords are sometimes written so that the message bits occupy the left-hand portion of the codeword and the parity bits occupy the right-hand portion.

Parity check matrix (H)

Will enable us to decode the received vectors. For each (kxn) generator matrix G, there exists an (n-k)xn matrix H, such that rows of G are orthogonal to rows of H i.e., $GH^T = 0$, where H^T is the transpose of H. to fulfil the orthogonal requirements for a systematic code, the components of H matrix are written as:

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

In a systematic code, the 1st k-digits of a code word are the data message bits and last (n-k) digits are the parity check bits, formed by linear combinations of message bits $m_0, m_1, m_2, \ldots\ldots m_{k-1}$

It can be shown that performance of systematic block codes is identical to that of non-systematic block codes.

A codeword (X) consists of n digits $x_0, x_1, x_2, \ldots\ldots x_{n-1}$ and a data word (message word) consists of k digits $m_0, m_1, m_2, \ldots\ldots m_{k-1}$

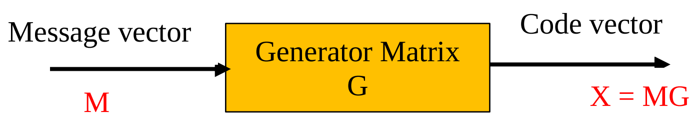
For the general case of linear block codes, all the n digits of X are formed by linear combinations (modulo-2 additions) of k message bits. A special case, where $x_0 = m_0$, $x_1 = m_1$, $x_2 = m_2 \ldots x_{k-1} = mk-1$ and the remaining digits from x_{k+1} to x_n are linear combinations of $m_0, m_1, m_2, \ldots.. m_{k-1}$ is known as a systematic code.

The codes described in this chapter are binary codes, for which the alphabet consists of symbols 0 and 1 only. The encoding and decoding functions involve the binary arithmetic operations of modulo-2 addition and multiplication.

Matrix representation of Block codes

- An (n, k) block code consists of n-bit vectors
- Each vector corresponding to a unique block of k-message bits
- There are 2^k different k-bit message blocks & 2^n possible n-bit vectors
- The fundamental strategy of block coding is to choose the 2^k code vectors such that the minimum distance is as large as possible. In error correction, distance of two words (of same length) plays a fundamental role.

Block codes in which the message bits are transmitted in unaltered form are called systematic code.



Linearity property

Linear means sum of any 2 codewords yields another codeword

A binary code is linear if and only if the modulo-2 sum of 2 codewords is also a codeword. One can check that the sum of any 2 codewords in this code is also a codeword. A desirable structure for a block code to possess is linearity, which greatly reduces the encoding complexity.

A code is said to be linear if any two codewords in the code can be added in modulo-2 arithmetic to produce a 3rd codeword in the code.

A linear block code is said to be linear provided that the sum of arbitrary two codewords is a codeword. We speak about binary coding if the code alphabet has two symbols 8421 (BCD code) is a non-linear code.
The binary arithmetic has 2 operation: **addition** and **multiplication**. The arithmetic operations of addition and multiplication are defined by the conventions of algebraic field. For example, in a binary field, the rules of addition and multiplication are as follows:

Mod-2 addition table

$0 \oplus 0 = 0$	A	B	$A \oplus B = \bar{A}\,B + A\,\bar{B}$
$0 \oplus 1 = 1$	0	0	0
$1 \oplus 0 = 1$	0	1	1
$1 \oplus 1 = 0$	1	0	1
	1	1	0

Ex-OR Logic

A	B	$A \oplus B = \bar{A}\,B + A\,\bar{B}$
0	0	0
0	1	1
1	0	1
1	1	0
If both the inputs are same, output = 0		

- The addition operation designated with $\oplus$ is same as mod-2 operation.
- $\oplus$ *represents Mod* $-$ 2 *addition*
- $\oplus$ *also represents Ex* $-$ *OR logic*
- Addition and subtraction have same meaning in modulo-2 arithmetic

modulo - 2 = mod - 2

Mod-2 subtraction table

$0 - 0 = 0$
$0 - 1 = 1$
$1 - 0 = 1$
$1 - 1 = 0$

Multiplication in modulo-2 algebra

0 . 0 = 0
0 . 1 = 1
1 . 0 = 1
1 . 1 = 0

Linear block codes are a class of parity check codes that can be characterised by the (n, k) notation. The encoder transforms a block of k-message digits (a message vector) into a longer block of n codeword digits (a code vector) constructed from a given alphabet of elements. When the alphabet consists of 2 elements (0 and 1), the code is a binary code.

k-bit messages from 2^k distinct message sequences, referred to as k-tuples (sequence of k digits). The n-bit blocks can form as many as 2^n distinct sequences referred to as n-tuples. A block code represents a one-to-one assignment.

Mathematical expressions related to block codes:

(n, k) linear block code
n = number of bits in code word
k = number of message bits
(n-k) = number of parity bits or parity check bits

N.B. parity bits are computed from message bits according to encoding rule. Encoding rule decides mathematical structure of the code.

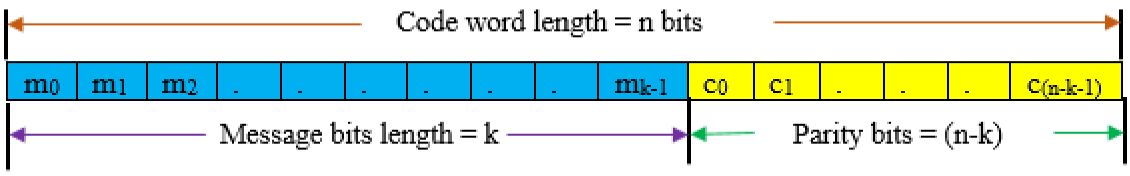
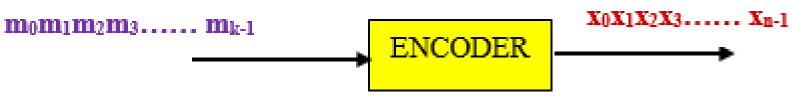


Fig: Structure of a codeword

Sequence of bits are applied to linear block code encoder to produce n-bit codeword. The elements of this codeword are: x_0, x_1, x_2, …..x_{n-1}



(n-k) parity bits are linear sums of k-message bits

The code vector can be mathematically represented as:

$$X = [M : C] \; where \; M = k \; number \; of \; message \; vectors$$

Where M = k-message vectors
C = (n-k) parity vectors

A block code generator generates the parity vectors (or parity bits) which are added to message bits to generate the codewords. Thus, code vector X can also be represented as….

$$X = [M : G] \; where \; M = k \; number \; of \; message \; vectors$$

Where

X = code vector of size **1xn**

M = message vector of size **1xk**

G = Generator matrix of size **kxn**

X can be represented in matrix form as:

$$[X]_{1xn} = [M]_{1xk} \, [G]_{kxn}$$

The generator matrix is dependent on the type of linear block code used:

$$[G] = [I_k \mid P]$$

Where I_k = kxk identity matrix
P = kx(n-k) coefficient matrix

For example, (5,3) code:

n =5, k = 3
(n-k) = (5-3) =2

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

$$P = \begin{bmatrix} p_{00} & p_{01} \\ p_{10} & p_{11} \\ p_{20} & p_{21} \end{bmatrix}$$

Now parity vector C can be computed as C = MP

$$C = [m_0 \quad m_1 \quad m_2]\begin{bmatrix} p_{00} & p_{01} \\ p_{10} & p_{11} \\ p_{20} & p_{21} \end{bmatrix}$$

Now solve for $c_0, c_1, c_2 \ldots c_{n-k}$

$$c_0 = m_0\, p_{00} \oplus m_1\, p_{10} \oplus m_2\, p_{20}$$

$$c_1 = m_0\, p_{01} \oplus m_1\, p_{11} \oplus m_2\, p_{21}$$

Similarly, we can obtain expressions for remaining parity bits if any.

Q. The generator matrix for a (6,3) block code is given below. Find all the code vectors of this code.

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

Sol. (n, k) = (6,3)

n = 6

k = 3

n – k = 6 - 3 =3 number of parity bits.

Step1:

Separate the identity matrix and coefficient matrix

Generator matrix is given by:

$$[G] = [I_k \mid P]$$

$$\therefore I_k = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}_{3x3} \qquad P = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}_{3x3}$$

(000)
(001)
(010)
(011)
(100)
(101)
(110)
(111)

As the size of message block k =3, there are 8 possible message sequences

Step 2: Obtain parity vector C = MP

$$\therefore [C] = [c_0 \quad c_1 \quad c_2] = [m_0 \quad m_1 \quad m_2]\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

$$c_0 = (m_0\,.0) \oplus (m_1\,.1) \oplus (m_2.1)$$

$$= 0 \oplus m_1 \oplus m_2$$

$$= m_1 \oplus m_2$$

Similarly,

$$c_1 = m_0 \oplus m_2$$

$$c_2 = m_0 \oplus m_1$$

For message word ($m_0\, m_1\, m_2 = 0\ 0\ 0$)

$c_0 = m_1 \oplus m_2 = 0 \oplus 0 = 0$

$c_1 = m_0 \oplus m_2 = 0 \oplus 0 = 0$

$c_2 = m_0 \oplus m_1 = 0 \oplus 0 = 0$

- $\oplus$ *represents Mod − 2 addition*
- $\oplus$ *also represents Ex − OR logic*
- Addition and subtraction have same meaning in modulo-2 arithmetic
- modulo-2 addition is the EX-OR operation in logic and modulo-2 multiplication is the AND operation.
- Binary matrix multiplication follows the usual rules with mod-2 addition instead of conventional addition.

Binary addition & multiplication:

Mod-2 addition and mod-2 multiplication on binary symbols 0 and 1. Multiplication defined same as for ordinary numbers. But for addition 1 + 1 = 0. This can be interpreted as 1 – 1 = 0 i.e., in binary computations, subtraction coincides with addition.

Mod-2 addition table

$0 \oplus 0 = 0$	A	B	$A \oplus B = \bar{A}\,B + A\,\bar{B}$
$0 \oplus 1 = 1$	0	0	0
$1 \oplus 0 = 1$	0	1	1
$1 \oplus 1 = 0$	1	0	1
	1	1	0

Ex-OR Logic

A	B	$A \oplus B = \bar{A}\,B + A\,\bar{B}$
0	0	0
0	1	1
1	0	1
1	1	0
If both the inputs are same, output = 0		

Mod-2 subtraction table

0 − 0 = 0
0 − 1 = 1
1 − 0 = 1
1 − 1 = 0

Multiplication in modulo-2 algebra

0 . 0 = 0
0 . 1 = 1
1 . 0 = 1
1 . 1 = 0

Complete codeword for message block (000)

m_0	m_1	m_2	c_0	c_1	c_2
0	0	0	0	0	0

Parity bits for message word ($m_0\, m_1\, m_2 = 0\ 0\ 1$)

$$[C] = [c_0 \quad c_1 \quad c_2] = [m_0 \quad m_1 \quad m_2] \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

$c_0 = m_1 \oplus m_2$

$c_1 = m_0 \oplus m_2$

$c_2 = m_0 \oplus m_1$

$m_0 = 0,\ m_1 = 0,\ m_2 = 1$

$c_0 = m_1 \oplus m_2 = 0 \oplus 1 = 1$

$c_1 = m_0 \oplus m_2 = 0 \oplus 1 = 1$

$c_2 = m_0 \oplus m_1 = 0 \oplus 0 = 0$

Complete codeword for message block (001)

m_0	m_1	m_2	c_0	c_1	c_2
0	0	1	1	1	0

Parity bits for message word ($m_0\ m_1\ m_2 = 0\ 1\ 0$)

$$[C] = [c_0 \quad c_1 \quad c_2] = [m_0 \quad m_1 \quad m_2] \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

$c_0 = m_1 \oplus m_2$

$c_1 = m_0 \oplus m_2$

$c_2 = m_0 \oplus m_1$

$m_0 = 0,\ m_1 = 1,\ m_2 = 0$

$c_0 = m_1 \oplus m_2 = 1 \oplus 0 = 1$

$c_1 = m_0 \oplus m_2 = 0 \oplus 0 = 0$

$c_2 = m_0 \oplus m_1 = 0 \oplus 1 = 1$

Complete codeword for message block (001)

m_0	m_1	m_2	c_0	c_1	c_2
0	1	0	1	0	1

Parity bits for message word ($m_0\ m_1\ m_2 = 0\ 1\ 1$)

$$[C] = [c_0 \quad c_1 \quad c_2] = [m_0 \quad m_1 \quad m_2] \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

$c_0 = m_1 \oplus m_2$

$c_1 = m_0 \oplus m_2$

$c_2 = m_0 \oplus m_1$

$m_0 = 0,\ m_1 = 1,\ m_2 = 1$

$c_0 = m_1 \oplus m_2 = 1 \oplus 1 = 0$

$c_1 = m_0 \oplus m_2 = 0 \oplus 1 = 1$

$c_2 = m_0 \oplus m_1 = 0 \oplus 1 = 1$

Complete codeword for message block (001)

m_0	m_1	m_2	c_0	c_1	c_2
0	1	1	0	1	1

Parity bits for message word ($m_0\, m_1\, m_2$ = 1 0 0)

$$[C] = [c_0 \quad c_1 \quad c_2] = [m_0 \quad m_1 \quad m_2] \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

$c_0 = m_1 \oplus m_2$

$c_1 = m_0 \oplus m_2$

$c_2 = m_0 \oplus m_1$

$m_0 = 1, \ m_1 = 0, \ m_2 = 0$

$c_0 = m_1 \oplus m_2 = 0 \oplus 0 = 0$

$c_1 = m_0 \oplus m_2 = 1 \oplus 0 = 1$

$c_2 = m_0 \oplus m_1 = 1 \oplus 0 = 1$

Complete codeword for message block (100)

m_0	m_1	m_2	c_0	c_1	c_2
1	0	0	0	1	1

Parity bits for message word ($m_0\, m_1\, m_2$ = 1 0 1)

$$[C] = [c_0 \quad c_1 \quad c_2] = [m_0 \quad m_1 \quad m_2] \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

$c_0 = m_1 \oplus m_2$

$c_1 = m_0 \oplus m_2$

$c_2 = m_0 \oplus m_1$

$m_0 = 1, \ m_1 = 0, \ m_2 = 1$

$c_0 = m_1 \oplus m_2 = 0 \oplus 1 = 1$

$c_1 = m_0 \oplus m_2 = 1 \oplus 1 = 0$

$c_2 = m_0 \oplus m_1 = 1 \oplus 0 = 1$

Complete codeword for message block (001)

m_0	m_1	m_2	c_0	c_1	c_2
1	0	1	1	0	1

Parity bits for message word ($m_0\, m_1\, m_2$ = 1 1 0)

$$[C] = [c_0 \quad c_1 \quad c_2] = [m_0 \quad m_1 \quad m_2] \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

$c_0 = m_1 \oplus m_2$

$c_1 = m_0 \oplus m_2$

$c_2 = m_0 \oplus m_1$

$m_0 = 1, \ m_1 = 1, \ m_2 = 0$

$c_0 = m_1 \oplus m_2 = 1 \oplus 0 = 1$

$c_1 = m_0 \oplus m_2 = 1 \oplus 0 = 1$

$c_2 = m_0 \oplus m_1 = 1 \oplus 1 = 0$

Complete codeword for message block (001)

m_0	m_1	m_2	c_0	c_1	c_2
1	1	0	1	1	0

Parity bits for message word ($m_0\, m_1\, m_2$ = 1 1 1)

$$[C] = [c_0 \quad c_1 \quad c_2] = [m_0 \quad m_1 \quad m_2] \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

$c_0 = m_1 \oplus m_2$

$c_1 = m_0 \oplus m_2$

$c_2 = m_0 \oplus m_1$

$m_0 = 1, \quad m_1 = 1, \;\; m_2 = 1$

$c_0 = m_1 \oplus m_2 = 1 \oplus 1 = 0$

$c_1 = m_0 \oplus m_2 = 1 \oplus 1 = 0$

$c_2 = m_0 \oplus m_1 = 1 \oplus 1 = 0$

Complete codeword for message block (111)

m_0	m_1	m_2	c_0	c_1	c_2
1	1	1	0	0	0

Code vectors for (6,3) linear block code

S.No.	Message vectors	Parity bits	Code vectors
1	000	000	000000
2	001	110	001110
3	010	101	010101
4	011	011	011011
5	100	011	100011
6	101	101	101101
7	110	110	110110
8	111	000	111000

Q. Check linearity of above (6,3) code

Add codewords at S.No. 2 & 3

0	0	1	1	1	0
$\oplus$	Mod-2 addition				
0	1	0	1	0	1
= 0	1	1	0	1	1

This codeword exists at S.No. 4

Add codewords at S.No. 7 & 8

1	1	0	1	1	0
$\oplus$	Mod-2 addition				
1	1	1	0	0	0
= 0	0	1	1	1	0

This codeword exists at S.No. 2

Add codewords at S.No. 5 & 8

1	0	0	0	1	1
⊕	Mod-2 addition				
1	1	1	0	0	0
= 0	1	1	0	1	1

This codeword exists at S.No. 4

Add codewords at S.No. 1 & 5

0	0	0	0	0	0
⊕	Mod-2 addition				
1	0	0	0	1	1
= 1	0	0	0	1	1

This codeword exists at S.No. 5

Similarly, we can verify addition of any 2 code vectors, which gives another code vector in the code. So, (6,3) block code is a linear code.

Q. The parity check matrix of a particular (7,4) linear block code is given by:

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

i. Find the generator matrix
ii. List all the codewords
iii. What is the minimum distance between the code vectors?
iv. How many errors can be detected? How many errors can be corrected?

Sol.

We know that $[H] = [P^T \mid I_{n-k}]$

Where, P^T $is\ (n-k)xk\ matrix\ and\ I_{n-k}\ is\ (n-k)x(n-k) identity\ matrix$

(n, k) = (7, 4)
n = 7, k = 4
(n-k) = (7 – 4) = 3

∴ P^T $is\ 3x4\ matrix\ and\ I_{n-k}\ is\ 3x3\ identity\ matrix$

Separate, P^T and I matrices

$$H = \left[\underbrace{\begin{matrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{matrix}}_{P^T_{3x4}} \;\vdots\; \underbrace{\begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix}}_{I_{3x3}} \right]$$

$$\therefore P^T = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}_{3x4} \quad and \quad P = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}_{4x3}$$

$\boldsymbol{Generator\ matrix\ [G] = \ [I_k \mid P]}$

Where I_k = kxk identity matrix

P = kx(n-k) coefficient matrix

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

0000
0001
0010
0011
0100
0101
0110
0111
1000
1001
1010
1011
1100
1101
1110
1111

As the size of message block k =4, there are $2^4 = 16$ possible message sequences

Step 2: obtain parity vector C = MP

$$\therefore [C] = [c_0 \quad c_1 \quad c_2] = [m_0 \quad m_1 \quad m_2 \quad m_3] \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

$$\begin{aligned} c_0 &= (m_0 .1) \oplus (m_1 .1) \oplus (m_2 .1) \oplus (m_3 .0) \\ &= m_0 \oplus m_1 \oplus m_2 \oplus 0 \\ &= m_0 \oplus m_1 \oplus m_2 \end{aligned}$$

Similarly,

$$\begin{aligned} c_1 &= (m_0 .1) \oplus (m_1 .1) \oplus (m_2 .0) \oplus (m_3 .1) \\ &= m_0 \oplus m_1 \oplus 0 \oplus m_3 \\ &= m_0 \oplus m_1 \oplus m_3 \end{aligned}$$

$$\begin{aligned} c_2 &= (m_0 .1) \oplus (m_1 .0) \oplus (m_2 .1) \oplus (m_3 .1) \\ &= m_0 \oplus 0 \oplus m_2 \oplus m_3 \\ &= m_0 \oplus m_2 \oplus m_3 \end{aligned}$$

Parity bits for message word ($m_0\, m_1\, m_2\, m_3 = 0\ 1\ 1\ 1$)

$c_0 = m_0 \oplus m_1 \oplus m_2$

$c_1 = m_0 \oplus m_1 \oplus m_3$

$c_2 = m_0 \oplus m_2 \oplus m_3$

$m_0 = 0, \quad m_1 = 1, \quad m_2 = 1, \quad m_3 = 1$

$c_0 = m_0 \oplus m_1 \oplus m_2 = 0 + 1 + 1 = 0$

$c_1 = m_0 \oplus m_1 \oplus m_3 = 0 + 1 + 1 = 0$

$c_2 = m_0 \oplus m_2 \oplus m_3 = 0 + 1 + 1 = 0$

Complete codeword for message block (001)

m_0	m_1	m_2	m_3	c_0	c_1	c_2
0	1	1	1	0	0	0

Similarly, find all parity vectors. The complete code of (7,4) linear code is given below.

S.No.	Message bits	Parity bits	Codeword X	Weight of the code vector
1	0000	000	0000 000	0
2	0001	011	0001 011	3
3	0010	101	0010 101	3
4	0011	110	0011 110	4
5	0100	110	0100 110	3
6	0101	101	0101 101	4
7	0110	011	0110 011	4
8	0111	000	0111 000	3
9	1000	111	1000 111	4
10	1001	100	1001 100	3
11	1010	010	1010 010	3
12	1011	001	1011 001	4
13	1100	001	1100 001	3
14	1101	010	1101 010	4
15	1110	100	1110 100	4
16	1111	111	1111 111	7

(iii). Minimum distance d_{min} = minimum weight of any non-zero code vector = 3 (see from table)

$$\therefore\ d_{min} = 3$$

Weight of the code vector
0
3
3
4
3
4
4
3
4
3
3
4
3
4
4
7

d_{min}: Minimum distance of a linear block code = the smallest non-zero vector weight

Number of errors that can be detected

$$d_{min} \geq s + 1$$
$$3 \geq s + 1$$
$$2 \geq s$$
$$s \leq 2$$
$$\therefore\ maximum\ errors\ that\ can\ be\ detected = 2$$

(iv). Number of errors that can be corrected is given by

$$d_{min} \geq 2t + 1$$
$$3 \geq 2t + 1$$
$$2 \geq 2t$$
$$t \leq 1$$

$$\therefore\ maximum\ errors\ that\ can\ be\ corrected = 1$$

$$\therefore\ for\ (7,4) linear\ block\ code, at\ the\ most\ 2\ errors\ can\ be\ detected\ and\ only\ 1\ error\ can\ be\ corrected.$$

Q. For a (6, 3) systematic linear block code, the codeword comprises m0m1m2p0p1p2 where the 3 parity check bits p0p1p2 are formed from the information bits as follows:

$c_0 = m_0 \oplus m_1$ $\quad$ $c_1 = m_0 \oplus m_2$ $\quad$ $c_2 = m_1 \oplus m_2$

Find

i. The parity check matrix
ii. The generator matrix
iii. All possible codewords
iv. The minimum weight
v. Minimum distance
vi. Error detecting & correcting capability of this code
vii. If the received sequence is 101000, calculate the syndrome and decode the received sequence

Sol.

Message bits			Parity bits			Codeword X	Weight W(X)
m_0	m_1	m_2	p_0	p_1	p_2		
0	0	0	0	0	0	00 00 00	0
0	0	1	0	1	1	00 10 11	3
0	1	0	1	0	1	01 01 01	3
0	1	1	1	1	0	01 11 10	4
1	0	0	1	1	0	10 01 10	3
1	0	1	1	0	1	10 11 01	4
1	1	0	0	1	0	11 00 10	4
1	1	1	0	0	0	11 10 00	3

Given parity equations are:

$c_0 = m_0 \oplus m_1$ $\quad$ $c_1 = m_0 \oplus m_2$ $\quad$ $c_2 = m_1 \oplus m_2$

$Hence\ parity\ vector\ C = (c_0, c_1, c_2)$

$For\ data\ word\ (000) \Rightarrow C = (0 \oplus 0,\quad 0 \oplus 0,\quad 0 \oplus 0) = (0\ 0\ 0)$

$For\ data\ word\ (001) \Rightarrow C = (0 \oplus 0,\quad 0 \oplus 1,\quad 0 \oplus 1) = (0\ 1\ 1)$

$For\ data\ word\ (010) \Rightarrow C = (0 \oplus 1,\quad 0 \oplus 0,\quad 1 \oplus 0) = (1\ 0\ 1)$

$For\ data\ word\ (011) \Rightarrow C = (0 \oplus 1,\quad 0 \oplus 1,\quad 1 \oplus 1) = (0\ 0\ 0)$

$For\ data\ word\ (100) \Rightarrow C = (1 \oplus 0,\quad 1 \oplus 0,\quad 0 \oplus 0) = (1\ 1\ 0)$

$For\ data\ word\ (101) \Rightarrow C = (1 \oplus 0,\quad 1 \oplus 1,\quad 0 \oplus 1) = (1\ 0\ 1)$

$For\ data\ word\ (110) \Rightarrow C = (1 \oplus 1,\quad 1 \oplus 0,\quad 1 \oplus 0) = (0\ 1\ 1)$

$For\ data\ word\ (111) \Rightarrow C = (1 \oplus 1,\quad 1 \oplus 1,\quad 1 \oplus 1) = (0\ 0\ 0)$

Weight W(X)
0
3
3
4
3
4
4
3

From all these values, minimum is 3. So, minimum weight of the code is 3.

(i). Parity check matrix H

$(6,3)\ code\ given. \quad \therefore \quad n = 6, k = 3\ and\ (n-k) = 3$

$Mesage\ vector\ M = [M]_{1x3} = [m_0 \quad m_1 \quad m_2]_{1x3}$

$Coefficient\ matrix\ P = [P]_{kx(n-k)} = [P]_{3x3} = \begin{bmatrix} p_{00} & p_{01} & p_{02} \\ p_{10} & p_{11} & p_{12} \\ p_{20} & p_{21} & p_{22} \end{bmatrix}_{3x3}$

$$C = MP = [m_0 \quad m_1 \quad m_2] \begin{bmatrix} p_{00} & p_{01} & p_{02} \\ p_{10} & p_{11} & p_{12} \\ p_{20} & p_{21} & p_{22} \end{bmatrix}$$

$$\Rightarrow [\underbrace{m_0\, p_{00} \oplus m_1\, p_{10} \oplus m_2\, p_{20}}_{c_0}, \quad \underbrace{m_0\, p_{01} \oplus m_1\, p_{11} \oplus m_2\, p_{21}}_{c_1}, \quad \underbrace{m_0\, p_{02} \oplus m_1\, p_{12} \oplus m_2\, p_{22}}_{c_2}]$$

$$c_0 = m_0\, p_{00} \oplus m_1\, p_{10} \oplus m_2\, p_{20}$$
$$c_1 = m_0\, p_{01} \oplus m_1\, p_{11} \oplus m_2\, p_{21}$$
$$c_2 = m_0\, p_{02} \oplus m_1\, p_{12} \oplus m_2\, p_{22}$$

Compare these equations with given parity equations & find coefficients

$$c_0 = m_0 \oplus m_1$$
$$c_1 = m_0 \oplus m_2$$
$$c_2 = m_1 \oplus m_2$$

$$\begin{aligned} & p_{00} = 1 \quad p_{10} = 1 \quad p_{20} = 0 \\ \therefore\ & p_{01} = 1 \quad p_{11} = 0 \quad p_{21} = 1 \\ & p_{02} = 0 \quad p_{12} = 1 \quad p_{22} = 1 \end{aligned}$$

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

We know parity-check matrix H = $[P^T \mid I_{n-k}]$

$P^T = transpose\ of\ matrix\ P = [P^T]_{(n-k)xk}$

$\therefore P^T = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$ & $I_{n-k} = [I]_{(n-k)x(n-k)} = [I]_{3x3} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

$$\therefore \text{parity} - \text{check matrix H} = \left[P^T \mid I_{n-k}\right] = \left[\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right]$$

P^T I

(ii).

$$Generaotor\ matrix\ G = [I\,|P] = \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right]$$

(iii). All possible codewords

Message bits			Parity bits			Codeword X	Weight W(X)
m_0	m_1	m_2	p_0	p_1	p_2		
0	0	0	0	0	0	00 00 00	0
0	0	1	0	1	1	00 10 11	3
0	1	0	1	0	1	01 01 01	3
0	1	1	1	1	0	01 11 10	4
1	0	0	1	1	0	10 01 10	3
1	0	1	1	0	1	10 11 01	4
1	1	0	0	1	0	11 00 10	4
1	1	1	0	0	0	11 10 00	3

(iv). Minimum weight & Minimum distance d_{min} = 3 (See from above table)

d_{min}: Minimum distance of a linear block code = the smallest non-zero vector weight

(vi). Error detecting & correcting capability of this code

Error detection: s = number of errors that can be detected

$$d_{min} \geq s+1 \Rightarrow 3 \geq s+1 \Rightarrow 2 \geq s \Rightarrow s \leq 2$$

Error correction: t = number of errors that can be corrected

$$d_{min} \geq 2t+1 \Rightarrow 3 \geq 2t+1 \Rightarrow 2t \leq 2 \Rightarrow t \leq 1$$

Comment: Double error correction and single error detection

vii. If the received sequence is 101000, calculate the syndrome and decode the received sequence

Let received word Y = 10 10 00

$$\text{Syndrome } S = [YH^T] = [1 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0]\begin{bmatrix}1 & 1 & 0\\1 & 0 & 1\\0 & 1 & 1\\1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix}$$

$$\Rightarrow [1+0+0+0+0+0, \quad 1+0+1+0+0+0, \quad 0+0+1+0+0+0]$$

$$\Rightarrow [1, 0, 1]$$

For (101) syndrome, error pattern E = 010000 (see from look-up decoding table)

(6,3) decoding look-up table

To find syndrome, we need to find Error vector (E). now write various error vectors. Various error vectors with single bit errors are shown below:

S. No.	Error vector	Bit in Error	Syndrome vector (S)
1	**1** 0 0 0 0 0	1st	1 1 0
2	0 **1** 0 0 0 0	2nd	1 0 1
3	0 0 **1** 0 0 0	3rd	Similarly, find remaining syndromes
4	0 0 0 **1** 0 0	4th	
5	0 0 0 0 **1** 0	5th	
6	0 0 0 0 0 **1**	6th	

$$For\ (6,3)\ code, \qquad n = 6, k = 3\ and\ (n-k) = 3$$

Now find syndrome corresponding to each error vector

$$[S_1] = EH^T = [1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0]\begin{bmatrix}1 & 1 & 0\\1 & 0 & 1\\0 & 1 & 1\\1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix} = [1 \;\; 1 \;\; 0]$$

$$\Rightarrow this\ is\ the\ syndrome\ for\ the\ first\ bit\ in\ error$$

$$[S_2] = EH^T = [0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0]\begin{bmatrix}1 & 1 & 0\\1 & 0 & 1\\0 & 1 & 1\\1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix} = [1 \;\; 0 \;\; 1]$$

$$\Rightarrow this\ is\ the\ syndrome\ for\ the\ 2nd\ bit\ in\ error$$

We know that $X = Y \oplus E \Rightarrow 101\,000 \oplus 010\,000 = 111\,000$
X = transmitted codeword

Q. Finding parity check matrix (H) from P (check bit equations). P = Parity matrix or coefficient matrix

$c_0 = m_0 \oplus m_1$ $\quad$ $c_1 = m_0 \oplus m_2$ $\quad$ $c_2 = m_1 \oplus m_2$

$(6{,}3)\ code\ given. \quad \therefore \quad n = 6, k = 3\ and\ (n-k) = 3$

m_0, m_1, m_2 = message bits

$Mesage\ vector\ M = [M]_{1x3} = [m_0 \quad m_1 \quad m_2]_{1x3}$

$$Coefficient\ matrix\ P = [P]_{kx(n-k)} = [P]_{3x3} = \begin{bmatrix} p_{00} & p_{01} & p_{02} \\ p_{10} & p_{11} & p_{12} \\ p_{20} & p_{21} & p_{22} \end{bmatrix}_{3x3}$$

$$C = MP = [m_0 \quad m_1 \quad m_2] \begin{bmatrix} p_{00} & p_{01} & p_{02} \\ p_{10} & p_{11} & p_{12} \\ p_{20} & p_{21} & p_{22} \end{bmatrix}$$

$$\Rightarrow [\underbrace{m_0 p_{00} \oplus m_1 p_{10} \oplus m_2 p_{20}}_{c_0}, \quad \underbrace{m_0 p_{01} \oplus m_1 p_{11} \oplus m_2 p_{21}}_{c_1}, \quad \underbrace{m_0 p_{02} \oplus m_1 p_{12} \oplus m_2 p_{22}}_{c_2}]$$

$$c_0 = m_0 p_{00} \oplus m_1 p_{10} \oplus m_2 p_{20}$$
$$c_1 = m_0 p_{01} \oplus m_1 p_{11} \oplus m_2 p_{21}$$
$$c_2 = m_0 p_{02} \oplus m_1 p_{12} \oplus m_2 p_{22}$$

Compare these equations with given parity equations & find coefficients

$$c_0 = m_0 \oplus m_1$$
$$c_1 = m_0 \oplus m_2$$
$$c_2 = m_1 \oplus m_2$$

$$\begin{matrix} & p_{00} = 1 & p_{10} = 1 & p_{20} = 0 \\ \therefore & p_{01} = 1 & p_{11} = 0 & p_{21} = 1 \\ & p_{02} = 0 & p_{12} = 1 & p_{22} = 1 \end{matrix}$$

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

We know parity-check matrix H = $[P^T \mid I_{n-k}]$

$P^T = transpose\ of\ matrix\ P = [P^T]_{(n-k)xk}$

$$\therefore P^T = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \quad \& \quad I_{n-k} = [I]_{(n-k)x(n-k)} = [I]_{3x3} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\therefore \text{ parity} - \text{check matrix H} = [P^T \mid I_{n-k}] = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Note: If we know H, we can find G and vice-versa

Hamming codes

Binary single error correcting perfect codes are called Hamming codes. Consider (n, k) linear block code that has following parameters:

- Block length $n = 2^q - 1$
- Number of message bits $k = 2^q - q - 1$
- Number of parity bits $q = (n-k)$
- Where $q \geq 3$. This code is called Hamming code.

Hamming codes are linear block codes. The (n, k) hamming codes for $q \geq 3$ is defined as

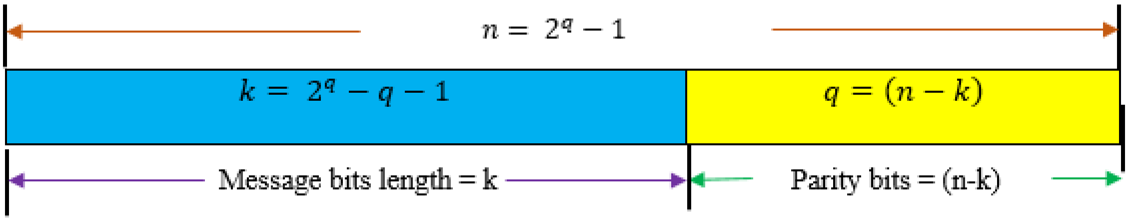
$$n = 2^q - 1$$
$$k = 2^q - q - 1$$

$p = (n-k) = q, where\ q \geq 3\ i.e., minimum\ number\ of\ parity\ bits = 3$

$d_{min} = minimum\ distance = 3$

$code\ rate\ or\ code\ efficiency, r = \frac{k}{n} = \frac{2^q - q - 1}{2^q - 1} = 1 - \frac{q}{2^q - 1}$

$error\ correction\ capability, t = 1$



Structure of a codeword

n = codeword length
k = message bits
q = number of parity bits

Hamming codes have a minimum distance of 3 and hence are capable of correcting ingle errors. Hamming codes are perfect codes and can be easily decoded using a table look-up scheme. Hamming codes have been widely used for error control in digital communications and data storage systems over the years owing to their high rates and decoding simplicity.

Error control capability: perfect codes for correcting **single** errors. Note that single errors are more probable than double errors

- In error correction, distance of two words (of same length) plays a fundamental role.

- Hamming codes are single error correcting binary perfect codes. A code corrects t errors if and only if its minimum distance (d_{min}) is greater than 2t.

- Error correction is more demanding than error detection. For example, a code with d_{min} = 4 corrects single errors only, but it detects triple errors.

A Hamming code is an (n, k) linear block code with $q \geq 3$ parity bits (check bits) and
$n = 2^q-1$, $k = (n-q) = 2^q-1-q$

Code rate, $r = \frac{k}{n}\ r \cong 1, if\ q \gg 1$

Independent of q, the minimum distance is fixed at $d_{min} = 3$. So, a Hamming code can be used for single-error correction or double error detection.

1. Detects **S** errors if and only if its minimum weight $d_{min} \geq s+1 \Rightarrow 3 \geq s+1$
   $s \leq 2 \Rightarrow Double\ error\ detection$

2. Corrects t errors if and only if its minimum weight $d_{min} \geq 2t+1 \Rightarrow 3 \geq 2t+1$
   a. $\Rightarrow 2 \geq 2t$
   2. $\Rightarrow 1 \geq t$
   $t \leq 1 \Rightarrow single-bit\ correction$

Hamming bound

Let n & k has actual meaning and having error correcting capability t. there is an upper bound on the performance of block codes which is given by:

$$2^k \leq \frac{2^n}{1+n+\ nC_2 +\ nC_3 \dots\dots.+nC_t}\ Or\ \mathbf{2^q \geq \sum_{i=0}^{t} nC_i}$$

Perfect codes

Hamming bound: $\mathbf{2^q \geq \sum_{i=0}^{t} nC_i}$

q = (n-k) = number of parity check bits

A code for which the inequalities in above equation become equalities is known as the perfect code.

$$\mathbf{2^q = \sum_{i=0}^{t} nC_i}$$

The above inequality is known as Hamming bound. It is necessary, but not sufficient condition to construct **t**-error correcting code of n-digits. For single-error correcting codes, it is necessary and sufficient condition.

Single error correcting codes, t = 1 ex. (3, 1) and (4, 1)

double error correcting codes, t = 2 ex. (10, 4) and (15, 8)

triple error correcting codes, t = 3 ex. (10, 2) and (15, 5)

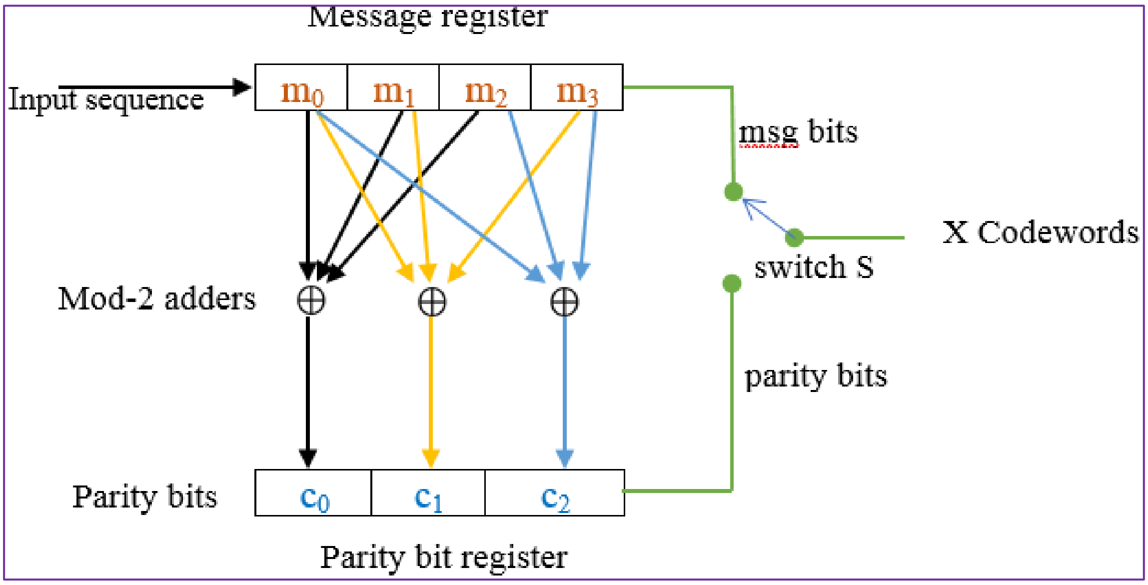
Encoder for (7, 4) linear block code

Parity bit equations for (7,4) Hamming code can be obtained as follows:

$c_0 = m_0 \oplus m_1 \oplus m_2$

$c_1 = m_0 \oplus m_1 \oplus m_3$

$c_2 = m_0 \oplus m_2 \oplus m_3$



Depicts an encoder that carries out the check bit calculations for (7,4) Hamming code. Each block of message bits is loaded into a message register. The cells of message register are connected to Ex-OR gates, whose output equal the check bits. The check bits are stored in another register and shifted out to the transmitter; the cycle then repeats with the next block of message bits.

The parity bits are obtained from message bits by means of mod-2 adders. The output switch S is connected to message register to transmit all the message bits in a codeword. Then it is connected to parity register to transmit the corresponding parity bits. Thus, we get 7-bit codeword at the output of the switch.

Decoding of Block codes

Syndrome

An important piece of information about the error pattern which we can derive directly from the received word is the syndrome.

The generator matrix G is used in the encoding operation at the transmitter. On the other hand, parity-check matrix H is used in the decoding operation at the receiver.

E = error vector = Error pattern

- Syndrome depends only on the error pattern and not on the transmitted codeword.

- $S = EH^T$

- The minimum distance d_{min} of a linear block code is defined as the smallest Hamming distance between any pair of code vectors in the code.

- The sum (or difference) of 2 code vectors is another code vector

- Minimum distance of a linear block code is the smallest Hamming weight of the non-zero code vectors in the code.
- d_{min} is an important parameter of the code. It determines the error correcting capabilities of the code.

Q. Syndrome calculation

The parity check matrix of a (7, 4) Hamming code is as under. Calculate syndrome vector for single bit errors.

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

Sol.

$$Syndrome\ vector\ [S] = [E]_{1x7}[H^T]_{7x3}$$

$$\therefore\ size\ of\ syndrome\ vector = 1x3\ \Rightarrow\ [S]_{1x3}$$

To find syndrome, we need to find Error vector (E). now write various error vectors. Various error vectors with single bit errors are shown below:

S. No.	Error vector	Bit in Error	Syndrome vector (S)
1	**1** 0 0 0 0 0 0	1^{st}	1 1 1
2	0 **1** 0 0 0 0 0	2^{nd}	1 0 0
3	0 0 **1** 0 0 0 0	3^{rd}	1 1 0
4	0 0 0 **1** 0 0 0	4^{th}	1 0 1
5	0 0 0 0 **1** 0 0	5^{th}	0 1 1
6	0 0 0 0 0 **1** 0	6^{th}	1 0 0
7	0 0 0 0 0 0 **1**	7^{th}	0 1 1

Now find syndrome corresponding to each error vector

$$[S_1] = EH^T = [1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0]\begin{bmatrix}1 & 1 & 1\\1 & 1 & 0\\0 & 1 & 1\\1 & 0 & 1\\1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix} = [1 \;\; 1 \;\; 1]$$

$$\Rightarrow this\ is\ the\ syndrome\ for\ the\ first\ bit\ in\ error$$

$$[S_2] = EH^T = [0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0]\begin{bmatrix}1 & 1 & 1\\1 & 1 & 0\\0 & 1 & 1\\1 & 0 & 1\\1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix} = [1 \;\; 0 \;\; 0]$$

$$\Rightarrow this\ is\ the\ syndrome\ for\ the\ 2nd\ bit\ in\ error$$

$$[S_3] = EH^T = [0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0]\begin{bmatrix}1 & 1 & 1\\1 & 1 & 0\\0 & 1 & 1\\1 & 0 & 1\\1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix} = [1 \;\; 0 \;\; 1]$$

$$\Rightarrow this\ is\ the\ syndrome\ for\ the\ 3rd\ bit\ in\ error$$

\

$$[S_4] = EH^T = [0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0]\begin{bmatrix}1 & 1 & 1\\1 & 1 & 0\\0 & 1 & 1\\1 & 0 & 1\\1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix} = [0 \;\; 1 \;\; 1]$$

$$\Rightarrow this\ is\ the\ syndrome\ for\ the\ 4th\ bit\ in\ error$$

$$[S_5] = EH^T = [0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0]\begin{bmatrix}1 & 1 & 1\\1 & 1 & 0\\0 & 1 & 1\\1 & 0 & 1\\1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix} = [1 \;\; 0 \;\; 0]$$

$$\Rightarrow this\ is\ the\ syndrome\ for\ the\ 5th\ bit\ in\ error$$

$$[S_6] = EH^T = [1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0] \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = [0 \ 1 \ 0]$$

$$\Rightarrow this\ is\ the\ syndrome\ for\ the\ 6th\ bit\ in\ error$$

$$[S_7] = EH^T = [1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0] \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = [0 \ 1 \ 1]$$

$$\Rightarrow this\ is\ the\ syndrome\ for\ the\ 7th\ bit\ in\ error$$

Syndrome decoding of block codes

We have seen encoder for block codes. Now we can look into decoder. Two important functions of decoder are:

- Error detection in received codeword
- Error correction

The decoding of linear block codes is done by using a special technique called syndrome decoding. This kind reduces the memory requirement of the decoder to a great extent.

Step1:

Practical assumptions:

Let X = transmitted codeword

Y = received codeword

If X = Y, no errors in the received signal if $X \neq Y$, then some errors are present.

The decoder detects or corrects errors in Y by looking at stored information about the code.
Information about the code are stored in Look-up table.

A direct way of performing error detection is to compare Y with every vector in the code. This method requires storing all 2^k code vectors at the receiver and performing up to 2^k comparisons. Note that efficient codes generally have large value of k, which implies expensive decoding hardware.

$Ex: To\ get\ code\ efficiency\ r\ \geq 0.8, we\ need\ q\ \geq 5\ (with\ Hamming\ code)$

Then r = k/n
q = 5, n = 2^5-1 = 31
k = 2^5 – 5 - 1 = 26

$$\therefore\ 2^k =\ 2^{26} code\ vectors\ to\ be\ stored\ at\ receiver, which\ is\ 10^9\ bits\ approximately.$$

Step 2: Detection of errors

(i). We know H = Parity check matrix

We know that $[H] = [P^T \mid I_{n-k}]$

Where, $P^T\ is\ (n-k)xk\ matrix\ and\ I_{n-k}\ is\ (n-k)x(n-k) identity\ matrix$

P = Coefficient matrix

(ii). Transpose of H exhibits a very important property:

$$XH^T = (000 \ldots..0)$$

i.e., product of any code vector X and the transpose of the parity check matrix will always be zero. We shall use this property for the detection of errors in the received codeword as under:

$if\ YH^T = (000 \ldots..0), the\ Y = X\ i.e., there\ is\ no\ error$

$But, XY \neq (000 \ldots..0), then\ Y \neq X\ i.e., error\ exists\ in\ the\ received\ codeword.$

Step 3: Dyndrome & its use for Error Detection

Syndrome is represented by

$S = YH^T$ or $[S]_{1x(n-k)} = [Y]_{1xn}\ [H^T]_{nx(n-k)}$

The syndrome is defined as the non-zero output of the product YH^T. Thus, the non-zero syndrome represents the presence of errors in the received codeword.

- All zero elements of syndrome represent there is no error
- Now zero value of an element in syndrome represents the presence of error
- Non-zero value of an element in syndrome represents the presence of error.

Note: Sometimes, even if all the syndrome elements have zero value, the error exists.

Step 4:

Let X and Y are transmitted and received codewords respectively. Let us define n-bit error vector E such that its non-zero elements represent the location of errors in the received codeword Y as shown below:

Transmitted Code word X	0	0	1	1	1	1	0
Received Code word Y	**1**	0	**0**	1	**0**	1	0
Error vector E	**1**	0	**1**	0	**1**	0	0

Bits in red color represent Errors

Non-zero elements of E vector represent the locations of errors in the received codeword Y.

The elements in the code vector Y can be obtained as follows:

$$Y = X \oplus E \Rightarrow X\ Ex-OR\ E \Rightarrow X\ mod-2\ E$$

$$\therefore Y = X \oplus E = [0 \oplus 1, 0 \oplus 0, 1 \oplus 1, 1 \oplus 0, 1 \oplus 1, 1 \oplus 0, 0 \oplus 0]$$

$$= [1, 0, 0, 1, 0, 1, 0]$$

The principle of mod-2 addition can be applied in a slightly different way

$$X = Y \oplus E \Rightarrow X = [0, 0, 1, 1, 1, 1, 0]$$

Relation between syndrome (S) & Error vector €

We know $S = YH^T$ & $Y = X \oplus E$

$$\begin{aligned} &= (X \oplus E)H^T \\ &= XH^T + EH^T \qquad \textit{since } XH^T = 0 \\ &= 0 \oplus EH^T \\ &= EH^T \end{aligned}$$

$$\therefore S = EH^T$$

Q. For a code vector X = (0111000) and the parity check matrix given below prove that

$$XH^T = (0,0,0 \ldots..0)$$

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

Sol.

For a valid codeword, the product

$$XH^T = [000]$$

$$XH^T = (0,0,0)$$

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

$$XH^T = [0 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0] \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

$$= [0.1 + 1.1 + 1.1 + 1.0 + 0.1 + 0.0 + 0.0 \quad 0.1 + 1.1 + 1.0 + 1.1 + 0.0 + 0.1 + 0.1 \quad 0.1 + 1.0 + 1.1 + 1.1 + 0.0 + 0.0 + 0.1]$$

$$= [0+1+1+0+0+0+0 \quad 0+1+0+1+0+0+0 \quad 0+0+1+1+0+0+0]$$

$$= [1+1 \quad 1+1 \quad 1+1]$$

$$= [0 \;\; 0 \;\; 0]$$

$$\therefore XH^T = (0,0,0)$$

$$X \longrightarrow \boxed{\text{Parity-check Matrix } H^T} \longrightarrow XH^T = 0$$

Q. The received vector for the (7, 4) code is Y = 1001101. Find the transmitted codeword using syndrome decoding technique. Given that

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

Sol. Find Syndrome S = [YH^T]

$$[S] = YH^T = [1 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1] \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = [1 \;\; 0 \;\; 0]$$

For syndrome (100), the error pattern is: 0000 100 (see syndrome table)

E = 0000 100

We know X = Y+E. Add Y and E vectors.

Y= 1	0	0	1	1	0	1
⊕	Mod-2 addition					
E= 0	0	0	0	1	0	0
X=1	0	0	1	0	0	1

Correct transmitted codeword

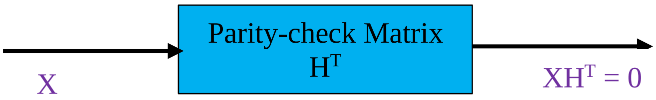
Note on Syndrome decoding

More practical decoding methods for codes with larger k involve parity decoding information derived from the code's P sub-matrix.

H = parity-check matrix
P = Coefficient matrix (submatrix) $[H] = [P^T \mid I_{n-k}]$

P^T = transpose of P matrix

Relative to error detection, the parity check matrix has the crucial property



$XH^T = (000\ldots0)$

Provided that X belongs to the set of code vectors. However, when Y is not a code vector, the product YH^T contains at least one non-zero element.

Therefore, given H^T and received vector Y, error detection can be based on $S = YH^T$, where S = syndrome vector

If all the elements of S = 0, then Y = X and there are no transmission errors. Errors are indicated by the presence of non-zero elements in S.

Q1. For a (6, 3) code, the generator matrix $G = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$. For all possible 8 data words, find the corresponding codewords and verify that this code is a single error correcting code.

Q2. The generator matrix for (7, 4) Hamming code is given below:

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

Find codewords and weight of all the codewords.

Q3. If G and H are generator and parity-check matrices, show that $GH^T = 0$.

Q4. given a generator matrix G = [1 1 1], construct a (3,1) code. How many errors can this code correct? Find the codeword for data vectors d =0 and d =1. Comment.

Q5. G = [1 1 1 1 1]. This gives a (5,1) code. Repeat above question.

Q6. Consider a generator matrix $G = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$ for a non-systematic (6, 3) code. Construct the code for this G and show that d_{min} between codewords is 3, consequently this code can correct at least one error.

Q7. Find a generator matrix G for a (15,11) single-error correcting linear block code. Find the codeword for the data vector 1 0 1 1 1 0 1 0 1 0 1.

Q8. Find out whether or not the following binary linear code is systematic?

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

Q9. Find a generator matrix of a binary code with the following parity-check matrix:

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

Q10. Consider a systematic (6, 3) block code generated by sub-matrix $P = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$. Write the check-bit equations and tabulate the codewords and their weights to show that $d_{min} = 3$.

Q11. For a (6, 3) block code, the generator matrix G is given by:

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

i. Realize an encoder for this code
ii. Verify that this code is a single-error correcting code
iii. If the received codeword is 100011, find the syndrome

Q12. given a (7, 4) linear block code whose generator matrix is given by:

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

i. Find all the codewords
ii. Find the parity-check matrix

Q13. An error control code has the following parity check matrix

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

i. Determine the generator matrix G
ii. Find the codeword that begins with 101….
iii. Decode the received codeword 110110. Comment on error detecting capability of this code.

Q14. Consider a systematic (8,4) code whose parity check equations are:

$c_0 = m_1 \oplus m_2 \oplus m_3$ $c_1 = m_0 \oplus m_1 \oplus m_2$ $c_2 = m_0 \oplus m_1 \oplus m_3$ $c_3 = m_0 \oplus m_2 \oplus m_3$ Where m_0, m_1, m_2, m_3 are message bits and c_0, c_1, c_2, c_3 are parity-check bits. Find the generator and parity-check matrices for this code. Show analytically that the minimum distance of this code is 4.

Q15. The generator matrix for linear block code is

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

i. Express G in systematic [I | P] form
ii. Determine the parity check matrix H for this code
iii. Construct the table of syndromes for the code
iv. Determine the minimum distance of the code
v. Demonstrate that the code word corresponding to the information sequence 101 is orthogonal to H

Q16. Consider a 127, 92) linear code capable of triple error corrections.

Q17. Consider a (7, 4) code whose generator matrix is:

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

i. Find all the codewords of the code
ii. Find H, the parity-check matrix of the code
iii. Compute the syndrome for the received vector 1101101. Is this a valid code vector?
iv. What is the error correcting capability of the code?
v. What is the error detecting capability of the code?

Q18. Is a (7,3) code a perfect code? Is a (7,4)? Is a (15, 11)? Justify your answer?

Q19. Consider a systematic block code, whose parity-check equations are:

$$c_0 = m_0 \oplus m_1 \oplus m_3$$

$$c_1 = m_0 \oplus m_2 \oplus m_3$$

$$c_2 = m_0 \oplus m_1 \oplus m_2$$

$$c_3 = m_1 \oplus m_2 \oplus m_3$$

Where m_i are message digits and c_j are check digits.

i. Find G and H for this code
ii. How many errors can the code correct?
iii. Is the vector 10101010 a codeword?
iv. Is the vector 01011100 a codeword?

Q20. The minimum Hamming distance of a block code is dmin = 11. Determine the error correction and detection capability of this code.

Q21. A linear block code has the following generator matrix in systematic form:

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

i. Find the parity-check matrix H and write down the parity-check equations
ii. Find the minimum Hamming distance of the code

Q22. The generator matrix of a binary linear block code is given below:

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

i. Write down the parity-check equations for the code
ii. Determine the code rate and minimum Hamming distance

Q23. Given a generator matrix G = [1 1 1]. Construct a (3, 1) code. How many errors can this code correct? Find the codeword for the data vectors (0) and (a). comment.

Q24. Repeat above for G = [1 1 1 1 1]. This gives a (5, 1) code.

Q25. Consider a generator matrix $G = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$. Construct the code for this G and show that dmin, the minimum distance between codewords is 3. Consequently, this code can correct at least one error.

Q26. For a (6, 3) systematic linear block code, the 3-parity check digits c4, c5, c6 are:

$c_4 = d_1 + d_2 + d_3$
$c_5 = d_1 + d_2$
$c_6 = d_1 + d_3$

i. Construct the appropriate G for this code
ii. Construct the code generated by this matrix
iii. Determine error correcting capabilities of this code
iv. Prepare a suitable decoding table
v. Decode the following received words: 101100, 000110, 101010

Q27. Consider a (6, 2) code generated by the matrix $G = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}$. Construct the code table for this code and determine the minimum distance between codewords.