Linear Block Codes

Sum of two code words will produce another code word.

- It shows that any code vector can be expressed as a linear combination of other code vector.
- Consider any code vector is having m1, m2, m3 ... mk message bits and c1, c2, c3 ... cn check bits then the code vector can be written as

$$X = (m_1, m_2, m_3 \dots m_k \;\; c_1, c_2, c_3 \dots c_n)$$

- Where q is the number of redundant bits added by the encoder $q = n-k$

- The code vector can also be written as $X = (M|C)$
- M = k bit message vector
- C = q bit check vector (Check bits play the role of error correction and detection)
- Code vector can be represented as $X = MG$
- X= Code vector of $1 \times n$ size or n bits
- M = Message vector of $1 \times k$ size or k bits
- G = Message vector of $k \times n$ size

In Matrix form $[X]_{1\times n} = [M]_{1\times k}\,[G]_{k\times n}$ and Generate matrix G can be represented as $G = \left[I_k[P_{k\times q}]\right]_{k\times n}$ where I = k×k identity matrix ; P = k×q Submatrix

Check vector cab be represented $C = MP$

The expanded form is

$$\left[C_1\; C_2\; C_3 \dots\; C_q\right]_{1\times q} = [M_1\; M_2\; M_3 \dots\; M_k]_{1\times k} \begin{bmatrix} P_{11} & P_{12} & \dots P_{1q} \\ P_{21} & P_{22} & \dots P_{2q} \\ P_{k1} & P_{k2} & \dots P_{kq} \end{bmatrix}_{k\times q}$$

By solving the above equation check vector can be obtained (additions are mod 2 addition)

$$C_1 = M_1P_{11} \oplus M_2P_{21} \oplus M_3P_{31} \oplus \dots \oplus M_kP_{k1}$$

$$C_2 = M_1P_{12} \oplus M_2P_{22} \oplus M_3P_{32} \oplus \dots \oplus M_kP_{k2}$$

$C_3 = M_1P_{13} \oplus M_2P_{23} \oplus M_3P_{33} \oplus \dots \oplus M_kP_{k3}$ and So on....

Problem

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

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

Solution :

(i) <u>Determination of P Submatrix from generator matrix</u>

We know that

$$\mathrm{G} = \left[\mathrm{I_k}\left[\mathrm{P_{k\times q}}\right]\right]_{\mathrm{k\times n}}$$

$$I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad \mathrm{P_{k\times q}} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

(ii) To obtain equations for check bits

Here k=3, q=3 and n=6, here the block size of message vector 3 bits. Hence there will be 8 message vector as shown in the table.

Sl.No	Message vector		
	M1	M2	M3
1	0	0	0
2	0	0	1
3	0	1	0
4	0	1	1
5	1	0	0
6	1	0	1
7	1	1	0
8	1	1	1

Then the check vector

$$[C_1\ C_2\ C_3] = [M_1\ M_2\ M_3]\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

$C_1 = M_1 0 \oplus M_2 \oplus M_3 = M_2 \oplus M_3$

$C_2 = M_1 \oplus M_2 0 \oplus M_3 = M_1 \oplus M_3$

$C_3 = M_1 \oplus M_2 \oplus M_3 0 = M_1 \oplus M_2$

(iii) <u>To determine check bits and code vectors for every message vector</u>

For m1, m2, m3 = (000)

$C_1 = \ M_2 \oplus M_3 \ = 0 \oplus 0 = 0$

$C_2 = \ M_1 \oplus M_3 \ = 0 \oplus 0 = 0$

$C_3 = M_1 \oplus M_2 \ = 0 \oplus 0 = 0$ ie $[C_1\ C_2\ C_3] = (0\ 0\ 0)$

For (001)

$C_1 = \ M_2 \oplus M_3 \ = 0 \oplus 1 = 1$

$C_2 = \ M_1 \oplus M_3 \ = 0 \oplus 1 = 1$

$C_3 = M_1 \oplus M_2 \ = 0 \oplus 0 = 0$ ie $[C_1\ C_2\ C_3] = (1\ 1\ 0)$

Sl.No	Message Bits			Check bits			Complete Code Vector					
	M_1	M_2	M_3	$C_1 = M_2 \oplus M_3$	$C_2 = M_1 \oplus M_3$	$C_3 = M_1 \oplus M_2$	M_1	M_2	M_3	C_1	C_2	C_3
1	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	1	1	1	0	0	0	1	1	1	0
3	0	1	0	1	0	1	0	1	0	1	0	1
4	0	1	1	0	1	1	0	1	1	0	1	1
5	1	0	0	0	1	1	1	0	0	0	1	1
6	1	0	1	1	0	1	1	0	1	1	0	1
7	1	1	0	1	1	0	1	1	0	1	1	0
8	1	1	1	0	0	0	1	1	1	0	0	0

Parity Check Matrix

For every block code the parity check matrix can be defined as

$$H = [P^T : I_q]_{q\times n}$$

Submatrix P is represented as

$$P = \begin{bmatrix} P_{11} & P_{12} & \dots\ P_{1q} \\ P_{21} & P_{22} & \dots\ P_{2q} \\ P_{k1} & P_{k2} & \dots\ P_{kq} \end{bmatrix}_{k\times q}$$

$$P^T = \begin{bmatrix} P_{11} & P_{21} & \dots\ P_{k1} \\ P_{12} & P_{22} & \dots\ P_{k2} \\ P_{1q} & P_{2q} & \dots\ P_{kq} \end{bmatrix}_{q\times k}$$

$$[H]_{q\times n} = \begin{bmatrix} P_{11} & P_{21} & \dots\ P_{k1} & & 1 & 0 \dots & 0 \\ P_{12} & P_{22} & \dots\ P_{k2} & : & 0 & 1 \dots & 0 \\ P_{1q} & P_{2q} & \dots\ P_{kq} & & 0 & 0 \dots & 1 \end{bmatrix}_{q\times n}$$

Hamming code

These are (n,k) linear block codes, will satisfy the following conditions.

1. Number of check bits $q \geq 3$.
2. Block length $n = 2^q - 1$
3. Number of message bits $k = n - q$
4. Minimum distance $d_{min} = 3$

We know that

Code rate $r = \frac{k}{n}$ $\quad 0 < r < 1$

$$r = \frac{n-q}{n} = 1 - \frac{q}{n} = 1 - \frac{q}{2q-1}$$

Error detection and correction capabilities of hamming codes

Since d_{min} is 3 for hamming code, it can detect double errors and correct single errors.

Problem

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

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

1. Find the generator Matrix G
2. List all the code vectors
3. What is the minimum distance between code vectors
4. How many errors can be detected and how many errors can be corrected.

Solution :

Here n =7, k =4

1. Number of check bits q= n-k = 7- 4 = 3.
2. Block length n= 2^q-1 = 8-1 = 7. This shows the given code is hamming code.

(1) <u>To determine the P Submatrix</u>

The parity check matrix of q×n size is given and q = 3, n=7, k=4.

$$[\mathrm{H}]_{3\times7} = \begin{bmatrix} P_{11} & P_{21} & P_{31} & \mathrm{P}_{41} \ldots & 1 & 0 & 0 \\ P_{12} & P_{22} & P_{32} & \mathrm{P}_{42} \ldots & 0 & 1 & 0 \\ P_{13} & P_{23} & P_{33} & \mathrm{P}_{43} \ldots & 0 & 0 & 1 \end{bmatrix}_{3\times7}$$

$$H = [P^T : I_3]$$

$$P^T = \begin{bmatrix} P_{11} & P_{21} & P_{31} & P_{41} \\ P_{12} & P_{22} & P_{32} & P_{42} \\ P_{13} & P_{23} & P_{33} & P_{43} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

Therefore

$$P = \begin{bmatrix} P_{11} & P_{12} & P_{13} \\ P_{21} & P_{22} & P_{23} \\ P_{31} & P_{32} & P_{33} \\ P_{41} & P_{42} & P_{43} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

(2) <u>To obtain generator matrix G</u>

$$G = \left[I_k : [P_{k\times q}]\right]_{k\times n} \qquad\qquad G = \left[I_4 : [P_{4\times 3}]\right]_{4\times 7}$$

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

(3) To find all Code words

Codeword C = MP

$$\left[C_1\ C_2\ C_3\ \dots\ C_q\right]_{1\times q} = [M_1\ M_2\ M_3\ \dots\ M_k]_{1\times k} \begin{bmatrix} P_{11} & P_{12} & \dots\ P_{1q} \\ P_{21} & P_{22} & \dots\ P_{2q} \\ P_{k1} & P_{k2} & \dots\ P_{kq} \end{bmatrix}_{k\times q}$$

$$[C_1\ C_2\ C_3]_{1\times3} = [M_1\ M_2\ M_3\ M_4]_{1\times4}\begin{bmatrix} p_{11} & p_{12} & p_{13} \\ p_{21} & p_{22} & p_{23} \\ p_{31} & p_{32} & p_{33} \\ p_{41} & p_{42} & p_{43} \end{bmatrix}_{4\times3}$$

$$[C_1\ C_2\ C_3]_{1\times3} = [M_1\ M_2\ M_3\ M_4]_{1\times4}\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}_{4\times3}$$

$$C_1 = M_1 1 \oplus M_2 1 \oplus M_3 1 \oplus M_4 0 = M_1 \oplus M_2 \oplus M_3$$

$$C_2 = M_1 1 \oplus M_2 1 \oplus M_3 0 \oplus M_4 1 = M_1 \oplus M_2 \oplus M_4$$

$$C_3 = M_1 1 \oplus M_2 0 \oplus M_3 1 \oplus M_4 1 = M_1 \oplus M_3 \oplus M_4$$

For example if (m1, m2, m3, m4) = (1011)

$$C_1 = M_1 \oplus M_2 \oplus M_3 = 1 \oplus 0 \oplus 1 = 0$$

$$C_2 = M_1 \oplus M_2 \oplus M_4 = 1 \oplus 0 \oplus 1 = 0$$

$$C_3 = M_1 \oplus M_3 \oplus M_4 = 1 \oplus 1 \oplus 1 = 1$$

Sl.No	Message Bits				Check bits			Complete Code Vector							Weight of the code vector
	M_1	M_2	M_3	M_4	C_1	C_2	C_3	M_1	M_2	M_3	M_4	C_1	C_2	C_3	
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	1	0	1	1	0	0	0	1	0	1	1	3
3	0	0	1	0	1	0	1	0	0	1	0	1	0	1	3
4	0	0	1	1	1	1	0	0	0	1	1	1	1	0	4
5	0	1	0	0	1	1	0	0	1	0	0	1	1	0	3
6	0	1	0	1	1	0	1	0	1	0	1	1	0	1	4
7	0	1	1	0	0	1	1	0	1	1	0	0	1	1	4
8	0	1	1	1	0	0	0	0	1	1	1	0	0	0	3
9	1	0	0	0	1	1	1	1	0	0	0	1	1	1	4
10	1	0	0	1	1	0	0	1	0	0	1	1	0	0	3
11	1	0	1	0	0	1	0	1	0	1	0	0	1	0	3
12	1	0	1	1	0	0	1	1	0	1	1	0	0	1	4
13	1	1	0	0	0	0	1	1	1	0	0	0	0	1	3
14	1	1	0	1	0	1	0	1	1	0	1	0	1	0	4
15	1	1	1	0	1	0	0	1	1	1	0	1	0	0	4
16	1	1	1	1	1	1	1	1	1	1	1	1	1	1	7

(4) Minimum distance between code vectors

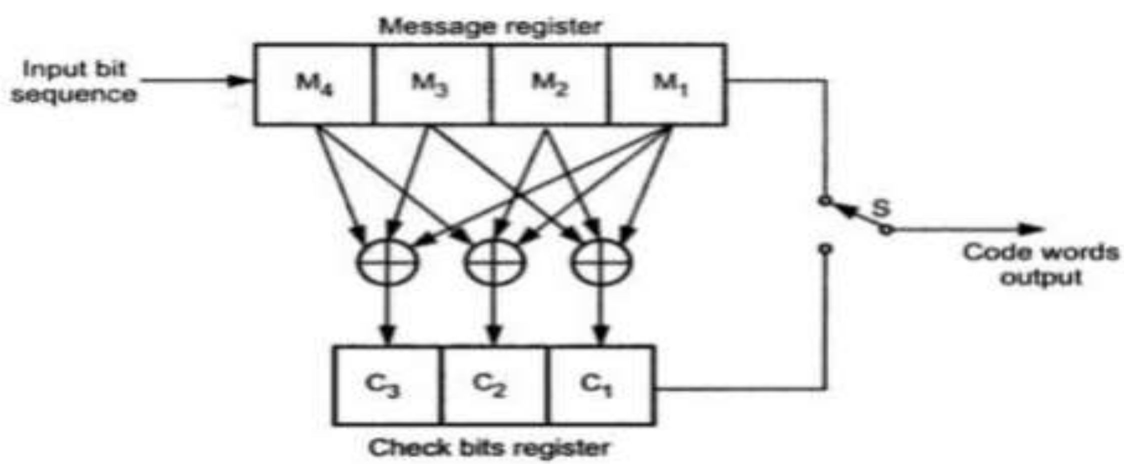
$2^k = 2^8 = 16$ code vectors along with their weights. The smallest weight of any non zero code vector is 3 therefore the minimum distance **d_{min} =3.**

(5) Error correction and Detection capabilities

$d_{min} = 3$

$d_{min} \geq s+1 \rightarrow 3 \geq s+1$ therefore $s \leq 2$ thus two errors will be detected. And
$d_{min} \geq 2t+1 \rightarrow 3 \geq s+1$ therefore $t \leq 1$ thus one errors will be corrected.

Encoder of (7,4) Hamming code



Definition of Syndrome:

When Some errors are present in received vector Y then it will be not from the valid vector and it will not satisfy the property

$$if\ XH^T = (0\ 0\ 0 \ldots..0) and\ YH^T = (0\ 0\ 0 \ldots..0)$$

then X=Y i.e no errors or Y is valid code vector or

$if\ XH^T = YH^T = non\ zero$ then X≠Y i.e some errors.

The non zero output of the product of YH^T is called as syndrome and it is used to detect the errors in Y. Syndrome represented by S cand be written as

$[S]_{1\times q} = [Y]_{1\times n}[H^T]_{n\times q}$ and $Y = X \oplus E$ & $X = Y \oplus E$

Relationship between syndrome vector (S)and Error vector (E)

$$\mathrm{S} = \mathrm{YH}^{\mathrm{T}} = (X \oplus E)H^T = XH^T \oplus EH^T$$

$$S = EH^T\ since\ XH^T = 0$$

Detecting error with the help of syndrome:

Problem

The parity check parity matrix of (7,4) block code is given as

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

Calculate the syndrome vector.

(1) To determine error pattern for single bit erros

Syndrome is 3 bit vector, here q=3. Therefore $2^q-1 = 7$ non zero syndrome. This shows that 7 single bit error pattern will be represented by these 7 non zero syndrome. Error vector E is a n bit vector representing error pattern.

Sl.No	Bit in error	Bits of vector (E), Non zero bits shows error						
1	1^{st}	1	0	0	0	0	0	0
2	2^{nd}	0	1	0	0	0	0	0
3	3^{rd}	0	0	1	0	0	0	0
4	4^{th}	0	0	0	1	0	0	0
5	5^{th}	0	0	0	0	1	0	0
6	6^{th}	0	0	0	0	0	1	0
7	7^{th}	0	0	0	0	0	0	1

(2) Calculation of Syndrome

$$[S]_{1\times q} = [Y]_{1\times n}[H^T]_{n\times q} \text{ and } [S]_{1\times 3} = [Y]_{1\times 7}[H^T]_{7\times 3}$$

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

For example Syndrome of first bit error is

$$S = EH^T = (1000000)\begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$S = (1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \quad 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \quad 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0)$$

$$\mathrm{S} = (1\ 0\ 1)$$

Syndrome of second bit error is

$$S = EH^T = (0100000)\begin{bmatrix}1 & 0 & 1\\ 1 & 1 & 1\\ 1 & 1 & 0\\ 0 & 1 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix}$$

$$S = (0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \quad 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \quad 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0)$$

$$S = (1\ 1\ 1)$$

Syndrome vector are rows of H^T

Sl.No	Bits of vector (E), Non zero bits shows error							Syndrome vector			
1	0	0	0	0	0	0	0	0	0	0	
2	1	0	0	0	0	0	0	1	0	1	1st of H^T
3	0	1	0	0	0	0	0	1	1	1	2nd of H^T
4	0	0	1	0	0	0	0	1	1	0	3rd of H^T
5	0	0	0	1	0	0	0	0	1	1	4th of H^T
6	0	0	0	0	1	0	0	1	0	0	5th of H^T
7	0	0	0	0	0	1	0	0	1	0	6th of H^T
8	0	0	0	0	0	0	1	0	0	1	7th of H^T

Error Correction and detection Using Syndrome Vector

Let us consider above (7,4) block code and the Code vector

$$X = (1\,0\,0\,1\,1\,1\,0)$$

Let the error created in 3rd bit so

$$Y = (1\,0\,(\mathbf{1})\,1\,1\,1\,0)$$

Now error correction can be done by adopting following steps

(1) Calculate the syndrome $S = YH^T$
(2) Check the row of H^T which is same as of S
(3) For P^{th} of row of H^T, P^{th} bit is in error. Hence write the corresponding error vector E.
(4) Obtain the correct vector by $X = Y \oplus E$

(1) To obtain syndrome Vector

$$S = YH^T$$

$$S = (1\,0\,1\,1\,1\,1\,0)\begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = (1\,1\,0)$$

(2) To determine the row of H^T which is same as of S = 3rd row
(3) To determine E ; E = (0 0 1 0 0 0 0)

(4) Correct Vector X

$$X = Y \oplus E$$

$$X = (1\,0\,1\,1\,1\,1\,0) \oplus (0\,0\,1\,0\,0\,0\,0) = (1\,0\,0\,1\,1\,1\,0)$$

Thus the single bit error can be corrected using syndrome.

If Double Error Occurs

Consider the same message vector

$$X = (1\,0\,0\,1\,1\,1\,0)$$

and

$$Y = (1\,0\,(\mathbf{1})\,(\mathbf{0})\,1\,1\,0)$$

S = YH^T

$$S = (1\,0\,1\,0\,1\,1\,0)\begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = (1\,0\,1)$$

S is equal to row of H^T which is same as of S = 1st row therefore E = 1000000. Thus the error correction and detection goes wrong. The probability occurrence of multiple errors is less compared to single errors. To correct multiple errors extended hamming codes are used. In these codes one extra bit is provided to correct double errors. We know that for (n,k) block codes there are 2^n-1distinct non zero syndromes. There are nC_1 = n single error pattern, nC_2 double error pattern, nC_3 triple error pattern and so on. Therefore to correct t error pattern

$$2^q - 1 \geq n\,C_1 + n\,C_2 + n\,C_3 + \ldots\ldots + n\,C_t$$