A block code is a set of words that has a well-defined mathematical property or structure, and where each word is a sequence of a fixed number of bits. The words belonging to a Block code are called Code Words.

A code whose code words have 'k' information bits and 'r' parity bits, has n-bit codewords where n=k+r. Such a code is referred to as an (n,k) Block code where n and k are respectively the Block Length and Information Length of the code.

Codeword whose information bits are kept together, show that they are readily identifiable, is said to be in a systematic form or to be Systematic Code, otherwise the code word is referred to as Non Systematic.

Hamming Code

$P_1 = i_1 + i_2 + i_3$

$P_2 = i_2 + i_3 + i_4$

$P_3 = i_4 + i_1 + i_2$

} 3 parity check bits

The final codeword = $(i_1, i_2, i_3, i_4, P_1, P_2, P_3)$

At the decoder stage the received word is $V = (V_1, V_2, V_3, V_4, V_5, V_6, V_7)$

$\equiv$

$(i_1, i_2, i_3, i_4, P_1, P_2, P_3)$

The decoder determines 3 parity-check sums :-

$S_1 = (V_1 + V_2 + V_3) + V_5$

$S_2 = (V_2 + V_3 + V_4) + V_6$

$S_3 = (V_4 + V_1 + V_2) + V_7$

} Error Syndrome of V :-

$S = (S_1, S_2, S_3)$

d_{min} → Minimum distance of 2 codes.

Error-detection capacity = $(d_{min} - 1)$

Error-correction capacity = $\frac{1}{2}(d_{min} - 1)$

$V = C + e$

C → codeword

e → error

Decoding in Hamming Code :-

1) Calculate s [i.e (s_1, s_2, s_3)] from decoder input v.

2) From the syndrome table obtain the error pattern $\hat{e}$ that corresponds to v.

3) The required codeword is given by $\boxed{\hat{c} = v + \hat{e}}$.

Weight = No. of 1's in the codeword.

Linear Codes

A blockcode is said to be a linear code if it's codewords satisfy the condition that the sum of any two codewords gives another codeword.

i.e $\boxed{c_k = c_i + c_j}$

A linear code has the following properties :-

1) The all-zero word (0 0 0 ..... 0) is always a codeword.

2) Given any three codewords c_i, c_j and c_k such that $c_k = c_i + c_j$

then, $d(c_i, c_j) = w(c_k)$ i.e the distance between two codewords equals the weight of the sum of the codewords.

3) The minimum distance of the code $d_{min} = w_{min}$, where w_{min} = weight of any non-zero codeword with the smallest weight.

Generator Matrices

2.2 Generator matrices

In Section 1.6 parity-check equations were used to generate codewords for the (7, 4) Hamming code. Given an information word $\boldsymbol{i} = (i_1, i_2, i_3, i_4)$ the parity-check bits p_1, p_2, and p_3 are obtained using eqns 1.17 and then added to $\boldsymbol{i}$ to give the codeword $\boldsymbol{c} = (i_1, i_2, i_3, i_4, p_1, p_2, p_3)$. A better approach to encoding is through the use of matrices and as we shall see, linear codes lend themselves naturally to a matrix representation. There is a unique correspondence between information words $\boldsymbol{i}$ and codewords $\boldsymbol{c}$, which can be expressed as

$$\boldsymbol{c} = \boldsymbol{iG} \tag{2.2}$$

where $\boldsymbol{G}$ is a matrix and is referred to as the *generator matrix* of the linear code. The generator matrix of an (n, k) linear code has k rows and n columns (note that a matrix with k rows and n columns is referred to as a 'k by n' or $k \times n$ matrix and is known as the order of the matrix). The generator matrix for the (7, 4) code is a 4 by 7 matrix given by

$$\boldsymbol{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \tag{2.3}$$

and later we shall see the relationship between the generator matrix and the code's parity-check equations. The product $\boldsymbol{iG}$ is determined by taking the product of $\boldsymbol{i}$ with every column in $\boldsymbol{G}$. Each element in $\boldsymbol{i}$ is multiplied by the corresponding element in the column and then summed, using modulo-2 addition, over all elements. Consider $\boldsymbol{i} = (1\ 1\ 1\ 0)$, then using eqns 2.2 and 2.3 the corresponding

codeword $\boldsymbol{c} = (c_1, c_2, c_3, c_4, c_5, c_6, c_7)$ is given by

$$\boldsymbol{c} = (1\ 1\ 1\ 0) \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

Multiplying $\boldsymbol{i}$ by the first (left-hand side) column of $\boldsymbol{G}$ gives the first bit c_1

$$(1\ 1\ 1\ 0) \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = 1 \cdot 1 + 1 \cdot 0 + 1 \cdot 0 + 0 \cdot 0 = 1$$

and the second column gives c_2

$$(1\ 1\ 1\ 0) \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = 1 \cdot 0 + 1 \cdot 1 + 1 \cdot 0 + 0 \cdot 0 = 1.$$

Likewise columns 3, 4, 5, and 6 give 1, 0, 1, and 0 for c_3, c_4, c_5, and c_6 respectively. The last column gives c_7

$$(1\ 1\ 1\ 0) \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = 1 \cdot 1 + 1 \cdot 1 + 1 \cdot 0 + 0 \cdot 1 = 1 + 1 = 0$$

and so $\boldsymbol{c} = (c_1, c_2, c_3, c_4, c_5, c_6, c_7) = (1\ 1\ 1\ 0\ 1\ 0\ 0)$, which is the correct codeword for $\boldsymbol{i} = (1\ 1\ 1\ 0)$. Equation 2.2 can be used to generate all the 16 codewords belonging to the (7, 4) code. Note that when $\boldsymbol{i} = (0\ 0\ 0\ 0)$, eqn 2.2 gives $\boldsymbol{c} = (0\ 0\ 0\ 0\ 0\ 0\ 0)$. Clearly the generator matrix provides a concise and convenient way of constructing codewords.

Example 2.3
Determine the set of codewords for the (6, 3) code with generator matrix

$$\boldsymbol{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}. \tag{2.4}$$

We need to consider the information words $(0\ 0\ 1)$, $(0\ 1\ 0)$, $(1\ 0\ 0)$, ..., $(1\ 1\ 1)$. Substituting $\boldsymbol{G}$ and $\boldsymbol{i} = (0\ 0\ 1)$ into eqn 2.2 gives the codeword

$$\boldsymbol{c} = (0\ 0\ 1) \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} = (0\ 0\ 1\ 1\ 1\ 0)$$

Identification of Parity bits :-

K = No. of bits , P = required parity bits

$2^P \geq P + K + 1$

For 5-bit code :

when P=1	when P=2	when P=3	when P=4
$2^1 \geq 1+5+1$	$2^2 \geq 2+5+1$	$2^3 \geq 9$	$2^4 \geq 4+5+1$
✗	✗	✗	✓

So, total no. of parity bits = 4

So, for P=4 and K=5 $\Rightarrow n = P + K = 9$

Hence, (9,5) Hamming Code.

Hamming Code formation :

Place parity bits as follows —

$P_1 = 2^0 = 1$ (check 1 skip 1)
$P_2 = 2^1 = 2$ (check 2 skip 2)
$P_3 = 2^2 = 4$ (check 4 skip 4)
$P_4 = 2^3 = 8$ (check 8 skip 8)
P_4
⋮
so on...

Consider (9,5) code :-

D_9	P_8	D_7	D_6	D_5	P_4	D_3	P_2	P_1

$P_1 \rightarrow D_3\ D_5\ D_7\ D_9$
$P_2 \rightarrow D_3\ D_6\ D_7$
$P_4 \rightarrow D_5\ D_6\ D_7$
$P_8 \rightarrow D_9$

Generator Matrix

$$[c] = [i][G]$$

$[c]$ = codeword
$[i]$ = information words
$[G]$ = generator matrix

The Generator Matrix for an (n, k) linear code has k rows and n columns

The Generator Matrix for (7,4) code is given by :–

$$[G] = [I : P]$$

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

Identity Matrix — Parity Matrix

If Message $[i] = [1\ 1\ 1\ 0]$

$\therefore$ Codeword $[c] = [i][G]$

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

$$= [1\ 1\ 1\ 0\ 1\ 0\ 0]$$

For getting Systematic Codeword from Non-systematic Generator Matrix, we need to first row-transform the generator matrix such that the first part becomes an Identity Matrix and then perform $[c] = [i][G]$

Parity Check Matrix

- From Generator Matrix $[G] = [I_K \mid P]$ we can identify Parity Matrix.
- By taking P^T we can make parity check matrix $[H]$

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

- Parity check matrix is used at the R_X to decode data.

Q) Generate parity check matrix for (7,4) code.

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

Identity matrix → I_4 ; Parity Matrix → P

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

Now, $I_{n-k} = I_{7-4} = I_3 = \begin{bmatrix} 1&0&0 \\ 0&1&0 \\ 0&0&1 \end{bmatrix}$

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

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

Properties: (i) $GH^T = 0$
(ii) $CH^T = 0 \longrightarrow C = [i][G]$

Error Syndromes in Linear Block Codes

Error Syndrome $[S]$ = [Received Codeword] $[H^T]$

$\Rightarrow [S] = [Y][H^T]$

$\Rightarrow [S] = ([C]+[e])[H^T]$, where $[C] = [i][G]$ and $[e]$: Error

If $[e] = 0 \Rightarrow [S] = [C][H^T] = 0$

Let received word $V_1 = [1\,1\,0\,1\,1\,0\,1]$

$$[H^T] = \begin{bmatrix} 1&0&1 \\ 1&1&1 \\ 1&1&0 \\ 0&1&1 \\ 1&0&0 \\ 0&1&0 \\ 0&0&1 \end{bmatrix} \begin{matrix} ① \\ ② \\ ③ \\ ④ \\ ⑤ \\ \\ \\ \end{matrix}$$

So error is at the 5th position.

Now, $[S] = [V_1][H^T] = [1\,0\,0]$

$\therefore V_1 = [1101101]$

$e = [0000100]$

So, corrected signal = $[V_1] + [e] = [1101001]$

Continue from Lecture Number 12

$g(x) = x^3 + x + 1$

$0\ 1\ x\ x^2\ x^3\ x^4\ x^5\ x^6$

x is a Root → Consideration ✓

Check :

1) 1 is a root

$1^3 + 1 + 1 \neq 0$ NOT ROOT

2) 0 is a root

$0^3 + 0 + 1 \neq 0$ NOT ROOT

3) x^2 is a root

$g(x) = x^3 + x + 1$

$g(x^2) = (x^2)^3 + x^2 + 1$

$= x^6 + x^2 + 1$

$= (x^2+1) + x^2 + 1 = 0$ Is A Root!

4) x^3

$g(x^3) = (x^3)^3 + x^3 + 1$

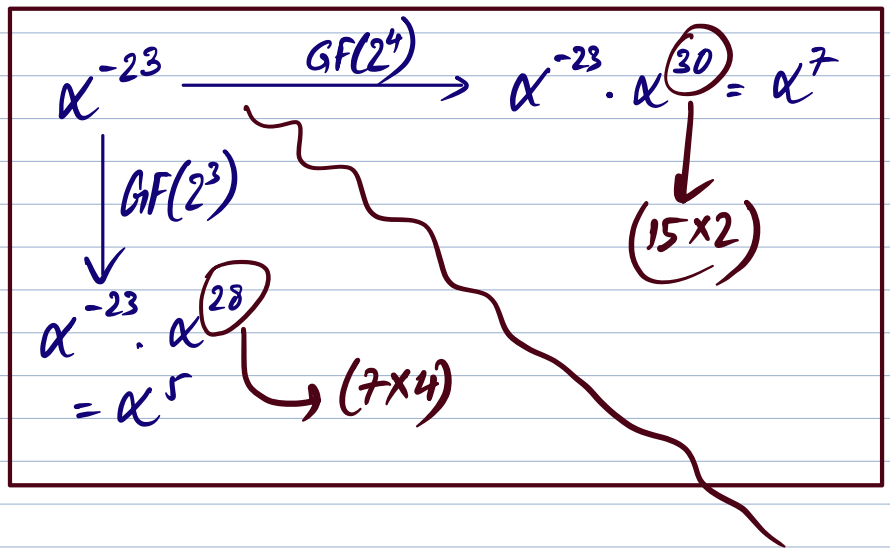
$= x^9 + x^3 + 1$

$= x^2 + x^3 + 1 = x^2 + (x+1) + 1 = x^2 + x \neq 0$ NOT ROOT

o o o

So, the roots are: $\alpha, \alpha^2, \alpha^4 \in GF(2^3)$

are the roots of x^3+x+1



Now, the roots for x^4+x+1 → $\alpha, \alpha^2, \alpha^4, \alpha^8$

$(\alpha^2)^4 + \alpha^2 + 1$

$= \alpha^8 + \alpha^2 + 1$

$= (\alpha^2+1) + \alpha^2 + 1 = 0$

$GF(2^3) \longrightarrow x^3+x+1 \longrightarrow \underbrace{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6}_{8=2^3}$ $\alpha^7 = 1$

Roots → $\alpha, \alpha^2, \alpha^4$

For any $\alpha^{(i+j)} = \alpha^{(i+j)\%7}$

$\alpha^{-23} = \alpha^{-23} \cdot \alpha^{28} = \alpha^5$

$g(x) = x^3+x+1$

$g(\alpha) = 0$

$\alpha^3+\alpha+1 = 0$

$\Rightarrow \alpha^3 = \alpha+1$

α^4

$\vdots$

α^6

Primitive Element, $\beta = \alpha^2, \alpha^5$

↳ β^m can generate all the non-zero elements of the field.

$GF(2^4) \longrightarrow x^4 + x + 1 \longrightarrow 0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{10}, \alpha^{11}, \alpha^{12}, \alpha^{13}, \alpha^{14}$ $\}\ \alpha^{15} = 1$

$16 = 2^4$

Roots $\rightarrow \alpha, \alpha^2, \alpha^4, \alpha^8$

For any $\alpha^{(i+j)} = \alpha^{(i+j)\%15}$

$\alpha^{-34} = \alpha^{-34} \cdot \alpha^{45} = \alpha^{11}$

$g(x) = x^4 + x + 1$

$g(\alpha) = 0$

$\alpha^4 + \alpha + 1 = 0$

$\Rightarrow \alpha^4 = \alpha + 1$

$\alpha^5 \ldots \alpha^{14}$

$GF(2^5) \longrightarrow x^5 + x^2 + 1$

Roots $\rightarrow \alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}$

$0, 1, \alpha, \alpha^2, \ldots, \alpha^{30}$ $\}\ \alpha^{31} = 1$

9) For $GF(2^4)$ find conjugate for α^5.

A) Let $\beta = \alpha^5$. Take $\beta, \beta^2, \beta^4, \ldots, \beta^{2n}$

$\beta = \alpha^5$ ✓

$\beta^2 = \alpha^{10}$ ✓

$\beta^4 = \alpha^{20} = \alpha^{20\%15} = \alpha^5$ ✓ ∴ Conjugates are α^5, α^{10}

$\beta^8 = \alpha^{40} = \alpha^{10}$ ✓

$\beta^{16} = \alpha^{80} = \alpha^{75} \cdot \alpha^5 = \alpha^5$ ✓

Internal Questions

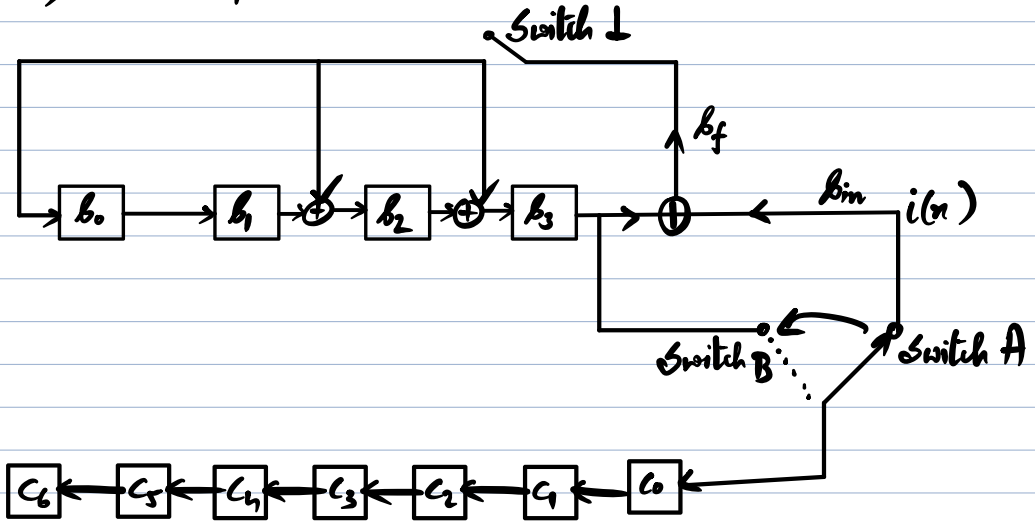
1) (7,3) cyclic code [Pg 113]

$g(x) = x^4 + x^3 + x^2 + 1$

$i = 110 \longrightarrow i(x) = x^2 + x$

$g(x) = x^4 + x^3 + x^2 + 1$

↳ Order = 4



$b_f = b_3 + b_{in}$ $\quad b_2 = b_1 + b_f$ $\quad b_0 = b_f$

$b_3 = b_f + b_2$ $\quad b_1 = b_0$

Shift	b_{in}	b_0	b_1	b_2	b_3	b_4	c_0	c_1	c_2	c_3	c_4	c_5	c_6	$r(x)$
	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	0	1	1	1	1	0	0	0	0	0	0	x^3+x^2+1
2	1	0	1	0	1	0	1	1	0	0	0	0	0	x^3+x
3	0	1	0	0	1	1	0	1	1	0	0	0	0	x^3+1
Switch A to B & Switch 1 OFF														
4	–	0	1	0	0	–	1	0	1	1	0	0	0	x
5	–	0	0	1	0	–	0	1	0	1	1	0	0	x^2
6	–	0	0	0	1	–	0	0	1	0	1	1	0	x^3
7	–	0	0	0	0	–	1	0	0	1	0	1	1	0

2/i) A) All zero-word is always a codeword (0 00....00)

B) For any 3 codewords c_i, c_j, c_k

if $c_i + c_j = c_k$,

then $d_{min}(c_i, c_j) = weight(c_k)$

C) Min. distance of the code, $d_{min} = w_{min}$

$i = (1\ 1\ 0\ 0)$

$$G = \begin{bmatrix} \overset{i_1}{1} & \overset{i_2}{0} & \overset{i_3}{0} & \overset{i_4}{0} & \vdots & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & \vdots & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & \vdots & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & \vdots & 0 & 1 & 1 \end{bmatrix}$$

$P_1 = i_1 + i_2 + i_3$

$P_2 = i_2 + i_3 + i_4$

$P_3 = i_4 + i_1 + i_2$

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

2(ii)

and ones). The probability of obtaining 3 errors in a 6-bit word is given by letting $n = 6$ and $j = 3$ in eqn 1.6, which gives

$$P_3 = {}^6C_3 p^3 (1-p)^3$$

and substituting $p = 0.01$ gives $P_3 = 1.94 \times 10^{-5}$. The probability of a decoding failure is therefore $p_f = P_3 = 1.94 \times 10^{-5}$. □

The repetition codes provide us with a very simple way of carrying out error correction and may be suitable in a system where a high level of redundancy is acceptable. But if a channel is to be used efficiently so that high levels of redundancy are not acceptable, then the repetition codes are quite inadequate and error-correcting codes are required that make better use of redundancy.

1.6 Hamming codes

The single-parity-check codes, product codes and repetition codes considered in the previous sections can be thought of as 'first steps' towards achieving error control. The codes allow a limited degree of error detection and correction, and are simple to implement. Moving on towards somewhat more interesting codes are the *Hamming codes* which were the first class of linear codes devised for error control and as we shall see, in Chapter 2, linearity is a good property for a code to possess. The Hamming codes occupy an important position in the history of error-control codes and we will refer to them repeatedly throughout the book. Here the Hamming codes are introduced and later they are reconsidered in terms of their linear properties.

The first in the class of Hamming codes is the (7, 4) code that takes 4-bit information words and encodes them into 7-bit codewords. Three parity-check bits are required, these are determined from the information bits using eqns 1.17 shown below. Given an information word $\boldsymbol{i} = (i_1, i_2, i_3, i_4)$ then the parity-check bits are

$$\begin{aligned} p_1 &= i_1 + i_2 + i_3 \\ p_2 &= i_2 + i_3 + i_4 \\ p_3 &= i_1 + i_2 + i_4 \end{aligned} \qquad (1.17)$$

where the information bits are added together using modulo-2 addition (see Table 1.4). Appending the parity bits to the information word gives the codeword

$$\boldsymbol{c} = (i_1, i_2, i_3, i_4, p_1, p_2, p_3). \qquad (1.18)$$

Table 1.6 shows the set of codewords for the (7, 4) code. There are 16 codewords, one for each information word. For reference purposes, the codewords and information words are labelled $\boldsymbol{c}_0$ to $\boldsymbol{c}_{15}$, and $\boldsymbol{i}_0$ to $\boldsymbol{i}_{15}$ respectively. The subscript i of the codeword $\boldsymbol{c}_i$ gives the numerical value of the corresponding information word, for example $\boldsymbol{c}_9$ is the codeword corresponding to the information word $\boldsymbol{i}_5 = (1\,0\,0\,1)$. Note that here, as with the repetition codes, the word 'parity' does not refer to whether there are an even or odd number of ones in a word, but rather refers to the code's check bits irrespective of the code's property or structure.

Table 1.6
The (7, 4) Hamming code

Information words $\boldsymbol{i} = (i_1, i_2, i_3, i_4)$	Codewords $\boldsymbol{c} = (i_1, i_2, i_3, i_4, p_1, p_2, p_3)$
$\boldsymbol{i}_0 = (0\,0\,0\,0)$	$\boldsymbol{c}_0 = (0\,0\,0\,0\,0\,0\,0)$
$\boldsymbol{i}_1 = (0\,0\,0\,1)$	$\boldsymbol{c}_1 = (0\,0\,0\,1\,0\,1\,1)$
$\boldsymbol{i}_2 = (0\,0\,1\,0)$	$\boldsymbol{c}_2 = (0\,0\,1\,0\,1\,1\,0)$
$\boldsymbol{i}_3 = (0\,0\,1\,1)$	$\boldsymbol{c}_3 = (0\,0\,1\,1\,1\,0\,1)$
$\boldsymbol{i}_4 = (0\,1\,0\,0)$	$\boldsymbol{c}_4 = (0\,1\,0\,0\,1\,1\,1)$
$\boldsymbol{i}_5 = (0\,1\,0\,1)$	$\boldsymbol{c}_5 = (0\,1\,0\,1\,1\,0\,0)$
$\boldsymbol{i}_6 = (0\,1\,1\,0)$	$\boldsymbol{c}_6 = (0\,1\,1\,0\,0\,0\,1)$
$\boldsymbol{i}_7 = (0\,1\,1\,1)$	$\boldsymbol{c}_7 = (0\,1\,1\,1\,0\,1\,0)$
$\boldsymbol{i}_8 = (1\,0\,0\,0)$	$\boldsymbol{c}_8 = (1\,0\,0\,0\,1\,0\,1)$
$\boldsymbol{i}_9 = (1\,0\,0\,1)$	$\boldsymbol{c}_9 = (1\,0\,0\,1\,1\,1\,0)$
$\boldsymbol{i}_{10} = (1\,0\,1\,0)$	$\boldsymbol{c}_{10} = (1\,0\,1\,0\,0\,1\,1)$
$\boldsymbol{i}_{11} = (1\,0\,1\,1)$	$\boldsymbol{c}_{11} = (1\,0\,1\,1\,0\,0\,0)$
$\boldsymbol{i}_{12} = (1\,1\,0\,0)$	$\boldsymbol{c}_{12} = (1\,1\,0\,0\,0\,1\,0)$
$\boldsymbol{i}_{13} = (1\,1\,0\,1)$	$\boldsymbol{c}_{13} = (1\,1\,0\,1\,0\,0\,1)$
$\boldsymbol{i}_{14} = (1\,1\,1\,0)$	$\boldsymbol{c}_{14} = (1\,1\,1\,0\,1\,0\,0)$
$\boldsymbol{i}_{15} = (1\,1\,1\,1)$	$\boldsymbol{c}_{15} = (1\,1\,1\,1\,1\,1\,1)$

At the decoding stage the received word is

$$\boldsymbol{r} = (r_1, r_2, r_3, r_4, r_5, r_6, r_7)$$

where

$$\begin{aligned} r_1 &= i_1 \\ r_2 &= i_2 \\ r_3 &= i_3 \\ r_4 &= i_4 \\ r_5 &= p_1 \\ r_6 &= p_2 \\ r_7 &= p_3 \end{aligned}$$

if no errors occur. The decoder determines 3 parity-check sums

$$\begin{aligned} s_1 &= (r_1 + r_2 + r_3) + r_5 \\ s_2 &= (r_2 + r_3 + r_4) + r_6 \\ s_3 &= (r_1 + r_2 + r_4) + r_7. \end{aligned} \qquad (1.19)$$

The first 3 bits in each parity-check sum correspond to the same combination of information bits as that used in the construction of the parity bits (see eqns 1.17), they are enclosed in parenthesis to emphasize this correspondence. From the parity-check sums we can define

$$\boldsymbol{s} = (s_1, s_2, s_3) \qquad (1.20)$$

Hamming Distance

Hamming distance is a metric for comparing two binary data strings. While comparing two binary strings of equal length, Hamming distance is the number of bit positions in which the two bits are different.

The Hamming distance between two strings, a and b is denoted as d(a,b).

It is used for error detection or error correction when data is transmitted over computer networks. It is also using in coding theory for comparing equal length data words.

Calculation of Hamming Distance

In order to calculate the Hamming distance between two strings, and , we perform their XOR operation, (a⊕ b), and then count the total number of 1s in the resultant string.

Example

Suppose there are two strings 1101 1001 and 1001 1101.

11011001 ⊕ 10011101 = 01000100. Since, this contains two 1s, the Hamming distance, d(11011001, 10011101) = 2.

Minimum Hamming Distance

In a set of strings of equal lengths, the minimum Hamming distance is the smallest Hamming distance between all possible pairs of strings in that set.

Example

Suppose there are four strings 010, 011, 101 and 111.

010 ⊕ 011 = 001, d(010, 011) = 1.

010 ⊕ 101 = 111, d(010, 101) = 3.

010 ⊕ 111 = 101, d(010, 111) = 2.

011 ⊕ 101 = 110, d(011, 101) = 2.

011 ⊕ 111 = 100, d(011, 111) = 1.

101 ⊕ 111 = 010, d(011, 111) = 1.

Hence, the Minimum Hamming Distance, d_{min} = 1.

1 0 1 1
1 0 1 0
1 1 0 0 0 1 → 3

1 0 1 1 0 1 → 4

2) 1)i) $x^{15}+1 = (x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$

a) All possible factors are:—

$f_1 = (x+1)$ ① $\longrightarrow (15,14)$ ✓

$f_2 = (x^2+x+1)$ ② $\longrightarrow (15,13)$ ✓

$f_3 = (x^4+x+1)$ ④ $\longrightarrow (15,11)$ ✓

$f_4 = (x^4+x^3+1)$ ④ $\longrightarrow (15,11)$ ✓

$f_5 = (x^4+x^3+x^2+x+1)$ ④ $\longrightarrow (15,11)$ ✓

$\hookrightarrow n-k=4$

$15-k=4$

$k=11 \Rightarrow (15,11)$ ✓

✓

$f_6 = f_1 \cdot f_2$ ③ $\longrightarrow (15,12)$

$f_7 = f_1 \cdot f_3$ ⑤ $\longrightarrow (15,10)$

$f_8 = f_1 \cdot f_4$ ⑤ $\longrightarrow (15,10)$

$f_9 = f_1 \cdot f_5$ ⑤ $\longrightarrow (15,10)$

$f_{10} = f_2 \cdot f_3$ ⑥ $\longrightarrow (15,9)$

$f_{11} = f_2 \cdot f_4$ ⑥ $\longrightarrow (15,9)$

$f_{12} = f_2 \cdot f_5$ ⑥ $\longrightarrow (15,9)$

$f_{13} = f_3 \cdot f_4$ ⑧ $\longrightarrow (15,7)$

$f_{14} = f_3 \cdot f_5$ ⑧ $\longrightarrow (15,7)$

$f_{15} = f_4 \cdot f_5$ ⑧ $\longrightarrow (15,7)$

$f_{16} = f_1 \cdot f_2 f_3$ ⑦ $\longrightarrow (15,8)$

$f_{17} = f_1 \cdot f_2 \cdot f_4$ ⑦ $\longrightarrow (15,8)$

$f_{18} = f_1 \cdot f_2 \cdot f_5$ ⑦ $\longrightarrow (15,8)$

$f_{19} = f_1 \cdot f_3 \cdot f_4$ ⑨ $\longrightarrow (15,6)$

$(15,14)$ $(15,5)$
$(15,13)$ $(15,4)$
$(15,11)$ $(15,3)$
$(15,12)$ $(15,2)$
$(15,10)$ $(15,1)$
$(15,9)$
$(15,7)$
$(15,8)$
$(15,6)$

$f_1 = (x+1) \longrightarrow (15,14)$

$f_2 = (x^2+x+1) \longrightarrow (15,13)$

$f_3 = (x^4+x+1) \longrightarrow (15,11)$

$f_{10} = f_1 \cdot f_3 \cdot f_5$ ✓ (9) → (15, 6)

$f_{21} = f_1 \cdot f_4 \cdot f_5$ ✓ (9) → (15, 6)

$f_{22} = f_2 \cdot f_3 \cdot f_4$ ✓ (10) → (15, 5)

$f_{23} = f_2 \cdot f_3 \cdot f_5$ ✓ (10) → (15, 5)

$f_{24} = f_2 \cdot f_4 \cdot f_5$ ✓ (10) → (15, 5)

$f_{25} = f_3 \cdot f_4 \cdot f_5$ ✓ (12) → (15, 3)

$f_{26} = f_1 \cdot f_2 \cdot f_3 \cdot f_4$ ✓ (11) → (15, 4)

$f_{27} = f_1 \cdot f_2 \cdot f_3 \cdot f_5$ ✓ (11) → (15, 4)

$f_{28} = f_1 \cdot f_2 \cdot f_4 \cdot f_5$ ✓ (11) → (15, 4)

$f_{29} = f_1 \cdot f_3 \cdot f_4 \cdot f_5$ ✓ (13) → (15, 2)

$f_{30} = f_2 \cdot f_3 \cdot f_4 \cdot f_5$ ✓ (14) → (15, 1)

$f_4 = (x^4 + x^3 + 1)$ ⟶ (15, 11)

$f_5 = (x^4 + x^3 + x^2 + x + 1)$ ⟶ (15, 11)

a) 14 different 'blocklength 15' cyclic codes are possible.

b) No. of (15, 11) codes = 3

c) (15, 7) → Order of $g(x) = 8$ } f_{13}, f_{14}, f_{15}

2) $G = \left[\begin{array}{ccc:cc} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{array}\right]$ (P = last 2 columns)

(5, 3)

↳ parity = 2 = n − k

Parity check matrix, $H = [P^T : I_{n-k}]$

To make systematic ⟶ Step 1: $R_3 = R_2 + R_3$

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

Step: $R_1 = R_1 + R_3$

$$G = \left[\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{array}\right] \quad (P)$$

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

$$H = [P^T : I_{n-k}] = \left[\begin{array}{ccc|cc} 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{array}\right]$$

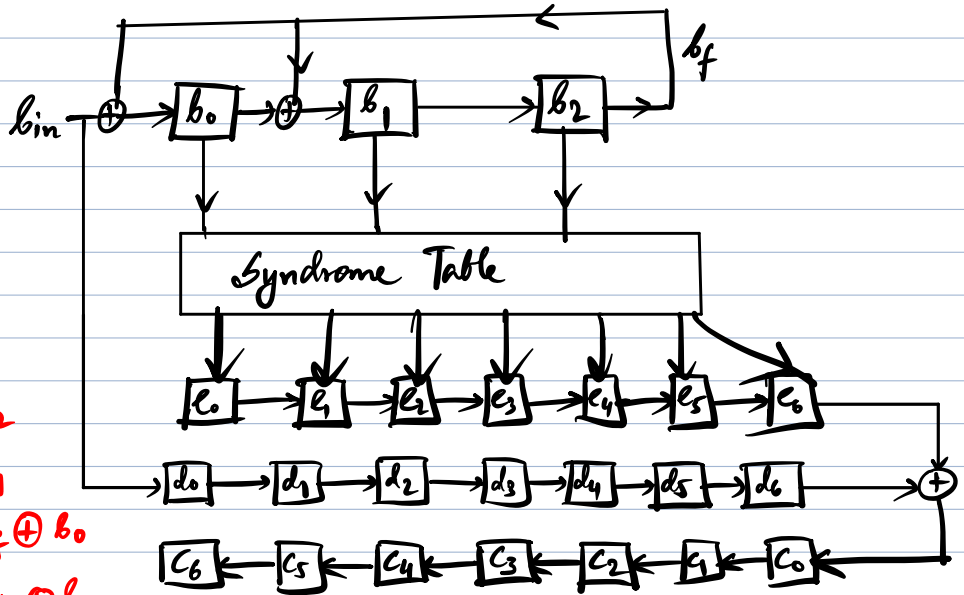
$$GH^T = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

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

3) i) ii) $V(x) = x^6 + x^5 + x^3 + x + 1$

$1\ 0\ 1\ 1\ 0\ 1\ 1$

$g(x) = x^3 + x + 1$



$b_f = b_2$

$b_2 = b_1$

$b_1 = b_f \oplus b_0$

$b_0 = b_{in} \oplus b_f$

$b_0 = b_{in} \oplus b_f$

Shift	b_{in}	b_0	b_1	b_2	b_f	l_0	l_1	l_2	l_3	l_4	l_5	l_6	d_0	d_1	d_2	d_3	d_4	d_5	d_6	c_0	c_1	c_2	c_3	c_4	c_5	c_6
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
3	1	1	0	1	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0
4	1	0	0	0	1	0	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0
6	1	1	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	1	0	0	0	0	0	0	0	0
7	1	1	1	0	0	0	0	0	1	0	0	0	1	1	0	1	1	0	1	0	0	0	0	0	0	0
8	–	–	–	–	–	0	0	0	0	1	0	0	0	1	1	0	1	1	0	1	0	0	0	0	0	0
9	–	–	–	–	–	0	0	0	0	0	1	0	0	0	1	1	0	1	1	0	1	0	0	0	0	0
10	–	–	–	–	–	0	0	0	0	0	0	1	0	0	0	1	1	0	1	1	0	1	0	0	0	0
11	–	–	–	–	–	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	1	0	0	0
12	–	–	–	–	–	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	1	0	0
13	–	–	–	–	–	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	1	0
14	–	–	–	–	–	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	1

1/ii) $i = (0\ 1\ 1\ 1) \Rightarrow i(x) = x^2 + x + 1$

$g(x) = x^3 + x + 1$

Non-systematic

$c(x) = i(x) \cdot g(x)$

$= (x^2+x+1)(x^3+x+1)$

$= x^5 + x^3 + x^2 + x^4 + x^2 + x + x^3 + x + 1$

$\boxed{c(x) = x^5 + x^4 + 1}$

Systematic

$c(x) = i(x) \cdot x^{n-k} + R_{g(x)}[i(x) \cdot x^{n-k}]$

$n - k = 7 - 4 = 3$

$i(x) \cdot x^3 = x^5 + x^4 + x^3$

Now, $R_{g(x)}[i(x) \cdot x^{n-k}]$:-

$$x^3+x+1 \;\overline{)\; x^5 + x^4 + x^3 \;(\; x^2 + x}$$
$$x^5 \quad + x^3 + x^2$$
$$\overline{x^4 + x^2}$$
$$x^4 + x^2 + x$$
$$\overline{x}$$

$\therefore \boxed{c(x) = x^5 + x^4 + x^3 + x}$

2/i) $G = \left[\begin{array}{ccc|cc} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \end{array}\right]$ (Parity) $(5,3)$ ↳ $r=2$

Systematic : $R_3 \rightarrow R_2 + R_3$

$R_1 \rightarrow R_1 + R_3$

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

4) $g(x) = x^4 + x^3 + x + 1 \longrightarrow b_0, b_1, b_2, b_3$

$c(x) = x^6 + x^5 + x^4 + x$

$e(x) = x^6$

$\Big\} V(x) = x^5 + x^4 + x$

$x^6\ x^5\ x^4\ x^3\ x^2\ x^1\ x^0$

$0\ 1\ 1\ 0\ 0\ 1\ 0$

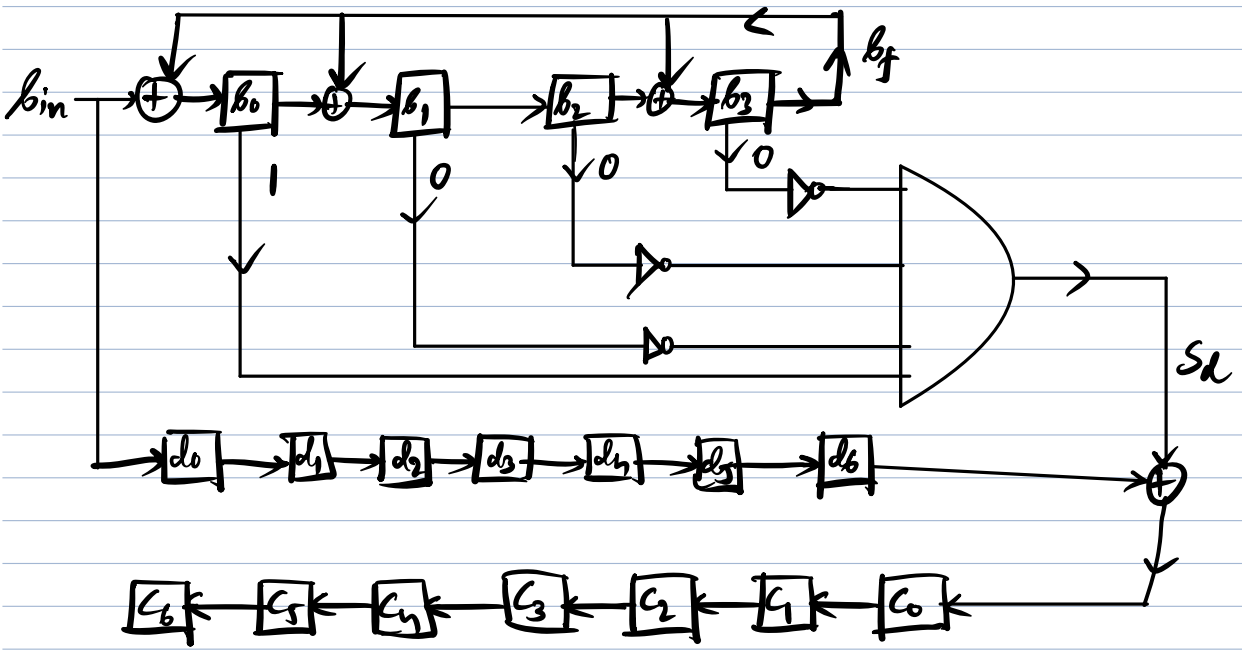
Now, $S_d(x) = R_{g(x)}[x^6] = 1 \longrightarrow$ $b_3 = 0 \rightarrow$ NOT

$b_2 = 0 \rightarrow$ NOT

$b_1 = 0 \rightarrow$ NOT

$b_0 = 1 \rightarrow$ NOT

$$
\begin{array}{r}
x^2 + x + 1 \\
x^4 + x^3 + x + 1 \;\big)\; x^6 \\
x^6 + x^5 + x^3 + x^2 \\
\hline
x^5 + x^3 + x^2 \\
x^5 \quad + x^2 + x^4 + x \\
\hline
x^4 + x^3 + x \\
x^4 + x^3 + x + 1 \\
\hline
1
\end{array}
$$



∵ Dilay is Khali!

shift	b_{in}	b_0	b_1	b_2	b_3	b_f	s_e	d_0	d_1	d_2	d_3	d_4	d_5	d_6	c_0	c_1	c_2	c_3	c_4	c_5	c_6	$s(x)$
	0	0	0	0	0	0	–	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
1	0	0	0	0	0	0	–	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
2	1	1	0	0	0	0	–	1	0	0	0	0	0	0	0	0	0	0	0	0	0	
3	1	1	1	0	0	0	–	1	1	0	0	0	0	0	0	0	0	0	0	0	0	
4	0	0	1	1	0	0	–	0	1	1	0	0	0	0	0	0	0	0	0	0	0	
5	0	0	0	1	1	0	–	0	0	1	1	0	0	0	0	0	0	0	0	0	0	
6	1	0	1	0	0	1	–	1	0	0	1	1	0	0	0	0	0	0	0	0	0	
7	0	0	0	1	0	0	0	0	1	0	0	1	1	0	0	0	0	0	0	0	0	
8	–	0	0	0	1	0	0	0	0	1	0	0	1	1	0	0	0	0	0	0	0	
9	–	1	1	0	1	1	0	0	0	0	1	0	0	1	1	0	0	0	0	0	0	
10	–	1	0	1	1	1	0	0	0	0	0	1	0	0	1	1	0	0	0	0	0	
11	–	1	0	0	0	1	1	0	0	0	0	0	1	0	0	1	1	0	0	0	0	
12	–	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	0	0	0	
13	–	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	0	0	
14	–	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	0	

0 1 1 0 0 1 0

$b_f = b_3$ $\quad b_1 = b_0 + b_f$

$b_3 = b_2 + b_f$ $\quad b_0 = b_{in} + b_f$

$b_2 = b_1$