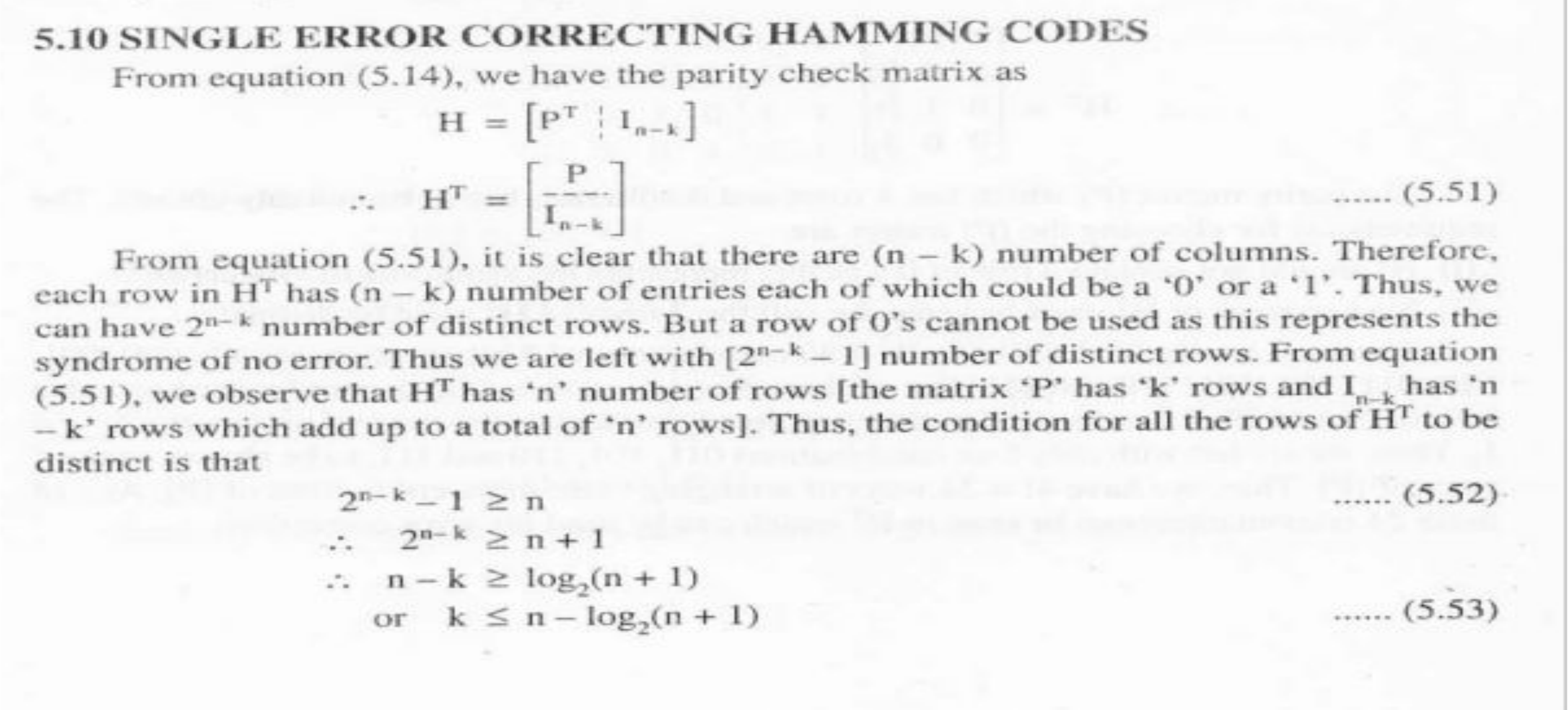
Hamming codes



5.10 SINGLE ERROR CORRECTING HAMMING CODES

From equation (5.14), we have the parity check matrix as

$$H = \left[P^T \;\vdots\; I_{n-k}\right]$$

$$\therefore \quad H^T = \left[\begin{array}{c} P \\ \hdashline I_{n-k} \end{array}\right] \qquad \text{...... (5.51)}$$

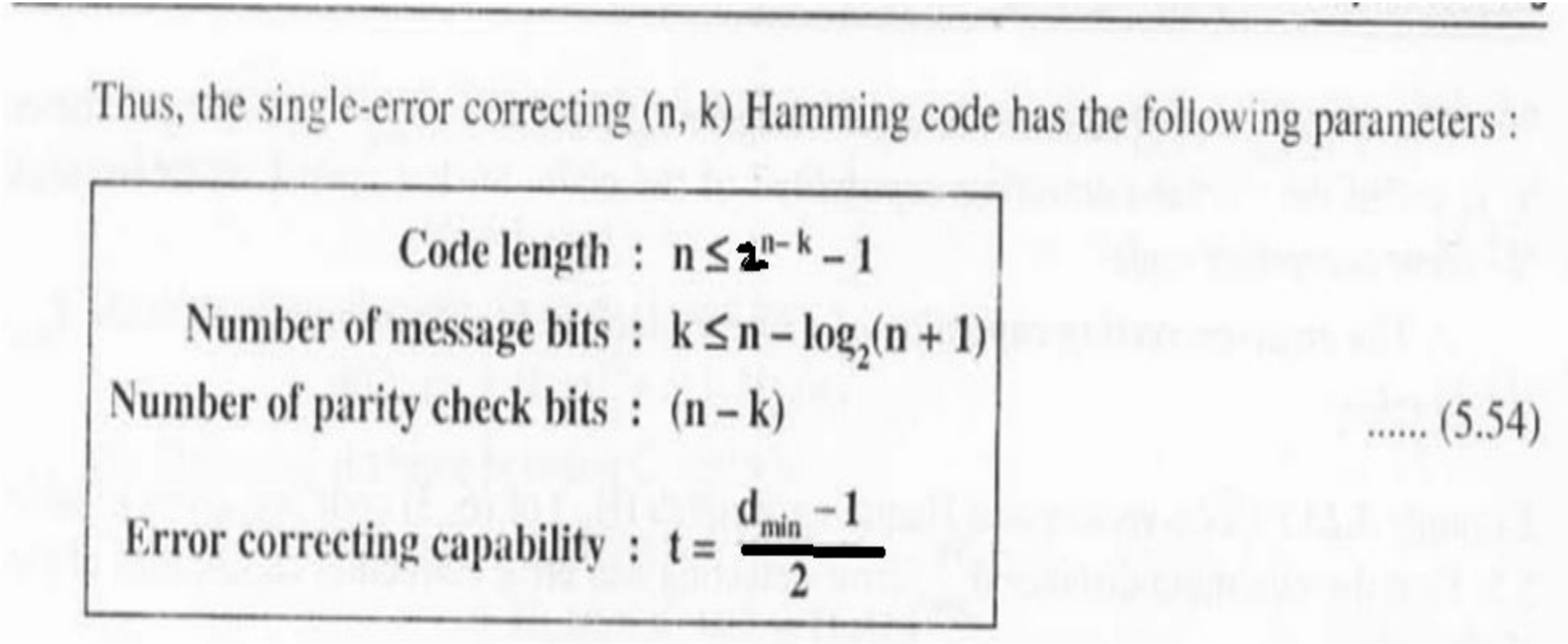
From equation (5.51), it is clear that there are (n – k) number of columns. Therefore, each row in H^T has (n – k) number of entries each of which could be a '0' or a '1'. Thus, we can have 2^{n-k} number of distinct rows. But a row of 0's cannot be used as this represents the syndrome of no error. Thus we are left with $[2^{n-k} - 1]$ number of distinct rows. From equation (5.51), we observe that H^T has 'n' number of rows [the matrix 'P' has 'k' rows and I_{n-k} has 'n – k' rows which add up to a total of 'n' rows]. Thus, the condition for all the rows of H^T to be distinct is that

$$2^{n-k} - 1 \geq n \qquad \text{...... (5.52)}$$

$$\therefore \quad 2^{n-k} \geq n + 1$$

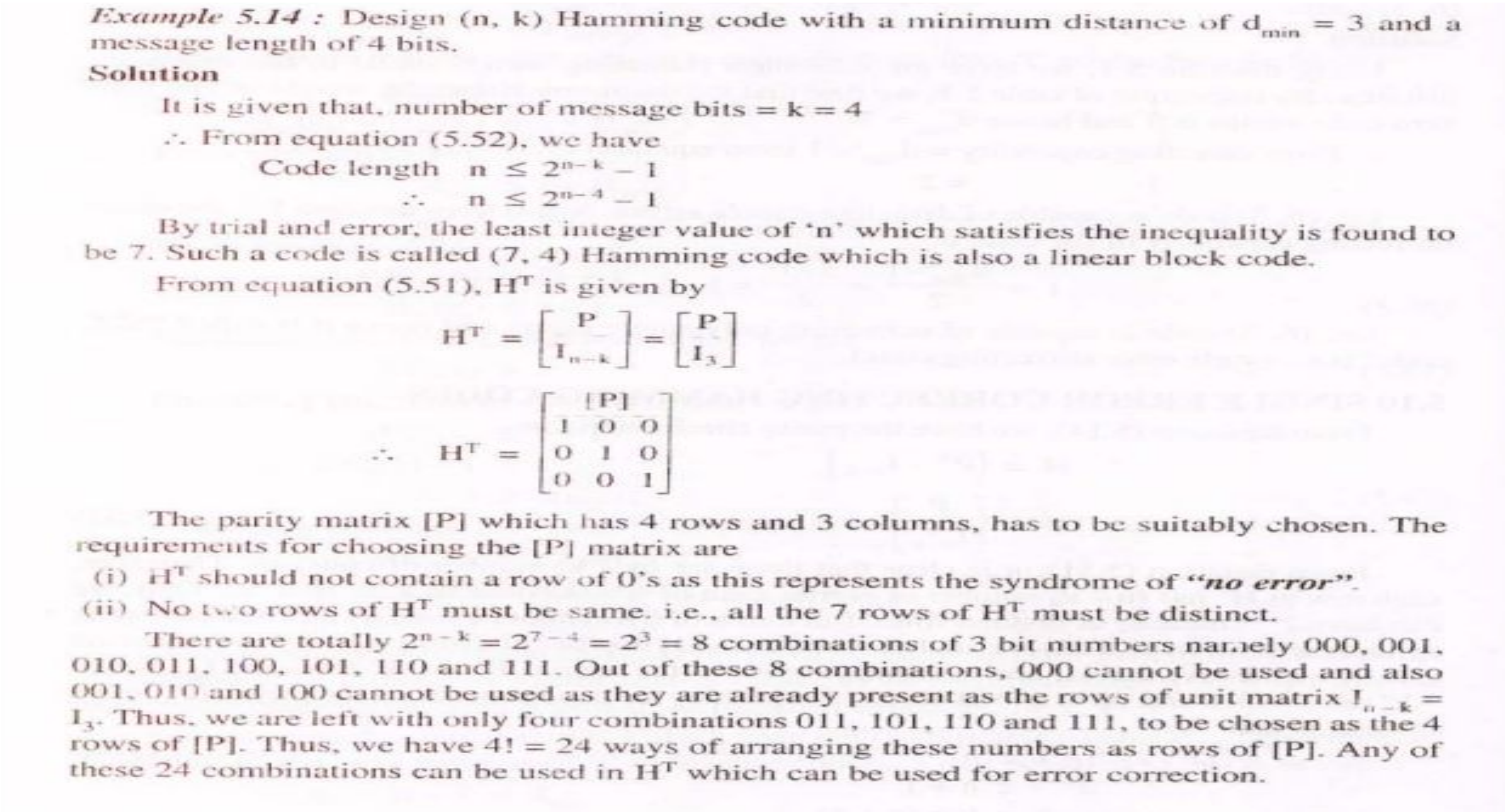
$$\therefore \quad n - k \geq \log_2(n + 1)$$

$$\text{or} \quad k \leq n - \log_2(n + 1) \qquad \text{...... (5.53)}$$



Thus, the single-error correcting (n, k) Hamming code has the following parameters :

$$\boxed{\begin{aligned} \text{Code length} &: \; n \le 2^{n-k} - 1 \\ \text{Number of message bits} &: \; k \le n - \log_2(n+1) \\ \text{Number of parity check bits} &: \; (n-k) \\ \text{Error correcting capability} &: \; t = \frac{d_{\min} - 1}{2} \end{aligned}} \qquad \text{......} \; (5.54)$$



Example 5.14 : Design (n, k) Hamming code with a minimum distance of $d_{min} = 3$ and a message length of 4 bits.

Solution

It is given that, number of message bits = k = 4

∴ From equation (5.52), we have

$$\text{Code length} \quad n \leq 2^{n-k} - 1$$

$$\therefore \quad n \leq 2^{n-4} - 1$$

By trial and error, the least integer value of 'n' which satisfies the inequality is found to be 7. Such a code is called (7, 4) Hamming code which is also a linear block code.

From equation (5.51), H^T is given by

$$H^T = \begin{bmatrix} P \\ \hline I_{n-k} \end{bmatrix} = \begin{bmatrix} P \\ \hline I_3 \end{bmatrix}$$

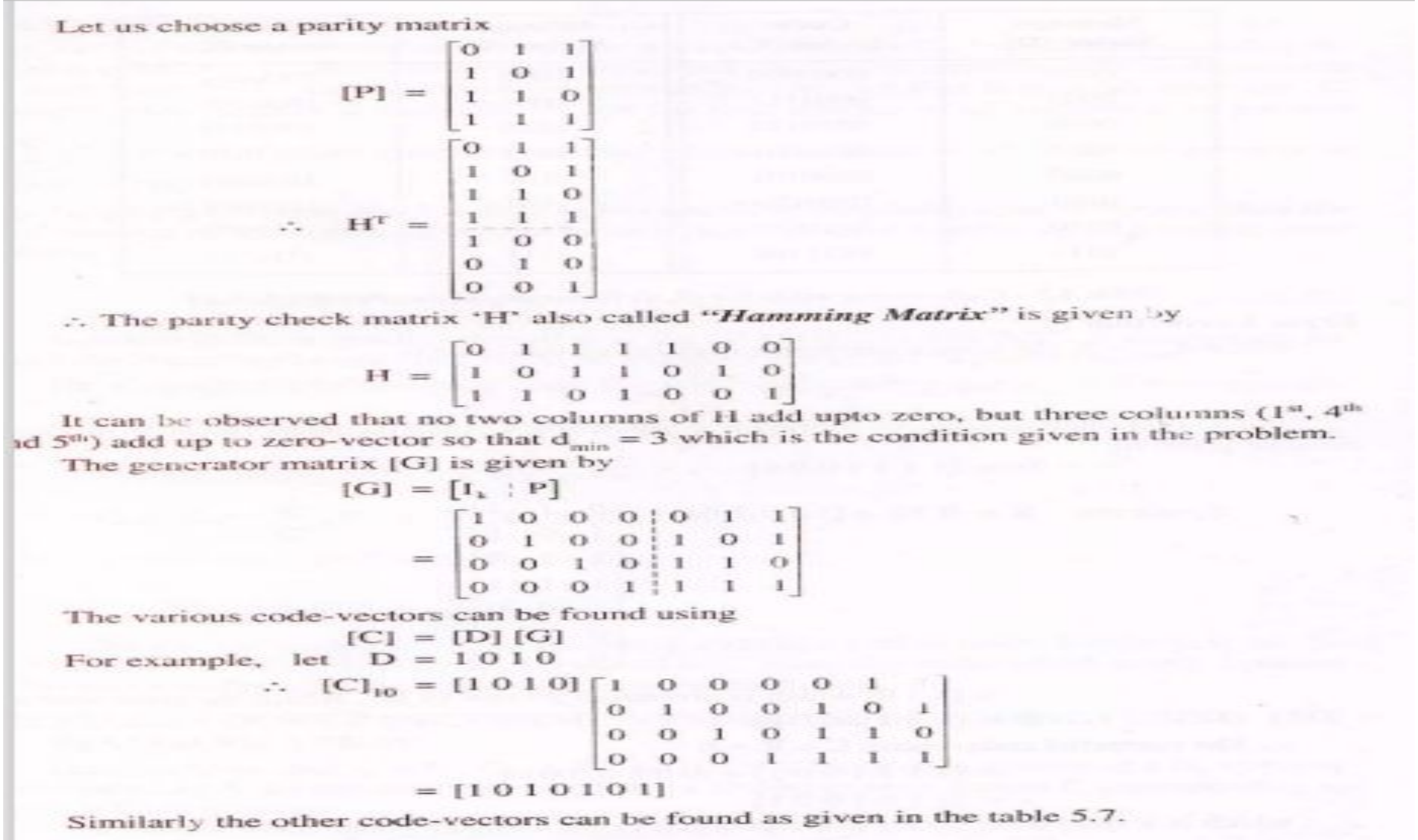
$$\therefore \quad H^T = \begin{bmatrix} & [P] & \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

The parity matrix [P] which has 4 rows and 3 columns, has to be suitably chosen. The requirements for choosing the [P] matrix are

(i) H^T should not contain a row of 0's as this represents the syndrome of ***"no error"***.

(ii) No two rows of H^T must be same. i.e., all the 7 rows of H^T must be distinct.

There are totally $2^{n-k} = 2^{7-4} = 2^3 = 8$ combinations of 3 bit numbers namely 000, 001, 010, 011, 100, 101, 110 and 111. Out of these 8 combinations, 000 cannot be used and also 001, 010 and 100 cannot be used as they are already present as the rows of unit matrix $I_{n-k} = I_3$. Thus, we are left with only four combinations 011, 101, 110 and 111, to be chosen as the 4 rows of [P]. Thus, we have 4! = 24 ways of arranging these numbers as rows of [P]. Any of these 24 combinations can be used in H^T which can be used for error correction.



Let us choose a parity matrix

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

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

∴ The parity check matrix 'H' also called ***"Hamming Matrix"*** is given by

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

It can be observed that no two columns of H add upto zero, but three columns (1st, 4th nd 5th) add up to zero-vector so that $d_{min} = 3$ which is the condition given in the problem.

The generator matrix [G] is given by

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

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

The various code-vectors can be found using

$$[C] = [D]\,[G]$$

For example, let D = 1 0 1 0

$$\therefore \quad [C]_{10} = [1\,0\,1\,0] \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

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

Similarly the other code-vectors can be found as given in the table 5.7.

Message Vector (D)	Code-vector (C)	Message Vector (D)	Code-vector (C)
0000	0000000	1000	1000011
0001	0001111	1001	1001100
0010	0010110	1010	1010101
0011	0011001	1011	1011010
0100	0100101	1100	1100110
0101	0101010	1101	1101001
0110	0110011	1110	1110000
0111	0111100	1111	1111111

Table 5.7 : Code-vector table for (7, 4) Hamming code of example 5.14

Error Correction :

Since $d_{min} = 3$, the error correcting capability of this code is

$$t = \frac{d_{min} - 1}{2} = \frac{3-1}{2} = 1$$

∴ (7, 4) Hamming code, so formed is a SEC code. Let the received vector with single error be given by

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

$$\therefore \text{ Syndrome } \quad S = R\,H^T = [1\ 1\ 1\ 1\ 0\ 0\ 1]\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$= [1\ 1\ 0]$ which is present in 3rd row of H^T. Hence the error-vector

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

∴ The corrected code-vector $C = R + E$

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

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

which is a valid code vector corresponding to the message vector 1101 in table 5.7.

Hamming Codes

- **Hamming Codes** are linear block codes designed to detect and correct errors introduced in message bits transmitted from an end to another through a communication channel. These are single error-correcting codes that offer ease in encoding and decoding. Hamming Code falls under the category of error correction coding and is a type of cyclic code.

Hamming Codes – Encoding

- The steps involved to perform encoding of hamming codes are as follows:

1. First, perform the calculation for the total number of redundant bits required to be added with the given message bits. The number of redundant bits can be obtained by:

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

: P is the number of parity bits,

- k is the number of information bits.

2. Once the number of redundant bits is detected then we have to check for the positions where the redundant bits are to be placed.

Note: The redundant bits within the message bits are placed at those positions which are powers of 2.

3. Now, determine the value of redundant bits to be inserted at the positions determined in the previous step.

The types of parity bits play a crucial role here. Meaning, if there is even parity, then the total number of 1s must be even in count. While if there is odd parity, then the total number of 1s must be odd in the count.

Example for Encoding

Suppose we are having a message signal given as:

k = 1001 and it is to be transmitted after encoding with **even parity**. Encode using Hamming code

Soln:

So, calculating the number of redundant bits using

equation for redundant bit calculation

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

For P =2

$4 \geq 4 + 3 + 1$ = Not satisfied

For P =3

$8 \geq 4 + 3 + 1$ = satisfied

So, we will take P = 3 for k = 4

Next, we to check at which positions these 4 parity bits are to be placed. So, according to hamming, the parity bits will be present at positions which are powers of 2 i.e., 2^0, 2^1, 2^2, 2^3, and so on.

So, forming the hamming code arrangement for code (7, 4). Also, placing the 3 bits of parity at the desired positions. This will be done in a way that in the 9 given blocks, according to the powers of 2, the parity bits will be present at positions,

$2^0 = 1$; $2^1 = 2$; $2^2 = 4$

P_4	P_2	P_1
0	0	**1**
0	1	0
0	1	**1**
1	0	0
1	0	**1**
1	1	0
1	1	**1**

7	6	5	4	3	2	1
1	0	0	P_4	1	P_2	P_1

P_1 = 1 for 1,3,5,7 = P_1 1 0 1 , P_1 = 0

P_2 = 1 for 2,3,6,7 = P_2 1 0 1, P_2 = 0

P_4 = 1 for 4,5,6,7 = P_4 0 0 1, P_4 = 1

7	6	5	4	3	2	1
1	0	0	1	1	0	0

The encoded message is 1001100

2) If the receiver receives the data as 1101100 with 1 bit error. Correct it

P_1 = 1 for 1,3,5,7 = 0 1 0 1 , P_1 = 0

P_2 = 1 for 2,3,6,7 = 0 1 1 1, P_2 = 1

P_4 = 1 for 4,5,6,7 = 1 0 0 1, P_4 = 1

If all values are 0 0 0, no error

But P_4 P_2 $P_{1\,=}$ 110 = 6, so bit position 6 is error.

So, the correct codeword is 1001100

3) If the receiver receives the data as 1001100 with 1 bit error. Correct it

P_1 = 1 for 1,3,5,7 = 0 1 0 1 , P_1 = 0

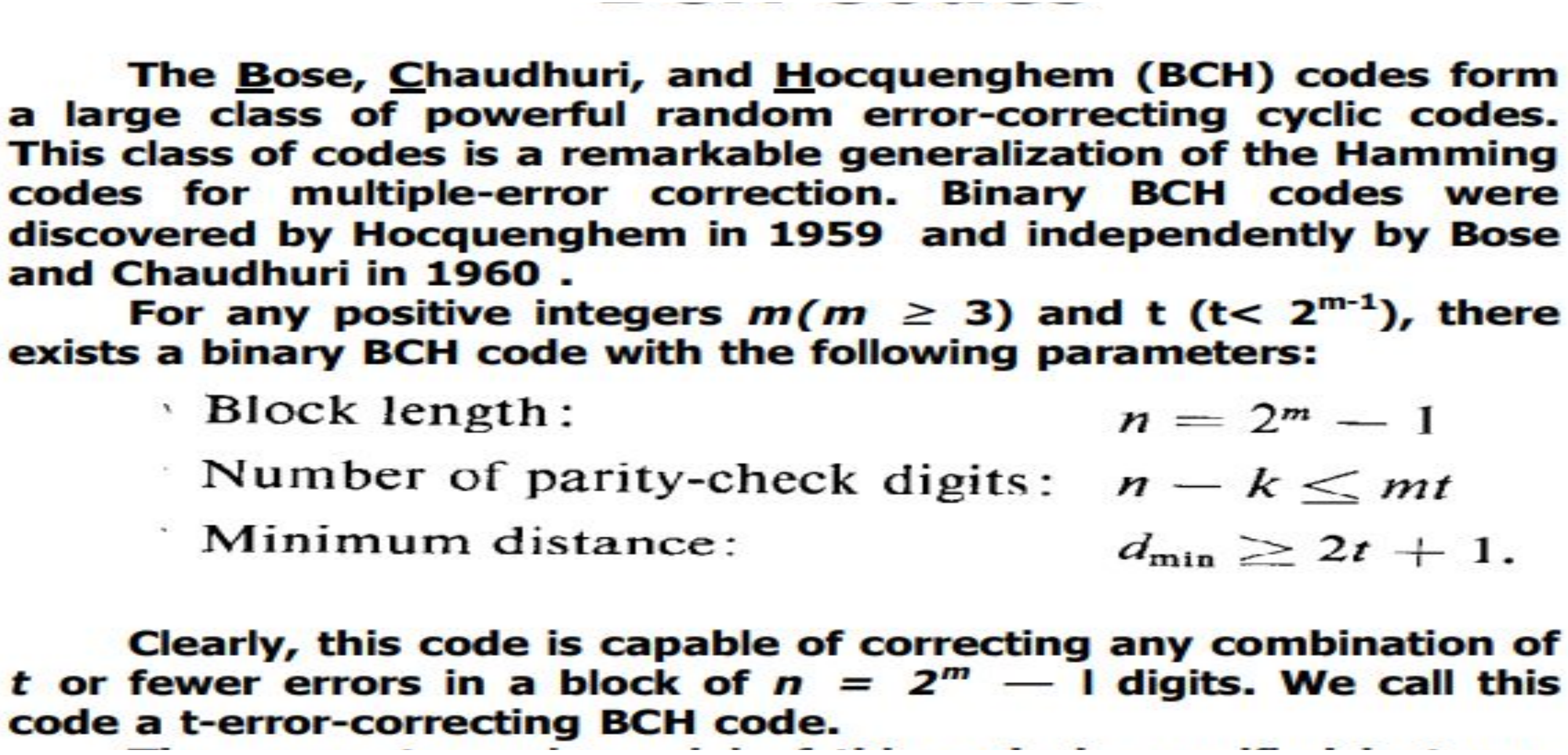
P_2 = 1 for 2,3,6,7 = 0 1 0 1, P_2 = 0

P_4 = 1 for 4,5,6,7 = 1 0 0 1, P_4 = 0

Since parity bits are all 0 0 0, no error

So, the codeword 1001100, is correct with no error.

BCH Codes



The Bose, Chaudhuri, and Hocquenghem (BCH) codes form a large class of powerful random error-correcting cyclic codes. This class of codes is a remarkable generalization of the Hamming codes for multiple-error correction. Binary BCH codes were discovered by Hocquenghem in 1959 and independently by Bose and Chaudhuri in 1960 .

For any positive integers $m(m \geq 3)$ and t ($t< 2^{m-1}$), there exists a binary BCH code with the following parameters:

- Block length: $n = 2^m - 1$
- Number of parity-check digits: $n - k \leq mt$
- Minimum distance: $d_{\min} \geq 2t + 1.$

Clearly, this code is capable of correcting any combination of t or fewer errors in a block of $n = 2^m - 1$ digits. We call this code a t-error-correcting BCH code.

It follows from (3) that the double-error-correcting BCH code of length n = $2^4 - 1 = 15$ is generated by

$$\mathbf{g}(X) = \text{LCM}\,\{\phi_1(X), \phi_3(X)\}.$$

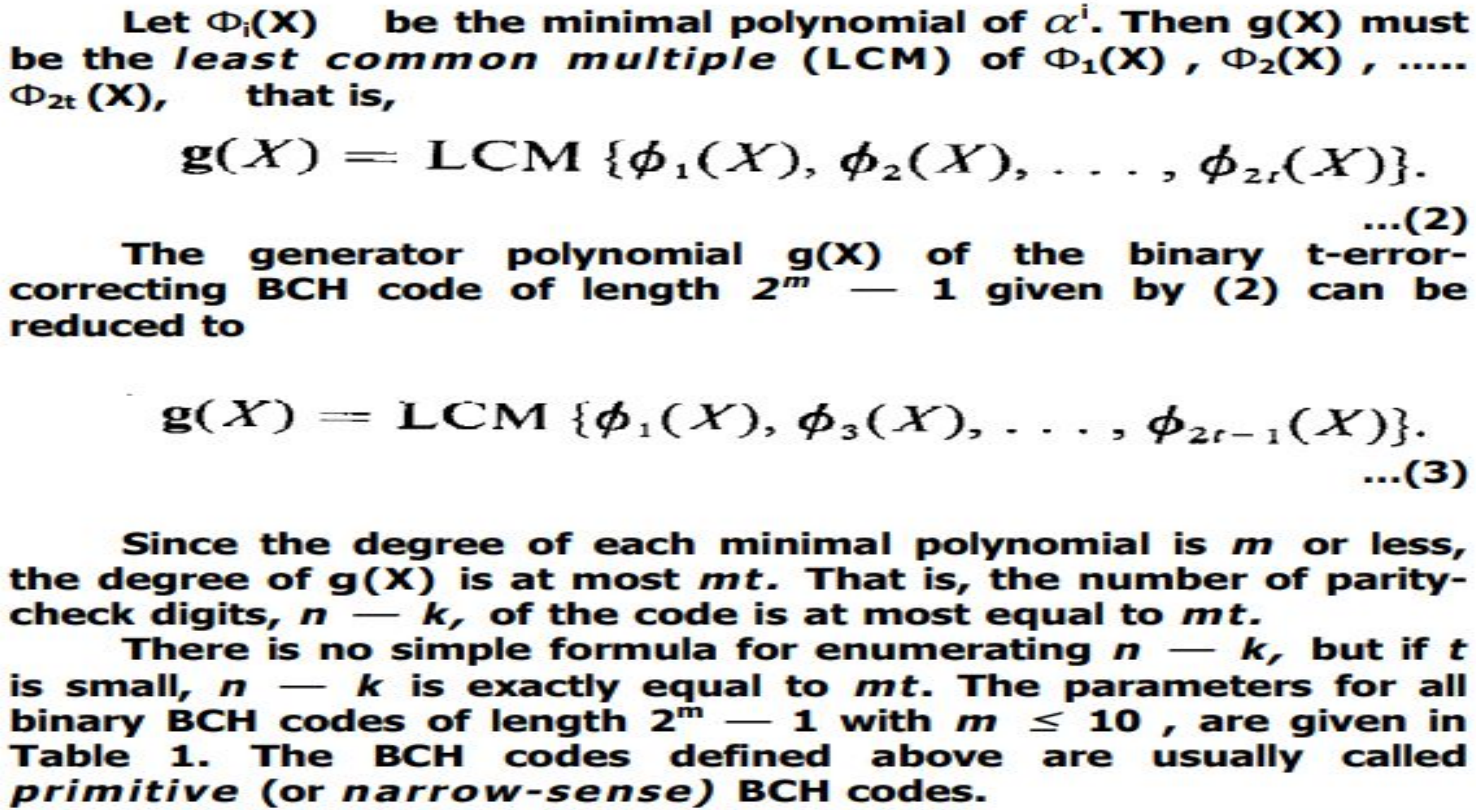
$$\begin{aligned} g(X) &= \phi_1(X)\phi_3(X) \\ &- (1 + X + X^4)(1 + X + X^2 + X^3 + X^4) \\ &= 1 + X^4 + X^6 + X^7 + X^8. \end{aligned}$$

Thus, the code is a (15, 7) cyclic code with $d_{min} \geq 5$. Since the generator polynomial is code polynomial of weight 5, the minimum distance of this code is exactly 5.

EXAMPLE 2: The triple-error-correcting BCH code of length 15 is generated by

$$\begin{aligned} g(X) &= \text{LCM}\,\{\phi_1(X), \phi_3(X), \phi_5(X)\} \\ &= (1 + X + X^4)(1 + X + X^2 + X^3 + X^4)(1 + X + X^2) \\ &= 1 + X + X^2 + X^4 + X^5 + X^8 + X^{10}. \end{aligned}$$

This triple-error-correcting BCH code is a (15, 5) cyclic code with $d_{min} \geq 7$. Since the weight of the generator polynomial is 7, the minimum distance of this code is exactly 7.



Let $\Phi_i(X)$ be the minimal polynomial of α^i. Then g(X) must be the *least common multiple* (LCM) of $\Phi_1(X)$, $\Phi_2(X)$, ... $\Phi_{2t}(X)$, that is,

$$g(X) = \text{LCM}\{\phi_1(X), \phi_2(X), \ldots, \phi_{2t}(X)\}. \quad \ldots(2)$$

The generator polynomial g(X) of the binary t-error-correcting BCH code of length $2^m - 1$ given by (2) can be reduced to

$$g(X) = \text{LCM}\{\phi_1(X), \phi_3(X), \ldots, \phi_{2t-1}(X)\}. \quad \ldots(3)$$

Since the degree of each minimal polynomial is *m* or less, the degree of g(X) is at most *mt*. That is, the number of parity-check digits, *n — k,* of the code is at most equal to *mt.*

There is no simple formula for enumerating *n — k,* but if *t* is small, *n — k* is exactly equal to *mt*. The parameters for all binary BCH codes of length $2^m - 1$ with $m \leq 10$, are given in Table 1. The BCH codes defined above are usually called *primitive* (or *narrow-sense)* BCH codes.

n	k	t	Generator polynomial
7	4	1	1101
15	11	1	11001
15	7	2	100010111
15	5	3	11101100101
31	26	1	101001
31	21	2	10010110111
31	16	3	1111010111110001
31	11	5	101010110110010001101
31	6	7	11100100010101111011010011

Table 6.15 : Parameters of some useful BCH code

Example : In order to construct a (15, 5) BCH code from the table (6.15), we have for (15.5) code, the coefficients of generator polynomial as

$$\begin{array}{ccccccccccc} 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\ x^0 & x & x^2 & x^3 & x^4 & x^5 & x^6 & x^7 & x^8 & x^9 & x^{10} \end{array}$$

$\therefore$ $g(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$ is the generator polynomial for (15, 5) triple-error correcting BCH code. Since the degree of g(x) is 10, there are 10-check bits and 5-information digits in (15, 5) BSC code.

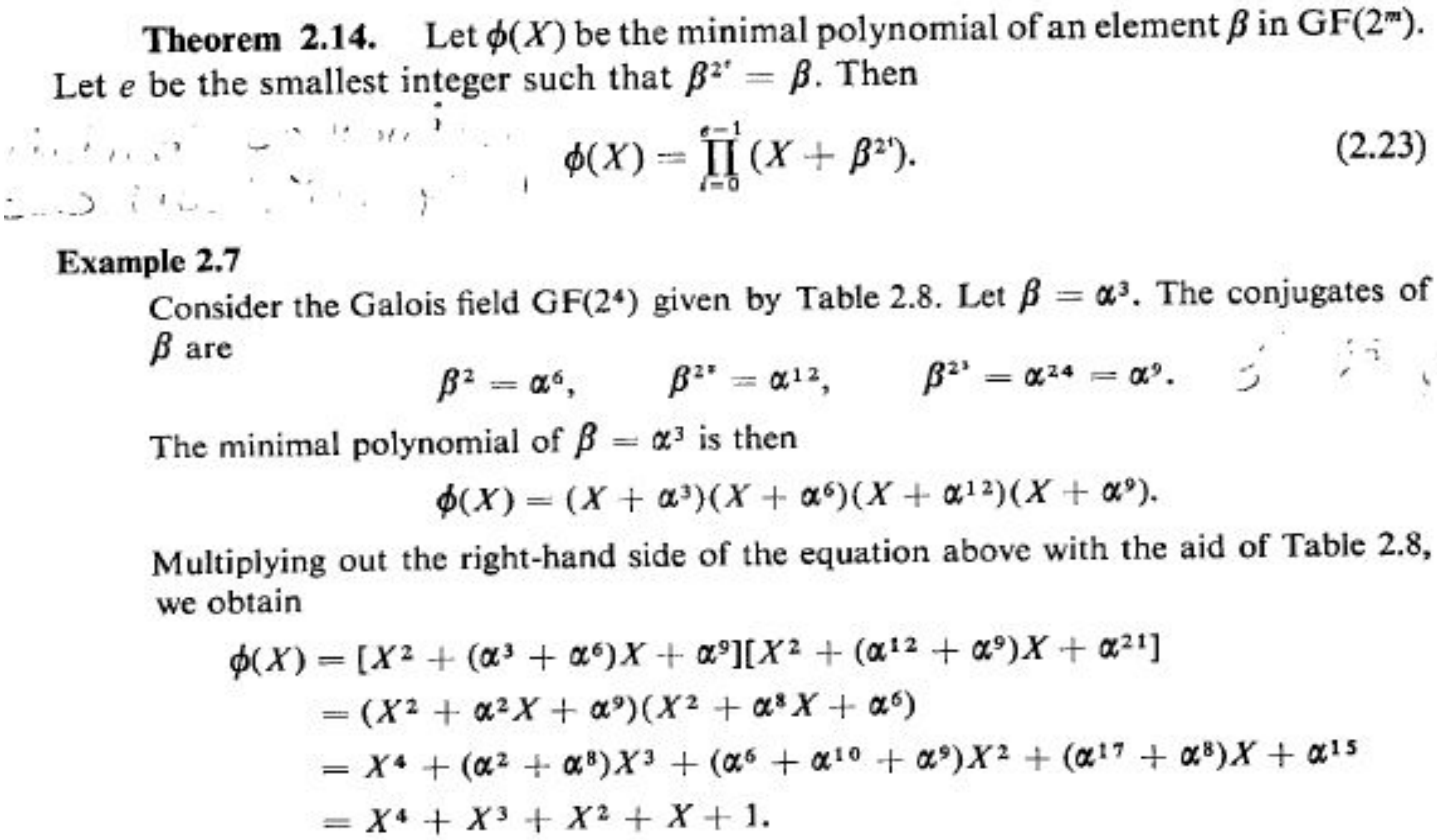
There are seven terms in g(x) including $x^0 = 1$. Hence the minimum distance $d_{min} = 7$. Thus the error-correcting capability of (15, 5) BCH code is

$$t \leq \frac{d_{min} - 1}{2}$$

$$\therefore \quad t_{max} \leq \frac{7 - 1}{2} = 3$$

Thus (15, 5) BCH code is capable of correcting upto a maximum of 3 errors. Several iterative procedures (such as Berlekamp iterative algorithm) are available for decoding BCH codes. These can be programmed on a general purpose digital computer which forms integral part of data communication network. However, software implementation of these algorithms has many advantages over hardware implementation.

Minimal Polynomial



Theorem 2.14. Let $\phi(X)$ be the minimal polynomial of an element β in GF(2^m). Let e be the smallest integer such that $\beta^{2^e} = \beta$. Then

$$\phi(X) = \prod_{i=0}^{e-1} (X + \beta^{2^i}). \tag{2.23}$$

Example 2.7

Consider the Galois field GF(2^4) given by Table 2.8. Let $\beta = \alpha^3$. The conjugates of β are

$$\beta^2 = \alpha^6, \qquad \beta^{2^2} = \alpha^{12}, \qquad \beta^{2^3} = \alpha^{24} = \alpha^9.$$

The minimal polynomial of $\beta = \alpha^3$ is then

$$\phi(X) = (X + \alpha^3)(X + \alpha^6)(X + \alpha^{12})(X + \alpha^9).$$

Multiplying out the right-hand side of the equation above with the aid of Table 2.8, we obtain

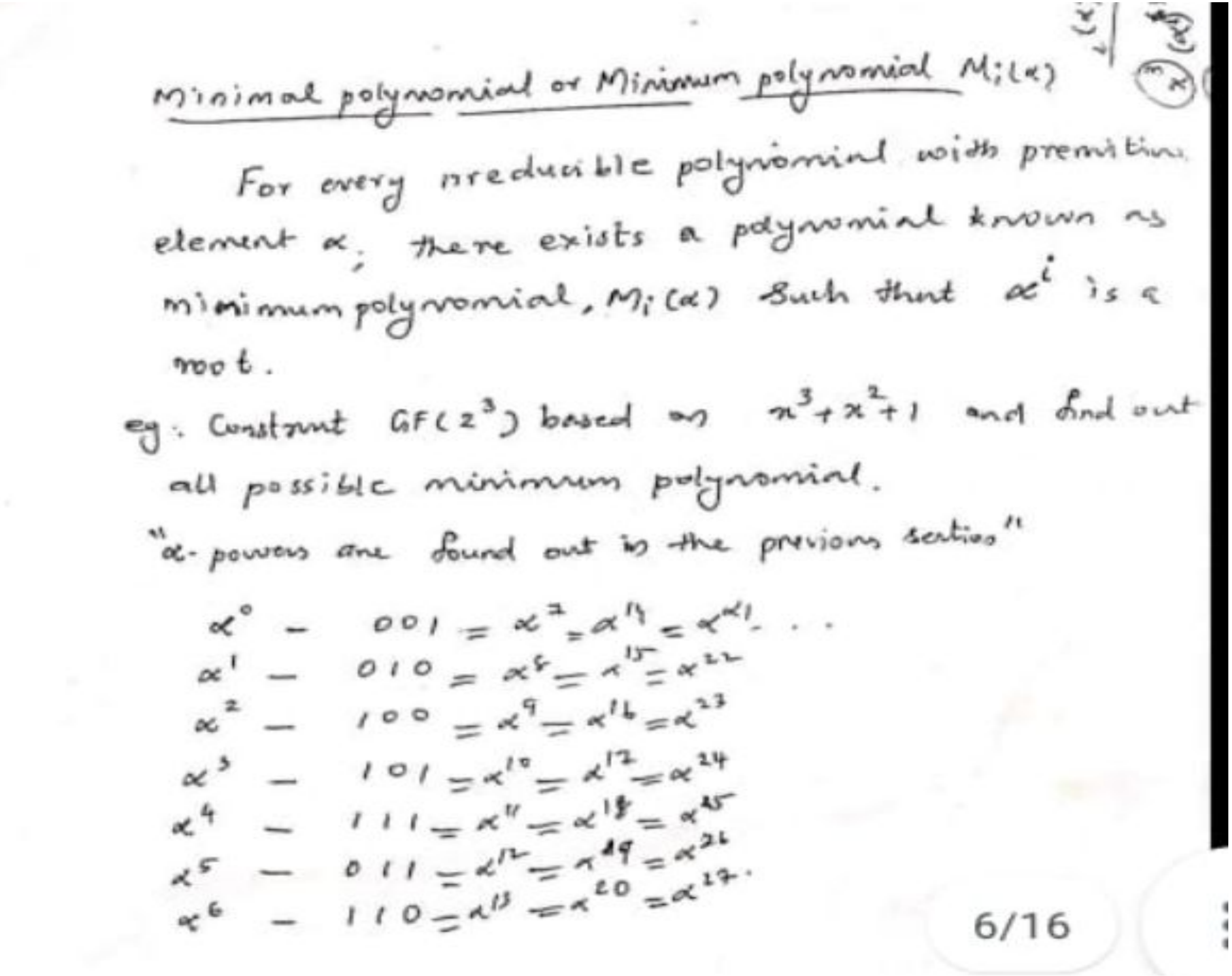
$$\begin{aligned}
\phi(X) &= [X^2 + (\alpha^3 + \alpha^6)X + \alpha^9][X^2 + (\alpha^{12} + \alpha^9)X + \alpha^{21}] \\
&= (X^2 + \alpha^2 X + \alpha^9)(X^2 + \alpha^8 X + \alpha^6) \\
&= X^4 + (\alpha^2 + \alpha^8)X^3 + (\alpha^6 + \alpha^{10} + \alpha^9)X^2 + (\alpha^{17} + \alpha^8)X + \alpha^{15} \\
&= X^4 + X^3 + X^2 + X + 1.
\end{aligned}$$

TABLE 2.8 THREE REPRESENTATIONS FOR THE ELEMENTS OF GF(2^4) GENERATED BY $p(X) = 1 + X + X^4$

Power representation	Polynomial representation	4-Tuple representation
0	0	$(0\ 0\ 0\ 0)$
1	1	$(1\ 0\ 0\ 0)$
α	α	$(0\ 1\ 0\ 0)$
α^2	α^2	$(0\ 0\ 1\ 0)$
α^3	α^3	$(0\ 0\ 0\ 1)$
α^4	$1 + \alpha$	$(1\ 1\ 0\ 0)$
α^5	$\alpha + \alpha^2$	$(0\ 1\ 1\ 0)$
α^6	$\alpha^2 + \alpha^3$	$(0\ 0\ 1\ 1)$
α^7	$1 + \alpha + \alpha^3$	$(1\ 1\ 0\ 1)$
α^8	$1 + \alpha^2$	$(1\ 0\ 1\ 0)$
α^9	$\alpha + \alpha^3$	$(0\ 1\ 0\ 1)$
α^{10}	$1 + \alpha + \alpha^2$	$(1\ 1\ 1\ 0)$
α^{11}	$\alpha + \alpha^2 + \alpha^3$	$(0\ 1\ 1\ 1)$
α^{12}	$1 + \alpha + \alpha^2 + \alpha^3$	$(1\ 1\ 1\ 1)$
α^{13}	$1 + \alpha^2 + \alpha^3$	$(1\ 0\ 1\ 1)$
α^{14}	$1 + \alpha^3$	$(1\ 0\ 0\ 1)$

TABLE 2.9 MINIMAL POLYNOMIALS OF THE ELEMENTS IN GF(2^4) GENERATED BY $p(X) = X^4 + X + 1$

Conjugate roots	Minimal polynomials
0	X
1	$X + 1$
$\alpha, \alpha^2, \alpha^4, \alpha^8$	$X^4 + X + 1$
$\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$	$X^4 + X^3 + X^2 + X + 1$
α^5, α^{10}	$X^2 + X + 1$
$\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14}$	$X^4 + X^3 + 1$



Minimal polynomial or Minimum polynomial $M_i(\alpha)$

For every irreducible polynomial with premitive element α; there exists a polynomial known as minimum polynomial, $M_i(\alpha)$ such that α^i is a root.

eg: Construct $GF(2^3)$ based on x^3+x^2+1 and find out all possible minimum polynomial.

"α- powers are found out in the previous section"

$$
\begin{aligned}
\alpha^0 &- 001 = \alpha^7 = \alpha^{14} = \alpha^{21} \ldots \\
\alpha^1 &- 010 = \alpha^8 = \alpha^{15} = \alpha^{22} \\
\alpha^2 &- 100 = \alpha^9 = \alpha^{16} = \alpha^{23} \\
\alpha^3 &- 101 = \alpha^{10} = \alpha^{17} = \alpha^{24} \\
\alpha^4 &- 111 = \alpha^{11} = \alpha^{18} = \alpha^{25} \\
\alpha^5 &- 011 = \alpha^{12} = \alpha^{19} = \alpha^{26} \\
\alpha^6 &- 110 = \alpha^{13} = \alpha^{20} = \alpha^{27}.
\end{aligned}
$$

To find $M_0(\alpha)$.

$x^3 \quad \alpha^0 \quad 0\,0\,1$

$x^2 \quad \alpha^0 \quad 0\,0\,1$

$\textcircled{x} \quad \alpha^0 \quad 0\,0\,1$ ✓

$\textcircled{1} \quad \alpha^0 \quad 0\,0\,1$ ✓

$\alpha + 1 = 0.$

s. $\underline{M_0(x) = x+1}$

$M_1(\alpha)$

$\textcircled{x^3} \quad \alpha^3 - 1\,0\,1$ ✓

$\textcircled{x^2} \quad \alpha^2 - 1\,0\,0$ ✓

$x \quad \alpha - 0\,1\,0$

$\textcircled{1} \quad 1 - 0\,0\,1$ ✓

$\alpha^3 + \alpha^2 + 1 = 0$

$\therefore \underline{M_1(x) = x^3 + x^2 + 1}$

$M_2(\alpha)$

$$\boxed{x^3}\ (\alpha^2)^3 - \alpha^6 - 1\,1\,0\ ✓$$

$$\boxed{x^2}\ (\alpha^2)^2 - \alpha^4 - 1\,1\,1\ ✓$$

$$x\ (\alpha^2) - \alpha^2 - 1\,0\,0$$

$$\boxed{1}\ (\alpha^2)^0 - 1 - \underline{0\,0\,1}\ ✓$$

$$M_2(x) = x^3 + x^2 + 1$$

$M_3(\alpha)$

$$\boxed{x^3}\ \alpha^9\ \ 1\,0\,0\ ✓$$

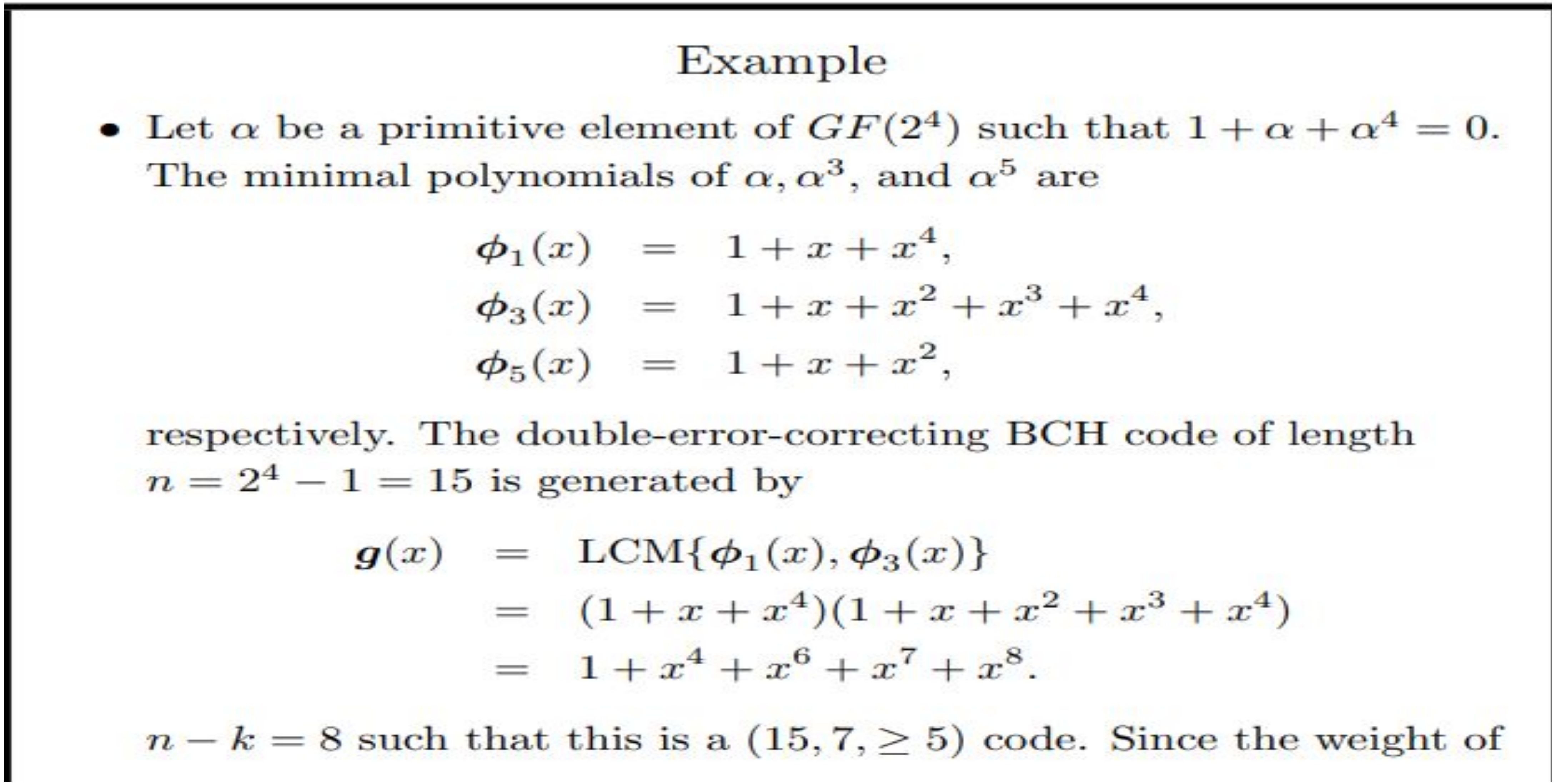
$$x^2\ \alpha^6\ \ 1\,1\,0$$

$$\boxed{x}\ \alpha^3\ \ 1\,0\,1\ ✓$$

$$\boxed{1}\ 1\ \ \underline{0\,0\,1}\ ✓$$

$$M_3(x) = x^3 + x + 1$$

Find the generator polynomial for t=2, and t=3



Example

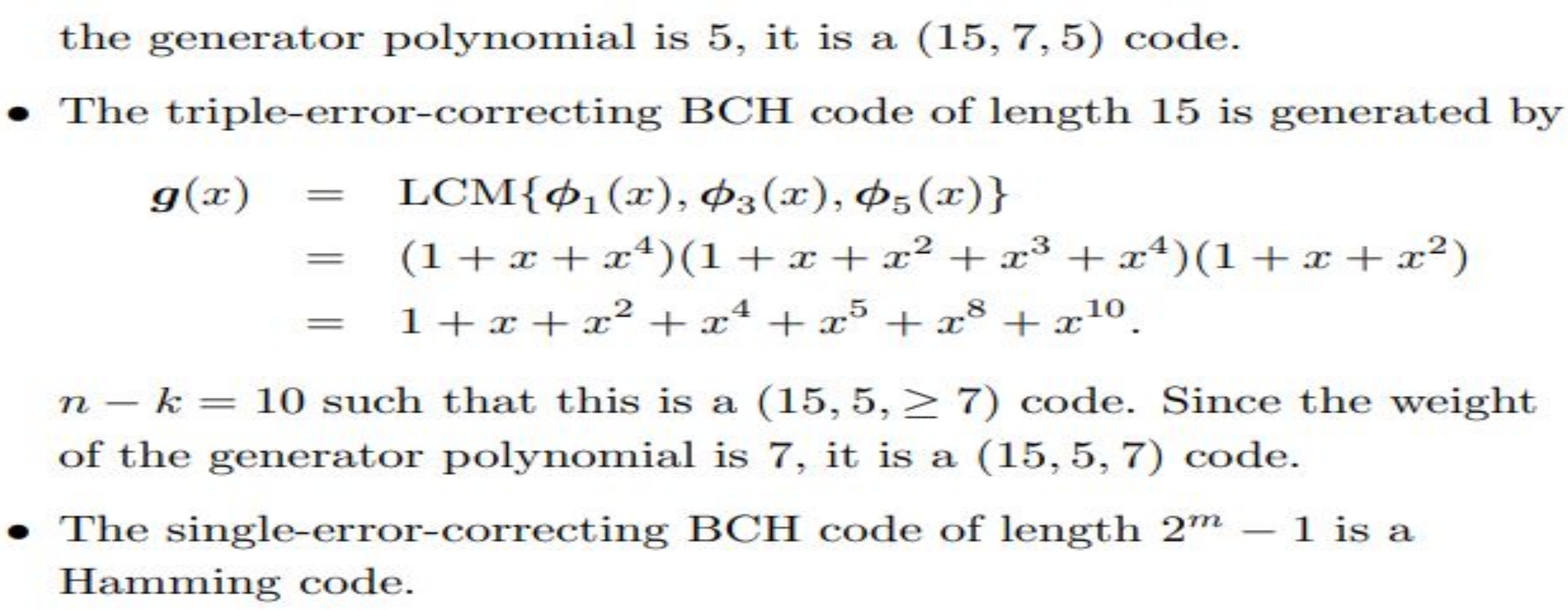
- Let α be a primitive element of $GF(2^4)$ such that $1+\alpha+\alpha^4=0$. The minimal polynomials of α, α^3, and α^5 are

$$\begin{aligned} \boldsymbol{\phi}_1(x) &= 1+x+x^4, \\ \boldsymbol{\phi}_3(x) &= 1+x+x^2+x^3+x^4, \\ \boldsymbol{\phi}_5(x) &= 1+x+x^2, \end{aligned}$$

respectively. The double-error-correcting BCH code of length $n=2^4-1=15$ is generated by

$$\begin{aligned} \boldsymbol{g}(x) &= \mathrm{LCM}\{\boldsymbol{\phi}_1(x), \boldsymbol{\phi}_3(x)\} \\ &= (1+x+x^4)(1+x+x^2+x^3+x^4) \\ &= 1+x^4+x^6+x^7+x^8. \end{aligned}$$

$n-k=8$ such that this is a $(15, 7, \geq 5)$ code. Since the weight of



the generator polynomial is 5, it is a $(15, 7, 5)$ code.

- The triple-error-correcting BCH code of length 15 is generated by

$$\begin{aligned} \boldsymbol{g}(x) &= \text{LCM}\{\boldsymbol{\phi}_1(x), \boldsymbol{\phi}_3(x), \boldsymbol{\phi}_5(x)\} \\ &= (1 + x + x^4)(1 + x + x^2 + x^3 + x^4)(1 + x + x^2) \\ &= 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}. \end{aligned}$$

  $n - k = 10$ such that this is a $(15, 5, \geq 7)$ code. Since the weight of the generator polynomial is 7, it is a $(15, 5, 7)$ code.

- The single-error-correcting BCH code of length $2^m - 1$ is a Hamming code.

$\alpha\ \alpha^2\ \alpha^4\ \alpha^8\ \alpha^{16} = \alpha$

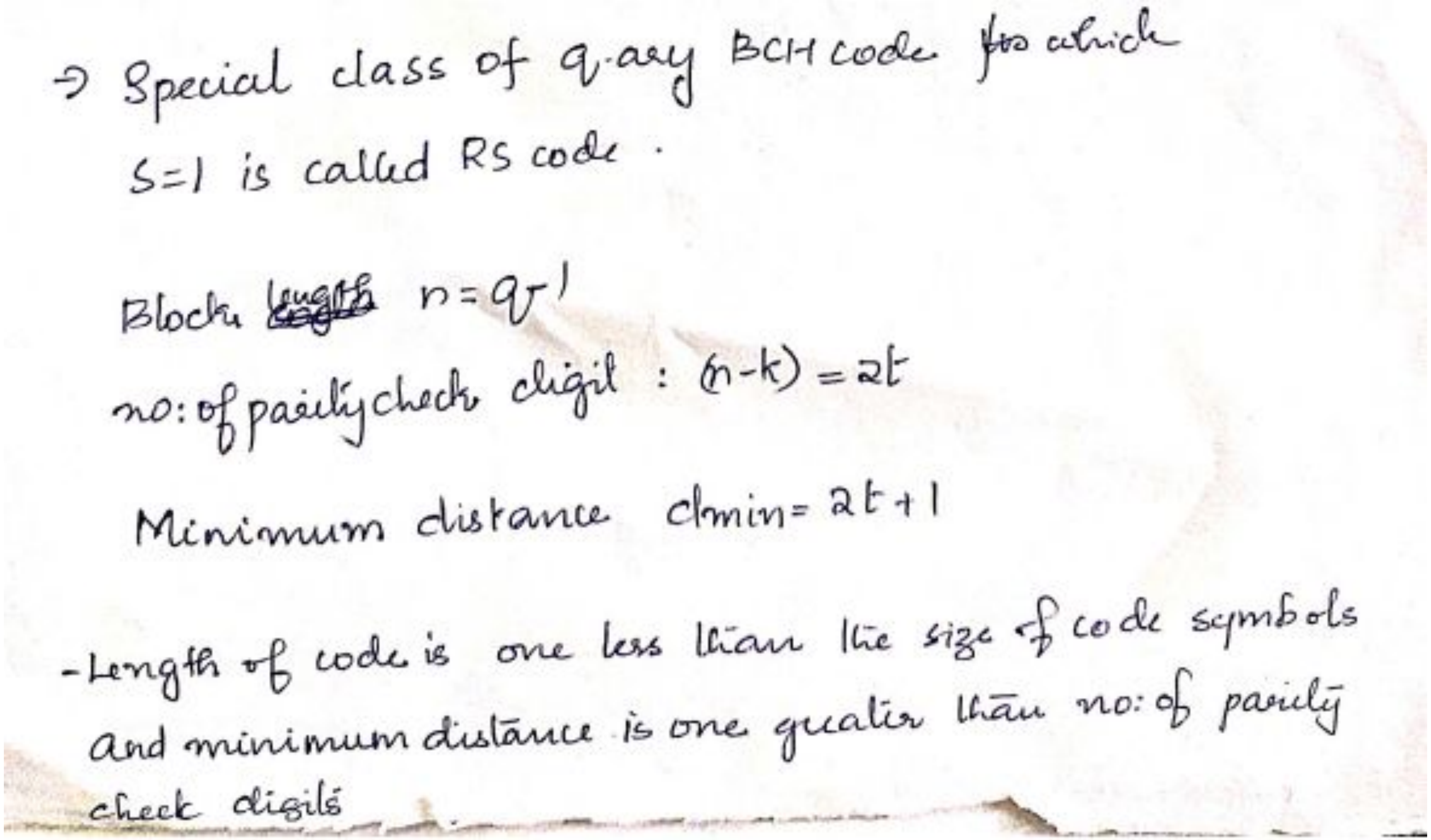
$\alpha^3\ \alpha^6\ \alpha^{12}\ \underline{\alpha}^{24}\ \alpha^{48} = \alpha^3$

$= \alpha^9$

Representations of GF(2^4). $p(z) = z^4 + z + 1$

Exponential Notation	Polynomial Notation	Binary Notation	Decimal Notation	Minimal Polynomial
0	0	0000	0	x
α^0	1	0001	1	$x + 1$
α^1	z	0010	2	$x^4 + x + 1$
α^2	z^2	0100	4	$x^4 + x + 1$
α^3	z^3	1000	8	$x^4 + x^3 + x^2 + x + 1$
α^4	$z + 1$	0011	3	$x^4 + x + 1$
α^5	$z^2 + z$	0110	6	$x^2 + x + 1$
α^6	$z^3 + z^2$	1100	12	$x^4 + x^3 + x^2 + x + 1$
α^7	$z^3 + z + 1$	1011	11	$x^4 + x^3 + 1$
α^8	$z^2 + 1$	0101	5	$x^4 + x + 1$
α^9	$z^3 + z$	1010	10	$x^4 + x^3 + x^2 + x + 1$
α^{10}	$z^2 + z + 1$	0111	7	$x^2 + x + 1$
α^{11}	$z^3 + z^2 + z + 1$	1110	14	$x^4 + x^3 + 1$
α^{12}	$z^3 + z^2 + z + 1$	1111	15	$x^4 + x^3 + x^2 + x + 1$
α^{13}	$z^3 + z^2 + 1$	1101	13	$x^4 + x^3 + 1$
α^{14}	$z^3 + 1$	1001	9	$x^4 + x^3 + 1$

Reed Solomon codes



→ Special class of q-ary BCH code for which S=1 is called RS code .

Block ~~length~~ length $n=q-1$

no: of paritycheck digit : $(n-k)=2t$

Minimum distance $d_{min}=2t+1$

- Length of code is one less than the size of code symbols and minimum distance is one greater than no: of parity check digits