Example 4.7 Decode the received vector $r = (010000000000000)$ using the (15, 11) parity check matrix.

Solution

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

The received vector is $r = (010000000000000)$
The corresponding syndrome $s = r * H^{\mathrm{T}}$ is

$$s = (0100)$$

The syndrome is the transposition of 1st column of H. Inverting the 1st coordinate of r, the following code word is obtained

$$c = (000000000000000)$$

Example 4.8 Decode the received vector $r = (001100011100000)$ vector using the (15, 11) parity check matrix vector.

Solution

The received vector is $r = (001100011100000)$
The corresponding syndrome $s = r * H^{T}$ is $s = (0011)$
The syndrome is the transposition of 7th column of H. Inverting the 7th coordinate of r, the following code word is obtained

$$c = (001100001100000)$$

4.3 Cyclic Codes

An (n, k) linear block code C is said to be a cyclic code if for every codeword $c = (c_0, c_1, \ldots., c_{n-2}, c_{n-1}) \epsilon C$, there is also a codeword $c_1 = (c_{n-1}, c_0, c_1, \ldots., c_{n-2})$ obtained by shifting c cyclically one place to the right is also code word in C.

4.3.1 The Basic Properties of Cyclic Codes

Property 1 In an (n, k) cyclic code, there exists a unique polynomial called generator polynomial $g(x)$ of minimal degree $(n - k)$ of the following form:

$$g(x) = g_1 x + g_2 x^2 + \ldots + g_{n-k-1} x^{n-k-1} + g_{n-k} x^{n-k} \tag{4.17}$$

Property 2 Every code polynomial in an (n, k) cyclic code is multiple of $g(x)$. Thus, it can be expressed as $c(x) = m(x)g(x)$ where $m(x)$ is a polynomial over GF(2) of degree $k - 1$ or less.

Property 3 The generator polynomial $g(x)$ of an (n, k) cyclic code over GF(2) divides $x^n + 1$.

Property 4 The generator polynomial $g(x)$ and the parity check matrix $h(x)$ are factor of the polynomial $1 + x^n$.

In modulo-2 arithmetic $1 + x^n$ has the same value $1 - x^n$.

Example 4.9 Let C_1 be the binary cyclic code of length 15 generated by $g(x) = x^5 + x^4 + x^2 + 1$. Compute the code polynomial in C_1 and the associated code word for the message polynomial $m(x) = x^9 + x^4 + x^2 + 1$ using the polynomial multiplication encoding technique.

Solution

$$m(x) = x^9 + x^4 + x^2 + 1; g(x) = x^5 + x^4 + x^2 + 1$$

code polynomial

$$\begin{aligned} c(x) &= m(x)g(x) \\ &= x^{14} + x^{13} + x^{11} + x^8 + x^7 + x^5 + x^4 + 1 \end{aligned}$$

Code word = (100011011001011).

Example 4.10 Let C_1 be the binary cyclic code of length 15 generated by $g(x) = x^5 + x^4 + x^2 + 1$. Determine the dimensions of C_1 and compute the number of code words in C_1.

Solution Since the order of the generator polynomial is 5. The C_1 has dimension (15, 10) with $k = (15 - 5) = 10$ and contains 2^{15-5} code words.

Example 4.11 Let C_1 be the binary cyclic code of length 15 generated by $g(x) = x^5 + x^4 + x^2 + 1$. Compute the parity check polynomial for C_1 and show that $g(x)$ is a valid generator polynomial.

Solution

$$g(x) = x^5 + x^4 + x^2 + 1$$

The parity check polynomial for C_1 is

$$h(x) = \frac{x^{15} + 1}{g(x)} = x^{10} + x^9 + x^8 + x^6 + x^5 + x^2 + 1$$

$g(x)$ is valid generator polynomial since it has the minimum polynomials $x^4 + x + 1$ and $x + 1$ as factors, i.e., $g(x) = \left(x^4 + x + 1\right)(x + 1)$.

4.3.2 *Encoding Algorithm for an (n, k) Cyclic Codes*

In an (n, k) cyclic code C with generator polynomial $g(x)$, let $m = (m_0, m_1, \ldots, m_{k-1})$ is the message block. By multiplying the message polynomial $m(x)$ by x^{n-k}, we obtain a polynomial $x^{n-k}m(x) = m_0x^{n-k} + m_1x^{n-k+1} + \cdots + m_{k-1}x^{n-1}$ of degree $n - 1$ or less. Now, dividing $x^{n-k}m(x)$ by $g(x)$ yields

$$x^{n-k}m(x) = q(x)g(x) + p(x) \tag{4.18}$$

where $q(x)$ and $p(x)$ are the quotient and remainder, respectively.

Equation (4.18) can be rearranged as

$$p(x) + x^{n-k}m(x) = q(x)g(x) \tag{4.19}$$

Equation (4.19) shows that $p(x) + x^{n-k}m(x)$ is divisible by $g(x)$. Hence, it must be a valid code polynomial $c(x) = p(x) + x^{n-k}m(x)$ of the (n, k) cyclic code C with generator polynomial $g(x)$. The n-tuple representation of the code polynomial $c(x)$ is

$$c = (p_0, p_1, \ldots, p_{n-k-1}, m_0, m_1, \ldots, m_{k-1}) \tag{4.20}$$

The systematic encoding algorithm is summarized as

Step 1 Multiply the message polynomial $m(x)$ by x^{n-k}.
Step 2 Divide the result of step 1 by the generator polynomial $g(x)$. Let $d(x)$ be the remainder.
Step 3 Set $c(x) = x^{n-k}m(x) - d(x)$.

Example 4.12 Let C_1 be the binary cyclic code of length 15 generated by $g(x) = x^5 + x^4 + x^2 + 1$. Compute the code polynomial in C_1 and the associated code word for the message polynomial $m(x) = x^8 + x^7 + x^6 + x^5 + x^4$ using the systematic encoding technique. Verify that the message has been systematically encoded.

Solution

$$g(x) = x^5 + x^4 + x^2 + 1;\ m(x) = x^8 + x^7 + x^6 + x^5 + x^4$$

Step 1: $x^5 m(x) = x^5\left(x^8 + x^7 + x^6 + x^5 + x^4\right) = x^{13} + x^{12} + x^{11} + x^{10} + x^9$

Step 2:

$$\begin{array}{r|l}
 & x^8 + x^6 + x^5 + x^2 + 1 \\
\hline
x^5 + x^4 + x^2 + 1\ ) & x^{13} + x^{12} + x^{11} + x^{10} + x^9 \\
 & x^{13} + x^{12} + x^{10} + x^8 \\
\hline
 & x^{11} + x^9 + x^8 \\
 & x^{11} + x^{10} + x^8 + x^6 \\
\hline
 & x^{10} + x^9 + x^6 \\
 & x^{10} + x^9 + x^7 + x^5 \\
\hline
 & x^7 + x^6 + x^5 \\
 & x^7 + x^6 + x^4 + x^2 \\
\hline
 & x^5 + x^4 + x^2 \\
 & x^5 + x^4 + x^2 + 1 \\
\hline
 & 1 = d(x)
\end{array}$$

Step3: $c_m(x) = x^{13} + x^{12} + x^{11} + x^{10} + x^9 + 1 \leftrightarrow c_m = (1000000000111110)$.

Example 4.13 Construct parity check and generator matrices for binary cyclic code of length 15 generated by $g(x) = x^5 + x^4 + x^2 + 1$.

Solution The systematic generator matrix is obtained by selecting as rows those code words associated with the message blocks (1000000000), (0100000000), (0010000000), (0001000000), (0000100000), (0000010000), (0000001000), (0000000100), (0000000010), and (1000000001).

$m(x)$	Code polynomial $c(x)$	Codeword
1	$1+x^2+x^4+x^5$	$\leftrightarrow$ (101011000000000)
x	$1+x+x^2+x^3+x^4+x^6$	$\leftrightarrow$ (111110100000000)
x^2	$1+x+x^3+x^7$	$\leftrightarrow$ (110100010000000)
x^3	$x+x^2+x^4+x^8$	$\leftrightarrow$ (011010001000000)
x^4	$1+x^3+x^4+x^9$	$\leftrightarrow$ (100110000100000)
x^5	$1+x+x^2+x^{10}$	$\leftrightarrow$ (111000000010000)
x^6	$x+x^2+x^3+x^{11}$	$\leftrightarrow$ (011100000001000)
x^7	$x^2+x^3+x^4+x^{12}$	$\leftrightarrow$ (001110000000100)
x^8	$1+x^2+x^3+x^{13}$	$\leftrightarrow$ (101100000000010)
x^9	$x+x^3+x^4+x^{14}$	$\leftrightarrow$ (010110000000001)

The generator matrix (G) and parity check matrix (H) for the cyclic code are

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

The corresponding parity check matrix is,

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

4.3.3 Encoder for Cyclic Codes Using Shift Registers

The systematic encoder for cyclic codes is shown in Fig. 4.2. The rectangular boxes represent flip flops which reside either in 0 or 1 state. The encoder operation is as follows.

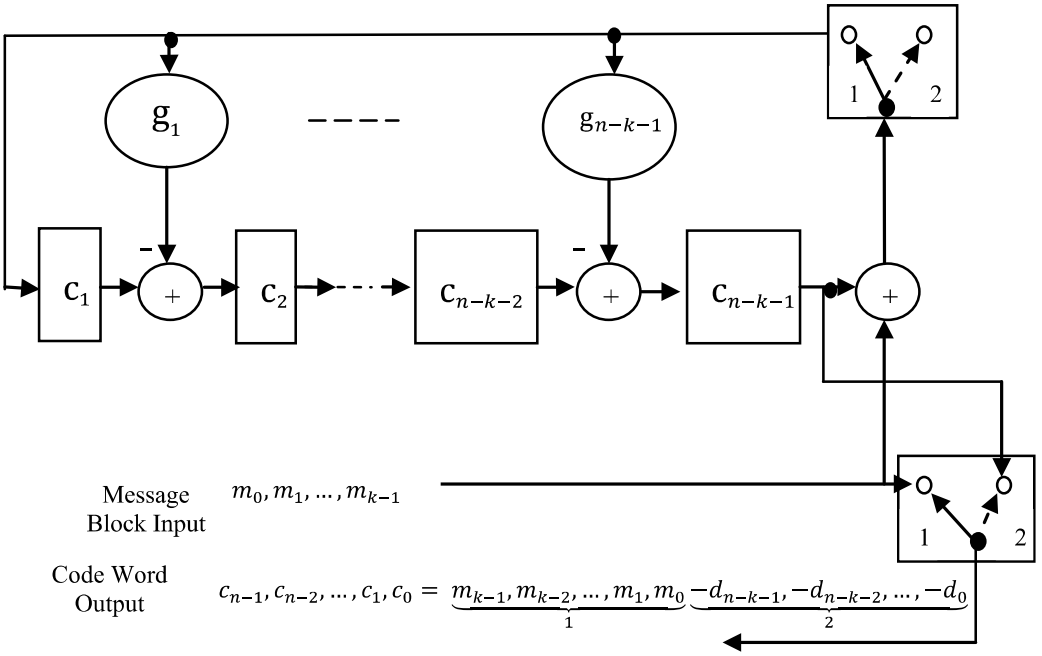

Fig. 4.2 Encoding circuit for (n, k) cyclic code

1. The switches are placed in position in 1. The k message bits are sent to the modulator and placed at the end of the systematic code word. As soon as the kth message bit fed into the shift register, the flip flops of the shift register contain $(n - k)$ parity bits.
2. The switches are moved to the position 2 to break the feedback connection.
3. The parity bits in the shift register are shifted out into the transmitter to form the parity bits of the systematic codeword.

Example 4.14 Construct the shift register encoder for a cyclic code of length 7 generated by $g(x) = x^4 + x^3 + x^2 + 1$ and obtain the code word for message $m = (010)$.

Solution The shift register for encoding the (7, 3) cyclic code with generator polynomial $g(x) = x^4 + x^3 + x^2 + 1$ is shown in Fig. 4.3. The given message bits are 010. The contents of the shift register are shown in Table 4.2. Hence, the four parity check bits are 0111. Therefore, the codeword output is 0111010.

4.3.4 Shift Register Encoders for Cyclic Codes

Suppose the code word $(c_0, c_1, \ldots c_{n-1})$ is transmitted over a noisy channel resulting in the received word $(r_0, r_1, \ldots r_{n-1})$. Let the received word be represented by a polynomial of degree $n - 1$ or less as

$$r(x) = r_0 + r_1 x + \ldots + r_{n-1} x^{n-1} \tag{4.21}$$

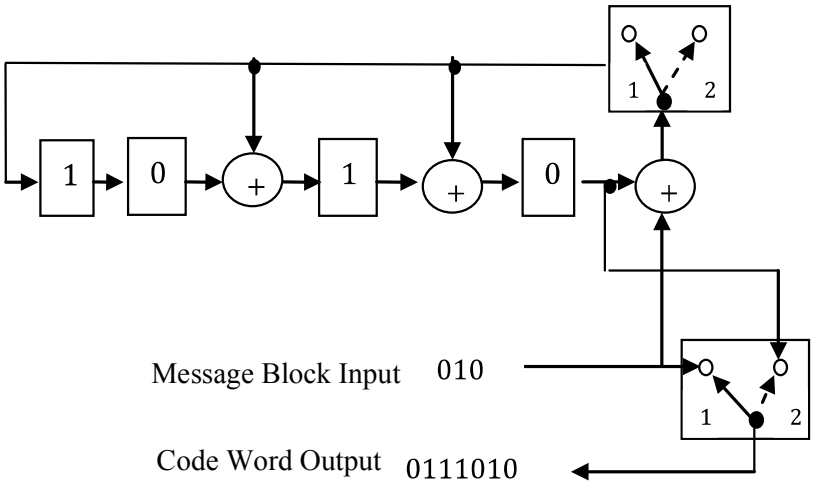

Fig. 4.3 Encoder for an (7,3) cyclic code generated by $g(x) = x^4 + x^3 + x^2 + 1$

Table 4.2 Contents of the shift register in the encoder of Fig. 4.3 for message sequence (010)

Shift	Input	Register codewords			
		0	0	0	0
1	0	0	0	0	0
2	1	1	0	1	0
3	0	0	1	1	1

Dividing the $r(x)$ by $g(x)$ results in the following

$$r(x) = q(x)g(x) + s(x) \tag{4.22}$$

where $q(x)$ is the quotient and $s(x)$ is the remainder known as syndrome. The $s(x)$ is a polynomial of degree $n - k - 1$ or less, and its coefficients make up the $(n - 1)$-by-1 syndrome s An error in the received word is detected only when the syndrome polynomial $s(x)$ is nonzero.

Syndrome Calculator

The syndrome calculator shown in Fig. 4.4 is similar to the encoder shown in Fig. 4.2. The only difference is that the received bits are fed from left into the $(n - k)$ stages of the feedback shift register. At the end of last received bit shifting, the contents of the shift register contain the desired syndrome s. If the syndrome is zero, there are no transmission errors in the received word or else the received code word contains transmission error. By knowing the value of syndrome, we can determine the corresponding error pattern and also make the appropriate correction.

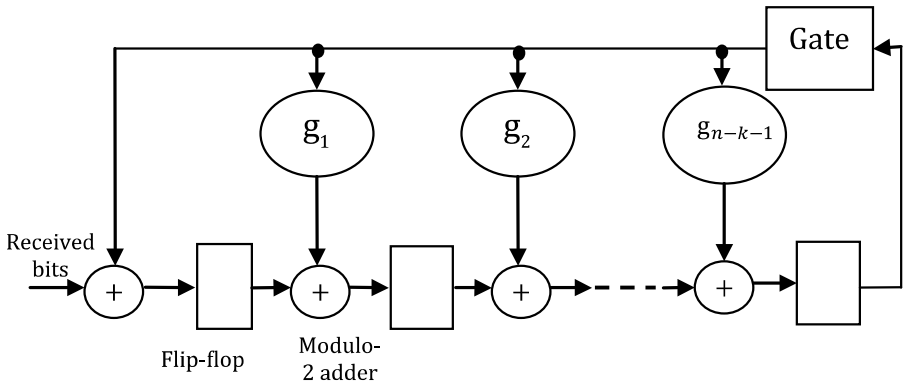

Fig. 4.4 Syndrome calculator

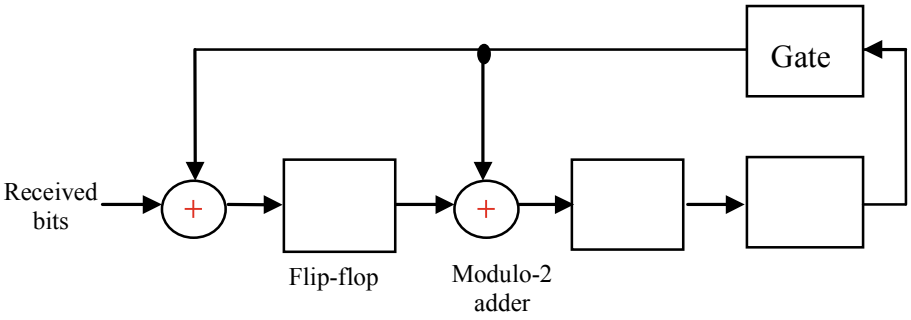

Fig. 4.5 Syndrome calculator of Example 4.15

Example 4.15 Consider the (7, 4) Hamming code generator polynomial $g(x) = x^3 + x + 1$ and the transmitted code word 1100101. Show the fifth bit of the received word is an error.

Solution

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

Transmitted codeword = 1100101

By considering the fifth bit as an error, the received word = 1110101 (Fig. 4.5).

At the end of the seventh shift, the contents of the shift register (syndrome) are 001. The nonzero value of the syndrome indicates the error, and the error pattern for the syndrome 001 is 0010000 from Table 4.1. This shows that the fifth bit of the received word is an error (Table 4.3).

4.3.5 Cyclic Redundancy Check Codes

Cyclic redundancy check (CRC) is a method of detecting accidental changes/burst errors in communication channel. CRC codes are implemented from cyclic codes

Table 4.3 Contents of the shift register in the encoder of Fig. 4.6

Shift	Input bit	Contents of shift register
		000
1	1	100
2	0	010
3	1	101
4	0	100
5	1	110
6	1	111
7	1	001

and hence the name, even they are generally not cyclic. The CRC generation and checking are shown in Fig. 4.6, in which a group of error control bits (which is the remainder of a polynomial division of a message polynomial by a generator polynomial) is appended to the end of the message block.

The encoding of an (n, k) CRC code is same as that of cyclic code generation. This is illustrated through the following example.

Example 4.16 Let C_1 be the binary CRC code of length 12 generated by $g(x) = x^4+x^3+1$. Compute the code polynomial in C_1 and the associated code word for the message polynomial $m(x) = x^7 + x^6 + x^5 + x^2 + x$ using the systematic encoding technique.

Solution $g(x) = x^4 + x^3 + 1;\ m(x) = x^7 + x^6 + x^5 + x^2 + x;$

Step 1: $x^4 m(x) = x^4\left(x^7 + x^6 + x^5 + x^2 + x\right) = x^{11} + x^{10} + x^9 + x^6 + x^5$

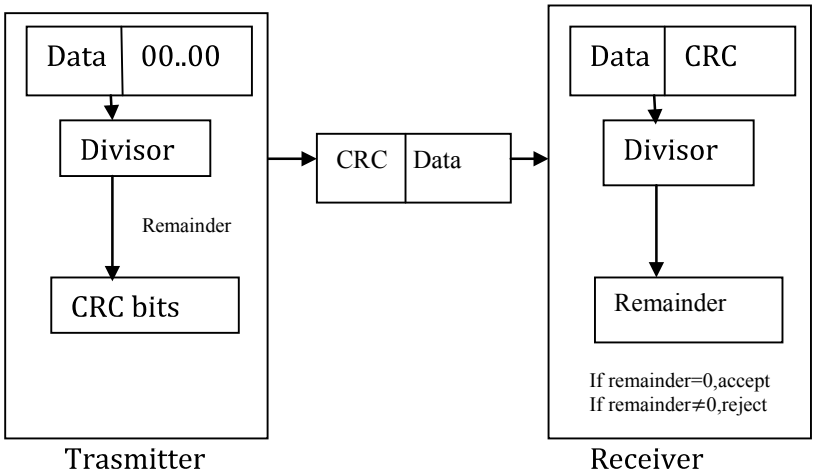

Fig. 4.6 CRC generation and checking

Step 2:

$$
\begin{array}{r|l}
 & x^7 + x^5 + x^4 + x^2 + x \\
\hline
x^4 + x^3 + 1 \;) & x^{11} + x^{10} + x^9 + x^6 + x^5 \\
 & \underline{x^{11} + x^{10} \quad + x^7} \\
 & x^9 \;\; + x^7 + x^6 + x^5 \\
 & \underline{\quad x^9 + x^8 \quad + x^5} \\
 & x^8 + x^7 \quad + x^6 \\
 & \underline{\quad x^8 + x^7 \quad + x^4} \\
 & \quad x^6 \;\; + x^4 \\
 & \quad \underline{x^6 \;\; + x^5 \;\; + x^2} \\
 & x^5 \;\; + x^4 \;\; + x^2 \\
 & \quad \underline{x^5 \;\; + x^4 \;\; + x} \\
 & \qquad x^2 \;\; + x = d(x)
\end{array}
$$

Therefore, the appended bits are 0110
Step 3: $c(x) = x^5 m(x) + d(x) = x^{11} + x^{10} + x^9 + x^6 + x^5 + x^2 + x \leftrightarrow c =$ (011001100111).

The following three CRC codes are given in Table 4.4 that have become international standard.

4.4 BCH Codes

BCH codes are a subclass of cyclic codes. The BCH codes are introduced independently by Bose, Ray-Chaudhuri, and Hocquenghem. For $m > 3$ and $t_{ec} < 2^{m-1}$, there exists a BCH code with parity check bits $(n - k) \leq m t_{ec}$ and $d_{\min} \geq 2t_{ec} + 1$.

4.4.1 BCH Code Design

If a primitive element α of $GF(2^m)$ is chosen, then the generator polynomial g(x) of the t_{ec}-error-correcting binary BCH code of length $2^m - 1$ is the minimum degree polynomial over GF(2) having $\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{2t_c}$ as roots. Suppose $\phi_i(\alpha)$ be the minimal polynomial of α^i, $1 \leq i \leq 2t_{ec}$ for t_{ec}-error-correcting binary BCH code. Then the generator polynomial g(x) is the least common multiple (LCM) of $\phi_1(\alpha), \phi_2(\alpha), \ldots, \phi_{2t_{ec}}(\alpha)$, i.e.,