Therefore

$$m_9(X) = X^3 + X^2 + 1$$

The encoding polynomial $g(X)$ of the code with minimum distance at least 11 is

$$\begin{aligned}
g(X) &= m_1(X)m_3(X)m_5(X)m_7(X)m_9(X) \\
&= (X^6 + X + 1)(X^6 + X^4 + X^3 + X^2 + X + 1)(X^6 + X^5 + X^2 + X + 1) \\
&\quad \times (X^6 + X^3 + 1)(X^3 + X^2 + 1) \\
&= (X^{12} + X^{10} + X^9 + X^8 + X^7 + X^6 + X^7 + X^5 + X^4 + X^3 + X^2 + X \\
&\quad + X^6 + X^4 + X^3 + X^2 + X + 1)(X^6 + X^5 + X^2 + X + 1) \\
&\quad \times (X^9 + X^8 + X^6 + X^6 + X^5 + X^3 + X^3 + X^2 + 1) \\
&= (X^{12} + X^{10} + X^9 + X^8 + X^5 + 1)(X^6 + X^5 + X^2 + X + 1) \\
&\quad \times (X^9 + X^8 + X^5 + X^2 + 1) \\
&= (X^{12} + X^{10} + X^9 + X^8 + X^5 + 1)(X^{15} + X^{14} + X^{11} + X^{10} + X^9 \\
&\quad + X^{14} + X^{13} + X^{10} + X^9 + X^8 + X^{11} + X^{10} + X^7 + X^6 + X^5 + X^8 \\
&\quad + X^7 + X^4 + X^3 + X^2 + X^6 + X^5 + X^2 + X + 1) \\
&= (X^{12} + X^{10} + X^9 + X^8 + X^5 + 1)(X^{15} + X^{13} + X^{10} + X^4 + X^3 \\
&\quad + X + 1) \\
&= (X^{27} + X^{25} + X^{24} + X^{23} + X^{20} + X^{15} + X^{25} + X^{23} + X^{22} + X^{21} \\
&\quad + X^{18} + X^{13} + X^{22} + X^{20} + X^{19} + X^{18} + X^{15} + X^{10} + X^{16} + X^{14} \\
&\quad + X^{13} + X^{12} + X^9 + X^4 + X^{15} + X^{13} + X^{12} + X^{11} + X^8 + X^3 + X^{13} \\
&\quad + X^{11} + X^{10} + X^9 + X^6 + X + X^{12} + X^{10} + X^9 + X^8 + X^5 + 1 \\
&= X^{27} + X^{24} + X^{21} + X^{19} + X^{16} + X^{15} + X^{14} + X^{12} + X^{10} + X^9 \\
&\quad + X^6 + X^5 + X^4 + X^3 + X + 1
\end{aligned}$$

Case (v)

To construct the minimal polynomial of a 2-error-correcting binary BCH code of length 21.

Solution

The length of the code is $21 \leq 2^5 - 1$ and so we need to construct an extension of $\mathbb{B}$ of degree 5. We know from Example 4.7 Case (iv) that $X^5 + X^2 + 1$ is a primitive polynomial of degree 5 over $\mathbb{B}$. Therefore

$$K = \mathbb{B}[X]/\langle X^5 + X^2 + 1 \rangle$$

is a field of order 32,

$$\alpha = X + \langle X^5 + X^2 + 1 \rangle$$

is a primitive element in K (Proposition 4.5) and $X^5 + X^2 + 1$ is the minimal polynomial of α.

The code is 2-error-correcting, therefore the minimum distance of the code is at least $2 \times 2 + 1 = 5$ (Theorem 1.2). We then need the minimal polynomials $m_i(X)$ of α^i, $1 \leq i \leq 4$. But it follows from Proposition 4.2 that

$$m_1(X) = m_2(X) = m_4(X)$$

and

$$m_3(X) = m_6(X) = m_{12}(X) = m_{24}(X) = m_{17}(X)$$

Thus $m_3(X)$ is the polynomial with roots α^3, α^6, α^{12}, α^{24} and α^{17}. Now $\alpha^5 = \alpha^2 + 1$ and so

$$\alpha^6 = \alpha^3 + \alpha \quad \alpha^{12} = \alpha^6 + \alpha^2 = \alpha^3 + \alpha^2 + \alpha$$

$$\alpha^{24} = \alpha^6 + \alpha^4 + \alpha^2 = \alpha^4 + \alpha^3 + \alpha^2 + \alpha$$

$$\alpha^{17} = \alpha^8 + \alpha^6 + \alpha^4 + \alpha^2 = \alpha^3 + \alpha^2 + 1 + \alpha^3 + \alpha + \alpha^4 + \alpha^2 = \alpha^4 + \alpha + 1$$

Then sum of the roots of $m_3(X) = 1$.

Sum of the roots of $m_3(X)$ taken 2 at a time

$$= \alpha^3(\alpha^6 + \alpha^{12} + \alpha^{24} + \alpha^{17}) + \alpha^6(\alpha^{12} + \alpha^{24} + \alpha^{17}) + \alpha^5 + \alpha^{29} + \alpha^{10}$$

$$= \alpha^3(1 + \alpha^3) + \alpha^6(1 + \alpha^3 + \alpha^6) + \alpha^5 + \alpha^{10} + \alpha^{29}$$

$$= \alpha^3 + \alpha^5 + \alpha^{10} + \alpha^9 + \alpha^{12} + \alpha^{29}$$

$$= \alpha^3 + \alpha^2 + 1 + \alpha^4 + 1 + (\alpha^4 + \alpha^3 + \alpha) + (\alpha^3 + \alpha^2 + \alpha)$$
$$+ (\alpha^4 + \alpha^3 + \alpha^2 + \alpha)(\alpha^2 + 1)$$

$$= \alpha^3 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha$$

$$= 1$$

Sum of the roots of $m_3(X)$ taken 3 at a time

$$= \alpha^{21} + \alpha^2 + \alpha^{26} + \alpha^8 + \alpha + \alpha^{11} + \alpha^4 + \alpha^{22} + \alpha^{13} + \alpha^{16}$$

$$= \alpha + \alpha^2 + \alpha^4 + \alpha^4(\alpha^4 + \alpha + 1) + \alpha^8 + (\alpha^2 + \alpha + 1) + (\alpha^2 + \alpha + 1)^2$$
$$+ \alpha^2(\alpha^2 + \alpha + 1) + \alpha^{16} + \alpha^{26}$$

$$= 1 + \alpha^5 + (\alpha^4 + \alpha^2 + 1) + (\alpha^4 + \alpha^3 + \alpha^2) + \alpha^4(\alpha^3 + \alpha^2 + \alpha)$$
$$+ \alpha^2(\alpha^4 + \alpha^3 + \alpha^2 + \alpha)$$

$$= \alpha^4 + \alpha^5 + \alpha^7 = \alpha^4 + \alpha^2 + 1 + \alpha^4 + \alpha^2$$

$$= 1$$

Sum of the roots of $m_3(X)$ taken 4 at a time

$$\begin{aligned}
&= \alpha^{14} + \alpha^7 + \alpha^{19} + \alpha^{25} + \alpha^{28} \\
&= \alpha^4 + \alpha^2 + \alpha^2(\alpha^3 + \alpha^2 + \alpha) + \alpha^2(\alpha^4 + \alpha + 1) + \alpha(\alpha^4 + \alpha^3 + \alpha^2 + \alpha) \\
&\quad + (\alpha^4 + \alpha + 1)(\alpha^2 + \alpha + 1) \\
&= \alpha^2 + \alpha^3 + \alpha^4 + \alpha^6 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + \alpha^2 + \alpha + 1 \\
&= 1 + \alpha^2 + \alpha^5 = 0
\end{aligned}$$

Therefore

$$m_3(X) = X^5 + X^4 + X^3 + X^2 + 1$$

Hence the encoding polynomial of the required BCH code is

$$\begin{aligned}
g(X) &= (X^5 + X^2 + 1)(X^5 + X^4 + X^3 + X^2 + 1) \\
&= X^{10} + X^9 + X^8 + X^6 + X^5 + X^3 + 1
\end{aligned}$$

Case (vi)

So far we have only constructed binary BCH codes. We now want to find the encoding polynomial of a 2-error-correcting BCH code of length 8 over GF(3).

The length of the code being $8 = 3^2 - 1$, we have to construct a field extension of GF(3) of degree 2. We have already proved (Example 4.6) that $X^2 + X + 2$ is a primitive polynomial of degree 2 over $\mathrm{GF}(3) = F_3$. Therefore

$$K = F_3[X]/\langle X^2 + X + 2 \rangle$$

is a field of order 9,

$$\alpha = X + \langle X^2 + X + 2 \rangle$$

is a primitive element of K (Proposition 4.5) and $X^2 + X + 2$ is the minimal polynomial of α over F_3. The code is 2-error-correcting and so the minimum distance of the code is at least $2 \times 2 + 1 = 5$ (Theorem 1.2). We therefore need to find the minimal polynomials $m_i(X)$ of α^i, $1 \leq i \leq 4$. We know from Proposition 4.2 that

$$m_1(X) = m_3(X) \quad \text{and} \quad m_2(X) = m_6(X)$$

Therefore

$$\begin{aligned}
m_2(X) &= (X - \alpha^2)(X - \alpha^6) = X^2 - (\alpha^2 + \alpha^6)X + 1 \\
&= X^2 - [(2\alpha + 1) + (2\alpha + 1)^3]X + 1 \\
&= X^2 - [2\alpha + 1 + 2\alpha^3 + 1]X + 1 \\
&= X^2 - [2\alpha + 2 + 2\alpha(2\alpha + 1)]X + 1 \\
&= X^2 + 1
\end{aligned}$$

$$\begin{aligned} m_4(X) &= X - \alpha^4 \\ &= X - (2\alpha + 1)^2 \\ &= X - 4\alpha^2 - 4\alpha - 1 \\ &= X - (2\alpha + 1) - \alpha - 1 \\ &= X - 2 \\ &= X + 1 \end{aligned}$$

The generating polynomial of the BCH code is

$$\begin{aligned} g(X) &= m_1(X)m_2(X)m_4(X) \\ &= (X^2 + X + 2)(X^2 + 1)(X + 1) \\ &= (X^4 + X^3 + 2X^2 + X^2 + X + 2)(X + 1) \\ &= X^5 + 2X^4 + X^3 + X^2 + 2 \end{aligned}$$

The generating polynomial contains 5 non-zero terms and, therefore, the minimum distance of the code is 5.

Case (vii)

We end this set of examples by constructing a single-error-correcting BCH code of length 10 over GF(5) = F_5, it being given that $X^2 + X + 2$ is primitive over F_5.

The length of the code is $10 \leq 5^2 - 1$ and so we have to construct an extension of F_5 of degree 2. It being given that $X^2 + X + 2$ is primitive over F_5,

$$K = F_5[X]/\langle X^2 + X + 2 \rangle$$

is an extension of F_5 of degree 2,

$$\alpha = X + \langle X^2 + X + 2 \rangle$$

is a primitive element of K (Proposition 4.5) and $X^2 + X + 2$ is the minimal polynomial of α over F_5. The code being single-error-correcting has to have minimum distance at least 3. Therefore, we have to find the minimal polynomials of α and α^2. But α^2 and α^{10} have the same minimal polynomial (Proposition 4.2) $m_2(X)$. In fact, these are the only two roots of $m_2(X)$ and so

$$\begin{aligned} m_2(X) &= (X - \alpha^2)(X - \alpha^{10}) \\ &= X^2 - X(\alpha^2 + \alpha^{10}) + \alpha^{12} \end{aligned}$$

Now $\alpha^2 = -\alpha - 2$ and so

$$\begin{aligned}\alpha^{10} &= -\alpha^5 - 2^5 \\ &= -\alpha^5 - 2 \\ &= -\alpha(\alpha^2 + 4\alpha + 4) - 2 \\ &= -\alpha(3\alpha + 2) - 2 \\ &= 3(\alpha + 2) - 2\alpha - 2 \\ &= \alpha - 1\end{aligned}$$

Also then

$$\begin{aligned}\alpha^{12} &= \alpha^2(\alpha - 1) \\ &= -(\alpha + 2)(\alpha - 1) \\ &= -\alpha^2 - \alpha + 2 \\ &= \alpha + 2 - \alpha + 2 \\ &= 4\end{aligned}$$

Hence

$$m_2(X) = X^2 + 3X + 4$$

Therefore the generating polynomial of the BCH code is

$$\begin{aligned}g(X) &= m_1(X)m_2(X) \\ &= (X^2 + X + 2)(X^2 + 3X + 4) \\ &= X^4 + 4X^3 + 4X^2 + 3\end{aligned}$$

Theorem 4.6
A binary BCH code with code word length $n = 2^m - 1$ and minimum distance at least $d = 2t + 1$ can always be constructed with check digits at most mt.

Proof
The code needed is of length $n = 2^m - 1$. We therefore construct an extension K of $\mathbb{B}$ of degree m and let α be a primitive element of K. The degree $[K:\mathbb{B}] = m$ is finite and so every element of K is algebraic over $\mathbb{B}$. Moreover if β is any element of K, then $\mathbb{B}(\beta)$ is a subfield of K and the degree relation

$$[K:\mathbb{B}] = [K:\mathbb{B}(\beta)][\mathbb{B}(\beta):\mathbb{B}]$$

(Proposition 4.3) then shows that $[\mathbb{B}(\beta):\mathbb{B}] \leq m$. This then shows that the degree of the minimal polynomial of β which equals $[\mathbb{B}(\beta):\mathbb{B}]$ is at most m.

For the construction of the code, we need the minimal polynomials $m_i(X)$ of α^i, $1 \leq i \leq 2t$. Let $g(X)$ be the generating polynomial of the code. Then

$$g(X) = \text{LCM}\{m_1(X), m_2(X), \ldots, m_{2t}(X)\}$$

We prove by induction on t that $\deg g(X) \leq mt$. For $t = 1$

$$g(X) = \text{LCM}\{m_1(X), m_2(X)\}$$

But α and α^2 have the same minimal polynomial. Therefore $g(X) = m_1(X)$ and we are through. Suppose that $t \geq 1$ and that we have proved the claim for t. Let:

$$g_1(X) = \text{LCM}\{m_1(X), \ldots, m_{2t}(X), m_{2t+1}(X), m_{2t+2}(X)\}$$

Then, since $m_{2t+2}(X) = m_{t+1}(X)$

$$\begin{aligned} g_1(X) &= \text{LCM}\{m_1(X), \ldots, m_{2t}(X), m_{2t+1}(X)\} \\ &= \text{LCM}[\text{LCM}\{m_1(X), \ldots, m_{2t}(X)\}, m_{2t+1}(X)] \\ &= \text{LCM}\{g(X), m_{2t+1}(X)\} \end{aligned}$$

Then

$$\begin{aligned} \deg g_1(X) &\leq \deg g(X) + \deg m_{2t+1}(X) \\ &\leq mt + m \\ &= m(t+1) \end{aligned}$$

which completes induction.

Since in a polynomial code, the number of check symbols equals the degree of the generating polynomial, the theorem follows.

Remark

If $g(X)$ is the generating polynomial of the binary BCH code with minimum distance at least $2t$, then in the notations of the proof of the above theorem

$$\begin{aligned} g(X) &= \text{LCM}\{m_1(X), \ldots, m_{2t-1}(X)\} \\ &= \text{LCM}\{m_1(X), \ldots, m_{2t-1}(X), m_{2t}(X)\} \end{aligned}$$

and, therefore, $g(X)$ is the generating polynomial of a BCH code with minimum distance at least $2t + 1$.

We have proved Theorem 4.6 from the point of view of practical utility. We can in fact prove the following theorem for BCH codes over a field of any prime order exactly on the lines of the proof of Theorem 4.6.

Theorem 4.7

A BCH code over GF(p) with code word length $n = p^m - 1$ and minimum distance at least $pt + 1$ can always be constructed with at most $(p-1)mt$ check digits.

Exercises 4.1

1. Prove that $X^2 + X + 1$ is the only irreducible polynomial of degree 2 in $\mathbb{B}[X]$.

2. Prove that $X^4 + X^3 + 1$, $X^4 + X + 1$ and $X^4 + X^3 + X^2 + X + 1$ are the only irreducible polynomials of degree 4 over $\mathbb{B}$.
3. Prove that $X^3 + X + 1$ and $X^3 + X^2 + 1$ are the only irreducible polynomials of degree 3 over $\mathbb{B}$.
4. Prove that the polynomial $X^6 + X^5 + X^3 + X^2 + 1$ is irreducible over $\mathbb{B}$. Prove that this polynomial is primitive.
5. If R is a commutative ring, $a, b \in R$ and n is a positive integer, prove that

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \cdots + \binom{n}{i}a^{n-i}b^i + \cdots + \binom{n}{n-1}ab^{n-1} + b^n$$

   where $\binom{n}{i}$ are the binomial coefficients.
6. Is GF(4) a subfield of GF(8)? Justify your answer.
7. Find a primitive element α of $F_3[X]/\langle X^2 + 1\rangle$. (Observe that if we put $\beta = X + \langle X^2 + 1\rangle$, then $1 + \beta, 1 - \beta, -1 - \beta, -1 + \beta$ are all the primitive elements of the field.)
8. Is the polynomial $X^2 - 2$ primitive over GF(3) $= F_3$? Justify your answer.
9. Let F be a field of order p^n, p a prime and let α be a primitive element of F. Prove that α^r is primitive iff GCD$(r, p^n - 1) = 1$.
10. Prove that the number of primitive elements in a field of order p^n, p a prime is $\phi(p^n - 1)$. (Here ϕ stands for Euler's ϕ-function.)
11. Can the words 'at least' be omitted from the statement of Theorem 4.5?
12. Compute all the code words of the code of Example 4.8 Case (i). Compare this code with the (4, 7) Hamming code.
13. Construct binary BCH code of length 7 with minimum distance 3 by using the primitive polynomial $X^3 + X^2 + 1$. Compare this code with
    (i) the (4, 7) Hamming code
    (ii) the code of Example 4.8 Case (i).