and hence $g(X)|h(X)$. Thus $g(X)$ is the polynomial of least possible degree (up to a constant factor) with roots $\alpha, \alpha^2, \ldots, \alpha^{d-1}$.

If $c(X)$ is a code polynomial in the polynomial code generated by $g(X)$, then $c(X) = a(X)g(X)$ for some $a(X) \in F[X]$ and, therefore, $\alpha, \alpha^2, \ldots, \alpha^{d-1}$ are roots of $c(X)$.

We know that in a group code the minimum distance of the code equals the minimum of the weights of non-zero code words. Since polynomial codes are group codes, it follows that the code generated by $g(X)$ has minimum distance at least d if there is no code word $c_0 c_1 \ldots c_{n-1}$ with less than d non-zero entries. Suppose, to the contrary, that a code word has less than d non-zero entries. Then the corresponding code polynomial is of the form

$$c(X) = b_1 X^{n_1} + b_2 X^{n_2} + \cdots + b_{d-1} X^{n_{d-1}}$$

where $b_1, b_2, \ldots, b_{d-1} \in F$ and also, we may assume that

$$n_1 > n_2 > \cdots > n_{d-1} \geq 0$$

Since the code is of length n, every code polynomial is of degree at most $n - 1$ and, therefore, $n_1 \leq n - 1\ (\leq q^r - 2)$. As already pointed out, $\alpha, \alpha^2, \ldots, \alpha^{d-1}$ are roots of $c(X)$ and we have

$$\begin{aligned}
b_1\alpha^{n_1} + b_2\alpha^{n_2} + \cdots + b_{d-1}\alpha^{n_{d-1}} &= 0 \\
b_1\alpha^{2n_1} + b_2\alpha^{2n_2} + \cdots + b_{d-1}\alpha^{2n_{d-1}} &= 0 \\
\ldots \qquad\qquad \ldots \qquad\qquad &\ldots \\
b_1\alpha^{(d-1)n_1} + b_2\alpha^{(d-1)n_2} + \cdots + b_{d-1}\alpha^{(d-1)n_{d-1}} &= 0
\end{aligned}$$

or

$$\mathbf{A}\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_{d-1} \end{pmatrix} = 0 \tag{4.2}$$

where

$$\mathbf{A} = \begin{pmatrix} \alpha^{n_1} & \alpha^{n_2} & \cdots & \alpha^{n_{d-1}} \\ \alpha^{2n_1} & \alpha^{2n_2} & \cdots & \alpha^{2n_{d-1}} \\ \cdots & & \ddots & \\ \alpha^{(d-1)n_1} & \alpha^{(d-1)n_2} & \cdots & \alpha^{(d-1)n_{d-1}} \end{pmatrix}$$

The determinant of $\mathbf{A}$ is a **Vandermonde determinant** and we know that

$$\det \mathbf{A} = \prod_{i>j} (\alpha^{n_i} - \alpha^{n_j})$$

The element α of K being primitive and

$$q^r - 1 > n_1 > n_2 > \cdots > n_{d-1} \geq 0$$

we have $\alpha^{n_i} - \alpha^{n_j} \neq 0$ for $i \neq j$ and, therefore, $\det \mathbf{A} \neq 0$. Now (4.2) is a system of $d-1$ homogeneous linear equations in $d-1$ variables $b_1, \ldots, b_{d-1}$ and $\det \mathbf{A} \neq 0$. Therefore the system of equations admits only the zero solution and $c(X) = 0$. Hence there is no non-zero code word with less than d non-zero entries and the code has minimum distance at least d.

Examples 4.8

Case (i)

Construct a binary BCH code of length 7 and minimum distance 3.

Here $n = 7$ and so we need to construct an extension of $\mathbb{B}$ of degree r where $2^r \geq 7 + 1 = 8$. Thus we take $r = 3$. We know from Example 4.7 (Case (iii)) that $X^3 + X + 1$ is a primitive polynomial of degree 3 over $\mathbb{B}$. Therefore

$$K = B[X]/\langle X^3 + X + 1\rangle$$

is a field of order 8 and

$$\alpha = X + \langle X^3 + X + 1\rangle$$

is a primitive element of K. Then α satisfies the relations $\alpha^3 + \alpha + 1 = 0$, and $\alpha^7 = 1$ and $X^3 + X + 1$ is the minimal polynomial of α. Since α and α^2 have the same minimal polynomial (Proposition 4.2), the generator polynomial of the required BCH code is $X^3 + X + 1$.

The message polynomials are of degree at most 3. If

$$a(X) = a_0 + a_1X + a_2X^2 + a_3X^3$$

is an arbitrary message polynomial, the corresponding code polynomial is $a(X)(X^3 + X + 1)$ and so the corresponding code word is

$$(a_0, a_1 + a_0, a_2 + a_1, a_3 + a_2 + a_0, a_3 + a_1, a_2, a_3)$$

The encoding polynomial has 3 non-zero terms and, therefore, the code has minimum distance 3.

If we had started with the primitive polynomial $X^3 + X^2 + 1$, the corresponding BCH code with code word length 7 and minimum distance at least 3 is the polynomial code with encoding polynomial $X^3 + X^2 + 1$.

Case (ii)

Next we construct a binary BCH code of length 15 and minimum distance 5.

Here $n = 15 \geq 2^4 - 1$ and so we need to construct an extension K of $\mathbb{B}$ of degree 4. We have seen earlier (Example 4.3 Case (ii)) that $X^4 + X + 1$ is a primitive polynomial and so

$$\alpha = X + \langle X^4 + X + 1\rangle$$

is a primitive element of

$$K = \mathbb{B}[X]/\langle X^4 + X + 1\rangle$$

The minimal polynomial of α is $m_1(X) = X^4 + X + 1$. Also

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

(Proposition 4.2). We next have to find the minimal polynomial of α^3. The elements α^3, α^6, α^{12}, α^9 have the same minimal polynomial and so

$$\begin{aligned} m_3(X) &= (X-\alpha^3)(X-\alpha^6)(X-\alpha^9)(X-\alpha^{12}) \\ &= X^4 + X^3(\alpha^3+\alpha^6+\alpha^9+\alpha^{12}) + X^2(\alpha^9+\alpha^{12}+\alpha^{15}+\alpha^{15}+\alpha^{18}+\alpha^{21}) \\ &\quad + X(\alpha^{18}+\alpha^{21}+\alpha^{24}+\alpha^{27}) + \alpha^{30} \\ &= X^4 + X^3(\alpha^3+\alpha^3+\alpha^2+\alpha^3+\alpha+\alpha^3+\alpha^2+\alpha+1) \\ &\quad + X^2(\alpha^9+\alpha^{12}+\alpha^3+\alpha^6) + X(\alpha^3+\alpha^6+\alpha^9+\alpha^{12}) + 1 \\ &= X^4 + X^3 + X^2 + X + 1 \end{aligned}$$

Therefore, the encoding polynomial of the BCH code with minimum distance at least 5 is

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

Since the encoding polynomial has 5 non-zero terms, the minimum distance of the code is exactly 5. The code being of length 15, a message polynomial is of degree at most 6. Let

$$a(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + a_4X^4 + a_5X^5 + a_6X^6$$

be an arbitrary message polynomial. The code word corresponding to the code polynomial $a(X)g(X)$ is

$$\begin{aligned} &(a_0, a_1, a_2, a_3, a_4+a_0, a_5+a_1, a_6+a_2+a_0, a_0+a_1+a_3, a_0+a_1+a_2+a_4, \\ &\quad a_1+a_2+a_3+a_5, a_2+a_3+a_4+a_6, a_3+a_4+a_5, a_4+a_5+a_6, a_5+a_6, a_6) \end{aligned}$$

Case (iii)

Find a generator polynomial of the binary BCH code of length 31 and minimum distance 5, it being given that $X^5 + X^2 + 1$ is an irreducible polynomial over $\mathbb{B}$.

Solution

The polynomial $X^5 + X^2 + 1$ being irreducible,

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

is a field of order 32. Since $F^* = F \setminus \{0\}$ is a cyclic group of order 31 – a prime – every non-identity element of F^* is a primitive element of F. In particular

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

is a primitive element of F and $X^5 + X^2 + 1$ is the minimal polynomial of α.

Let $m_i(X)$ be the minimal polynomial of α^i, $1 \le i \le 4$. Observe that α, α^2, α^4 have the same minimal polynomial. So,

$$m_1(X) = m_2(X) = m_4(X) = X^5 + X^2 + 1$$

We now have to find $m_3(X)$. As α^3, α^6, α^{12}, α^{24}, α^{17} have the same minimal polynomial and $\{3, 6, 12, 24, 17\}$ is the complete cyclotomic class modulo 31 relative to 2,

$$m_3(X) = (X - \alpha^3)(X - \alpha^6)(X - \alpha^{12})(X - \alpha^{17})(X - \alpha^{24})$$

In $m_3(X)$, the coefficient of X^4 is

$$\begin{aligned}
\alpha^3 + \alpha^6 + \alpha^{12} + \alpha^{17} + \alpha^{24} &= \alpha^3 + \alpha^3 + \alpha + \alpha^{12} + (\alpha^3 + \alpha)^4 + (\alpha^2 + 1)(\alpha^6 + \alpha^2) \\
&= \alpha + \alpha^{12} + \alpha^{12} + \alpha^4 + \alpha^8 + \alpha^6 + \alpha^4 + \alpha^2 \\
&= \alpha + \alpha^2 + \alpha^6 + \alpha^8 \\
&= \alpha + \alpha^2 + \alpha^3 + \alpha + \alpha^3(\alpha^2 + 1) \\
&= \alpha^5 + \alpha^2 \\
&= 1
\end{aligned}$$

The coefficient of X^3 is

$$\begin{aligned}
&\alpha^9 + \alpha^{15} + \alpha^{20} + \alpha^{27} + \alpha^{18} + \alpha^{23} + \alpha^{30} + \alpha^{29} + \alpha^5 + \alpha^{10} \\
&\quad = \alpha^9 + \alpha^{17} + \alpha^7(\alpha^2 + 1)^4 + \alpha^{20} + (\alpha^4 + 1)(\alpha^8 + 1) + \alpha^9(\alpha^8 + 1) + \alpha^7 \\
&\quad = \alpha^9 + \alpha^{17} + \alpha^{15} + \alpha^7 + \alpha^8 + 1 + \alpha^{12} + \alpha^8 + \alpha^4 + 1 + \alpha^{17} + \alpha^9 + \alpha^7 \\
&\quad = \alpha^{15} + \alpha^{12} + \alpha^4 \\
&\quad = (\alpha^2 + 1)^3 + \alpha^2(\alpha^4 + 1) + \alpha^4 \\
&\quad = \alpha^6 + \alpha^4 + \alpha^2 + 1 + \alpha^6 + \alpha^2 + \alpha^4 \\
&\quad = 1
\end{aligned}$$

The coefficient of X^2 is

$$\begin{aligned}
&\alpha^{21} + \alpha^{26} + \alpha^2 + \alpha + \alpha^8 + \alpha^{13} + \alpha^4 + \alpha^{11} + \alpha^{16} + \alpha^{22} \\
&\quad = \alpha^{23} + \alpha^2 + \alpha + \alpha^{10} + \alpha^4 + \alpha^{13} + \alpha^2(\alpha^8 + 1) \\
&\quad = \alpha^3(\alpha^8 + 1) + \alpha + \alpha^4 + \alpha^3(\alpha^4 + 1) \\
&\quad = \alpha^{11} + \alpha + \alpha^4 + \alpha^7 \\
&\quad = \alpha(\alpha^4 + 1) + \alpha + \alpha^4 + \alpha^2(\alpha^2 + 1) \\
&\quad = \alpha^5 + \alpha^2 \\
&\quad = 1
\end{aligned}$$

The coefficient of X is

$$\begin{aligned}\alpha^7+\alpha^{14}+\alpha^{19}+\alpha^{25}+\alpha^{28} &= \alpha^7+\alpha^{16}+\alpha^5(\alpha^8+1)+\alpha^8(\alpha^8+1)\\ &= \alpha^7+\alpha^{13}+\alpha^5+\alpha^8\\ &= \alpha^2(\alpha^2+1)+\alpha^{10}+\alpha^5\\ &= \alpha^4+\alpha^2+\alpha^4+1+\alpha^2+1\\ &= 0\end{aligned}$$

The constant term is

$$\alpha^{3+6+12+17+24}=\alpha^{62}=1$$

Hence

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

Therefore the generator polynomial of the BCH code of length 31 over $\mathbb{B}$ is

$$\begin{aligned}g(X) &= \mathrm{LCM}\{m_1(X),m_2(X),m_3(X),m_4(X)\}\\ &= \mathrm{LCM}\{m_1(X),m_3(X)\}\\ &= m_1(X)m_3(X)\\ &= (X^5+X^2+1)(X^5+X^4+X^3+X^2+1)\\ &= X^{10}+X^9+X^8+X^6+X^5+X^3+1\end{aligned}$$

Case (iv)

Find a generator polynomial for a 5-error-correcting binary BCH code of length 63, it being given that X^6+X+1 is a primitive polynomial over $\mathbb{B}$.

Solution

The length of the code is $63=2^6-1$ and we need to find an extension of $\mathbb{B}$ of degree 6. It being given that X^6+X+1 is a primitive polynomial over $\mathbb{B}$,

$$K=\mathbb{B}[X]/\langle X^6+X+1\rangle$$

is a field of order 2^6,

$$\alpha=X+\langle X^6+X+1\rangle$$

is a primitive element of K and X^6+X+1 is the minimal polynomial of α.

Since the code we are looking for is to be 5-error-correcting, the minimum distance of the code is at least $2\times 5+1=11$ (Theorem 1.2). We thus have to find the minimal polynomials $m_i(X)$ of α^i for $1\le i\le 10$. It follows from

Proposition 4.2 that

$$m_1(X) = m_2(X) = m_4(X) = m_8(X) = m_{16}(X) = m_{32}(X)$$
$$m_3(X) = m_6(X) = m_{12}(X) = m_{24}(X) = m_{48}(X) = m_{33}(X)$$
$$m_5(X) = m_{10}(X) = m_{20}(X) = m_{40}(X) = m_{17}(X) = m_{34}(X)$$
$$m_7(X) = m_{14}(X) = m_{28}(X) = m_{56}(X) = m_{49}(X) = m_{35}(X)$$
$$m_9(X) = m_{18}(X) = m_{36}(X)$$

Thus $m_1(X), m_3(X), m_5(X), m_7(X)$ are of degree 6 each while $m_9(X)$ is of degree 3. Also then the encoding polynomial of the BCH code we are looking for is

$$g(X) = m_1(X)m_3(X)m_5(X)m_7(X)m_9(X)$$

which is of degree 27. Now

$$\alpha^6 = \alpha + 1 \Rightarrow \alpha^{12} = \alpha^2 + 1$$
$$\alpha^{24} = \alpha^4 + 1$$
$$\alpha^{48} = \alpha^8 + 1 = \alpha^3 + \alpha^2 + 1$$
$$\alpha^{33} = (\alpha^4 + 1)(\alpha^4 + \alpha^3) = \alpha^8 + \alpha^7 + \alpha^4 + \alpha^3 = \alpha^3 + \alpha^2 + \alpha^2 + \alpha + \alpha^4 + \alpha^3$$
$$= \alpha^4 + \alpha$$

Therefore

$$\begin{aligned} m_3(X) &= (X + \alpha^3)(X + \alpha + 1)(X + \alpha^2 + 1)(X + \alpha^4 + 1)(X + \alpha^3 + \alpha^2 + 1) \\ &\quad \times (X + \alpha^4 + \alpha) \\ &= [X^2 + X(\alpha^3 + \alpha + 1) + \alpha^4 + \alpha^3][X^2 + X(\alpha^4 + \alpha^2) + \alpha^4 + \alpha^2 + \alpha] \\ &\quad \times [X^2 + X(\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1) + \alpha^3 + \alpha^2 + \alpha + 1] \\ &= [X^4 + X^3(\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1) + X^2(\alpha^4 + \alpha^2) + X(\alpha^5 + \alpha^2 + 1) \\ &\quad + \alpha^4 + \alpha^3 + 1][X^2 + X(\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1) + \alpha^3 + \alpha^2 + \alpha + 1] \\ &= X^6 + X^4(\alpha^8 + \alpha^6 + \alpha^4 + \alpha^2 + 1 + \alpha^4 + \alpha^2 + \alpha^3 + \alpha^2 + \alpha + 1) \\ &\quad + X^3(\alpha^8 + \alpha^2 + \alpha^3) + X^2(\alpha^9 + \alpha^8 + \alpha^6 + \alpha^4 + \alpha^2 + \alpha) \\ &\quad + X(\alpha^2 + \alpha^6 + \alpha^7) + (\alpha^7 + \alpha^2 + \alpha + 1) \\ &= X^6 + X^4 + X^3 + X^2 + X + 1 \end{aligned}$$

Again

$$\alpha^{10} = \alpha^5 + \alpha^4 \quad \alpha^{20} = \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2$$
$$\alpha^{40} = \alpha^5 + \alpha^3 + \alpha^2 + \alpha + 1$$
$$\alpha^{17} = (\alpha^5 + \alpha + 1)(\alpha + 1) = \alpha^5 + \alpha^2 + \alpha$$
$$a^{34} = \alpha^{10} + \alpha^4 + \alpha^2 = \alpha^5 + \alpha^2$$

Therefore

$$\begin{aligned}
m_5(X) &= (X+\alpha^5+\alpha^4)(X+\alpha^5+\alpha^4+\alpha^3+\alpha^2)(X+\alpha^5+\alpha^3+\alpha^2+\alpha+1)\\
&\quad \times (X+\alpha^5+\alpha^2+\alpha)(X+\alpha^5+\alpha^2)(X+\alpha^5)\\
&= [X^2+X(\alpha^3+\alpha^2)+\alpha^5+\alpha^4+\alpha+1]\\
&\quad \times [X^2+X(\alpha^3+1)+\alpha^5+\alpha^4+\alpha^3+\alpha^2+\alpha]\\
&\quad \times [X^2+\alpha^2X+\alpha^5+\alpha^4+\alpha^2+\alpha]\\
&= [X^4+X^3(\alpha^2+1)+X^2(\alpha^3+\alpha^2+1+\alpha^5+\alpha^3+\alpha^2+\alpha+1)\\
&\quad +X(\alpha^5+\alpha^2+1)+\alpha^4+1][X^2+\alpha^2X+\alpha^5+\alpha^4+\alpha^2+\alpha]\\
&= X^6+X^5(\alpha^2+1+\alpha^2)+X^4(\alpha^5+\alpha^4+\alpha^2+\alpha+\alpha^4+\alpha^2+\alpha^5+\alpha)\\
&\quad +X^3[(\alpha^2+1)(\alpha^5+\alpha^4+\alpha^2+\alpha)+\alpha^2(\alpha^5+\alpha)+\alpha^5+\alpha^2+1]\\
&\quad +X^2[\alpha^4+1+\alpha^2(\alpha^5+\alpha^2+1)+(\alpha^5+\alpha)(\alpha^5+\alpha^4+\alpha^2+\alpha)]\\
&\quad +X[\alpha^2(\alpha^4+1)+(\alpha^5+\alpha^2+1)(\alpha^5+\alpha^4+\alpha^2+\alpha)]\\
&\quad +(\alpha^4+1)(\alpha^5+\alpha^4+\alpha^2+\alpha)\\
&= X^6+X^5+X^2+X+1
\end{aligned}$$

For finding $m_7(X)$:

$$\begin{aligned}
\alpha^7 &= \alpha^2+\alpha\\
a^{14} &= \alpha^4+\alpha^2\\
\alpha^{28} &= \alpha^4+\alpha^3+\alpha^2\\
\alpha^{56} &= \alpha^4+\alpha^3+\alpha^2+\alpha+1\\
\alpha^{49} &= \alpha^4+\alpha^3+\alpha\\
a^{35} &= \alpha^3+\alpha+1
\end{aligned}$$

Then

$$\alpha^7+\alpha^{14}+\alpha^{28}+\alpha^{56}+\alpha^{49}+\alpha^{35}=0$$

$$\alpha^7\times\alpha^{14}\times\alpha^{28}\times\alpha^{56}\times\alpha^{49}\times\alpha^{35}=\alpha^{189}=1$$

Sum of the products of these 6 powers of α taken 5 at a time

$$\begin{aligned}
&= \alpha^{63-7}+\alpha^{63-14}+\alpha^{63-28}+\alpha^{63-56}+\alpha^{63-49}+\alpha^{63-35}\\
&= \alpha^{56}+\alpha^{49}+\alpha^{35}+\alpha^7+\alpha^{14}+\alpha^{28}\\
&= 0
\end{aligned}$$

Since α is an element of a field K and

$$\alpha^7\times\alpha^{56}=\alpha^{14}\times\alpha^{49}=\alpha^{28}\times\alpha^{35}=1$$

sum of products of these elements taken 2 at a time

$$\begin{aligned}
&= \text{sum of products of these elements taken 4 at a time}\\
&= \alpha^7(\alpha^{14} + \alpha^{28} + \alpha^{35} + \alpha^{49} + \alpha^{56}) + \alpha^{14}(\alpha^{28} + \alpha^{35} + \alpha^{49} + \alpha^{56})\\
&\quad + \alpha^{28}(\alpha^{35} + \alpha^{49} + \alpha^{56}) + \alpha^{35}(\alpha^{49} + \alpha^{56}) + \alpha^{49} \times \alpha^{56}\\
&= \alpha^7 \times \alpha^7 + \alpha^{14}(\alpha^7 + \alpha^{14}) + (1 + \alpha^{14} + \alpha^{21}) + (\alpha^{21} + \alpha^{28}) + \alpha^{42}\\
&= \alpha^{14} + \alpha^{21} + \alpha^{28} + 1 + \alpha^{14} + \alpha^{21} + \alpha^{21} + \alpha^{28} + \alpha^{42}\\
&= 1 + \alpha^{21} + \alpha^{42}\\
&= 1 + (\alpha^2 + \alpha)^3 + (\alpha^2 + \alpha)^6\\
&= 1 + (\alpha^5 + \alpha^4 + \alpha^3 + \alpha + 1) + (\alpha^5 + \alpha^4 + \alpha^3 + \alpha + 1)^2\\
&= 1 + (\alpha^5 + \alpha^4 + \alpha^3 + \alpha + 1) + (\alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 + \alpha^2 + 1)\\
&= 0
\end{aligned}$$

Sum of the products of these powers of α taken 3 at a time

$$\begin{aligned}
&= (\alpha^{49} + \alpha^{56} + \alpha^7 + \alpha^{14}) + (\alpha^7 + \alpha^{21} + \alpha^{28}) + (\alpha^{28} + \alpha^{35}) + \alpha^{49}\\
&\quad + (\alpha^{14} + \alpha^{28} + \alpha^{35}) + (\alpha^{35} + \alpha^{42}) + \alpha^{56} + (\alpha^{49} + \alpha^{56}) + \alpha^7 + \alpha^{14}\\
&= \alpha^7 + \alpha^{14} + \alpha^{21} + \alpha^{28} + \alpha^{35} + \alpha^{42} + \alpha^{49} + \alpha^{56}\\
&= \alpha^{21} + \alpha^{42}\\
&= 1
\end{aligned}$$

Therefore

$$m_7(X) = X^6 + X^3 + 1$$

We are now left with computing $m_9(X)$.

$$\begin{aligned}
m_9(X) &= (X + \alpha^9)(X + \alpha^{18})(X + \alpha^{36})\\
&= X^3 + X^2(\alpha^9 + \alpha^{18} + \alpha^{36}) + X(\alpha^{27} + \alpha^{45} + \alpha^{54}) + 1\\
&= X^3 + X^2[(\alpha^4 + \alpha^3) + (\alpha^4 + \alpha^3)^2 + (\alpha^4 + \alpha^3)^4]\\
&\quad + X[\alpha^{27} + \alpha^{45} + \alpha^{54}] + 1
\end{aligned}$$

Now

$$\begin{aligned}
\alpha^{18} &= (\alpha^4 + \alpha^3)^2 = \alpha^8 + \alpha^6 = \alpha^3 + \alpha^2 + \alpha + 1\\
\alpha^{36} &= (\alpha^3 + \alpha^2 + \alpha + 1)^2 = \alpha^4 + \alpha^2 + \alpha\\
\alpha^{27} &= (\alpha^4 + \alpha^3)(\alpha^3 + \alpha^2 + \alpha + 1) = \alpha^7 + \alpha^3 = \alpha^3 + \alpha^2 + \alpha\\
\alpha^{54} &= (\alpha^3 + \alpha^2 + \alpha)^2 = \alpha^4 + \alpha^2 + \alpha + 1\\
\alpha^{45} &= (\alpha^3 + \alpha^2 + \alpha + 1)(\alpha^3 + \alpha^2 + \alpha) = \alpha^4 + \alpha^3 + 1
\end{aligned}$$