

1. This exercise, you are asked to construct BCH-codes of length 15 and designed distance 5 over certain fields. Try to find an example with maximal dimension. For each code, you must identify  $b$  and the dimension.

(a) over  $GF(4)$ .

(b) over  $GF(16)$ .

Solution : (a) The cyclotomic cosets depending on  $n = 15$  and  $q = 4$  are

$$\{0\} , \{1, 4\} , \{2, 8\} , \{3, 12\} , \{5\} , \{6, 9\} , \{7, 13\} , \{10\} \text{ and } \{11, 14\}$$

From the cyclotomic cosets, we get that

$$\begin{aligned} g_0(x) &:= m_{\beta^0}(x) = x - \beta^0 \\ g_1(x) &:= m_{\beta^1}(x) = m_{\beta^4}(x) = (x - \beta^1)(x - \beta^4) \\ g_2(x) &:= m_{\beta^2}(x) = m_{\beta^8}(x) = (x - \beta^2)(x - \beta^8) \\ g_3(x) &:= m_{\beta^3}(x) = m_{\beta^{12}}(x) = (x - \beta^3)(x - \beta^{12}) \\ g_4(x) &:= m_{\beta^5}(x) = x - \beta^5 \\ g_5(x) &:= m_{\beta^6}(x) = m_{\beta^9}(x) = (x - \beta^6)(x - \beta^9) \\ g_6(x) &:= m_{\beta^7}(x) = m_{\beta^{13}}(x) = (x - \beta^7)(x - \beta^{13}) \\ g_7(x) &:= m_{\beta^{10}}(x) = x - \beta^{10} \\ g_8(x) &:= m_{\beta^{11}}(x) = m_{\beta^{14}}(x) = (x - \beta^{11})(x - \beta^{14}) \end{aligned}$$

Since  $\delta = 5$  we need  $\delta - 1 = 4$  consecutive roots. So

$$g(x) = \text{lcm}(m_{\beta^b}(x), m_{\beta^{b+1}}(x), m_{\beta^{b+2}}(x), m_{\beta^{b+3}}(x))$$

for some  $b$ . We want to choose  $b$  such that  $\deg(g(x))$  is minimal. By going over all possibilities for  $b$ , we get that

$$\deg(g(x)) = \begin{cases} 6 & \text{if } b \in \{1, 6, 11\} \\ 7 & \text{if } b \in \{0, 2, 3, 4, 5, 7, 8, 9, 10, 12, 13, 14\} \end{cases}$$

For example, if  $b = 1$  then

$$g(x) = \text{lcm}(m_{\beta^1}(x), m_{\beta^2}(x), m_{\beta^3}(x), m_{\beta^4}(x)) = \text{lcm}(g_1(x), g_2(x), g_3(x), g_1(x)) = g_1(x)g_2(x)g_3(x)$$

So

$$\deg(g(x)) = \deg(g_1(x)g_2(x)g_3(x)) = \deg(g_1(x)) + \deg(g_2(x)) + \deg(g_3(x)) = 2 + 2 + 2 = 6$$

Hence

$$\dim(C) = n - \deg(g(x)) = 15 - 6 = 9$$

(b) This exercise is actually about Reed-Solomon codes.

Let  $\beta$  be an element of order 15 in some field extension of  $GF(16)$ . Then we have that  $\beta \in GF(16)$ . So  $\beta^i \in GF(16)$  for all  $i$ . Hence the minimal polynomial  $m_{\beta^i}(x)$  of  $\beta^i$  over  $GF(16)$  is

$$m_{\beta^i}(x) = x - \beta^i$$

Or put another way: all the cyclotomic cosets are singletons.

Since  $\delta = 5$ , we need to pick  $\delta - 1 = 4$  consecutive roots. So no matter what value of  $b$  we choose, we always have that

$$g(x) = \text{lcm}(m_{\beta^b}(x), m_{\beta^{b+1}}(x), m_{\beta^{b+2}}(x), m_{\beta^{b+3}}(x)) = (x - \beta^b)(x - \beta^{b+1})(x - \beta^{b+2})(x - \beta^{b+3})$$

So  $\deg(g(x)) = 4$  and  $\dim(C) = 15 - 4 = 11$ . □

2. Construct a BCH-code of length 17 and dimension 9 over  $GF(4)$  that can correct at least three errors.

*Solution* : Since the code must be able to correct at least three errors, the minimum distance of the code must be at least  $2 \cdot 3 + 1 = 7$ . So we choose  $\delta = 7$ . Since the dimension of the code is 9, the degree of the generator polynomial must be  $17 - 9 = 8$ .

The cyclotomic cosets depending on  $n = 17$  and  $q = 4$  are

$$\{0\} , \{1, 4, 16, 13\} , \{2, 8, 15, 9\} , \{3, 12, 14, 5\} , \text{ and } \{6, 7, 11, 10\}$$

From the cyclotomic cosets, we get that

$$\begin{aligned} g_0(x) &:= m_{\beta^0}(x) = x - \beta^0 \\ g_1(x) &:= m_{\beta^1}(x) = m_{\beta^4}(x) = m_{\beta^{16}}(x) = m_{\beta^{13}}(x) = (x - \beta^1)(x - \beta^4)(x - \beta^{16})(x - \beta^{13}) \\ g_2(x) &:= m_{\beta^2}(x) = m_{\beta^8}(x) = m_{\beta^{15}}(x) = m_{\beta^9}(x) = (x - \beta^2)(x - \beta^8)(x - \beta^{15})(x - \beta^9) \\ g_3(x) &:= m_{\beta^3}(x) = m_{\beta^{12}}(x) = m_{\beta^{14}}(x) = m_{\beta^5}(x) = (x - \beta^3)(x - \beta^{12})(x - \beta^{14})(x - \beta^5) \\ g_4(x) &:= m_{\beta^6}(x) = m_{\beta^7}(x) = m_{\beta^{11}}(x) = m_{\beta^{10}}(x) = (x - \beta^6)(x - \beta^7)(x - \beta^{11})(x - \beta^{10}) \end{aligned}$$

Since  $\delta = 7$ , we need to pick  $\delta - 1 = 6$  consecutive roots. So

$$g(x) = \text{lcm}(m_{\beta^b}(x), m_{\beta^{b+1}}(x), m_{\beta^{b+2}}(x), m_{\beta^{b+3}}(x), m_{\beta^{b+4}}(x), m_{\beta^{b+5}}(x))$$

It turns out that

$$\deg(g(x)) = \begin{cases} 13 & \text{if } b \in \{0, 12, 13, 14, 15, 16\} \\ 12 & \text{if } b \in \{1, 5, 7\} \\ 16 & \text{if } b \in \{2, 3, 4, 8, 9, 10, 11\} \\ 8 & \text{if } b = 6 \end{cases}$$

We choose  $b = 6$ . Then

$$\begin{aligned} g(x) &= \text{lcm}(m_{\beta^6}(x), m_{\beta^7}(x), m_{\beta^8}(x), m_{\beta^9}(x), m_{\beta^{10}}(x), m_{\beta^{11}}(x)) \\ &= \text{lcm}(g_4(x), g_4(x), g_2(x), g_2(x), g_4(x), g_4(x)) \\ &= g_2(x)g_4(x) \end{aligned}$$

So

$$\deg(g(x)) = \deg(g_2(x)g_4(x)) = \deg(g_2(x)) + \deg(g_4(x)) = 4 + 4 = 8$$

and so

$$\dim(C) = n - \deg(g(x)) = 17 - 8 = 9 \quad \square$$

3. Construct a binary BCH-code of length 31 of designed distance 5 with minimum distance at least 11.

*Solution* : The cyclotomic cosets depending on  $n = 31$  and  $q = 2$  are

$$\{0\} , \{1, 2, 4, 8, 16\} , \{3, 6, 12, 24, 17\} , \{5, 10, 20, 9, 18\} , \{7, 14, 28, 25, 19\} , \{11, 22, 13, 26, 21\} \text{ and } \{15, 30, 29, 27, 23\}$$

From the cyclotomic cosets, we get that

$$\begin{aligned} g_0(x) &:= m_{\beta^0}(x) && \text{and } \deg(g_0(x)) = 1 \\ g_1(x) &:= m_{\beta^1}(x) = m_{\beta^2}(x) = m_{\beta^4}(x) = m_{\beta^8}(x) = m_{\beta^{16}}(x) && \text{and } \deg(g_1(x)) = 5 \\ g_2(x) &:= m_{\beta^3}(x) = m_{\beta^6}(x) = m_{\beta^{12}}(x) = m_{\beta^{24}}(x) = m_{\beta^{17}}(x) && \text{and } \deg(g_2(x)) = 5 \\ g_3(x) &:= m_{\beta^5}(x) = m_{\beta^{10}}(x) = m_{\beta^{20}}(x) = m_{\beta^9}(x) = m_{\beta^{18}}(x) && \text{and } \deg(g_3(x)) = 5 \\ g_4(x) &:= m_{\beta^7}(x) = m_{\beta^{14}}(x) = m_{\beta^{28}}(x) = m_{\beta^{25}}(x) = m_{\beta^{19}}(x) && \text{and } \deg(g_4(x)) = 5 \\ g_5(x) &:= m_{\beta^{11}}(x) = m_{\beta^{22}}(x) = m_{\beta^{13}}(x) = m_{\beta^{26}}(x) = m_{\beta^{21}}(x) && \text{and } \deg(g_5(x)) = 5 \\ g_6(x) &:= m_{\beta^{15}}(x) = m_{\beta^{30}}(x) = m_{\beta^{29}}(x) = m_{\beta^{27}}(x) = m_{\beta^{23}}(x) && \text{and } \deg(g_6(x)) = 5 \end{aligned}$$

We choose  $b = 4$  and  $\delta = 5$ . So we need  $\delta - 1 = 4$  consecutive roots. Hence

$$g(x) = \text{lcm}(m_{\beta^4}(x), m_{\beta^5}(x), m_{\beta^6}(x), m_{\beta^7}(x)) = \text{lcm}(g_1(x), g_3(x), g_2(x), g_4(x)) = g_1(x)g_2(x)g_3(x)g_4(x)$$

However, this generator polynomial has actually ten consecutive roots:

$$\beta, \beta^2, \beta^3, \beta^4, \beta^5, \beta^6, \beta^7, \beta^8, \beta^9 \text{ and } \beta^{10}$$

So the minimum distance is at least  $10 + 1 = 11$  (because if we choose  $b = 1$  and  $\delta = 10$ , we end up with exactly the same generator polynomial as when we choose  $b = 4$  and  $\delta = 5$ ).  $\square$

4. Put  $\beta = \alpha$  where  $\alpha$  is a primitive element of  $GF(16)$  as defined in the table for  $GF(16)$  in the notes. Consider the binary BCH-code of length 15 with generator polynomial

$$\text{lcm}(m_\beta(x), m_{\beta^2}(x), m_{\beta^3}(x), m_{\beta^4}(x))$$

- (a) What is the dimension of this code?
- (b) What is the designed distance of this code?
- (c) Use the Peterson-Gorenstein-Zierler decoding algorithm to decode the following word:

$$\mathbf{y} = 111000000000000$$

Solution : (a)(b) Careful: the code is a BINARY code so  $q = 2$ . This is not a Reed-Solomon code!  
The cyclotomic cosets depending on  $n = 15$  and  $q = 2$  are

$$\{0\} , \{1, 2, 4, 8\} , \{3, 6, 12, 9\} , \{5, 10\} \text{ and } \{7, 14, 13, 11\}$$

From the cyclotomic cosets, we get that

$$\begin{aligned} g_0(x) &:= m_{\beta^0}(x) = x - \beta^0 \\ g_1(x) &:= m_{\beta^1}(x) = m_{\beta^2}(x) = m_{\beta^4}(x) = m_{\beta^8}(x) = (x - \beta^1)(x - \beta^2)(x - \beta^4)(x - \beta^8) \\ g_2(x) &:= m_{\beta^3}(x) = m_{\beta^6}(x) = m_{\beta^{12}}(x) = m_{\beta^9}(x) = (x - \beta^3)(x - \beta^6)(x - \beta^{12})(x - \beta^9) \\ g_3(x) &:= m_{\beta^5}(x) = m_{\beta^{10}}(x) = (x - \beta^5)(x - \beta^{10}) \\ g_4(x) &:= m_{\beta^7}(x) = m_{\beta^{14}}(x) = m_{\beta^{13}}(x) = m_{\beta^{11}}(x) = (x - \beta^7)(x - \beta^{14})(x - \beta^{13})(x - \beta^{11}) \end{aligned}$$

From the given generator polynomial, we get that  $b = 1$  and  $\delta = 4 + 1 = 5$ .

So

$$g(x) = \text{lcm}(m_\beta(x), m_{\beta^2}(x), m_{\beta^3}(x), m_{\beta^4}(x)) = \text{lcm}(g_1(x), g_1(x), g_2(x), g_1(x)) = g_1(x)g_2(x)$$

Hence

$$\deg(g(x)) = \deg(g_1(x)g_2(x)) = \deg(g_1(x)) + \deg(g_2(x)) = 4 + 4 = 8$$

Thus

$$\dim(C) = n - \deg(g(x)) = 15 - 8 = 7$$

(c) We have that

$$\mathbf{y}(x) = 1 + x + x^2$$

First, we calculate  $\delta - 1 = 4$  syndromes. We get

$$\begin{aligned} S_1 = \mathbf{y}(\beta) = \mathbf{y}(\alpha) &= 1 + \alpha + \alpha^2 = 0001 + 0010 + 0100 = 0111 = \alpha^7 \\ S_2 = \mathbf{y}(\beta^2) = \mathbf{y}(\alpha^2) &= 1 + \alpha^2 + \alpha^4 = 0001 + 0100 + 1001 = 1100 = \alpha^{14} \\ S_3 = \mathbf{y}(\beta^3) = \mathbf{y}(\alpha^3) &= 1 + \alpha^3 + \alpha^6 = 0001 + 1000 + 1111 = 0110 = \alpha^{13} \\ S_4 = \mathbf{y}(\beta^4) = \mathbf{y}(\alpha^4) &= 1 + \alpha^4 + \alpha^8 = 0001 + 1001 + 1110 = 0110 = \alpha^{13} \end{aligned}$$

Next, we calculate  $k$ , the number of errors that occurred. Since  $\delta = 5$ , we have that  $t = 2$ . We get

$$\begin{vmatrix} \alpha^7 & \alpha^{14} \\ \alpha^{14} & \alpha^{13} \end{vmatrix} = \alpha^7\alpha^{13} + \alpha^{14}\alpha^{14} = \alpha^{20} + \alpha^{28} = \alpha^5 + \alpha^{13} = 1011 + 0110 = 1101 = \alpha^{11} \neq 0$$

Hence we assume that  $k = 2$  : two errors occurred.

Next, we find the error-locating polynomial. So we have to solve

$$\begin{bmatrix} \alpha^7 & \alpha^{14} \\ \alpha^{14} & \alpha^{13} \end{bmatrix} \begin{bmatrix} s_2 \\ s_1 \end{bmatrix} = \begin{bmatrix} \alpha^{13} \\ \alpha^{13} \end{bmatrix}$$

We use Cramer's Rule.

Since

$$\begin{vmatrix} \alpha^{13} & \alpha^{14} \\ \alpha^{13} & \alpha^{13} \end{vmatrix} = \alpha^{13}\alpha^{13} + \alpha^{13}\alpha^{14} = \alpha^{26} + \alpha^{27} = \alpha^{11} + \alpha^{12} = 1101 + 0011 = 1110 = \alpha^8$$

we get that

$$s_2 = \frac{\alpha^8}{\alpha^{11}} = \alpha^{-3} = \alpha^{12}$$

Since

$$\begin{vmatrix} \alpha^7 & \alpha^{13} \\ \alpha^{14} & \alpha^{13} \end{vmatrix} = \alpha^7\alpha^{13} + \alpha^{14}\alpha^{13} = \alpha^{20} + \alpha^{27} = \alpha^5 + \alpha^{12} = 1011 + 0011 = 1000 = \alpha^3$$

we get that

$$s_1 = \frac{\alpha^3}{\alpha^{11}} = \alpha^{-8} = \alpha^7$$

So the error-locating polynomial is

$$s(x) = 1 + s_1x + s_2x = 1 + \alpha^7x + \alpha^{12}x^2$$

Next, we need to find the roots of  $s(x)$ . We should find two roots and they should be powers of  $\beta$ . Since we really want the reciprocals of the roots, we start

$$\begin{aligned} s(\beta^0) &= s(1) = 1 + \alpha^7 + \alpha^{12} = 0001 + 0111 + 0011 = 0101 \neq 0 \\ s(\beta^{-1}) &= s(\alpha^{-1}) = 1 + \alpha^7\alpha^{-1} + \alpha^{12}\alpha^{-2} = 1 + \alpha^6 + \alpha^{10} = 0001 + 1111 + 1010 = 0100 \neq 0 \\ s(\beta^{-2}) &= s(\alpha^{-2}) = 1 + \alpha^7\alpha^{-2} + \alpha^{12}\alpha^{-4} = 1 + \alpha^5 + \alpha^8 = 0001 + 1011 + 1110 = 0100 \neq 0 \\ s(\beta^{-3}) &= s(\alpha^{-3}) = 1 + \alpha^7\alpha^{-3} + \alpha^{12}\alpha^{-6} = 1 + \alpha^4 + \alpha^6 = 0001 + 1001 + 1111 = 0111 \neq 0 \\ s(\beta^{-4}) &= s(\alpha^{-4}) = 1 + \alpha^7\alpha^{-4} + \alpha^{12}\alpha^{-8} = 1 + \alpha^3 + \alpha^4 = 0001 + 1001 + 1000 = 0000 = 0 \end{aligned}$$

So  $\alpha^{-4}$  is a root of  $s(x)$ . Since the product of the roots is  $\alpha^{-12}$ , we get that  $\alpha^{-8}$  is the other root of  $s(x)$ .

Hence

$$X_1 = \alpha^4 = \beta^4 \quad \text{and} \quad X_2 = \alpha^8 = \beta^8$$

That means that the first error occurred in the fourth position while the second error occurred in the eighth position (recall that we start numbering the position from zero).

Finally, we find the error-sizes  $Y_1$  and  $Y_2$ . Since we are working binary, we should find  $Y_1 = Y_2 = 1$ . We have to solve

$$\begin{bmatrix} \alpha^4 & \alpha^8 \\ \alpha^8 & \alpha^{16} \\ \alpha^{12} & \alpha^{24} \\ \alpha^{16} & \alpha^{32} \end{bmatrix} \begin{bmatrix} Y_1 \\ Y_2 \end{bmatrix} = \begin{bmatrix} \alpha^7 \\ \alpha^{14} \\ \alpha^{13} \\ \alpha^{13} \end{bmatrix}$$

or

$$\begin{bmatrix} \alpha^4 & \alpha^8 \\ \alpha^8 & \alpha \\ \alpha^{12} & \alpha^9 \\ \alpha & \alpha^2 \end{bmatrix} \begin{bmatrix} Y_1 \\ Y_2 \end{bmatrix} = \begin{bmatrix} \alpha^7 \\ \alpha^{14} \\ \alpha^{13} \\ \alpha^{13} \end{bmatrix}$$

A quick check does indeed show that  $Y_1 = Y_2 = 1$ :

$$\begin{aligned} \alpha^4 + \alpha^8 &= 1001 + 1110 = 0111 = \alpha^7 \\ \alpha^8 + \alpha &= 1110 + 0010 = 1100 = \alpha^{14} \\ \alpha^{12} + \alpha^9 &= 0011 + 0101 = 0110 = \alpha^{13} \\ \alpha + \alpha^2 &= 0010 + 0100 = 0110 = \alpha^{13} \end{aligned}$$

So the error vector is

$$\mathbf{e} = 000010001000000$$

Hence we decode  $\mathbf{y}$  as

$$\mathbf{y} - \mathbf{e} = \mathbf{0} = 111010001000000$$

□

5. Put  $\beta = \alpha$  where  $\alpha$  is a primitive element of  $GF(8)$  as defined in the table for  $GF(8)$  in the notes. Consider the binary BCH-code of length 7 with generator polynomial  $\text{lcm}(m_\beta(x), m_{\beta^2}(x))$ . Use the Peterson-Gorenstein-Zierler decoding algorithm to decode the following words:

(a) 1000110

(b) 1000001

Solution : Note that  $\delta = 2 + 1 = 3$  and  $b = 1$ .

(a) Put  $\mathbf{y} = 1000110$ . Then  $\mathbf{y}(x) = 1 + x^4 + x^5$ .

First, we calculate  $\delta - 1 = 2$  syndromes. We get

$$\begin{aligned} S_1 &= \mathbf{y}(\beta) = \mathbf{y}(\alpha) = 1 + \alpha^4 + \alpha^5 = 001 + 110 + 111 = 000 = 0 \\ S_2 &= \mathbf{y}(\beta^2) = \mathbf{y}(\alpha^2) = 1 + \alpha^8 + \alpha^{10} = 1 + \alpha + \alpha^3 = 001 + 010 + 011 = 000 = 0 \end{aligned}$$

Hence  $\mathbf{y}$  is a codeword and we decode as  $\mathbf{y}$ .

(b) Put  $\mathbf{y} = 1000001$ . Then  $\mathbf{y}(x) = 1 + x^6$ .

First, we calculate  $\delta - 1 = 2$  syndromes. We get

$$\begin{aligned} S_1 &= \mathbf{y}(\beta) = \mathbf{y}(\alpha) = 1 + \alpha^6 = 001 + 101 = 100 = \alpha^2 \\ S_2 &= \mathbf{y}(\beta^2) = \mathbf{y}(\alpha^2) = 1 + \alpha^{12} = 1 + \alpha^5 = 001 + 111 = 110 = \alpha^4 \end{aligned}$$

Next, we calculate  $k$ , the number of errors that occurred. Since  $\delta = 3$ , we have that  $t = 1$ . So we ‘calculate’

$$|\alpha^2| = \alpha^2 \neq 0$$

Hence we assume that  $k = 1$  : one error occurred.

Next, we find the error-locating polynomial. So we have to solve

$$\alpha^2 s_1 = \alpha^4$$

Hence

$$s_1 = \frac{\alpha^4}{\alpha^2} = \alpha^2$$

So the error-locating polynomial is

$$s(x) = 1 + s_1 x = 1 + \alpha^2 x$$

Next, we need to find the roots of  $s(x)$ . We easily get that

$$x = \frac{1}{\alpha^2} = \alpha^{-2}$$

So

$$X_1 = \alpha^2 = \beta^2$$

That means that the error occurred in the second position (recall that we start numbering the position from zero). Finally, we find the error-size  $Y_1$ . We have to solve

$$\begin{bmatrix} \alpha^2 \\ \alpha^4 \end{bmatrix} [ Y_1 ] = \begin{bmatrix} \alpha^2 \\ \alpha^4 \end{bmatrix}$$

We easily get that

$$Y_1 = \frac{\alpha^2}{\alpha^2} = \frac{\alpha^4}{\alpha^4} = 1$$

So the error vector is

$$\mathbf{e} = 0010000$$

Hence we decode  $\mathbf{y}$  as

$$\mathbf{y} - \mathbf{e} = 1010001$$

□

**6.** Put  $\beta = \alpha^3$  where  $\alpha$  is a primitive element of  $GF(16)$  as defined in the table for  $GF(16)$  in the notes. Then  $GF(4) = \{0, 1, \alpha^5, \alpha^{10}\}$  is a subfield of  $GF(16)$ . Consider the BCH-code of length 5 over  $GF(4)$  with generator polynomial  $\text{lcm}(m_{\beta^2}(x), m_{\beta^3}(x))$ . So  $b = 2$ .

- (a) What is the dimension of this code?
- (b) What is the designed distance of this code?
- (c) Use the Peterson-Gorenstein-Zierler decoding algorithm to decode the word  $\mathbf{y} = 1\alpha^5 100$

Solution : (a) The cyclotomic cosets depending on  $n = 5$  and  $q = 4$  are

$$\{0\} , \{1, 4\} \text{ and } \{2, 3\}$$

Hence

$$m_{\beta^2}(x) = m_{\beta^3}(x) = (x - \beta^2)(x - \beta^3)$$

and

$$g(x) = \text{lcm}(m_{\beta^2}(x), m_{\beta^3}(x)) = (x - \beta^2)(x - \beta^3)$$

So  $\deg(g(x)) = 2$  and thus

$$\dim(C) = n - \deg(g(x)) = 5 - 2 = 3$$

(b) Since  $g(x) = \text{lcm}(m_{\beta^2}(x), m_{\beta^3}(x))$ , we have that  $\delta = 2 + 1 = 3$ .

(c) Note that  $\mathbf{y}(x) = 1 + \alpha^5 x + x^2$ .

First, we calculate  $\delta - 1 = 2$  syndromes. We get

$$\begin{aligned} S_1 &= \mathbf{y}(\beta^2) = \mathbf{y}(\alpha^6) = 1 + \alpha^{11} + \alpha^{12} = 0001 + 1101 + 0011 = 1111 = \alpha^6 \\ S_2 &= \mathbf{y}(\beta^3) = \mathbf{y}(\alpha^9) = 1 + \alpha^{14} + \alpha^{18} = 1 + \alpha^{14} + \alpha^3 = 0001 + 1100 + 1000 = 0101 = \alpha^9 \end{aligned}$$

Next, we calculate  $k$ , the number of errors that occurred. Since  $\delta = 3$ , we have that  $t = 1$ . So we ‘calculate’

$$|\alpha^6| = \alpha^6 \neq 0$$

Hence we assume that  $k = 1$  : one errors occurred.

Next, we find the error-locating polynomial. So we have to solve

$$\alpha^6 s_1 = \alpha^9$$

Hence

$$s_1 = \frac{\alpha^9}{\alpha^6} = \alpha^3$$

So the error-locating polynomial is

$$s(x) = 1 + s_1 x = 1 + \alpha^3 x$$

Next, we need to find the roots of  $s(x)$ . We easily get that

$$x = \frac{1}{\alpha^3} = \alpha^{-3}$$

So

$$X_1 = \alpha^3 = \beta^1$$

That means that the error occurred in the first position (recall that we start numbering the position from zero). Finally, we find the error-size  $Y_1$ . We have to solve

$$\begin{bmatrix} \alpha^6 \\ \alpha^9 \end{bmatrix} [ Y_1 ] = \begin{bmatrix} \alpha^6 \\ \alpha^9 \end{bmatrix}$$

We easily get that

$$Y_1 = \frac{\alpha^6}{\alpha^6} = \frac{\alpha^9}{\alpha^9} = 1$$

So the error vector is

$$\mathbf{e} = 01000$$

Hence we decode  $\mathbf{y}$  as

$$\mathbf{y} - \mathbf{e} = 1\alpha^5 100 - 01000 = 1\alpha^{10} 100$$

since  $\alpha^5 - 1 = 1011 + 0001 = 1010 = \alpha^{10}$ . □

---

---