For $(7,4)$ code, our $g(x) = x^3 + x + 1$

if $x = \alpha$, then $g(x) = \alpha^3 + \alpha + 1$

consider α is a factor of $g(x)$, then $\alpha^3 + \alpha + 1 = 0$

$\Rightarrow \alpha^3 = \alpha + 1$ (In digital)

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

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

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

$= \alpha \cdot \alpha^4$

$= \alpha(\alpha^2 + \alpha)$

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

$= \alpha + 1$

$\alpha^6 = \alpha(\alpha^2 + \alpha + 1)$

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

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

$= \alpha^2 + 1$

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

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

$\alpha^6 = \alpha^2 + 1$

$\alpha^7 = \alpha(\alpha^2 + 1)$

$= \alpha^3 + \alpha$

$= (\alpha + 1) + \alpha = 1$

A factor that can find out each & every non-zero element or factors of a polynomial is called a Primitive Element, (α)

And a polynomial that can generate all the factors of an highest power polynomial is called a Primitive Polynomial. $(x^3 + x + 1)$

$x^4 + x^2 + x + 1$ is a factor of x^{15}

$x = 1$ is a factor, so $(x+1)$ is a factor of $(x^4 + x^2 + x + 1)$

The polynomials that cannot be factorised are called Irreducible Poly.

$GF(2^4)$ ⟶ factor x^{15} & irreducible $GF(2^3) \rightarrow \underbrace{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6}_{7}$

$g(x) = x^4 + x^3 + 1$ / $x^4 + x^3 + x$ / $x^2 + x + 1$

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

Let, α be a factor, $x(\alpha) = 0$

$x^4 \mid x^4 + x + 1 \mid x^{15}$

$\alpha^4 + \alpha + 1 = 0$

$\Rightarrow \alpha^4 = \alpha + 1$ —— (1)

$\alpha^5 = \alpha^2 + \alpha$ —— (2) $= \alpha(\alpha+1)$

$\alpha^6 = \alpha^3 + \alpha^2$ —— (3)

$x^7 = x^4 + \alpha^3 = \alpha^3 + \alpha + 1$ —— (4)

$x^8 = \alpha^4 + \alpha^2 + \alpha$ $\quad \alpha + 1 + \alpha + \alpha^2$

$= \alpha^2 + 1$ —— (5)

$x^9 = \alpha^3 + \alpha$ —— (6)

$x^{10} = \alpha^4 + \alpha^2 = (\alpha + 1) + \alpha^2 = \alpha^2 + \alpha + 1$ —— (7)

$x^{11} = \alpha^3 + \alpha^2 + \alpha =$ —— (8)

$x^{12} =$ $\quad \alpha^4 + \alpha^3 + \alpha^2 =$ (9)

$\alpha + 1 + \alpha^3 + \alpha^2$ —— (9)

$(\alpha + 1) + \alpha$

$x^{13} = \alpha^4 + \alpha^3 + \alpha^2 = \alpha^3 + \alpha^2 + 1$ —— (10)

$+ \alpha$

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

$x^{14} = \alpha^4 + \alpha^3 + \alpha$ —— (11) $= \alpha^3 + 1$

$x^{15} = \alpha^4 + \alpha^2 + \alpha = \alpha + 1 + \alpha^3 + \alpha^2$

$= 1$

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

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

α^0
α^1
α
α^2
α^3
α^4
α^5
α^6
α^7
α^8
α^9
α^{10}
α^{11}
α^{12}
α^{13}
α^{14}

$\alpha^i \cdot \alpha^j = \alpha^{(i+j)\%7}$ for (7,4) code.

$$\frac{\alpha^2}{\alpha^5} = \alpha^2 \cdot \alpha^{-5} = \alpha^2 \cdot \alpha^{(-5)\%7} = \alpha^2 \cdot \alpha^2 = \alpha^4$$

$\beta \rightarrow$ Search for primitive elements among α.

$$\beta = \alpha^2$$
$$\beta^2 = \alpha^4$$

9) Show that α^5 is a primitive element of $GF(2^3)$ i.e prove $\beta = \alpha^5$

$GF(2^3) \longrightarrow g(x) = x^3 + x + 1$

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

Let $\beta = \alpha^5$

$\beta^2 = \alpha^{10} = \alpha^3$

$\beta^3 = \alpha^{15} = \alpha^8 \cdot \alpha^7 = \alpha^1$

$\beta^4 = \alpha^{20} = \alpha^{16} \cdot \alpha^4 = \alpha^6$

$\beta^5 = \alpha^{25} = \alpha^4$

$\beta^6 = \alpha^{30} = \alpha^2$

$\beta^7 = \alpha^{35} = 1$

So $\beta = \alpha^5$ can generate all the elements

9) Find conjugate α^5 for $GF(2^4)$

$\beta = \alpha^5$

$\beta^2 = \alpha^{10} = \alpha^{10}$

$\beta^3 = \alpha^{15} = 1$

$\beta^4 = \alpha^{20} = \alpha^5$

$\beta^5 = \alpha^{25} = \alpha^{10}$

$\beta^6 = \alpha^{30} = 1$

$\beta, \beta^2, \beta^4, \beta^8, \ldots, \beta^{2^{n-1}}$

$\beta = \alpha^5$

$\beta^2 = \alpha^{10}$

$\beta^4 = \alpha^{20} = \alpha^5$

$\beta^8 = \alpha^{40} = \beta^{10}$

7th chapter

9.) α^7 in $GF(2^4)$

$\beta = \alpha^7$

$\beta^2 = \alpha^{14}$

$\beta^4 = \alpha^{28} = \alpha^{13}$

$\beta^8 = \alpha^{56} = \alpha^{11}$

$\beta^{16} = \alpha^{112} = \alpha^7$

conjugates are $\alpha^{11}, \alpha^{13}, \alpha^{14}$

$112 / 7 = 16$

$15 \times 6 = 90$

So, minimal polynomial, $m(x) = (x + \alpha^7)(x + \alpha^{11})(x + \alpha^{13})(x + \alpha^{14})$

$= (x^2 + \alpha^{11}x + x^7 x + \alpha^{18})(x^2 + \alpha^{14}x + \alpha^{13}x + \alpha^{27})$

$= x^4 + \alpha^{14}x^3 + \alpha^{13}x^3 + \alpha^{27}x^2 + \alpha^{25}x + x^3 + \alpha^{14}x^2 + \alpha^{13}x^2 + \alpha^{27}x + \alpha^{18}x^2 + \alpha^{32}x + \alpha^{31} + \alpha^{45}$

$= \alpha$

$m(x) = x^4 + x^3 + 1$

Degree of $g(x)$ is $(m-k)$, $\boxed{m = \log_2(n+1)}$ where $n = 2^m - 1$

(m → GF order)

$k = (2^m - 1) - mt$, $t \rightarrow$ no. of error correction

$\Rightarrow \boxed{k = n - mt}$

and, $d_{min} = 2t + 1$

Q) Design a BCH code with blocklength $n = 15$ and $t = 2$.

$m = \log_2(n+1)$

$m = \log_2 16 = 4$

$k = 15 - (4 \times 2) = 7$

Given $n = 15$

so, $m = \log_2(n+1) = \log_2 16$

$\therefore$ We have $GF(2^4)$.

$g(x) = LCM[m_1(x), m_3(x), \ldots m_{2t}(x)]$

$\downarrow\downarrow$

$m_4(x)$

$\because$ Even part is negated.

$g(x) = LCM[m_1(x), m_3(x)]$

α $\quad$ α^3

From Table multiply elements

$= (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)$

$= x^8 + x^7 + x^6 + x^5 + x^5 + x^4 + x^3 + x^2 + x + x^4 + x^3 + x^2 + x + 1$

$g(x) = x^8 + x^7 + x^6 + x^4 + 1$

$\because$ Order = 8, $\therefore$ BCH code structure = (15, 7).

$n - k = 8$

$\Rightarrow 15 - k = 8 \Rightarrow k = 7$

g.) Construct a triple error correcting BCH code with blocklength $n = 31$, over $GF(2^5)$

$t = 3$

$2t \rightarrow 6$

$g(x) = LCM[m_1(x), m_3(x), m_5(x)]$

$\alpha^1 \quad \alpha^3 \quad \alpha^5$

$= (x^5+x^2+1)(x^5+x^4+x^3+x^2+1)(x^5+x^4+x^2+x+1)$

Order = 15

$n - k = 15$

$31 - k = 15$

$\boxed{k = 16}$

$g(x) = x^{15} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1$

$Sy = x^{n-k} \cdot i(x) + R_{g(x)}[x^{n-k} \cdot i(x)]$

$N.S = i(x) \cdot g(x)$ ✓

Decoding [Double error decoding → pg 193]

g.) For single bit correcting BCH code in $(7,4)$ code if given received word is (1010000)

$\boxed{1011000}$

$(7,4)$ code → $GF(2^3)$ → $0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$

$r(x) = x^6 + x^4$

$r(\alpha) = \alpha^6 + \alpha^4 = 0$

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

$r(x) = \alpha + 1 = \alpha^3$ → ∴ Error in the 2^3th position

$\alpha^3 = \alpha + 1$

$\alpha^4 = \alpha^2 + \alpha$

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

$\alpha^6 = \alpha^2 + 1$

$\alpha^3 + \alpha^2$

$\alpha + 1 + \alpha^2$

$\alpha^3 + \alpha^2 + \alpha$

$\alpha + 1 + \alpha^2 + \alpha$

∴ $v(x) = r(x) + e(x) = 1010000 + 0001000$

Peterson Gorenstein Zierler (Generalised multiple error decoding structure)

Step 1: Calculate error syndrome from $r(x)$,

$$S_i = r(\alpha^i)$$

Step 2: Let no. of errors be 'l'.

Step 3: If $l = 0$, then "NO ERROR"

Step 4: Construct $M =$

Step 5: Find determinant of M.

Step 6: If $\det(M) = 0$, then $M = 1$

Step 7: Find M^{-1} and construct S

Step 8: Find $\boxed{\Lambda = M^{-1} \cdot S}$

Step 9: Construct $\Lambda(x) = 1 + \Lambda_1 x + \Lambda_2 x^2 + \ldots + \Lambda_l x^l$

Step 10: Find roots of $\Lambda(x)$ and take reciprocal which are error locations.

Step 11: Construct $e(x)$.

Step 12: $c(x) = e(x) + r(x)$.

$$\Lambda(x) = 1 + \Lambda_1 x + \Lambda_2 x^2 + \Lambda_3 x^3 + \ldots + \Lambda_l x^l.$$

$$\begin{bmatrix} S_{l+1} \\ S_{l+2} \\ \vdots \\ S_{2l} \end{bmatrix} = \underbrace{\begin{bmatrix} S_1 & S_2 & S_3 & \cdots & S_l \\ S_2 & S_3 & S_4 & \cdots & S_{l+1} \\ \vdots & & & & \\ S_l & S_{l+1} & S_{l+2} & \cdots & S_{2l} \end{bmatrix}}_{M} \begin{bmatrix} \lambda_l \\ \lambda_{l-1} \\ \lambda_{l-2} \\ \vdots \\ \lambda_2 \\ \lambda_1 \end{bmatrix}$$

$$S = M\lambda$$

$$\Rightarrow \lambda = M^{-1} S$$

9.) Consider (15,7) double-error correcting BCH code with $g(x) = x^8 + x^7 + x^6 + x^4 + 1$

and received word $r = [000001101111010]$

$$r(x) = x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + x + 1$$

$l = 2$, $n = 15$, $k = 7$ $\Rightarrow GF(2^4)$

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

$l = 2$

$$\begin{bmatrix} S_3 \\ S_4 \end{bmatrix} = \begin{bmatrix} S_1 & S_2 \\ S_2 & S_3 \end{bmatrix} \begin{bmatrix} \lambda_2 \\ \lambda_1 \end{bmatrix} \qquad M = \begin{bmatrix} \alpha^{13} & \alpha^{11} \\ \alpha^{11} & 0 \end{bmatrix}$$

$$|M| = \alpha^{22} = \alpha^7$$

$$M^{-1} = \frac{1}{|M|} adj(M)$$

$$\Rightarrow M^{-1} = \frac{1}{\alpha^7} \begin{bmatrix} 0 & \alpha^{11} \\ \alpha^{11} & \alpha^{13} \end{bmatrix}$$

$$M^{-1} = \begin{bmatrix} 0 & \alpha^4 \\ \alpha^4 & \alpha^6 \end{bmatrix}$$

$S_{2i} = S_i^2$

$$S_1 = r(\alpha) = \alpha^9 + \alpha^8 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha + 1 = \alpha^{13}$$

$$S_2 = r(\alpha^2) = S_1^2 = (\alpha^{13})^2 = \alpha^{26} = \alpha^{11}$$

$$S_3 = r(\alpha^3) = \alpha^{27} + \alpha^{24} + \alpha^{18} + \alpha^{15} + \alpha^{12} + \alpha^5 + \alpha^3 = 0$$

$$S_4 = r(\alpha^4) = S_2^2 = S_1^4 = \alpha^{22} = \alpha^7$$

$$M^{-1} = \begin{bmatrix} 0 & \alpha^4 \\ \alpha^4 & \alpha^6 \end{bmatrix}$$

Now, $[S] = \begin{bmatrix} S_3 \\ S_4 \end{bmatrix} = \begin{bmatrix} 0 \\ \alpha^7 \end{bmatrix}$

Now, $\Lambda = M^{-1} S$

$$= \begin{bmatrix} 0 & \alpha^4 \\ \alpha^4 & \alpha^6 \end{bmatrix} \begin{bmatrix} 0 \\ \alpha^7 \end{bmatrix}$$

$$\Lambda = \begin{bmatrix} \alpha^{11} \\ \alpha^{13} \end{bmatrix} = \begin{bmatrix} \lambda_e \\ \lambda_{e-1} \end{bmatrix} = \begin{bmatrix} \lambda_2 \\ \lambda_1 \end{bmatrix}$$

Now, $\lambda(x) = 1 + \lambda_1 x + \lambda_2 x^2 + \cdots$

$\lambda(x) = 1 + \alpha^{13} x + \alpha^{11} x^2 = (1 + \alpha^3 x)(1 + \alpha^8 x)$

↳ Locations of errors

↳ $\alpha_1 + \alpha_2 = \alpha^{13}$

$\alpha_1 \alpha_2 = \alpha^{11}$

$\Rightarrow e(x) = x^3 + x^8$

$$c(x) = e(x) + r(x)$$