# Peterson-Gorenstein-Zierler Decoder

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

(1) $e(X) = e_0 + e_1X + \dots + e_{n-1}X^{n-1}$ where at most t coefficients are nonzero

(2) Suppose <u>v errors actually occur</u>, $\boxed{0 \le v \le t}$, in unknown locations

$i_1, i_2, \dots, i_v$

$\therefore e(X) = e_{i_1}X^{i_1} + e_{i_2}X^{i_2} + \dots + e_{i_v}X^{i_v}$

$i_j$, $e_{i_j}$, v are unknown !

(3) $S_1 = v(\alpha) = c(\alpha) + e(\alpha) = e(\alpha)$

$= e_{i_1}\alpha^{i_1} + e_{i_2}\alpha^{i_2} + \dots + e_{i_v}\alpha^{i_v}$

Let $Y_l = e_{i_l}$ : error magnitude $\quad 1 \le l \le v$

$X_l = \alpha^{i_l}$ : error-location number

Note : all $X_l$ are different ($\because \alpha^n = 1$)

$S_1 = Y_1X_1 + Y_2X_2 + \dots + Y_vX_v$

$\alpha^{i} = \alpha^{j} \quad j > i$

$\alpha^{j-i} = 1$

$(\neq)$

Q

Q: If $j_0$ is equal to 2, not 1, how do the peterson's method work?



(3)

$S_1 = v(\beta) = c(\beta) + e(\beta) = e(\beta)$

$= e_{i_1}\beta^{i_1} + e_{i_2}\beta^{i_2} + \dots + e_{i_v}\beta^{i_v}$

Let $Y_l = e_{i_l}$ : error magnitude $\quad 1 \le l \le v$

$X_l = \beta^{i_l}$ : error-location number

Note : all $X_l$ are different ($\because \alpha^n = 1$)

$S_1 = Y_1X_1 + Y_2X_2 + \dots + Y_vX_v$

Note: If $\beta = \alpha^3$ and $v=1$ & $i_1=6$

Then $S_1 = Y_1X_1 = Y_1\,\beta^6 = Y_1\,\alpha^{18}$

(4) For $\alpha\ \alpha^2\ \alpha^3 \ldots \alpha^{2t}$

(＊) nonlinear equations

$$\begin{cases} S_1 = Y_1X_1 + Y_2X_2 + \ldots + Y_vX_v \\ S_2 = Y_1X_1^2 + Y_2X_2^2 + \ldots + Y_vX_v^2 \\ S_3 = Y_1X_1^3 + Y_2X_2^3 + \ldots + Y_vX_v^3 \\ . \\ . \\ , \\ S_{2t} = Y_1X_1^{2t} + Y_2X_2^{2t} + \ldots + Y_vX_v^{2t} \end{cases}$$

$Y_l \in GF(q)$

$X_l \in GF(q^m)$

$\underset{2t\times v}{X}\ \underset{v\times 1}{Y} = \underset{2t\times 1}{S}$

1.(＊)至少有一解 ∵Syndrome $S_i$ is defined in such way

2.證明此解unique



Consider the polynomial $\Lambda(x) \equiv (1-X_1x)(1-X_2x)\ldots(1-X_vx)$

$$= 1 + \Lambda_1x + \Lambda_2x^2 + \ldots + \Lambda_vx^v - (1)$$

error-locator polynomial

If we knew the coefficients $\Lambda_l$ of $\Lambda(x)$

we could find the zeros of $\Lambda(x)$ to obtain the error locations $X_l$

$S_i \leftrightarrow \Lambda_l$

$1 \le i \le 2t \qquad 1 \le l \le v$

Multiply both sides of (1) by $Y_lX_l^{j+v}$ and set $x = X_l^{-1}$

$$0 = Y_l X_l^{j+v}\left(1 + \Lambda_1 X_l^{-1} + \Lambda_2 X_l^{-2} + \ldots + \Lambda_v X_l^{-v}\right)$$

$$\Rightarrow Y_l\left(X_l^{j+v} + \Lambda_1 X_l^{j+v-1} + \ldots + \Lambda_v X_l^{j}\right) = 0$$

$$\Rightarrow \sum_{l=1}^{v} Y_l\left(X_l^{j+v} + \Lambda_1 X_l^{j+v-1} + \ldots + \Lambda_v X_l^{j}\right) = 0$$

$$\sum_{l=1}^{v} Y_l X_l^{j+v} + \Lambda_1 \sum_{l=1}^{v} Y_l X_l^{j+v-1} + \ldots + \Lambda_v \sum_{l=1}^{v} Y_l X_l^{j} = 0$$

$$S_{j+v} + \Lambda_1 S_{j+v-1} + \Lambda_2 S_{j+v-2} + \ldots + \Lambda_v S_j = 0$$

$$\Lambda_1 S_{j+v-1} + \Lambda_2 S_{j+v-2} + \ldots + \Lambda_v S_j = -S_{j+v} \qquad \underline{1 \le j \le v}$$

$$\begin{bmatrix} S_1 & S_2 & S_3 & . & . & . & S_{v-1} & S_v \\ S_2 & S_3 & S_4 & . & . & . & S_v & S_{v+1} \\ S_3 & S_4 & S_5 & . & . & . & S_{v+1} & S_{v+2} \\ . & & & & & & & \\ . & & & & & & & \\ . & & & & & & & \\ S_v & S_{v+1} & S_{v+2} & . & . & . & S_{2v-2} & S_{2v-1} \end{bmatrix} \begin{bmatrix} \Lambda_v \\ \Lambda_{v-1} \\ \Lambda_{v-2} \\ . \\ . \\ . \\ \Lambda_1 \end{bmatrix} = \begin{bmatrix} -S_{v+1} \\ -S_{v+2} \\ -S_{v+3} \\ . \\ . \\ . \\ -S_{2v} \end{bmatrix}$$

$\because v \le t$

$\therefore S_1 \sim S_{2v}$

all known



Thm : The Vandermonde matrix has a nonzero determinant iff all of $X_i$ $1 \le i \le u$ are distinct

$$A = \begin{bmatrix} 1 & 1 & . & . & . & 1 \\ X_1 & X_2 & . & . & . & X_u \\ X_1^2 & X_2^2 & . & . & . & X_u^2 \\ . & . & & & & . \\ . & . & & & & . \\ . & . & & & & . \\ X_1^{u-1} & X_2^{u-1} & . & . & . & X_u^{u-1} \end{bmatrix}$$

Thm : The matrix of syndromes M is nonsingular if u is equal to v, <u>the number of errors that actually occurred</u>. The matrix is singular if u > v.

$$M = \begin{bmatrix} S_1 & S_2 & . & . & . & S_u \\ S_2 & S_3 & . & . & . & S_{u+1} \\ . & . & & & & . \\ . & . & & & & . \\ . & . & & & & . \\ S_u & S_{u+!} & . & . & . & S_{2u-1} \end{bmatrix}$$

If v > t

i.e. u < v時

det(M) = ?

Pf:Let $X_u = 0$ for $u > v$

$$\text{Let } A = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ X_1 & X_2 & \cdots & X_u \\ \vdots & \vdots & & \vdots \\ X_1^{u-1} & X_2^{u-1} & \cdots & X_u^{u-1} \end{bmatrix} \text{ with } A_{ij} = X_j^{i-1}$$

$$B = \begin{bmatrix} Y_1X_1 & 0 & \cdots & 0 \\ 0 & Y_2X_2 & \cdots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \cdots & Y_uX_u \end{bmatrix} \text{ with } B_{ij} = Y_iX_i\delta_{ij}, \delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

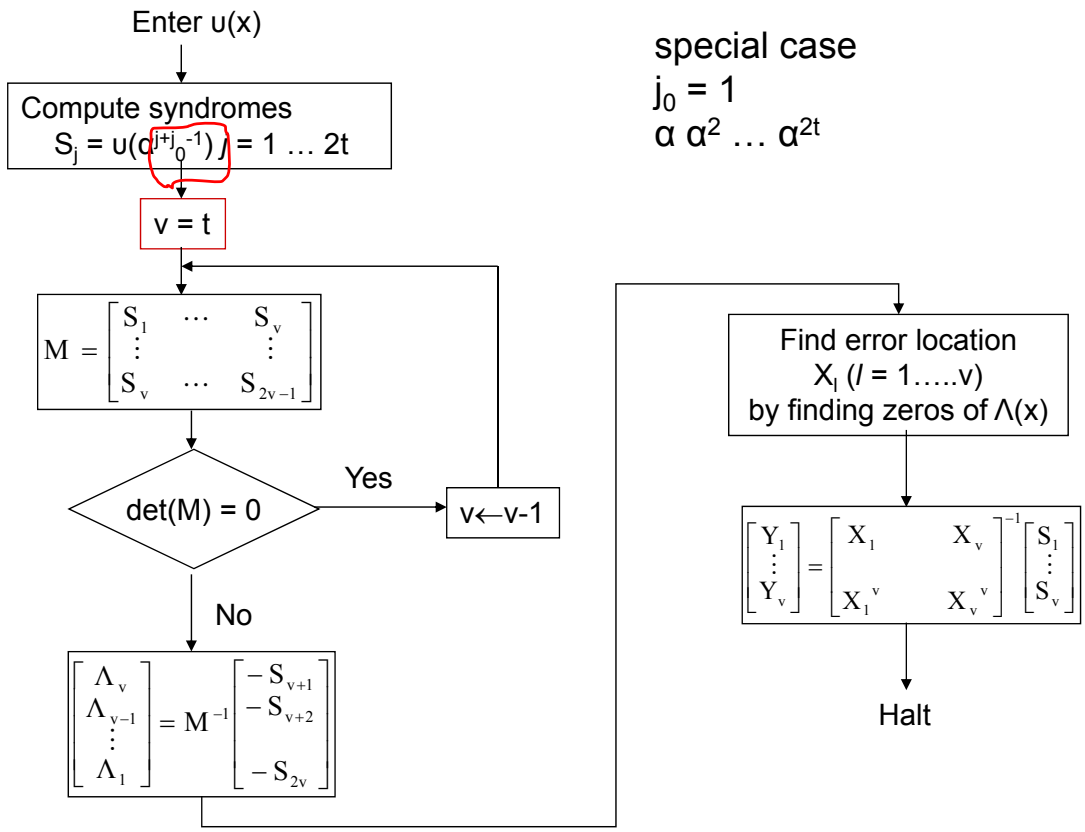
$$\left(ABA^T\right)_{ij} = \sum_{l=1}^{u} X_l^{i-1} \sum_{k=1}^{u} Y_l X_l \delta_{lk} X_k^{j-1} = \sum_{l=1}^{u} X_l^{i-1} Y_l X_l X_l^{j-1} = \sum_{l=1}^{u} Y_l X_l^{i+j-1} = M_{ij}$$

$\therefore M = ABA^T$

(1) $u > v$ $\det(B) = 0 \Rightarrow \det(M) = \det(A)\det(B)\det(A^T) = 0$

(2) $u = v$ $\det(B) \neq 0$ & $\det(A) \neq 0$ $\therefore \det(M) \neq 0$






special case
$j_0 = 1$
$\alpha\ \alpha^2 \ldots \alpha^{2t}$

**Figure 7.1** The Peterson-Gorenstein-Zierler decoder.

Eg:

BCH(15,5) triple-error-correcting code.

$g(X) = X^{10} + X^8 + X^5 + X^4 + X^2 + X + 1$

received code polynomial

$\Rightarrow$ $V(X) = X^7 + X^2$

In $GF(2^4)$

$S_1 = \alpha^7 + \alpha^2 = \alpha^{12}$

$S_2 = \alpha^{14} + \alpha^4 = \alpha^9$

$S_3 = \alpha^{21} + \alpha^6 = 0$

$S_4 = \alpha^{28} + \alpha^8 = \alpha^3$

$S_5 = \alpha^{35} + \alpha^{10} = \alpha^0$

$S_6 = \alpha^{42} + \alpha^{12} = 0$



$$\text{set } v = 3 \quad M = \begin{bmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{bmatrix} = \begin{bmatrix} \alpha^{12} & \alpha^9 & 0 \\ \alpha^9 & 0 & \alpha^3 \\ 0 & \alpha^3 & 1 \end{bmatrix} \quad \det(\mathrm{M}) = 0$$

$$v = 2 \quad M = \begin{bmatrix} S_1 & S_2 \\ S_2 & S_3 \end{bmatrix} = \begin{bmatrix} \alpha^{12} & \alpha^9 \\ \alpha^9 & 0 \end{bmatrix} \quad \det(\mathrm{M}) \neq 0$$

$$M^{-1} = \begin{bmatrix} 0 & \alpha^6 \\ \alpha^6 & \alpha^9 \end{bmatrix}$$

$$\therefore \begin{bmatrix} \Lambda_2 \\ \Lambda_1 \end{bmatrix} = M^{-1} \bullet \begin{bmatrix} 0 \\ \alpha^3 \end{bmatrix} = \begin{bmatrix} \alpha^9 \\ \alpha^{12} \end{bmatrix}$$

$$\therefore \Lambda(X) = 1 + \alpha^{12}x + \alpha^9 x^2$$

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

$$= \alpha^9 (x - \alpha^8)(x - \alpha^{13})$$

$$\frac{1}{\alpha^8} = \alpha^7$$

$$\frac{1}{\alpha^{13}} = \alpha^2$$

$$\therefore e(X) = X^7 + X^2$$

# Reed-Solomon Code (maximum-distance code)

(1)The symbol field GF(q) and the error-locator field GF($q^m$) are the same

($Y_l$) ($X_l$)

(i.e. m = 1)

(2)Take α as primitive $n = q^m - 1 = q - 1$

(3)The minimal polynomial over GF(q) of an element β in the same GF(q) is $f_\beta(X) = X - \beta$

(4)Take $j_0 = 1$ $g(X) = (X - \alpha)(X - \alpha^2)\ldots(X - \alpha^{2t})$ $\therefore n - k = 2t$

eg1. (15,11) t = 2 GF(16) $j_0 = 1$

$$g(X) = (X - \alpha)(X - \alpha^2)(X - \alpha^3)(X - \alpha^4)$$
$$= X^4 + (Z^3 + Z^2 + 1)X^3 + (Z^3 + Z^2)X^2 + Z^3X + (Z^2 + Z + 1)$$
$$= X^4 + \alpha^{13}X^3 + \alpha^6X^2 + \alpha^3X + \alpha^{10}$$

$n - k = 4 \Rightarrow k = 11$ (11 16-ary symbols ≈ 44 bits)



eg2. (7,3) t = 2 GF(8) $j_0 = 4$

$$g(X) = (X - \alpha^4)(X - \alpha^5)(X - \alpha^6)(X - \alpha^0)$$
$$= X^4 + (Z^2 + 1)X^3 + (Z^2 + 1)X^2 + (Z + 1)X + Z$$

$n - k = 4 \Rightarrow k = 3$ (3 8-ary symbols ≈ 9 bits)

If $i(X) = (Z^2 + Z)X^2 + X + (Z + 1)$

$$c(X) = i(X)g(X) = (\alpha^4X^2 + X + \alpha^3)(X^4 + \alpha^6X^3 + \alpha^6X^2 + \alpha^3X + \alpha)$$
$$= \alpha^4X^6 + \alpha X^5 + \alpha^6X^4 + 0X^3 + 0X^2 + \alpha^5X + \alpha^4$$

※ 1. $n - k + 1 = 2t + 1 \le d^* \le 1 + n - k$

$\therefore d^* = 1 + n - k$

2. R-S codes always have relatively short block-length as compared to other cyclic codes over the same alphabet !