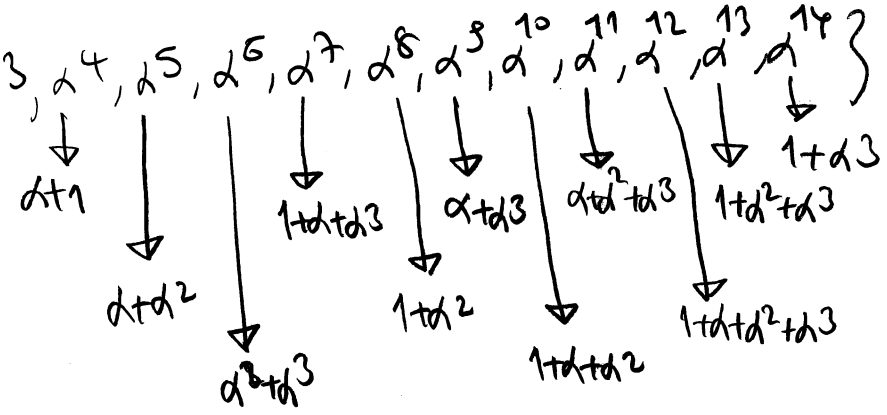
(13)

Note: Polynomials can be represented using binary strings

$p(x) = 1 + x + x^4$ using $p(x)$ we can extend $GF(2)$ to $GF(2^4)$ $\quad \alpha \in GF(2^4)$

$p(\alpha) = 0 \longrightarrow \alpha^4 = \alpha + 1$

$GF(2^4) = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{10}, \alpha^{11}, \alpha^{12}, \alpha^{13}, \alpha^{14}\}$



0	0000
1	0001
α	0010
α^2	0100
α^3	1000
$\alpha+1$	0011
$\alpha^2+\alpha$	0110
$\alpha^3+\alpha^2$	1100
$\alpha^3+\alpha+1$	1011
α^2+1	0101
$\alpha^3+\alpha$	1010
$\alpha^2+\alpha+1$	0111
$\alpha^3+\alpha^2+\alpha$	1110
$\alpha^3+\alpha^2+\alpha+1$	1111
$\alpha^3+\alpha^2+1$	1101
α^3+1	1001

→ binary strings representing polynomials.

Hence $GF(2^4)$ can also be written as

$GF(2^4) = \{0000, 0001, 0010, \ldots\ldots 1001\}$

Bose-Chaudhuri-Hocquenghem Codes (BCH codes) & Reed Solomon Codes

BCH codes: BCH code is a cyclic code

The generator polynomial of a t-error correcting BCH code is given by

$$g(x) = LCM\left(m_1(x), m_2(x), m_3(x), \ldots m_{2t}(x)\right)$$

↓ Least Common Multiple

where $m_i(x)$ is the minimal polynomial of α^i

Since $m_i(x) = m_{2i}(x)$

$g(x)$ can be written as

$$g(x) = LCM\left(m_1(x), m_3(x), m_5(x), \ldots m_{2t-1}(x)\right)$$

- The blocklength of a primitive BCH code constructed over $GF(2^m)$ is $n = 2^m - 1$
- BCH codes are cyclic codes and the degree r of the generator polynomial of an (n,k) cyclic code is $n-k$ and k is $k = 2^m - 1 - r$

i.e., $(n,k) = (2^m - 1, 2^m - 1 - r)$

↓ degree of $g(x)$

↓

$GF(2^m)$

Ex: Find the generator polynomial of a double error correcting BCH code over GF(2^4)

Sln: GF(2^4) → $m=4$, blocklength $n=2^m-1$

$n=2^4-1$

$=15$

$k=2^m-1-r$

$t=2$ → double error correcting

generator polynomial is

$g(x)=LCM(m_1(x), m_3(x) \cdots m_{2t-1}(x))$

↓ $t=2$

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

$m_1(x)$ → minimal polynomial of α

$m_3(x)$ → minimal polynomial of α^3

To find $m_1(x)$ first find conjugates of α in GF(2^4) $\alpha^{15}=1$

Conjugates of α are $\alpha, \alpha^2, \alpha^4, \alpha^8$

Hence $m_1(x)=(x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)$

To find $m_3(x)$, first write conjugates of α^3

Conjugates of α^3 are $\alpha^6, \alpha^{12}, \alpha^9$

Hence $m_3(x)=(x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^9)$

Assume that we used $p(x) = x^4 + x + 1$ primitive polynomial to generate our $GF(2^4)$ α is a root of $p(x)$, i.e, $p(\alpha) = 0 \rightarrow \alpha^4 = \alpha + 1$

Then $m_1(x)$ & $m_3(x)$ can be simplified as

$$m_1(x) = x^4 + x + 1 \quad , \quad m_3(x) = x^4 + x^3 + x^2 + x + 1$$

$$g(x) = Lcm\left(m_1(x), m_3(x)\right)$$

$$g(x) = m_1(x)\, m_3(x)$$

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

$$= x^8 + x^7 + x^6 + x^4 + 1$$

degree of $g(x)$ is $r = 8$

Hence $k = 2^m - 1 - r \rightarrow k = 16 - 1 - 8$

$$k = 7$$

Our BCH code is (16, 7) cyclic code

It is a double error correcting code

and its generator polynomial is

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

Exercise: Using $g(x)$ find generator matrix of (16, 7) double error correcting BCH code.

Ex°: Construct single error correcting BCH code over GF(2⁴).

Sln: GF(2⁴) → m=4 $n=2^m-1$ → n=15

$k=2^m-1-r$ r → degree of g(x)

$g(x)=LCM(m_1(x), m_3(x), \ldots m_{2t-1}(x))$

t=1 → single error correcting code

2t-1=1 $g(x)=LCM(m_1(x))$

$=m_1(x)$

$m_1(x)$ → is the minimal polynomial of α

To find $m_1(x)$ form conjugate class of α

In GF(2⁴) $\alpha^{15}=1$

Conjugate class of α is $\{\alpha, \alpha^2, \alpha^4, \alpha^8\}$

$m_1(x)=(x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)$

Obtain your GF(2⁴) using the primitive polynomial $p(x)=x^4+x+1$ → $p(\alpha)=0$ → $\alpha^4=\alpha+1$

Then $m_1(x)$ is simplified as

$m_1(x)=x^4+x+1$

Then $g(x) = m_1(x)$

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

Degree of $g(x)$ is $r = 4$

Hence $k = 2^m - 1 - r \longrightarrow k = 2^4 - 1 - 4$

$$k = 11$$

Hence our single error correcting BCH code is a $(15, 11)$ cyclic code with generator polynomial $g(x) = x^4 + x + 1$

(n = 15, k = 11)

Exercise: Find generator matrix of BCH(15,11) single error correcting cyclic code.

Exercise: Construct a triple-error correcting BCH code over $GF(2^5)$

Sol^n: $n = 2^m - 1 \longrightarrow n = 2^5 - 1 \longrightarrow n = 31$

$m = 5$

$t = 3 \longrightarrow 2t - 1 = 5$

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

($2t - 1$)

$p(x) = x^5 + x^2 + 1$

Generator polynomial of t-error correcting BCH code is

$$g(x) = LCM\left[m_1(x), m_2(x), \ldots m_{2t-1}(x)\right]$$

$m_1(x)$ → minimal poly of α

i.e, $m_1(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4)\ldots\ldots(x-\alpha^{2^n-1})$

$m_3(x)$ → min. poly. of α^3

$$m_3(x) = (x-\alpha^3)(x-\alpha^6)\ldots(x-\alpha^{3(2^n-1)})$$

and similarly

$$m_{2t-1}(x) = (x-\alpha^{2t-1})(x-\alpha^{(2t-1)\cdot 2})\ldots\ldots$$

It is clear that

For a t-error correcting code

$\alpha, \alpha^2, \alpha^3, \ldots \alpha^{2t}$ are roots of the generator polynomial $g(x)$.

Since BCH is a cyclic code

The codeword polynomial is $c(x) = d(x)\,g(x)$

$d(x)$ → is the data polynomial

Then we can conclude that $c(\alpha^i) = 0 \quad i = 1, \ldots 2t$

Since $c(x) = d(x)g(x)$ and $g(\alpha^i) = 0$

for $i = 1 \ldots 2t$

Now consider a codeword $c(x)$ which incurs an error pattern $e(x)$, so giving

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

Then $r(\alpha^i) = c(\alpha^i) + e(\alpha^i)$

$\downarrow 0$

Error Syndrome for BCH codes

ith error syndrome of $r(x)$ is defined as

$$S_i = r(\alpha^i) \quad \text{where } i = 1, 2, \ldots, 2t$$

The error syndromes $S_1, S_2, \ldots S_{2t}$ are elements of the field $GF(2^m)$ containing α.

Error Syndromes

	Linear	Cyclic	BCH
Codewords	$cH^T = 0$	$R_{g(x)}(c(x)) = 0$	$c(\alpha^i) = 0$
Error Syndromes	$S = rH^T$	$s(x) = R_{g(x)}(r(x))$	$S_i = r(\alpha^i)$

Ex°: Double error correcting BCH(15,7) code $t = 2$

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

Let $d(x) = x + 1$ then

$$c(x) = d(x)\,g(x) \longrightarrow c(x) = (x+1)(x^8 + x^7 + x^6 + x^4 + 1)$$

(127)

$c(x) = x^9 + x^6 + x^5 + x^4 + x + 1$

Assume that we use $p(x) = x^4 + x + 1$ to construct $GF(2^4)$ i.e, $\alpha^4 = \alpha + 1$ let $e(x) = 0$

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

Now lets compute

$r(\alpha^i)$ $i = 1, \ldots 2t$

$$r(\alpha) = \alpha^9 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha + 1$$

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

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

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

$$= 0$$

$$r(\alpha^2) = (\alpha^2)^9 + (\alpha^2)^6 + (\alpha^2)^5 + (\alpha^2)^4 + (\alpha^2) + 1$$

$$= (\alpha^9 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + 1)^2$$

Since we know that

$$(x_1 + x_2 + \ldots x_n)^2 = (x_1^2 + x_2^2 + \ldots x_n^2)$$

So $r(\alpha^2) = (0)^2$

$= 0$

In similar manner $r(\alpha^4) = 0$

It can also be shown that $r(\alpha^3) = 0$

Now assume that the error polynomial is expressed as

$$e(x) = x^{p_1} + x^{p_2} + \cdots x^{p_\nu}$$

where error positions are $p_1, p_2 \cdots p_\nu$.

Ex:

$e = (00101001) \longrightarrow e(x) = x^5 + x^3 + 1$

$p_1 = 5,\ p_2 = 3,\ p_3 = 0$

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

Syndromes are

$$r(\alpha^i) = c(\alpha^i) + e(\alpha^i)$$

$c(\alpha^i) \to 0$

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

$$S_1 = r(\alpha) = e(\alpha) = \alpha^{p_1} + \alpha^{p_2} + \cdots \alpha^{p_\nu}$$

$$S_2 = r(\alpha^2) = e(\alpha^2) = \alpha^{2p_1} + \alpha^{2p_2} + \cdots + \alpha^{2p_\nu}$$

$$S_3 = r(\alpha^3) = e(\alpha^3) = \alpha^{3p_1} + \alpha^{3p_2} + \cdots + \alpha^{3p_\nu}$$

$$\vdots$$

$$S_{2t} = r(\alpha^{2t}) = \alpha^{2tp_1} + \alpha^{2tp_2} + \cdots + \alpha^{2tp_\nu}$$

→ Eqn A

Let $X_i = \alpha^{p_i}$

We can express eqn A in terms of X_i's as

$$S_1 = X_1 + X_2 + \cdots + X_\nu$$
$$S_2 = X_1^2 + X_2^2 + \cdots + X_\nu^2$$
$$S_3 = X_1^3 + X_2^3 + \cdots + X_\nu^3$$
$$\vdots$$
$$S_{2t} = X_1^{2t} + X_2^{2t} + \cdots + X_\nu^{2t}$$

$S_{2i} = S_i^2$

→ we have t equations with ν unknowns, and if $\nu \leq t$ then a unique solution exists.

In other words, if the number of errors falls within the error correction capability of the code, then the error-location numbers can be determined.

One of the most popular methods to solve syndrome equations is called Peterson-Gorenstein-Zierler decoder which will be covered soon.

Decoding BCH codes:

Consider single error correcting BCH code over $GF(2^3)$

Let $p(x)$ be used to construct $GF(2^3)$

and $p(x) = x^3 + x + 1$

$g(x) = LCM[m_1(x), \cdots m_{2t-1}(x)]$ $t=1$

$g(x) = m_1(x) \longrightarrow g(x) = x^3 + x + 1$

(138)

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

$n = 2^m - 1 \longrightarrow n = 2^3 - 1 \longrightarrow n = 7$

$(n, k) \rightarrow$ BCH code $\longrightarrow (7, 4) \rightarrow$ code

BCH (7,4) code $\quad g(x) = x^3 + x + 1$

Let $d(x) = x^2 + 1$ then $c(x) = d(x)\, g(x)$

$\Rightarrow c(x) = (x^2+1)(x^3+x+1)$

$= x^5 + x^2 + x + 1$

$c(x) = x^5 + x^2 + x + 1$

Let the error polynomial be $e(x) = x^5$

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

$r(x) = x^2 + x + 1$

Error syndromes

$S_1 = r(\alpha) \longrightarrow S_1 = \alpha^2 + \underbrace{\alpha + 1}_{\alpha^3}$

Since $\alpha^3 = \alpha + 1$

$S_1 = \alpha^2 + \alpha^3$

$= \alpha^2 (\underbrace{1 + \alpha}_{\alpha^3})$

$S_1 = \alpha^5$

$S_1 = \alpha^5 \rightarrow S_1 = X_1 \quad X_1 = \alpha^5 \rightarrow e(x) = x^5$ is the decoder's estimate the error pattern. The resulting codeword is $c(x) = r(x) + e(x) \rightarrow c(x) = x^5 + x^2 + x + 1$

Ex: Consider double-error correcting BCH codes.

Assume $t = 2$, i.e., assume the occurrence of the maximum number of correctable errors.

Syndrome equations becomes of

$$S_1 = X_1 + X_2$$
$$S_2 = X_1^2 + X_2^2$$
$$S_3 = X_1^3 + X_2^3$$
$$S_4 = X_1^4 + X_2^4$$

$$e(x) = x^{p_1} + x^{p_2}$$

$$X_i = \alpha^{p_i}$$

→ from the set it is obvious that $S_2 = S_1^2$ & $S_4 = S_2^2$

Hence reduce the set to

$$S_1 = X_1 + X_2$$
$$S_3 = X_1^3 + X_2^3$$

→ solve this one

$S_1 = X_1 + X_2$ → take cube of both sides

$$S_1^3 = (X_1 + X_2)^3 \Rightarrow$$

$$S_1^3 = (X_1 + X_2)^2 (X_1 + X_2) \Rightarrow$$

$$S_1^3 = (X_1^2 + X_2^2)(X_1 + X_2) \Rightarrow$$

$$S_1^3 = X_1^3 + X_1 X_2^2 + X_2 X_1^2 + X_2^3$$

$$= \underbrace{X_1^3 + X_2^3}_{S_3} + X_1 X_2 \underbrace{(X_1 + X_2)}_{S_1} \Rightarrow$$

$$\Rightarrow S_1^3 = S_3 + S_1 X_1 X_2 \longrightarrow X_2 = S_1 + X_1$$

$$S_1^3 = S_3 + S_1 X_1 X_2$$

$$\downarrow X_2 = S_1 + X_1$$

$$S_1^3 = S_3 + S_1 X_1 (S_1 + X_1)$$

$$\Rightarrow X_1^2 + S_1 X_1 + \frac{S_1^3 + S_3}{S_1} = 0$$

write the above equation as

$$X^2 + S_1 X + \frac{S_1^3 + S_3}{S_1} = 0$$

roots are X_1 & X_2

Ex: BCH(15,7) code $p(x) = x^4 + x + 1$

$\alpha^4 = \alpha + 1$ $\quad g(x) = LCM(m_1(x), m_3(x))$

$= x^8 + x^7 + x^6 + x^4 + 1$

Let ~~$c(x)$~~ $= d(x) g(x)$

be $c(x) = x^{11} + x^8 + x^7 + x^6 + x^3 + x^2$

& $e(x) = x^{10} + x^2$

$r(x) = c(x) + e(x) \rightarrow r(x) = x^{11} + x^{10} + x^8 + x^7 + x^6 + x^3$

The syndrome table is

$S_1 = r(\alpha) \rightarrow S_1 = \alpha^{11} + \alpha^{10} + \alpha^8 + \alpha^7 + \alpha^6 + \alpha^3 = \alpha^4$

$S_3 = r(\alpha^3) \rightarrow S_3 = \alpha^3 + 1 + \alpha^3 + \alpha^6 + \alpha^3 + \alpha^9 = \alpha^{13}$

(133)

$S_1 = \alpha^4$ and $S_1 = X_1 + X_2$

$S_3 = \alpha^{13}$ $\quad S_2 = X_1^2 + X_2^2$

$$\left.\begin{aligned} X_1 + X_2 &= \alpha^4 \\ X_1^2 + X_2^2 &= \alpha^{13} \end{aligned}\right\} \qquad \underline{\alpha^4 = \alpha + 1}$$

can be solved as outlined before

Or we can use $x^2 + S_1 x + \dfrac{S_1^3 + S_3}{S_1} = 0$

directly then $x^2 + \alpha^4 x + \dfrac{\alpha^{12} + \alpha^{13}}{\alpha^4} = 0$

↓ how to simplify

$\alpha^{12} + \alpha^{13} = \alpha^{12}(\underbrace{1+\alpha}_{\alpha^4})$

$= \alpha^{16}$ $\qquad \alpha^{15} = 1$

Then $\dfrac{\alpha^{16}}{\alpha^4} = \alpha^{16-4}$

$= \alpha^{12}$

$x^2 + \alpha^4 x + \alpha^{12} = 0$

To find the roots of $x^2 + \alpha^4 x + \alpha^{12} = 0$

try all the field elements $\alpha, \alpha^2, \alpha^3, \ldots \alpha^{14}$

and determine the roots.

(34)

Let $p(x) = x^2 + \alpha^4 x + \alpha^{12}$ $\quad \alpha^4 = \alpha + 1$

$p(1) = 1 + \alpha^4 + \alpha^{12} \rightarrow p(1) = \alpha^{13}$

$p(\alpha) = \alpha^2 + \alpha^5 + \alpha^{12} \longrightarrow p(\alpha) = \alpha^{13}$

$p(\alpha^2) = \alpha^4 + \alpha^6 + \alpha^{12}$

$= (\alpha+1) + \alpha^2(\alpha+1) + \alpha^8 \alpha^4$

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

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

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

$= 0$

Hence one root is found at α^2 the other root can be found at α^{10} i.e, $p(\alpha^{10}) = 0$

Then $X_1 = \alpha^2$ $\quad X_2 = \alpha^{10}$

we know that $X_i = \alpha^{p_i}$ and $e(x) = x^{p_1} + \ldots + x^{p_2}$

then $p_1 = 2$ $\quad p_2 = 10$

error pattern is $e(x) = x^2 + x^{10}$

Decoded codeword is

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

$\downarrow x^2 + x^{10}$

Exercise:

For BCH(15,7) code

2 error and 1 error incurred codewords are

a) $r_1(x) = x^{11} + x^9 + x^8 + x^6 + x^5 + x + 1$

b) $r_2(x) = x^{12} + x^{11} + x^{10} + x^9 + x^7 + x^5 + x$

Decode $r_1(x)$ & $r_2(x)$ using syndrome approach

Exercise:

For BCH(15,7) code

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

If a) $e(x) = x^{11} + x^9 + x^6 + x^4$

b) $e(x) = x^7 + x^2 + 1$

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

Decode $r(x)$ using syndrome approach.

The error-location Polynomials

While studying double error correcting BCH code we obtained the following equation from syndrome equations

$$x^2 + S_1 x + \frac{S_1^3 + S_3}{S_1} = 0$$

Let $\sigma_1 = S_1$ & $\sigma_2 = \dfrac{(S_1^3 + S_3)}{S_1}$

then $x^2 + \sigma_1 x + \sigma_2 = 0$

↓ for double error correcting BCH code

For a t-error correcting code we need to consider polynomials of the form

$$x^\nu + \sigma_1 x^{\nu-1} + \dots + \sigma_{\nu-1} x + \sigma_\nu = 0$$

where $\nu \le t$

replace x by $\frac{1}{x}$ we get

$$\sigma_0 + \sigma_1 x + \sigma_2 x^2 + \dots + \sigma_{\nu-1} x^{\nu-1} + \sigma_\nu x^\nu = 0$$

where $\sigma_0 = 1$

Now define the error location polynomial

$$\sigma(x) = \sigma_0 + \sigma_1 x + \dots \sigma_{\nu-1} x^{\nu-1} + \sigma_\nu x^\nu$$

which is a polynomial whose roots are the reciprocal of the error-location numbers.

Ex^{n} BCH(15, 7) code → double error correcting

$r(x) = x^3 + x^8 + x^5 + x^4 + 1$ → includes 2-errors

$S_1 = r(\alpha) \rightarrow S_1 = 1$ $\quad S_3 = r(\alpha^3) \rightarrow S_3 = \alpha^4$

$\sigma_1 = S_1 \rightarrow \sigma_1 = 1$ $\quad \sigma_2 = \dfrac{S_1^3 + S_3}{S_1} \rightarrow \sigma_2 = \alpha$

The error location polynomial is

$$\sigma(x) = 1 + \sigma_1 x + \sigma_2 x^2$$
$$= 1 + x + \alpha x^2$$

roots of $\sigma(x)$ can be determined using a trial approach of α^6 & α^8 over GF(24).

The error location numbers are

$$X_1 = 1/\alpha^6 \longrightarrow X_1 = \alpha^9$$
$$X_2 = 1/\alpha^8 \longrightarrow X_2 = \alpha^7$$

which give the error polynomial $e(x) = x^9 + x^7$

and codeword polynomial

$$c(x) = r(x) + e(x) \longrightarrow c(x) = x^8 + x^7 + x^6 + x^4 + 1$$

- If the roots of the error-location polynomial are the field elements $\beta_1, \beta_2, \ldots, \beta_t$ then the error location numbers are

$$X_1 = 1/\beta_1 \quad X_2 = 1/\beta_2 \quad \ldots \quad X_t = \frac{1}{\beta_t}$$

and the error location polynomial can be expressed as $\sigma(x) = (xX_1 + 1)(xX_2 + 1) \ldots (xX_t + 1)$

expanding it and comparing it to

$$\sigma(x) = \sigma_0 + \sigma_1 x + \sigma_2 x^2 + \ldots + \sigma_{t-1} x^{t-1} + \sigma_t x^t$$

we find that

$$\sigma_0 = 1$$

$$\sigma_1 = X_1 + X_2 + X_3 + \cdots + X_{\nu-1} + X_\nu$$

$$\sigma_2 = X_1X_2 + X_2X_3 + X_3X_4 + \cdots + X_{\nu-1}X_\nu$$

$$\vdots$$

$$\sigma_\nu = X_1X_2X_3\cdots X_{\nu-1}X_\nu$$

and remember that we have syndrome equations

i.e,

$$S_1 = X_1 + X_2 + \cdots X_\nu$$

$$S_2 = X_1^2 + X_2^2 + \cdots X_\nu^2$$

$$\vdots$$

$$S_{2t} = X_1^{2t} + X_2^{2t} + \cdots X_\nu^{2t}$$

From these two sets of equations we can find that

$$S_1 = \sigma_1 \rightarrow 0$$

$$S_2 = \sigma_1 S_1 + 2\sigma_2 \rightarrow 1$$

(E1)
$$S_3 = \sigma_1 S_2 + \sigma_2 S_1 + 3\sigma_3$$

$$\vdots$$

$$S_\nu = \sigma_1 S_{\nu-1} + \sigma_2 S_{\nu-2} + \cdots \sigma_{\nu-1} S_1 + \nu\sigma_\nu$$

The remaining syndromes are

$$S_{\nu+1} = \sigma_1 S_\nu + \sigma_2 S_{\nu-1} + \cdots \sigma_{\nu-1} S_2 + \sigma_\nu S_1$$

$$S_{\nu+2} = \sigma_1 S_{\nu+1} + \sigma_2 S_\nu + \cdots + \sigma_{\nu-1} S_3 + \sigma_\nu S_2$$

(E2)
$$\vdots$$

$$S_{2\nu} = \sigma_1 S_{2\nu-1} + \sigma_2 S_{2\nu-2} + \cdots + \sigma_{\nu-1} S_{\nu+1} + \sigma_\nu S_\nu$$

Equation sets E1 & E2 are called Newton's identities, from which the coefficients of $\sigma(x)$ can be determined.

The eqn sets E1 & E2 can also be expressed in matrix form as

$$\begin{bmatrix} S_1 \\ S_2 \\ \vdots \\ S_\nu \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ S_1 & 2 & 0 & \cdots & 0 & 0 \\ S_2 & S_1 & 3 & \cdots & 0 & 0 \\ \vdots & & & & & \\ S_{\nu-1} & S_{\nu-2} & \cdots & \cdots & S_1 & \nu \end{bmatrix} \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_\nu \end{bmatrix} \quad (E1)$$

and

$$\begin{bmatrix} S_{\nu+1} \\ S_{\nu+2} \\ \vdots \\ S_{2\nu} \end{bmatrix} = \begin{bmatrix} S_\nu & S_{\nu-1} & S_{\nu-2} & \cdots & S_2 & S_1 \\ S_{\nu+1} & S_\nu & S_{\nu-1} & \cdots & S_3 & S_2 \\ \vdots & & & & & \\ S_{2\nu-1} & S_{2\nu-2} & \cdots & \cdots & S_{\nu+1} & S_\nu \end{bmatrix} \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_\nu \end{bmatrix} \quad (E2)$$

For binary case since $S_{2i} = S_i^2$

E1 & E2 can be combined as

$$\begin{bmatrix} S_1 \\ S_3 \\ \vdots \\ S_{2\nu-1} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ S_2 & S_1 & 1 & \cdots & 0 & 0 \\ S_4 & S_3 & S_2 & \cdots & 0 & 0 \\ \vdots & & & & & \\ S_{2\nu-2} & S_{2\nu-3} & \cdots & & S_\nu & S_{\nu-1} \end{bmatrix} \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_\nu \end{bmatrix} \quad (E3)$$

Ex: For triple error correcting BCH code obtain error location polynomial in terms of syndromes

Sol^n:

$$\sigma(x) = 1 + \sigma_1 x + \sigma_2 x^2 + \sigma_3 x^3 \qquad t = 3$$

Using eqn (E3)

$$\begin{bmatrix} S_1 \\ S_3 \\ S_5 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ S_2 & S_1 & 1 \\ S_4 & S_3 & S_2 \end{bmatrix} \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \sigma_3 \end{bmatrix}$$

$2t-1$

$t=3$

$$\Rightarrow S_1 = \sigma_1 \qquad S_3 = S_2\sigma_1 + S_1\sigma_2 + \sigma_3 \qquad S_5 = S_4\sigma_1 + S_3\sigma_2 + S_2\sigma_3$$

$$S_2S_3 + S_5 = (S_2^2 + S_4)\sigma_1 + (S_2S_1 + S_3)\sigma_2 + (S_2 + S_2)\sigma_3$$

$S_2^2 = S_1^4$, $S_4 = S_1^4$, $S_2 + S_2 = 0$, $S_2S_1 = S_1^2$

$$S_2S_3 + S_5 = (S_1^3 + S_3)\sigma_2 \rightarrow \sigma_2 = \frac{S_2S_3 + S_5}{S_1^3 + S_3}$$

The other terms in $\sigma(x)$ are found as

$$\sigma_3 = (S_3 + S_1^3) + \frac{S_1(S_2S_3 + S_5)}{S_1^3 + S_3} \qquad \sigma_1 = S_1$$

Hence

$$\sigma_1 = S_1$$

$$\sigma_2 = \frac{S_2 S_3 + S_5}{S_1^3 + S_3}$$

$$\sigma_3 = (S_3 + S_1^3) + \frac{(S_1)(S_2 S_3 + S_5)}{S_1^3 + S_3}$$

Exercise: For triple-error correcting BCH code if $S_1 = \alpha^3$, $S_3 = \alpha^8$ and $S_5 = 1$ over GF(24) $p(x) = x^4 + x + 1$, determine the error location polynomial $\sigma(x)$.

Exercise: For double error correcting BCH code find error location polynomial in terms of syndromes.

The Peterson-Gorenstein Zierler Decoder:

The equation (E2) can also be written as

$$\begin{bmatrix} S_{\nu+1} \\ S_{\nu+2} \\ \vdots \\ S_{2\nu} \end{bmatrix} = \begin{bmatrix} S_1 & S_2 & S_3 & \cdots & S_{\nu-2} & S_\nu \\ S_2 & S_3 & S_4 & \cdots & S_\nu & S_{\nu+1} \\ \vdots & & & & & \\ S_\nu & S_{\nu+1} & S_{\nu+2} & \cdots & S_{2\nu-2} & S_{2\nu-1} \end{bmatrix} \begin{bmatrix} \sigma_\nu \\ \sigma_{\nu-1} \\ \vdots \\ \sigma_1 \end{bmatrix}$$

The previous equation can be written in matrix form of

$$S = M\sigma$$

Assuming that M is non-singular

$$\sigma = M^{-1}S$$

Let $M = \begin{bmatrix} S_1 & S_2 & \cdots & S_i \\ S_2 & S_3 & \cdots & S_{i+1} \\ \vdots & & & \\ S_i & S_{i+1} & \cdots & S_{2i-1} \end{bmatrix}$

M is non-singular if $i = t$, but singular if $i > t$

For example consider a code that can correct 5 errors but only 3 errors actually occur, so $t=5$ and $\tau=3$ Taking $i=5$ and constructing

$$M = \begin{bmatrix} S_1 & S_2 & S_3 & S_4 & S_5 \\ S_2 & S_3 & S_4 & S_5 & S_6 \\ S_3 & S_4 & S_5 & S_6 & S_7 \\ S_4 & S_5 & S_6 & S_7 & S_8 \\ S_5 & S_6 & S_7 & S_8 & S_9 \end{bmatrix}$$

$\det(M) = 0$, so M is singular

Peterson-Gorenstein Zierler Decoders

1) Calculate the error syndromes $S_1, S_2, \ldots S_{2t}$ from $r(x)$

2) Assume the maximum number of errors $i = t$

3) Construct the matrix M

4) Compute $\det(M)$, if $\det(M) = 0$ reduce i by 1 and go to step-3, otherwise continue to step-5

5) Determine M^{-1} and construct S

6) Find the polynomial coefficients using $\sigma = M^{-1} S$ and construct $\sigma(x)$ from σ

7) Determine the roots of $\sigma(x)$ and take the reciprocals. The error location numbers are given by the reciprocal roots.

Example: BCH(15,5) triple error correcting code

$$r(x) = x^8 + x^5 + x^2 + x + 1$$

Decode $r(x)$ using PGZ decoding technique

$p(x) = x^4 + x + 1$ primitive polynomial is used to construct $GF(2^4)$

144

Sln°3

$r(x) = x^8 + x^5 + x^2 + x + 1$ $\qquad \alpha^4 = \alpha + 1$

Step 1 Compute the syndromes of

$$S_1 = r(\alpha) = \alpha^8 + \alpha^5 + \alpha^2 + \alpha + 1$$

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

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

$$= \alpha^2$$

$$S_2 = r(\alpha^2) = S_1^2 \longrightarrow S_2 = \alpha^4$$

$$S_3 = r(\alpha^3) = \alpha^{24} + \alpha^{15} + \alpha^6 + \alpha^3 + 1 \qquad \alpha^{15} = 1$$

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

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

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

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

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

$$= \alpha^3 + \alpha\alpha^4$$

$$= \alpha^3 + \alpha^5$$

$$= \alpha^3(1+\alpha^2) \quad (1+\alpha^2 = \alpha^8)$$

$$= \alpha^{11}$$

$$S_4 = S_2^2 = \alpha^8 \qquad S_5 = 0 \qquad S_6 = S_3^2 = \alpha^7$$

Step 2 Assume that the maximum number of errors occured i.e, $i=3$

Step 3 The maximum M is

$$M=\begin{bmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{bmatrix}=\begin{bmatrix} \alpha^2 & \alpha^4 & \alpha^{11} \\ \alpha^4 & \alpha^{11} & \alpha^8 \\ \alpha^{11} & \alpha^8 & 0 \end{bmatrix}$$

Step 4 The determinant of M is

$$\det(M)=\alpha^2\begin{vmatrix} \alpha^{11} & \alpha^8 \\ \alpha^8 & 0 \end{vmatrix}+\alpha^4\begin{vmatrix} \alpha^4 & \alpha^8 \\ \alpha^{11} & 0 \end{vmatrix}+\alpha^{11}\begin{vmatrix} \alpha^4 & \alpha^{11} \\ \alpha^{11} & \alpha^8 \end{vmatrix}$$

$$=\alpha^2\alpha+\alpha^4\alpha^4+\alpha^{11}\alpha^2$$

$$=\alpha^3+\alpha^8+\alpha^{13}$$

$$=0$$

The matrix M is singular, so i is reduced by 1 to give $i=2$ and steps 3&4 are repeated.

Step-3 repeated $M=\begin{bmatrix} S_1 & S_2 \\ S_2 & S_3 \end{bmatrix}=\begin{bmatrix} \alpha^2 & \alpha^4 \\ \alpha^4 & \alpha^{11} \end{bmatrix}$

Step-4 repeated $\det(M)=\begin{vmatrix} \alpha^2 & \alpha^4 \\ \alpha^4 & \alpha^{11} \end{vmatrix}=\alpha^{13}+\alpha^8=\alpha^3$

M is non-singular

Step 5 $M^{-1} = adj(M) / det(M)$

$$adj(M) = \begin{bmatrix} \alpha^{11} & \alpha^{4} \\ \alpha^{4} & \alpha^{2} \end{bmatrix}$$

remarks $adj(M_{ij})$ → remove i-row j-column
compute determinant
multiply the result by $(-1)^{i+j}$

$adj(M_{12}) = \alpha^{11}$ for our case

$$M^{-1} = \frac{adj(M)}{det(M)} = \frac{\begin{bmatrix} \alpha^{11} & \alpha^{4} \\ \alpha^{4} & \alpha^{2} \end{bmatrix}}{\alpha^{3}}$$

$$= \begin{bmatrix} \alpha^{8} & \alpha \\ \alpha & \alpha^{14} \end{bmatrix} \qquad S = \begin{bmatrix} S_3 \\ S_4 \end{bmatrix} = \begin{bmatrix} \alpha^{11} \\ \alpha^{8} \end{bmatrix}$$

Step 6

$$\sigma = M^{-1} S$$

$$\begin{bmatrix} \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} \alpha^{8} & \alpha \\ \alpha & \alpha^{14} \end{bmatrix} \begin{bmatrix} \alpha^{11} \\ \alpha^{8} \end{bmatrix} = \begin{bmatrix} \alpha^{14} \\ \alpha^{2} \end{bmatrix}$$

So $\sigma_2 = \alpha^{14}$, $\sigma_1 = \alpha^{2}$ and the error location polynomial is therefore

147

$$\sigma(x) = 1 + \sigma_1 x + \sigma_2 x^2$$

$$= 1 + \alpha^2 x + \alpha^{14} x^2$$

Step 7 The roots of $\sigma(x)$ are found as α^5 and α^{11} by trial

the reciprocal of these roots are $\frac{1}{\alpha^5} = \alpha^{10}$

$\frac{1}{\alpha^{11}} = \alpha^4$ So the error pattern is

$x^{10} + x^4$ and so the required

codeword polynomial is

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

$$= x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$$

Ex: BCH(15,5) code is given

A codeword incurs errors so as to give

$$r(x) = x^{13} + x^{10} + x^8 + x^4 + x + 1$$

Find the number of errors that $c(x)$ (codeword) has incurred, find error pattern and decode $r(x)$ using PGZ algorithm

Remark primitive polynomial is

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