

Cyclic Codes

$$\begin{smallmatrix} 5 & 4 & 3 & 2 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 \end{smallmatrix} \rightarrow x^5 + x^3 + x^2 + x$$

cyclic operation on valid codeword gives valid codeword.

$$e(x) = i(x) \cdot g(x)$$

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

$$\text{for decoding } R \frac{g(x)}{c(x)} = 0$$

↓
Residual.

$$c(x) \div g(x) \Rightarrow \text{remainder} = 0 \Rightarrow \text{valid codeword}$$

$$\text{syndrome } s(x) = R g(x) e(x).$$

$g(x)$: For (n, k) binary cyclic code, the generator polynomial has the form

$$g(x) = g_{n-k} x^{n-k} + g_{n-k-1} x^{n-k-1} + \dots + g_1 x + g_0.$$

where the co-efficients

$$g_{n-k} = g_p = 1$$

but are 0 or 1

$g_p(x)$ is an unique polynomial from which all the codeword polynomial can be generated.

Theorem: 1.

The non zero code polynomial of min \geq degree in a cyclic code C is unique

code: (n, k)

$$c(x) = c_{n-1} x^{n-1} + c_{n-2} x^{n-2} + \dots + c_1(x) + c_0$$

$$i(x) = i_{k-1} x^{k-1} + \dots + i_1(x) + i_0$$

Let there exists a

$$g(x) = g_{n-k} x^{n-k} + \dots + g_1 x + g_0 \quad \text{--- (1)}$$

a generator polynomial with min degree $= n-k$.

Proof using contradiction.

$$g'(x) = g_{n-k} x^{n-k} + \dots + g_1 x + g_0 \quad \text{--- (2)}$$

let there is another polynomial g' with min degree $n-k$.

$$\text{also } g_{n-k} = g'^{n-k} = 1$$

$$\begin{aligned} g(x) + g'(x) &= (1 \oplus 1) x^{n-k} + \dots + (g \oplus g') \\ \text{modulo 2:} \\ &= (g_{n-k-1} + g'^{n-k-1}) x^{n-k-1} + \dots \end{aligned}$$

another polynomial with degree $n-k-1$.
but we assume that $n-k$ is minimum
degree. Therefore it contradict the assumption
and we cannot have g' .

g is unique.

Cyclic operation: $c_{n-1} c_{n-2} c_{n-3} \dots c_2 c_1 c_0$
 $\Rightarrow c_{n-2} c_{n-3} \dots c_1 c_0 c_{n-1}$ (all left/right
rotation are valid.)

$$\text{Code } (6,4) = x^5 + x^3 + x^2 + 1 = c(x)$$

$$= 101101 \xrightarrow{\text{left rotation}} 01101$$

$$R_{x^{n+1}}(x c(x)) = x^6 + x^4 + x^3 + x^2$$

$$= 1011010 \rightarrow \text{new code length } 7.$$

$$\begin{array}{r} x^6 + 1 \\ \overline{x^6 + 1} \\ \hline x^4 + x^2 + x + 1 \\ \downarrow \\ (011011) \text{ - 6 length.} \end{array}$$

\therefore function $R_{x^{n+1}}(x c(x))$ = left shift operation.
 (multiply by x and divide by x^{n+1} , n = original code length.)

Theorem: 2

$$\text{Def: } g(x) = x^r + g_{r-1}x^{r-1} + \dots + g_1x + g_0.$$

$$\Rightarrow g_0 = 1.$$

Proof: Let $g_0 = 0$. using contradiction.

$$\begin{aligned} g(x) &= x^r + g_{r-1}x^{r-1} + \dots + g_1x + g_0 \\ &= x(r + g_{r-1}x^{r-2} + \dots + g_1). \\ &= x(g'(x)) \end{aligned}$$

Left shift operation. $\therefore g'(x)$ will be a valid code word with degree $r-1$.

\therefore degree $g'(x) <$ original $g(x)$ degree
 \therefore contradiction.

Theorem: 3.

Def: $g(x) = 1 + g_1x + \dots + g_{r-1}x^{r-1}$
 be the non-zero code polynomial of min degree in a (n,k) cyclic code C . A binary polynomial of degree $(n-1)$ or less is a code polynomial iff it is a multiple of $g(x)$.

Proof: There exist a valid code word $v(x)$ not perfectly divisible by $g(x)$

$$v(x) = \underbrace{a(x)g(x)}_{\substack{\text{valid} \\ \text{code word}}} + r(x), \quad r(x) \neq 0$$

$$\begin{aligned} r(x) &= a(x) + v(x) \\ r(x) &= c_2(x) \end{aligned}$$

thus addition of 2 valid code word is also valid.
 $r(x)$ is valid.

also $\deg(r(x)) < \deg(g(x))$
 (as per division rule.)

$r(x)$ is another valid $v(x)$ at per assumption.

But then, $\deg(v(x)) < \deg(g(x))$

but $g(x)$ is minimum degree polynomial.

True contradiction.

$\rightarrow g(x)$ is a factor of $x^n + 1$

$R_{x^n+1} \ x^n \ g(x) = \text{valid codeword}$

$$\therefore x^n g(x) = 1 \cdot (x^n + 1) + g'_n(x)$$

$$\therefore x^n + 1 = x^n \cdot g(x) + g'_n(x)$$

Residue = cyclic code

$$x^n + 1 = (x^n + a(x)) \cdot g(x).$$

$$g'_n(x) = a(x) \cdot g(x)$$

Theorem 3.

$g(x)$ is a factor of $x^n + 1$

(7,4) cyclic code:

$$n=7 \quad x^7 + 1 = (x+1) (x^6 + x^5 + 2x^4 + x^3 + x^2 + x + 1)$$

↓
modulo 2 division
 $1+1=0$

further factorize

$$\begin{aligned} & \rightarrow \deg(1) \times \deg(5) \rightarrow x+1 \text{ is not a factor} \\ & \quad (\deg(1 \times 5) \text{ not prime}) \\ & \deg(2) \times \deg(4) \\ & \deg(3) \times \deg(3) \end{aligned}$$

$$\therefore x^6 + x^5 + \dots + x + 1 = (a_1 x^2 + a_2 x + a_3) (b_1 x^4 + b_2 x^3 + b_3 x^2 + b_4 x + b_5)$$

↓
this does not have a solution for this equation

$$\therefore x^6 + x^5 + \dots + x + 1 = (a_1 x^3 + a_2 x^2 + a_3 x + a_4) (b_1 x^3 + b_2 x^2 + b_3 x + b_4)$$

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

$$\therefore x^7 + 1 = (x+1) \underbrace{(x^3 + x + 1)(x^3 + x^2 + 1)}_{\text{this cannot be further factored...}}$$

$$g(x) = x^{n-k} + g_{n-k-1} x^{n-k-1} + \dots + g_1 x + 1$$

$n=7, k=4$

$$\therefore g(x) = (x^3 + \dots)$$

$g(x)$ is one of root of $x^7 + 1$

$\therefore g(x) = x^3 + x + 1 \text{ or } x^3 + x^2 + 1$ will be generator polynomial of $(7,4)$

for $(7,3)$

$$g(x) = (x+1)(x^3 + x + 1) \text{ or } (x+1)(x^3 + x^2 + 1)$$

↳ possible generator polynomial with degree 4. ($n-k = 7-3 = 4$)

Example:

$$x^{15} + 1 = (x+1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)$$

1) find number of cyclic codes with $(15,11)$.

$$\text{Ans: } n=15 \quad n-k=4.$$

$$k=11$$

$\therefore g(x)$ with degree 4.

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

3 cyclic codes possible.

2) find $g(x)$ of $(15,7)$

$$n-k=8$$

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

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

$$\text{or } (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1).$$

End

Encoding of Cyclic codes:

$$c(x) = i(x) \cdot g(x)$$

example: for (7,4) let $g(x) = x^3 + x + 1$

$$\text{and if } i(x) = \frac{1010}{x^3+x}$$

$$\begin{aligned} c(x) &= (x^3+1)(x^3+x+1) \\ &= x^6 + x^2 + \cancel{x^4} + x^3 + x \quad (\bmod 2) \\ &= x^6 + x^3 + x^2 + x \end{aligned}$$

$$1010 \longrightarrow = 1001110$$

code words are not in systematic form.
(cannot separate info and parity)

Systematic codeword:

$$(7,4) \rightarrow 1010 \underset{\substack{\times x \\ \text{fill the parity.}}}{\underset{x}{\underset{x}{\underset{x}{\underset{x}{\underset{x}{\underset{x}{\underset{x}{\underset{x}{}}} }}}}}}$$

To do this shifting.

$$= x^{n-k} \cdot i(x)$$

$$x^4 \cdot (x^3+x) = x^3 \cdot (x^3+x) = x^6 + x^4 = 1010 \underset{\substack{\text{parity.} \\ \text{unknown.}}}{\underset{000}{\underset{0}{\underset{0}{\underset{0}{\underset{0}{\underset{0}{\underset{0}{}}}}}}}}$$

Now this polynomial is not divisible by $g(x)$

but cyclic code should be.

$$\therefore v(x) = a(x) \cdot g(x) + r(x)$$

$$\begin{array}{r} x^3+x+1 \\ \overline{x^6+x^4} \\ x^6+x^4+x^3 \\ \hline x^3+x+1 \\ \hline x+1 \end{array}$$

$$\begin{aligned} \text{Now, } a(x) \cdot g(x) &= v(x) + r(x), \\ &\downarrow \\ c(x) &= (x^6+x^4) + (x+1) \end{aligned}$$

$$\begin{matrix} 1010 & 011 \\ & \text{parity.} \end{matrix}$$

$$\begin{array}{ccc} \text{thus.} & 1010 & 011 \\ & \downarrow & \\ & \text{code word in systematic form.} & \end{array}$$

Algorithm: Encoding of Cyclic Codes:

I/P : $i(x)$

$$\text{Step 1 : } x^{n-k} \cdot i(x)$$

$$\text{Step 2 : } r(x) = Rg(x) \quad (x^{n-k} \cdot i(x))$$

$$\text{Step 3 : } c(x) = x^{n-k} \cdot i(x) + r(x)$$

Decoding of Cyclic Codes:

$$\text{find, } s(x) = Rg(x) \quad v(x) \quad \text{syndrome polynomial.}$$

If $s(x) = 0$ valid code word.

$$\text{If } s(x) \neq 0 \quad v(x) = c(x) + e(x)$$

$v(x) = \text{received code word}$

$$e(x) = \text{error polynomial}$$

$$s(x) = Rg(x) \quad v(x)$$

$$e(x) = Rg(x) \cdot c(x) + Rg(x) \cdot e(x)$$

$$\therefore s(x) = Rg(x) \cdot e(x)$$

{module 2
+,- same
Galois field.}

Linear

Cyclic

(9)

$$1) C = i \cdot Gc$$

$$1) C(x) = i(x) \cdot g(x)$$

$$2) GcH^T = 0$$

$$2) g(x) \cdot h(x) = x^n + 1$$

• $h(x)$ = parity check polynomial.

$$3) R_{x^n+1} v(x) h(x) = 0$$

$$\Rightarrow v(x) = \text{valid}$$

Proof:

$$\begin{aligned} v(x) \cdot h(x) &= i(x) g(x) h(x) \\ &= i(x) (x^n + 1) \\ \therefore R_{x^n+1} v(x) h(x) &= 0 \end{aligned}$$

$$1) R_{g(x)} v(x) = 0$$

- Linear codes are subset of block codes.
- Cyclic codes are subset of linear code.

Generator matrix when $g(x)$ is known:

$$g(x) = g_r x^r + g_{r-1} x^{r-1} \dots + g_1 x + g_0$$

$$Gc = \left[\begin{array}{cccccc|cc} g_r & g_{r-1} & g_{r-2} & \dots & g_1 & g_0 & 0 & 0 \\ 0 & g_r & g_{r-1} & \dots & g_1 & g_0 & 0 & 0 \\ 0 & 0 & \ddots & & & & & \\ \vdots & & & & & & & \\ 0 & 0 & 0 & \dots & & & & \end{array} \right]$$

$\underbrace{\quad}_{k \times n}$

$\underbrace{\quad}_{R-1 \text{ zeros.}}$

Example: (7,4) $g(x) = x^3 + x + 1 = 1011$

$$Gc = \left[\begin{array}{cccc|ccc} 1 & 0 & 1 & 01 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array} \right] \xrightarrow{(4, x^7)} k \times n$$

$$\begin{aligned} h(x) &= \frac{x^7+1}{g(x)} = \frac{x^7+1}{x^3+x+1} \\ &= x^4 + x^2 + x + 1 \\ &= h_4 x^4 + h_3 x^3 + h_2 x^2 + h_1 x + h_0 \\ &\quad h_4 \ h_3 \ h_2 \ h_1 \ h_0 \\ \therefore & \quad 1 \ 0 \ 1 \ 1 \ 1 \end{aligned}$$

$x^3+x+1 \mid x^7+1 \mid (x^4+x^2+x+1)$

$x^2+x^5+x^4+1$

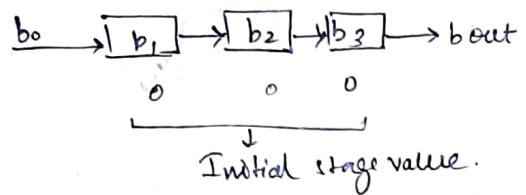
$x^6+x^5+x^2$

$\overline{x^4+x^3+x^2+1}$

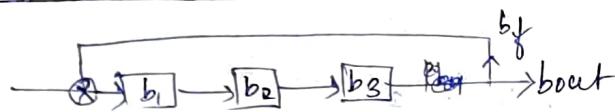
$$h = \left[\begin{array}{cccccc|cc} h_0 & h_1 & h_2 & h_3 & h_4 & 0 & 0 \\ 0 & h_0 & h_1 & h_2 & h_3 & h_4 & 0 \\ 0 & 0 & h_0 & h_1 & h_2 & h_3 & h_4 \end{array} \right]$$

$$= \left[\begin{array}{cccccc|cc} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{array} \right]$$

(11)

LFSRForward LFSR:

$$\begin{aligned}b_{out} &= b_3 \\b_3 &= b_2 \\b_2 &= b_1 \\b_1 &= b_0.\end{aligned}$$

Feedback LFSR:

$$\begin{aligned}b_{out} &= b_3 \\b_3 &= b_2 \\b_2 &= b_1 \\b_1 &= b_0 \oplus b_3\end{aligned}$$

Encoding and decoding in systematic form:

$$\text{as, } v(x) = Rg(x) \quad x^{n-k} i(x)$$

$$\Rightarrow c(x) = x^{n-k} i(x) + r(x).$$

Example:

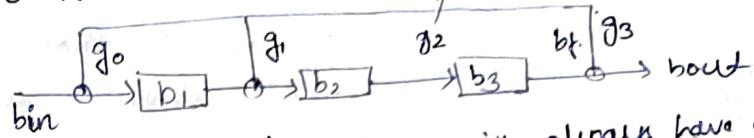
$$v(x) = x^5 + x^3 + x^2 + 1, \quad g(x) = x^3 + x + 1.$$

Here $\frac{v(x)}{g(x)} = r(x)$ then $r(x)$ of the form $a_0 + a_1 x + a_2 x^2$
3 coefficient values.

∴ needed 3 shift registers.

$$\text{first, represent } g(x) \text{ as } \underbrace{g_3}_{1} x^3 + \underbrace{g_2}_{0} x^2 + \underbrace{g_1}_{1} x + \underbrace{g_0}_{1}$$

To make a feedback LFSR from $g(x)$. if $g_i = 1$, make a connection.
 $g_i = 0$ no connection.



first g_0 and last g_{n-1} will always have a connection, as $g_0 = g_{n-1} = 1$.

$$b_{out} = b_1 = b_3.$$

$$\begin{aligned}b_3 &= b_2 \\b_2 &= b_1 + b_3 \\b_1 &= b_0 + b_3\end{aligned}$$

~~b0 = b3~~ (b0 or bin same)

$$v(x) = \underbrace{x^5 + x^3 + x^2 + 1}_{1 \ 0 \ 1 \ 1 \ 0 \ 1} \quad \text{MSB} \quad \text{LSB}$$

bin	b ₁	b ₂	b ₃	b _f	b _{out}
Initial:	—	0	0	0	0
MSB → 1	1	0	0	0	0
v ↓ 0	0	1	0	0	0
1	1	0	1	0	0
1	0	0	0	1	1
0	0	0	0	0	0
LSB 1	1	0	0	0	0

$\underbrace{r(x)}_{r_0 \ r_1 \ r_2}$

Fill the table using above rules.

$$\therefore v(x) = q(x) \cdot g(x) + r(x)$$

$$= \underbrace{(x^2 + 0 \cdot x + 0)}_{q(x)} (x^3 + x + 1) + \underbrace{(0 \cdot x^2 + 0 \cdot x + 1)}_{r(x)}$$

In LFSR,

$$r(x) = Rg(x) x^{n-k} i(x).$$

Here first multiplication of $x^{n-k} \cdot i(x)$ and then division is not happening, rather $n-k$ times division with $g(x)$ happens.

Example: (7,4) $g(x) = x^3 + x + 1$

Let $i(x) = 1010 = x^2 + x$ given.

bin	b_1	b_2	b_3	b_f	b_{out}
-	0	0	0	0	-
1	1	0	0	0	0
0	0	1	0	0	0
1	1	0	1	0	0
0	1	0	0	1	1
-	0	1	0	0	1
-	0	0	1	0	0
-	1	0	1	1	1
	Hence we get $Rg(x) i(x)$ but we want $Rg(x) x^{n-k} i(x)$ \therefore continue to it another $n-k$ times. $n-k = 3$.				
	$r(x) = Rg(x) x^{n-k} i(x)$ without any input.				
	$x+1$				

Compare with old process. multiply then divide.

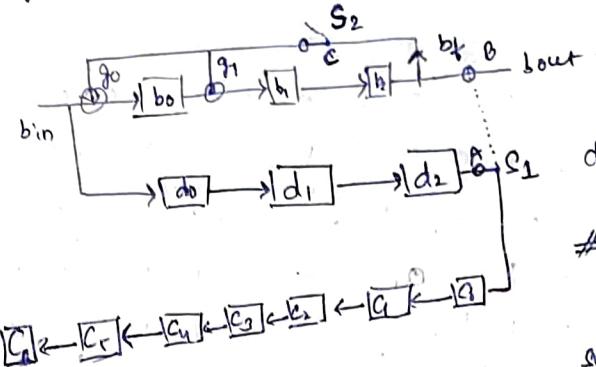
$$x^3 + x + 1 \overline{) x^6 + x^4 + }$$

Encoding using LFSR:

(7,4)

$$g(x) = x^3 + x + 1, i(x) = x^2 + x$$

$g_3 g_1 g_0$



$$\# of d = n-k = 7-4=3$$

switch S, A can connect at A or B .
and one switch at C .

$$b_f = b_{out} = b_2$$

$$b_2 = b_1$$

$$b_1 = b_0 + b_f$$

$$b_0 = b_{in} + b_f$$

$$c_6 = c_5$$

$$c_5 = c_4$$

$$c_4 = c_3$$

$$\vdots \\ c_0 = d_2 \quad (\text{Till } \neq \text{ shift operation})$$

$$d_2 = d_1$$

$$d_1 = d_0$$

$$d_0 = b_{in}$$

** Initially s_1 connected at A and s_2 connected.

After $\neq n$ shifts
 s_1 connected at B and s_2 disconnected

Example: $i(x) = x^2 + 1, g(x) = x^3 + x + 1$
systematic code word: $x^3(x^2 + 1) = x^5 + x^3$

$$Rg(x)(x^5 + x^3) = x^2$$

$$c(x) = x^5 + x^3 + x^2$$

old method

Now using LFSR:

$$\text{Example: } \begin{aligned} f(x) &= x^2 + x + 1 \\ i(x) &= x^3 + x^2 + 1 \end{aligned} \quad \text{so } f \circ i = \text{no input} = 0 \quad (15)$$

	bin	b_0	b_1	b_2	b_3	d_0	d_1	d_2	c_0	c_1	c_2	c_3	c_4	c_5	c_6
	-	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	10	1	0	0	0	1	0	0	0	0	0	0	0	0	0
2	10	1	1	0	0	1	1	0	0	0	0	0	0	0	0
3	0	0	1	1	0	0	1	1	0	0	0	0	0	0	0
4	1	0	1	1	1	1	0	1	1	0	0	0	0	0	0
5	-	1	1	1	1	1	0	1	1	0	0	0	0	0	0
6	-	1	0	1	1	0	0	1	0	1	1	0	0	0	0
7	-	1	0	0	1	0	0	0	1	0	1	1	0	0	0

Now switch S_1 connected to B.
and switch S_2 disconnected. $\Rightarrow \frac{I_{C_0}}{I_{C_2}} = b_2$
 I_{C_0} is constant shifted to C_2 , (Di noque)

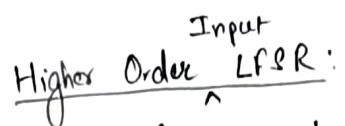
Now just b_i content shifted to C_i , (D_i no use)

Now just bit written sequence
 8 - 0 1 0 0 - - - 0 1 0 1 1 0 0
 9 - 0 0 1 - - - 0 0 1 0 1 1 0
 10 - 0 0 0 - - - 1 0 0 1 0 1 1
codeword =

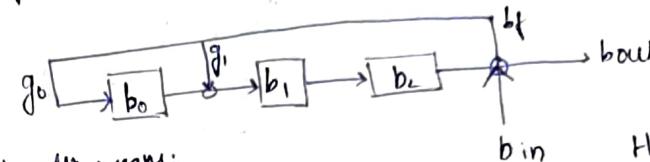
To cross check:
make sure $b_i = 0$

$$\text{code} = \begin{array}{c} \cancel{1} \cancel{1} \cancel{0} \cancel{1} \\ 1101001 \end{array} \leftarrow$$

Verify using old method:



Objective: Reduce number of shifts



High order means:
bin given at max (bi)

Example: (7,4)

Above circuit is for $f(x) = x^3 + x + 1$

$$\text{mt } i(x) = x^3 + x^2 + 1 \Rightarrow 1101$$

bin	b_0	b_1	b_2	b_f	b_{out}
-	0	0	0	0	0
1	1	1	0	1	1
1	1	0	1	1	1
0	1	0	0	1	1
1	1	0	0	1	1

$$\overline{b_i \text{ content.}} = R g(2) x^{n-k} z(x)$$

We need only a shift

R_{gry} x^{n-k} i(x) :

High order LFSR \rightarrow k output

Low " " → n shift

LFSR based cyclic codes

$$\begin{aligned} \textcircled{1} & \quad x^{n^k} i(x) \\ \textcircled{2} & \quad R_g(x) x^{n^k} i(x) \end{aligned}$$

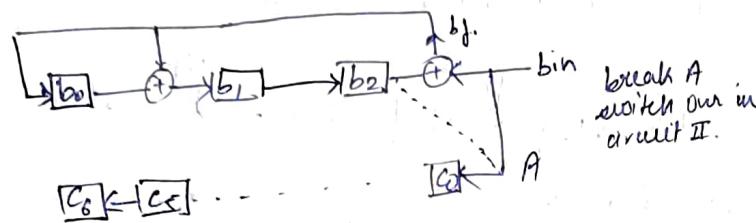
$$\textcircled{3} \quad x^{n_k i(x)} + R g(x) x^{n_k i(x)}$$

↑
syndrome codeword.

\uparrow
Systematic codeword.

Encoding using higher Order LFSR:

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



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

(1101)

bin	b_0	b_1	b_2	c_0	c_1	c_2	c_3	c_4	c_5	c_6	b_f
-	0	0	0	0	0	0	0	0	0	0	0
1	1	1	0	1	0	0	0	0	0	0	1
1	1	0	1	1	1	0	0	0	0	0	1
0	1	0	0	0	1	1	0	0	0	0	1
1	1	0	0	1	0	1	1	0	0	0	1

remainder.

msg. code.

shift after change in switch connection.
 ↳ another 3 shift needed.

$$c_6 = c_5$$

$$c_5 = c_4$$

$$c_0 = b_{in}/b_2$$

(based on switch A)

$$b_f = b_2 \oplus b_{in}$$

$$b_2 = b_1$$

$$b_1 = b_0 \oplus b_f$$

c register content after total n steps

$$\begin{matrix} c_0 & c_1 & \dots & c_6 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{matrix}$$

∴ systematic code word = 1101001.

∴ Encoding needed only n shifts in total

∴ (In lower order we have $n-k$ shifts)

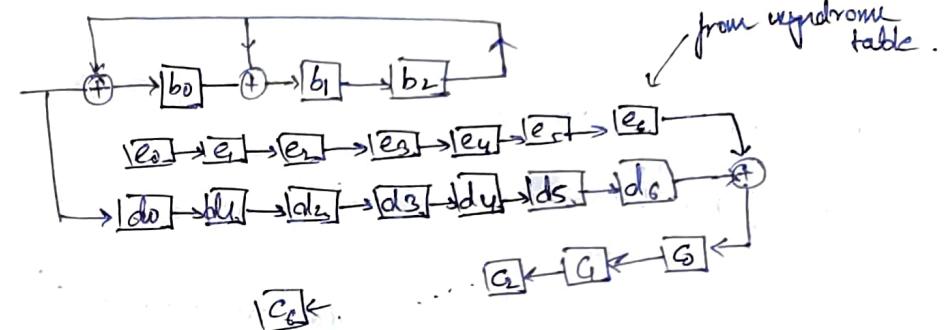
Decoding using LFSR.

$v(x)$

$$g(x) = R_{gen} v(x)$$

If $v(x) = 0$, $v(x)$ is valid codeword.

$$\text{else } v(x) = c(x) + e(x)$$



Limitation:

Need to utilize syndrome table in memory

$$e(x) = R_{gen} v(x) = R_{gen} e(x)$$

$$s(x) = R_{gen} e(x)$$

$$e(x) = x e(x)$$

cyclic shifting of $e(x)$

$$\begin{aligned} s'(x) &= R_{gen} x e(x) \\ &= R_{gen} x s(x). \end{aligned}$$

$$s''(x) = R_{gen} x^2 s(x) = R_{gen} x^2 e(x).$$

Meggith Decoder

$$e(x) = R_{g(x)} e(x)$$

$$s'(x) = R_{g(x)} x e(x)$$

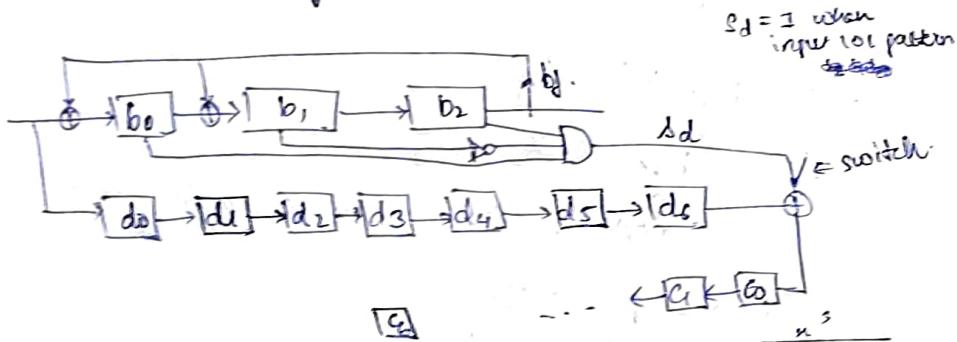
$$= R_{g(x)} x s(x)$$

$$\begin{aligned} s''(x) &= R_{g(x)} x^2 e(x) \\ &= R_{g(x)} x^2 s'(x) \end{aligned}$$

(7,4)

$$\begin{aligned} g(x) &= x^3 + x + 1 \\ h(x) &= x^6 + x^4 + x^3 + 1 \\ v(x) &= x^6 + x^5 + x^3 + x + 1 \\ &\text{single bit error} \end{aligned}$$

$$\begin{aligned} 1\text{ bit error, if } e(x) &= x^6 & (\text{initial error pattern } x^{n-2}) \\ s(x) &= R_{g(x)} x^6 = x^6 + 1 \end{aligned}$$



syndrome of $v(x)$

$$s(x) = R_{g(x)} v(x) = x^3 + 1$$

$$d_1 = b_2$$

$$d_2 = b_1$$

$$d_3 = b_0 + b_1$$

$$d_4 = b_0 + b_1 + b_2$$

$$\frac{x^3 + x + 1}{x^6 + x^4 + x^3 + 1} \xrightarrow{n=6}$$

⑨

$$v(x) = 1011011$$

bin	b_0	b_1	b_2	b_3	d_0	d_1	d_2	d_3	d_4	d_5	s_d	s_u	C_0	C_1	C_2	C_3	C_4	C_5	C_6
-	0	0	0	0	0	0	0	0	0	0	-	0	0	0	0	0	0	0	0
1	1	0	0	0	1	0	0	0	0	0	-	0	0	0	0	0	0	0	0
0	0	1	0	0	0	1	0	0	0	0	-	0	0	0	0	0	0	0	0
1	1	0	1	0	1	0	1	0	0	0	-	0	0	0	0	0	0	0	0
1	0	0	1	1	0	1	0	0	0	0	-	0	0	0	0	0	0	0	0
0	0	0	0	0	1	1	0	1	0	0	-	0	0	0	0	0	0	0	0
1	1	0	0	1	0	1	1	0	1	0	-	0	0	0	0	0	0	0	0
1	1	1	0	0	1	1	0	1	1	0	-	0	0	0	0	0	0	0	0
→ another 7 times																			
-	0	1	1	0	0	1	0	1	1	0	-	0	1	0	0	0	0	0	0
-	1	1	1	1	0	0	1	1	0	1	-	1	1	1	0	0	0	0	0
-	1	0	1	1	0	0	0	1	0	1	-	1	0	1	0	0	0	0	0
→ 2 ² value = 2																			
= value jupped.																			

Higher Order decoding:

$$\text{Here, } S(x) = R_{g(x)} x^{n-k} v(x).$$

$$\text{Example: } e(x) = x^6 \quad (2,4)$$

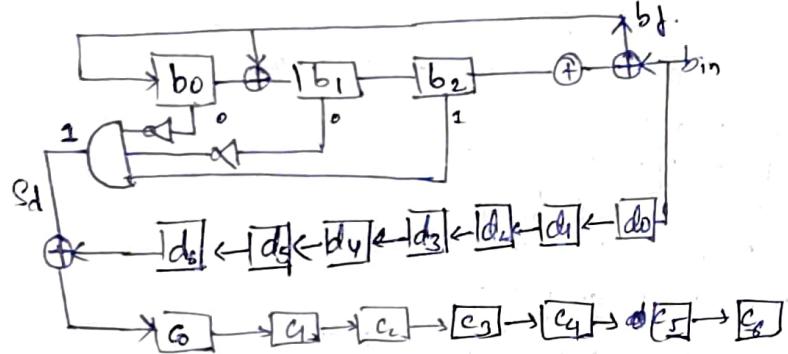
$$\text{Lower order } S(x) = x^2 + 1$$

$$\text{Higher order } e(x) = R_{x^3 + x + 1} x^3 (v(x))$$

$$\begin{aligned} &= R_{x^3 + x + 1} x^3 \cdot x^6 \\ &= x^2 \end{aligned}$$

⇒ syndrome is unique.

Higher order circuit:



2 bit errors :-

$\rightarrow (15,7)$ cyclic code.

Correction of 2 bit error.

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

$g(x) = x^6 + x^5 + x^4 + x^3 + 1$

15 single bit error pattern ← can be corrected using χ^{14}

105 double " " " . (15c₂)

15 patterns

$\begin{matrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ \vdots & & & & & & & & & & & & & & \end{matrix}$	\leftarrow 2 bit consecutive error. \leftarrow 2 bit error with 1 interval
$\begin{matrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{matrix}$	

(cyclic shift of consecutive error)

↓ [000000000000110
 |
 |
 | 110000000000000

Also circular shift of
 1000000000000000
 is same as
 0000000000000001

similarly,
 2 circular shift of

∴ out of 15 only 7 patterns are needed.

~~Gardens field~~ Grapes field.

Ring.

fred.

Group: $(a, b, *)$

1. $a^* b$ closure
 2. $a^* b = b^* a$ commutative
 3. $a^* e = a$ identity
 4. $a^* a = e$ inverse
 5. $a^* (b^* c) = (a^* b)^* c$ associative

A field with finite set is called Galois field / finite field.

Types

Prime
Let 'P' be a prime

then, set = $\{0, 1, 2, \dots, p-1\}$

$$\text{Eg: } \text{Gcf}(2) = \{0, 1\} \\ \text{(binary)}$$

Steps :

~~Priyank~~

Steps:
1. Irreducible polynomial : A prime polynomial. (cannot be factored)
eg: $x^3 + x + 1$

Q. Primitive polynomial: have primitive roots and can derive all elements of field.

3. Imaginary roots

4. Field elements

For $GCF(p)$ \rightarrow take polynomial $x^{p-1} + 1$
 factors of above are irreducible polynomial
 for given GCF.

$$\text{eg: } \text{GF}(2^3) : x^{2^3-1} + 1 = x^7 + 1 \quad \text{GF}(2) = \{0,1\}$$

~~$x^7 + x^5 + x^4 + x^2$~~
 ~~$-x^5 - x^4$~~
 ~~$x + 1$~~

$$(x+1)\overline{x^7+1} \quad \begin{matrix} x^6 + x^5 + x^4 + x^2 \\ + x + 1 \\ \hline x^6 + 1 \\ x^6 + x^5 \end{matrix} \quad \text{modulo 2.}$$

$$x^7 + 1 = (x+1)(x^6 + x^5 + \dots + x+1)$$

$$x^6 + x^5 + x^4 \dots x + 1$$

$x+1$ is not a factor

∴ factors of degree 2, 4.

$$= (ax^2 + bx + c)(dx^4 + ex^3 + fx^2 + gx + h)$$

↓
this also does not have a solution
for this polynomial.

factor 3×3 $= (am^3 + bm^2 + cm + d)(en^3 + fn^2 + gn + h)$
multiple and compare.
 $= (x^3 + x + 1)(x^3 + x^2 + 1)$

$$\therefore x^7 + 1 = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1)$$

$x+1$ → SR of degree 1.

$$\begin{array}{r} x^3 + x + 1 \\ x^3 + x^2 + 1 \\ \hline \end{array} \quad \begin{array}{r} 1 \\ 1 \\ 1 \\ \hline 0 \end{array}$$

field element of GF is represented as a polynomial.

$$GF(p^r)$$

$$a_0 x^r + a_1 x^{r-1} + a_2 x^{r-2} \dots + a_r$$

where $a_i \in GF(p)$

$$GF(2^3) \quad \begin{array}{l} x^3 + x + 1 \\ x^3 + x^2 + 1 \end{array}$$

$$GF(2^4) \quad \begin{array}{l} x^4 + x + 1 \end{array}$$

considering ~~$x^3 + x + 1$~~

Primitive example: $GF(7) = \{0, 1, \dots, 6\}$.

If x is considered primitive
then $x^n = x$ then x is primitive element.
(mod 7) here

$$x = 3$$

$$x^2 = 2$$

$$x^3 = (3^3 \bmod 7) = 6$$

$$x^4 = 4$$

$$x^5 = 1$$

$$x^6 = 3$$

$$x^7 = (3^7 \bmod 7) = 3$$

Thus 3 is primitive element.

(25)

primitive polynomial:

If a polynomial of degree r then it must divide a polynomial $f(x^{2^r-1})$
and it does not divide any other polynomial of degree less than
 2^r-1 .

$$g(x) = x^3 + x + 1$$

$$r = 3.$$

$$R_{G(x)} x^7 + 1 \neq 0, R_{G(x)} x^5 + 1 \neq 0, R_{G(x)} x^4 + 1 \neq 0.$$

$$R_{G(x)} x^3 + 1 \neq 0.$$

$$E.g. \quad p_1(x) = x^4 + x + 1$$

$$p_2(x) = x^4 + x^3 + x^2 + x + 1$$

$$\frac{x^{15} + 1}{x^4 + x + 1} \sim \frac{x^i + x}{x^4 + x + 1} \quad i < 15 \quad \text{not divisible}$$

$\frac{x^5 + 1}{p_2(x)}$ perfectly divisible. $5 < 15 \therefore p_2(x)$ is irreducible but not a primitive polynomial.

Method 2:

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

let α be the imaginary root.

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

$$GF(2^4) \text{ elements: } 0, 1, \alpha, \alpha^2, \alpha^3 \dots, \alpha^{13}, \alpha^{14}$$

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

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

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

$$\alpha^7 = \alpha^4 + \alpha^3 = \alpha^3 + \alpha + 1$$

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

$$\alpha^9 = \alpha^3 + \alpha$$

$$\alpha^{10} = \alpha^4 + \alpha^2 = \alpha^2 + \alpha + 1$$

$$\alpha^{11} = \alpha^3 + \alpha^2 + \alpha$$

$$\alpha^{12} = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + \alpha + 1$$

$$\alpha^{13} = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + \alpha + 1$$

$$\alpha^{14} = \alpha^4 + \alpha^3 + \alpha = \alpha^3 + \alpha + 1$$

$$\alpha^{15} = \underline{\alpha^4 + 1 = 1}$$

when we take

$$\beta = \alpha$$

$$\text{then } \beta^2$$

$$\beta^4 = 1 \Rightarrow \text{order } 15 = 2^4 - 1$$

$$\beta^6 = \alpha$$

then α is primitive

element.

$\Rightarrow p(x)$ is primitive polynomial.

* Note: Modulo 2 operation.

(25)

$$\text{Ex: } p(x) = x^4 + x^3 + x^2 + x + 1.$$

$$\Rightarrow \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0 \\ \Rightarrow \alpha^4, \alpha^3, \alpha^2, \alpha \\ \alpha^4 = \alpha^3 + \alpha^2 + \alpha + 1$$

$$\alpha^5 = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = 1. \Rightarrow \text{order} = 5$$

thus not a primitive element
 $\therefore p(x)$
 Then $p(x)$ not a primitive polynomial.

$$\text{Ex: } x^3 + x + 1 = p(x) \Rightarrow x^3 + x + 1 = 0.$$

 $\text{GF}(2^3)$

$\begin{cases} 0 \\ 1 \\ \alpha \\ \alpha^2 \\ \alpha^3 = \alpha + 1 \\ \alpha^4 = \alpha^2 + \alpha \\ \alpha^5 = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1 \\ \alpha^6 = \alpha^3 + \alpha^2 + \alpha = \alpha^2 + 1 \end{cases}$	$\overline{\alpha^7 = \alpha^3 + \alpha = 1}$ <small>thus α is primitive element of order 7.</small>
---	---

$\Rightarrow \alpha^{2^7-1}$ must come 1 for a primitive polynomial.

\rightarrow Representing elements in form of polynomial.

	$\alpha x^2 + bx + c$
0	$\begin{matrix} a & b & c \\ 0 & 0 & 0 \end{matrix}$
1	$\begin{matrix} a & b & c \\ 0 & 0 & 1 \end{matrix}$
α	$\begin{matrix} a & b & c \\ 0 & 1 & 0 \end{matrix}$
α^2	$\begin{matrix} a & b & c \\ 1 & 0 & 0 \end{matrix}$
$\alpha^3 = \alpha^2 + 1$	$\begin{matrix} a & b & c \\ 0 & 1 & 1 \end{matrix}$
α^4	$\begin{matrix} a & b & c \\ 1 & 1 & 0 \end{matrix}$
α^5	$\begin{matrix} a & b & c \\ 1 & 1 & 1 \end{matrix}$
α^6	$\begin{matrix} a & b & c \\ 1 & 0 & 1 \end{matrix}$

(26)

Q) value of $\sqrt{\alpha}$ in $\text{GF}(2^3)$

$$\text{Ans: } \sqrt{\alpha} = \sqrt{\alpha \cdot 1} = \sqrt{\alpha \cdot \alpha^7} = \sqrt{\alpha^8} = \alpha^4 = \alpha^4$$

Q) find α^{-1} in $\text{GF}(2^4)$

$$= \frac{1}{\alpha} = \frac{\alpha^{15}}{\alpha} = \alpha^{14}$$

Q) $(\alpha + \alpha^2)(\alpha^3 + \alpha)$ in $\text{GF}(2^3)$

$$\text{Ans: } \alpha^4 + \alpha^2 + \alpha^5 + \alpha^3 = \text{to substitute from given element table or generate from given primitive polynomial}$$

$$\Rightarrow \alpha^2 + \alpha + \alpha^5 + \alpha^3 + \alpha + 1 = \alpha^2 + \alpha + \alpha^2 + 1 = 1$$

Q) Given α is primitive element in $\text{GF}(2^3)$

$$\text{find } \sqrt{\alpha^4 \alpha^5 + \sqrt{\alpha}}$$

$$\text{doubt} = \sqrt{\alpha^9 + \sqrt{\alpha^8}} = \sqrt{\alpha^2 + \alpha^4} \quad (\alpha^2 = \alpha + 1)$$

$$\text{Q) } p(x) = x^2 + x + 1$$

$$\alpha^2 + \alpha + 1 = 0.$$

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

$$\alpha^2 = \alpha + 1 \quad \therefore \text{ primitive polynomial.}$$

$$\alpha^3 = \alpha^2 + \alpha \quad \text{degree} = 3 \\ = 1$$

$$Q = A = \begin{bmatrix} 1 & \alpha^4 & \alpha^3 \\ \alpha^2 & 0 & \alpha \\ \alpha^4 & \alpha & \alpha^5 \end{bmatrix} \text{ over } \text{GF}(2^4)$$

Minimal Polynomial:

A polynomial $m(x)$ is called so if $m(x) = 0$ & if $p(x)$ is any non-zero polynomial with $p(x) = 0$ then degree of m must be $\leq \deg p$.

$$\deg(m(x)) \leq \deg(p(x))$$

$a+ib$ is one of the roots
 $a-ib$ is also root.

$$[x - (a-ib)][x - (a+ib)] = 0$$

$$x^2 - (2a)x + (a^2 + b^2) = 0$$

$$x \quad x^2 \quad x^4 \quad x^8 \quad \dots \quad x^{2^t}$$

$$\begin{aligned} \beta &= x^3 \\ \beta^2 &= x^6 \\ \beta^4 &= x^{12} \\ \beta^8 &= x^{24} = x^3 \end{aligned}$$

$$\begin{aligned} (x+x^3)(x+x^5)(x+x^7) \\ = x^2 + (x^3 + x^5 + x^6)x + x^8 \end{aligned}$$

$$x^8(x^3+x+1)$$

$$\begin{aligned} (x+x^3)(x+x^5)(x+x^7) &= 0. \\ x^3 + (x^3 + x^5 + x^6)x^2 + (x^9 + x^{11} + x^{13})x + x^{19} \\ &= x^3 + x^2 + 1 \end{aligned}$$

conjugates (x, x^2, x^4)

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

minimal polynomial of
 x, x^2, x^4 .

27

BCH Codes: cyclic code ✓ user defined error correcting - as per $g(x)$ used.

Def: A t -error correcting cyclic code with generator polynomial $g(x)$ is a binary BCH code iff $g(x)$ is least degree polynomial of $\text{GF}(2)$ where $\beta, \beta^2, \beta^3, \dots, \beta^{2t}$ are roots over $\text{GF}(2^m)$ and length of block code will be $n = 2^m - 1$.

$$t=2 \\ \beta, \beta^2, \beta^3, \beta^4 \rightarrow \text{roots of } g(x) + \underline{\underline{c(x)}} \\ c(x) = i(x)g(x)$$

$$\text{GF}(2^4) \quad g(x) = x^4 + x + 1$$

Field Elements:

$$\begin{aligned} 0 \\ 1 \\ x \\ x^2 \\ x^3 \\ x^4 = x+1 \\ x^5 = x^2 + x \\ x^6 = x^3 + x^2 \\ x^7 = x^4 + x^3 = x^3 + x + 1 \end{aligned}$$

$$\begin{aligned} x^8 &= x^4 + x^2 + x = x^2 + 1 \\ x^9 &= x^3 + x \\ x^{10} &= x^4 + x^3 = x^2 + x + 1 \\ x^{11} &= x^3 + x^2 + x \\ x^{12} &= x^3 + x^2 + x + 1 \\ x^{13} &= x^3 + x^2 + 1 \\ x^{14} &= x^3 + 1 \end{aligned}$$

$$t=2, \quad x \quad x^2 \quad x^3 \quad x^4$$

$$\begin{aligned} g(x) &= (x+x)(x+x^2)(x+x^3)(x+x^4) \\ &= [x^2 + (x^2 + x)x + x^3][x^2 + (x^3 + x + 1)x + x^7] \\ &= (x^2 + x^5x + x^3)(x^2 + x^7x + x^7) \\ &= x^4 + x^3(2x^3 + x^2 + 1) + x^2(x^3 + x^2) + x(x^3 + x^1) \end{aligned}$$

$$= x^4 + x^3x^{13} + x^2x^6 + x^3x^3 + x^{10}$$

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

(29)

\downarrow
imaginary but $g(x) \in \mathbb{R}$
 \therefore replace $(x+x)$ with minimal polynomial of x .
 \downarrow
 $\in \mathbb{R}$

$$g(x) = \text{LCM} [m_1(x), m_2(x^2), m_3(x^3), m_4(x^4)]$$

$$m_1(x) = (x+x)(x+x^4)(x+x^8)(x+x^{12}) = x^4 + x + 1$$

$$m_2(x^2) = m_1(x)$$

$$m_3(x^3) = (x+x^3)(x+x^6)(x+x^9)(x+x^{12}) = x^4 + x^3 + x^{2t}$$

$$m_4(x^4) = m_1(x)$$

$$\text{LCM } [m_1(x), m_2(x^2), m_3(x^3), m_4(x^4)]$$

$$= m_1(x) m_3(x^3)$$

$$= (x^4 + x + 1)(x^4 + x^3 + x^{2t} + 1)$$

$$\text{Block length} = 2^4 - 1 = 15$$

$$n-k = 8$$

(15,7) cyclic code
(2 bit error correction)

(30)

BCH
Codes Decoding:

$$C(x) = i(x) g(x) \quad \leftarrow \text{code word with no error.}$$

$$= i(x) \underbrace{x^2, x^3, \dots, x^{2t}}_{\text{root of } g(x)}$$

$$\begin{aligned} C(x) &= 0 \\ C(x^2) &= 0 \\ &\vdots \\ C(x^{2t}) &= 0 \end{aligned}$$

If some error:

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

$$e(x) = x^{\mu_1} + x^{\mu_2} + \dots + x^{\mu_k} \Rightarrow \text{error at } \mu_i \text{ position.}$$

$$v(x) = \underbrace{c(x)}_{=0} + e(x)$$

$$s_1 = v(x) = e(x)$$

$$\begin{aligned} s_1 &= v(x) = x^{\mu_1} + x^{\mu_2} + \dots + x^{\mu_k} \\ s_2 &= v(x^2) = x^{2\mu_1} + x^{2\mu_2} + \dots + x^{2\mu_k} \quad (\text{if all } 2t \text{ syndrome } = 0 \Rightarrow \text{no error.}) \end{aligned}$$

$$s_{2t} = v(x^{2t}) = x^{2t\mu_1} + x^{2t\mu_2} + \dots + x^{2t\mu_k}$$

$$\text{Let } x^{\mu_i} = X_i$$

$$\begin{aligned} s_1 &= X_1 + X_2 + \dots + X_k \\ s_2 &= X_1^2 + X_2^2 + \dots + X_k^2 \\ &\vdots \\ s_{2t} &= X_1^{2t} + X_2^{2t} + \dots + X_k^{2t} \end{aligned} \quad \begin{matrix} \text{(To solve this)} \\ k \leq t \end{matrix}$$

$$\text{In Galois field } (a+b)^2 = a^2 + b^2 + \underbrace{(ab+ba)}_{=0} = a^2 + b^2$$

$$(X_1 + X_2 + \dots + X_k)^2 = X_1^2 + X_2^2 + \dots + X_k^2$$

$$\text{Thus. } \begin{aligned} s_1^2 &= s_2 \\ s_2^2 &= s_4 \\ s_{2t}^2 &= s_{2t} \end{aligned} \Rightarrow \boxed{s_{2t} = s_{2t}^2}$$

Example:

(7,4) in $Gf(2^5)$

$$c(x) = x^5 + x^3 + x + 1, \quad v(x) = x^7$$

$$\Rightarrow v(x) = x^7 + x + 1$$

thus $t=1$.

\therefore roots x, x^2 .

$$S_1 = v(x) = x^7 + x + 1$$

$$S_2 = v(x^2) = x^14 + x^8 + 1, \quad S_3 = S_1^2 \quad \text{no need of 2nd eqn.}$$

$$S_1 = x^7 + x + 1 = x^5$$

$$x^\mu = x^5, \quad \mu=5 \quad \text{thus error} = x^5$$

$$c(x) = v(x) + e(x) = x^2 + x + 1 + x^5 = \text{given } c(x).$$

Example:

$$t=2 \\ x, x^2, x^3, x^4$$

$$S_1 = x_1 + x_2$$

$$S_2 = x_1^3 + x_2^3$$

$$S_3 = x_1^5 + x_2^5$$

$$S_4 = S_2^2$$

$$x_1 = x^{\mu_1}$$

$$x_2 = x^{\mu_2}$$

solve 2nd eqn to get μ_1, μ_2

$$(x_1 + x_2)^3 = (x_1 + x_2)^2 (x_1 + x_2)$$

$$S_1^3 = (x_1^2 + x_2^2)(x_1 + x_2)$$

$$= x_1^3 + x_1^2 x_2 + x_2^2 x_1 + x_2^3$$

$$= x_1^3 + x_2^3 + x_1 x_2 (x_1 + x_2)$$

$$S_1^3 = S_3 + x_1 x_2 (S_1)$$

$$S_1^3 = S_3 + (S_1 + x_1) S_1 x_1$$

$$S_1^3 + S_1^2 + S_3 \text{ vs } x_1 \text{ vs } x_2$$

$$\text{Eqn } (x_1^2 + S_1 x_1) S_1 + S_3 + S_1^3 = 0$$

$$\boxed{x_1^2 + S_1 x_1 + \frac{S_3 + S_1^3}{S_1} = 0} \quad \leftarrow \begin{array}{l} \text{same eqn} \\ \text{w.r.t } x_1 \\ \text{all } t \end{array}$$

$$\text{generalise } \boxed{f(x) = x^2 + S_1 x + \frac{S_3 + S_1^3}{S_1} = 0} \quad \leftarrow \begin{array}{l} x_1, x_2 \text{ are} \\ \text{roots of this} \\ \text{eqn.} \end{array}$$

To solve this eqn we can search

i.e. put elements one by one and check whether it's 0 or not. If 0, element is a root.

Example:

$$(15,7) \text{ BCH in } Gf(2^4)$$

$$v(x) = x^{11} + x^{10} + x^8 + x^7 + x^6 + x^3$$

$$S_1 = x^{11} + x^{10} + x^8 + x^7 + x^6 + x^3$$

$$S_3 = x^{33} + x^{30} + x^{24} + x^{18} + x^9$$

$$S_1 = (\underbrace{x^3 + x^2 + x}_x) + (x^2 + x + 1) + (x^2 + 1) + (x^3 + x + 1) - (x^3 + x^2) + x^3.$$

$$\rightarrow 4x^3 + 4x^2 + 3x + 3 = x + 1 = x^4$$

$$S_3 = \underbrace{x^3 + 1}_{x^{35}} + x^2 = x^{13}$$

$$\frac{S_3 + S_1^3}{S_1} = \frac{x^{13} + x^{12}}{x^4} = \frac{x \cdot 1}{x^4} = \cancel{x^3} = \frac{x^{15}}{x^3} = x^{12}$$

$$f(x) = x^2 + x^4 x + x^{12}$$

$$f(1) = 1 + x^4 + x^{12} = x^3 + x^2 + 1 = x^3 \neq 0$$

$$f(x) = x^2 + x^5 + x^{12} = x^{13} \neq 0$$

$$f(x^2) = x^4 + x^6 + x^{12} = 0$$

$$\rightarrow x_1 = x^2$$

$$\text{also } x_1 + x_2 = S_1$$

$$x^2 + x_2 = x^4$$

$$x_2 = x^4 + x^2 = x^2 + x + 1 = x^{10}$$

$$\therefore x_1 = x^2, \quad x_2 = x^{10}$$

$$\text{thus } e(x) = x^2 + x^{10}$$

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

When more than t bits of error:

$$x^2 + s_1 x + \frac{s_1^3 + s_3}{s_1} = 0$$

$$x^2 + \sigma_1 x + \sigma_2 = 0, \quad \sigma_1 = s_1, \quad \sigma_2 = \frac{s_1^3 + s_3}{s_1}$$

\downarrow
2-bit.

for t bit error:

$$\sigma_0 x^t + \sigma_1 x^{t-1} + \sigma_2 x^{t-2} + \dots + \sigma_t = 0 \quad \text{--- (1)}$$

$$f\left(\frac{1}{x}\right) = \sigma_0 + \sigma_1 x + \sigma_2 \dots + \sigma_t x^t = 0$$

Wt roots = $\beta_1, \beta_2 \dots \beta_t$ of $f\left(\frac{1}{x}\right)$

$$\text{actual roots of } f(x) = \left(\frac{1}{\beta_1}, \frac{1}{\beta_2}, \dots, \frac{1}{\beta_t}\right)$$

$$\therefore f(x) = (1+x\beta_1)(1+x\beta_2) \dots (1+x\beta_t) \quad \text{--- (2)}$$

Multiply (2) and compare with (1).

$$\sigma_0 = 1$$

$$\sigma_1 = x_1 + x_2 + \dots + x_t$$

$$\sigma_2 = x_1 x_2 + x_1 x_3 + \dots + x_{t-1} x_t$$

⋮

$$\sigma_t = x_1 x_2 \dots x_t$$

$$x_i = \beta_i$$

$$s_1 = \sigma_1$$

$$s_2 = \sigma_1 s_1 + 2\sigma_2 = \sigma_1 s_1 + 0 \quad (2\sigma_2 = 0)$$

$$s_3 = \sigma_1 s_2 + \sigma_2 s_1 + 3\sigma_3$$

⋮

$$s_t = \sigma_1 s_{t-1} + \sigma_2 s_{t-2} + \dots + t\sigma_t$$

(3)

$$\begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ \vdots \\ s_t \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ s_1 & 2 & 0 & 0 & \cdots & 0 \\ s_2 & s_1 & 3 & 0 & \cdots & 0 \\ s_3 & s_2 & s_1 & 4 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ s_{t-1} & s_{t-2} & & & & s_1 t \end{bmatrix} \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_t \end{bmatrix}$$

$$\begin{bmatrix} s_{t+1} \\ s_{t+2} \\ \vdots \\ s_{2t} \end{bmatrix} = \begin{bmatrix} s_2 & s_{t-1} & s_{2t-2} \\ s_{t+1} & s_t & s_{2t-1} \\ \vdots & \vdots & \vdots \\ s_{2t-1} & s_{2t-2} & s_{2t} \end{bmatrix} \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_t \end{bmatrix}$$

$$\begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \\ s_5 \\ \vdots \\ s_{2t-1} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ s_1 & 2 & 0 & 0 & \cdots & 0 \\ s_2 & s_1 & 2 & 0 & \cdots & 0 \\ s_3 & s_2 & s_1 & 2 & \cdots & 0 \\ s_4 & s_3 & s_2 & s_1 & 2 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ s_{2t-1} & s_{2t-2} & s_{2t-3} & & & s_{2t-1} \end{bmatrix} \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_t \end{bmatrix}$$

(3%2 = 1)

2 bit error:

$$\begin{bmatrix} s_1 \\ s_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \sigma_1 \\ \sigma_2 \end{bmatrix}$$

$$e_1 = \sigma_1$$

$$e_3 = s_2\sigma_1 + s_1\sigma_2$$

$$= \sigma^2 s_1 + s_1\sigma_2$$

$$e_3 = \sigma_1^3 + s_1\sigma_2$$

$$\therefore \sigma_2 = \frac{s_1^3 + e_3}{s_1} \quad (\text{not 2 bit}).$$

3 bit error:-

$$v(x) = 1 + \sigma_1 x + \sigma_2 x^2 + \cancel{\sigma_3 x^3} + \sigma_4 x^4$$

$$\begin{bmatrix} s_1 \\ s_3 \\ s_5 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ s_2 & s_1 & 1 \\ s_4 & s_3 & s_2 \end{bmatrix} \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \sigma_3 \end{bmatrix}$$

$$s_1 = \sigma_1$$

$$s_3 = s_2\sigma_1 + s_1\sigma_2 + \sigma_3$$

$$s_5 = s_4\sigma_1 + s_3\sigma_2 + s_2\sigma_3$$

$$s_3 = \cancel{\sigma_3} s_1^3 + s_1\sigma_2 + \sigma_3$$

$$s_5 = s_1^5 + s_3\sigma_2 + s_1^2\sigma_3$$

$$\sigma_2 = \frac{s_2 s_3 + s_5}{s_1^3 + s_3}$$

$$s_3 = (s_3 + s_1^3) + s_1 \frac{(s_2 s_3 + s_5)}{s_1^3 + s_3}$$

Easy to solve.

$$\text{take } \sigma_1 = x^3$$

$$\sigma_2 = x^6$$

$$\sigma_3 = x^9$$

$$v(x) = 1 + x^3 + x^6 + x^9$$

$$\text{using chin method.}$$

if roots: $x_1 = \alpha^i$ $x_3 = \alpha^k$
 $x_2 = \alpha^j$

$$\text{then } e(x) = \frac{1}{x^2} + \frac{1}{x^3} + \frac{1}{x^6} \quad \boxed{C(x) = v(x) + e(x)}$$

PgZ Algo

$$\begin{bmatrix} s_{t+1} \\ s_{t+2} \\ \vdots \\ s_{2t} \end{bmatrix} = \begin{bmatrix} s_1 & s_2 & s_3 & \dots & s_{t-1} & s_t \\ s_2 & s_3 & s_4 & \dots & & \\ \vdots & & & & & \\ s_t & s_{t+1} & s_{t+2} & \dots & s_{2t-1} & s_{2t} \end{bmatrix} \begin{bmatrix} \sigma_t \\ \sigma_{t-1} \\ \vdots \\ \sigma_1 \end{bmatrix}$$

$$C = M\sigma$$

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

Steps in PgZ Algo:

1. Calculate the error syndrome s_1, s_2, \dots, s_{2t} from $v(x)$.
2. Assume max no. of error.
Suppose $i = t$
3. Construct matrix M
4. Find if $(\det(M)) = 0$
{Then reduce $i = i-1$
Go back to step 3.}
5. Compute $\sigma = M^{-1}S$.
6. Determine the roots of $e(x)$
7. Take reciprocal of roots
8. Basis of new roots find $e(x)$
9. $C(x) = v(x) + e(x)$.