Cyclic codes ⇒ any circular shift of a code is also a code word

$101110 \Rightarrow 1\cdot x^5 + 0\cdot x^4 + 1\cdot x^3 + 1\cdot x^2 + 1\cdot x + 0\cdot x^0$

$= x^5 + x^3 + x^2 + x$.

Advantage of cyclic code :

1) It is easy to implement in hardware.

* If codeword size is large then time in standard array increases exponentially.

$c(x) = i(x)\,g(x) \qquad v \cdot H^T = 0$

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

$R_{g(x)}\ c(x) = 0$ (R = Residual)

$R_{g(x)}\ v(x) = R_{g(x)}\ (c(x) + e(x))$

$s(x) = R_{g(x)}\ e(x)$ → residue of $e(x)/g(x)$

$G(x)$:-

for an (n,k) binary cyclic code. The generator polynomial has the form

$g(x) = g_{n-k}\,x^{n-k} + g_{n-k-1}\,x^{n-k-1} + \cdots + g_2 x^2 + g_1 x^1 + g_0$

where coefficient

$g_{n-k} = g_0 = 1$

$g_i = 0/1$

The generator polynomial is a unique polynomial from which all the codepolynomials can be generated.

Theorem 1 :- A non zero code polynomial of min^n degree in a cyclic code c is unique → this is generator polynomial

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

$I(x) = I_{k-1}x^{k-1} + \cdots + I_1 x + I_0$

Let there be two codeword with minimum degrees

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

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

Adding these two codeword we get a new codeword but for this c_k

$g''(x) = 0\, x^{n-k}$.

↳ So less than x^{n-k}

So not valid. Hence our assumption is wrong.

Property :- Cyclic operation produces valid codeword

$c_{n-1}\ c_{n-2} \cdots c_2\ c_1\ c_0$

$c_{n-2}\ c_{n-3} \cdots c_1\ c_0\ c_{n-1}$

(6,ik) → $x^5 + x^3 + x^2 + 1$

↳ 101101

011011 (also a codeword)

next zero codeword $= R_{x^6+1}(x \cdot c(x))$

↳ $R_{x^n+1}(x \cdot c(x))$

↳ shift by 1

$x^6+1 \;)\; x^5 + x^4 + x^3 + x \;(\; 1$

$x^6 + 1$

$x^4 + x^3 + x + 1$

Representation of cyclic codeword

$R_{x^n+1}[x^r c(x)]$

Theorem 2 :- Let $g(x) = x^r + g_{r-1}x^{r-1} + \cdots + g_2x^2 + g_1x + g_0$

Then $g(x)$ is a non zero polynomial of min degree then const. for $g_0 = 1$

Assume $g_0 = 0$

then $g(x) = x(x^{r-1} + g_{r-1}x^{r-2} + \cdots + g_1)$

$= x \cdot g'(x)$

Here we are getting valid code word with min degree.

So $g_0 = 1$

Theorem 3 :- Let $g(x) = 1 + g_1x + \cdots + g_{r-1}x^{r-1} + x^r$ be the non-zero codepolynomial of min degree in (n,k) cyclic code C. A binary polynomial of degree $(n-1)$ or less is a _____ polynomial if and only if it is a multiple of $g(x)$

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

$v(x)$ = valid codeword

$a(x) \cdot g(x)$ = valid codeword

$r(x) \neq 0$

$\therefore r(x) = v(x) + c_1(x)$

$= c_2(x)$

$\deg(v(x)) < \deg(g(x))$ ↯ contradiction

$C(x) = i(x) g(x)$

$g(x) = x^{n-k} + g_{n-k-1} x^{n-k-1} + \dots g_2 x^2 + g_1 x + 1$

$g(x)$ = factor of $(x^n + 1)$

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

residual.

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

↳ cyclic codes

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

$= g(x)[x^n + a(x)]$

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

eg construct $g(x)$ of $(7, 4)$ cyclic code.

$n = 7$

$g(x)$ will be a factor of $x^7 + 1$

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

mod 2 sum

$x^6 + x^6 = 0$

$x = 1$ is a factor

$1 \times 1 = 1$

$0 \times 1 = 0$

for $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

deg(1) x deg(5) ✗

deg(2) x deg(4)

deg(3) x deg(3)

But its solution does not exist.

its solution exist

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

further decomposition is not possible.

$$g(x) = x^{n-k} + g^{n-k-1} x^{n-k-1} + \cdots + g_2 x^2 + g_1 x + 1$$

$n = 7 \quad k = 4$

$g(x) = x^3 + \cdots$

we have already proved it earlier

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

eg: (7,5) cyclic code.

$n = 7, \quad k = 5$

$g(x) = x^2 \ldots$

eg (7,3) cyclic code.

$g(x) = x^4 + \cdots$

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

So (7,3) cyclic code not possible

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

$f_4 \quad f_5 \quad f_1 \quad f_2 \quad f_3$

(15,11)

$n = 15$

$k = 11$

$n - k = 4$

we have $g(x)$ of power $4 = 3$

So 3 cyclic code possible

(15,7) $n = 15 \quad k = 7 \quad n - k = 8$

$f_1 f_2, \; f_2 f_3, \; f_1 f_3$

3 $g(x)$ of power 8

So 3 cyclic code possible.

(15,12) $n = 15 \quad k = 12 \quad n - k = 3$

$f_4 f_5$

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

$\downarrow$ cyclic code

Encoding of Cyclic Code

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

i(x)g(x) will not give codeword in systematic form.

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

(7,4)

1010 $\quad i(x) = x^3 + x$

$c(x) = i(x) \cdot g(x) = (x^3+x)(x^3+x+1)$

$= x^6 + x^2 + x^4 + x^3 + x$

$= x^6 + x^3 + x^2 + x$

$c(x) = 1001110$

code word is not in systematic form

Systematic code word

(7,4)

1010 xxx, or xxx 1010

parity

cyclic code always divisible by g(x)

$x^{n-k} \cdot i(x) = x^3 \times (x^3 + x)$

$u(x) = x^6 + x^4 = 1010000$

parity

it got placed. now find this

$v(x) = a(x)g(x) + r(x)$

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

$a(x)g(x) = v(x) + r(x)$

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

$= 1010011$

parity

$o/p = i(x)$

1. multiply info by x^{n-k} : $= x^{n-k} \cdot i(x)$
2. divide polyn. by $g(x)$

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

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

Decoding of Systematic code

$v(x)$ given.

Syndrome, $s(x) = R_{g(x)}\, v(x)$

if $s(n) = 0$ valid.

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

$s(x) = R_{g(x)}\, v(x) = R_{g(x)}[c(x) + e(x)]$

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

↳ syndrome totally dependent on error pattern.

linear	cyclic
$c = i \cdot G$	$c(x) = i(x) \cdot g(x)$
$G H^T = 0$	$g(x)\, h(x) = x^n + 1$
	↳ parity check polynomial
$v \cdot H^T = 0$ then v is valid	$R_{x^n+1}\, v(x)\, h(x)$ then $v(x)$ is valid
linear code is superset of block code.	$R_{g(x)}\, v(x) = 0$
	cyclic code is subset of linear code.

⟹ using $g(x)$ we can find generator matrix

$g(x) = g_r x^r + g_{r-1} x^{r-1} + \cdots g_2 x^2 + g_1 x^1 + g_0$

$$G_{k \times n} = \begin{bmatrix} g_r & g_{r-1} & g_{r-2} & \cdots & g_2 & g_1 & g_0 & 0 & 0 \\ 0 & g_r & g_{r-1} & & g_3 & g_2 & g_1 & g_0 & 0 \\ 0 & 0 & g_r & & g_4 & g_3 & g_2 & g_1 & g_0 \end{bmatrix}$$

$r = n - k$

Cyclic codes

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

$c = i \cdot G$

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

$= g_3x^3 + g_2x^2 + g_1x + g_0$

$g_3 = 1 \quad g_2 = 0 \quad g_1 = 1 \quad g_0 = 1$

$$G = \begin{bmatrix} g_3 & g_2 & g_1 & g_0 & 0 & 0 & 0 \\ 0 & g_3 & g_2 & g_1 & g_0 & 0 & 0 \\ 0 & 0 & g_3 & g_2 & g_1 & g_0 & 0 \\ 0 & 0 & 0 & g_3 & g_2 & g_1 & g_0 \end{bmatrix}$$

$h(x) = \dfrac{x^7+1}{g(x)} = x^4 + x^2 + x + 1$

$= h_4x^4 + h_3x^3 + h_2x^2 + h_1x + h_0$

$h_4 = 1 \quad h_3 = 0 \quad h_2 = 1 \quad h_1 = 1 \quad h_0 = 1$

h dim $= (n-k) \times k$.

$$h = \begin{bmatrix} h_0 & h_1 & h_2 & h_3 & h_4 & 0 & 0 \\ 0 & h_0 & h_1 & h_2 & h_3 & h_4 & 0 \\ 0 & 0 & h_0 & h_1 & h_2 & h_3 & h_4 \end{bmatrix}$$

~~h_0 h_1 h_2 h_3 h_4~~

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

$x^7 + x^5 + x^4$

$x^5 + x^4 + 1$

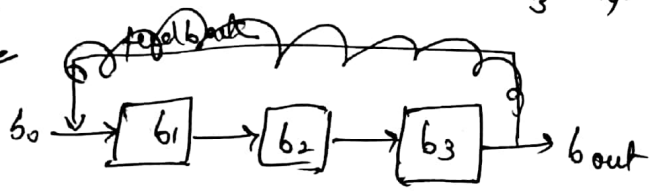
$x^5 + x^3 + x^2$

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

$x^4 + x^2 + x$

$x^3 + x + 1$

LFSR



$b_{out} = b_3$

$b_3 = b_2$

$b_2 = b_1$

$b_1 = b_0$

similarly $b_0\, b_1\, b_2$ ~~b_3~~ $b_2 = 0$

$b_{out} = b_3 \quad b_3 = b_2 \quad b_2 = b_1$

$b_1 = b_0 + b_f$

$$r(x) = R_{g(x)}\left[x^{n-k} i(x)\right]$$

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

⇒ eg ⇒ $i(x) = x^5 + x^3 + x^2 + 1$

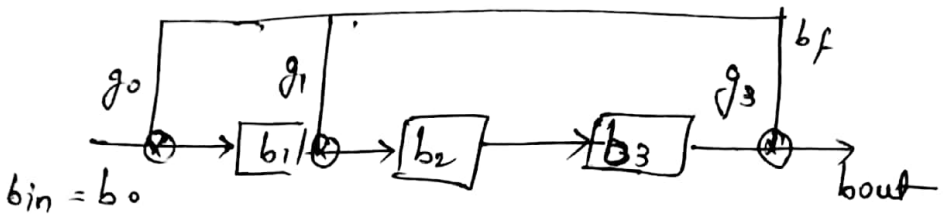
$g(x) = x^3 + x + 1 = g_3 x^3 + g_2 x^2 + g_1 x + g_0$

remainder will have max. degree 2.
so can be $a_0 + a_1 x + a_2 x^2$.

$g_3 = 1 \quad g_2 = 0 \quad g_1 = 1 \quad g_0 = 1$

if $g_i = 1$ then there will be connection
if $g_i = 0$ then no connection

So circuit will be.



$g_2 = 0$, so no connection for g_2.

$b_{out} = b_f = b_3$

$b_3 = b_2$

$b_2 = b_1 + b_f$

$b_1 = b_0 + b_f$

input = $i(x) = x^5 + x^3 + x^2 + 1 = 101101$

b_0 or b_{in}	b_1	b_2	b_3	b_f	b_{out}
–	0	0	0	0	–
1 (MSB)	1	0	0	0	0
0	0	1	0	0	0
1	1	0	1	0	0
1	1	1	0	1	1
0	0	0	1	0	0
1 (LSB)	1	0	0	0	0

$q(x)$

$r(x)$

shift register has $b_1\ b_2\ b_3 = 100$
and remainder = 100

$q(x) = 0 \cdot x^5 + 0 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x + 0$

$r(x) = 0 \cdot x^2 + 0 \cdot x + 1$

$$U(x) = q_x(g_x) + r_{l_x}$$

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

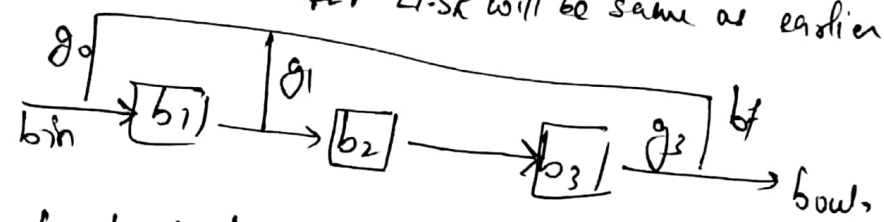
$$= x^5 + x^3 + x^2 + 1$$

$$r(x) = f_{g(x)}\left(x^{n-k} \cdot i(x)\right)$$

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

I/P = 1010 = $x^3 + x$

LFSR will be same as earlier.



bin	b_1	b_2	b_3	bf	bout
—	0	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	0
—	0	0	1	0	0
—	1	1	0	1	1

7 rows

So add 3 more rows

$$x^{n-k} i(x) = x^6 + x^4$$

$$x^3 + x + 1 \;\big)\; x^6 + x^4 \;(\; x^3 + 1$$

$$x^6 + x^4 + x^3$$

$$x^3$$

$$x^3 + x + 1$$

$$x + 1$$

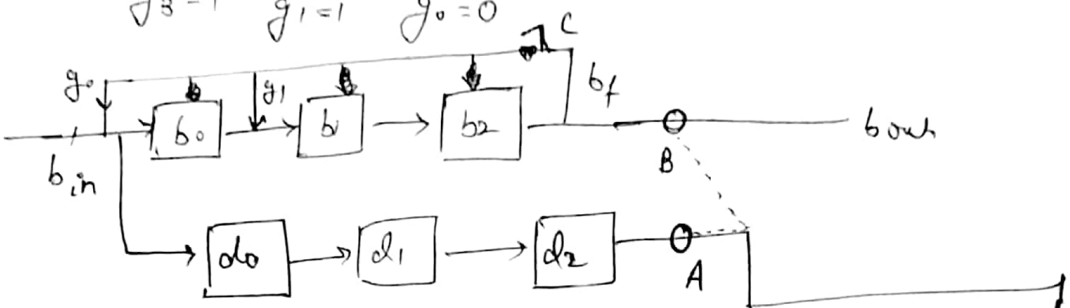
$$c(x) = x^{n-k} i(x) + f_{g(x)}\, x^{n-k}\, e(x)$$

Encoding through LFSR

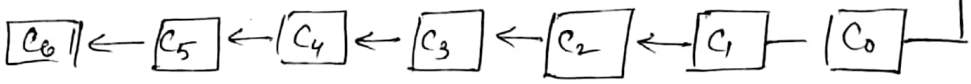
(7,4) $g(x) = x^3 + x + 1$

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

$g_3 = 1 \quad g_1 = 1 \quad g_0 = 0$



d register = n-k



A, B, C ⇒ 3 switches

result can come from either A or B, based on connection.

$b_f = b_{out} = b_2$

$b_2 = b_1$

$b_1 = b_0 + b_f$

$b_0 = b_{in} + b_f$

$C_6 = C_5$

$C_5 = C_4 \text{ ----- } C_1 = C_0$

$C_0 = d_2$ (till n shift) ⇒ take input from d_2.

$d_2 = d_1$

$d_1 = d_0$

$d_0 = b_{in}$

After n shift switch will be connected to ~~B~~ B, but switch C will be disconnected

Initial switch was as A

→ then make n-k shift operation with C_0 to b_2

shift = n-k.

this LFSR called lower order shifting operation LFSR process

eg. $u(x) = x^2 + x + 1 = 101$

$x^3(x^2 + x) = x^5 + x^4 + x^3$ = $q_x(g_x)$

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

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

$x^3 + x + 1 \overline{)x^5 + x^4 + x^3}$

$x^5 + x^3 + x^2$

$x^4 + x^2$

$x^4 + x^2 + x$

x

systematic ← codeword

eg

	b_{in}	b_0	b_1	b_2	b_{out}	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	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0
2	1	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	0	1	0	1	1	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
		0	1	0	-	0	0	0	0	1	0	1	1	0	0
		0	0	1					0	0	1	0	1	1	0
		0	0	0					1	0	0	1	0	1	1

→ feedback will not work; so just b_i content will be shifted to c_i ⇒ switch C is disconnected & A is connected to B

$C_0 = b_2$

at end If $b_i = 0$ then you have done in correct way.

codeword = 1101001

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

$g(x) \cdot g(x) = x^6 + x^5 + x^3$

$R_{g(x)}\ q \cdot g(x) = 1$

$v(x) = x^6 + x^5 + x^3 + 1 = 1101001$

both are same. So we did right

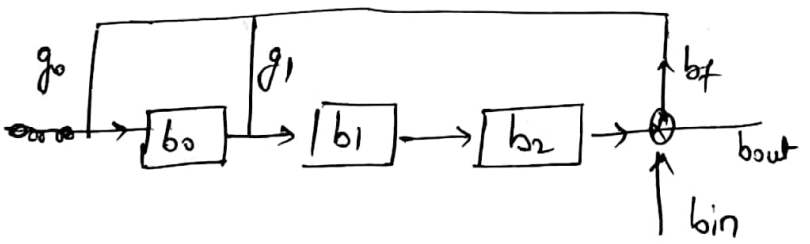
Now we will try to reduce $q n-k$ no. of shifts, the resulthant LFSR will be known as high order shift operate proxy

High order architecture.

(7,4)

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

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



⇐ o/p is provided at b_2.

b_{in}	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

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

$b_2 = b_1$

$b_1 = b_0 + b_f$

$b_0 = b_f$

here we did only 4 shift but in lower order we did 7 shift

$R_{g(x)}\ x^{n-k}\ i(x)$

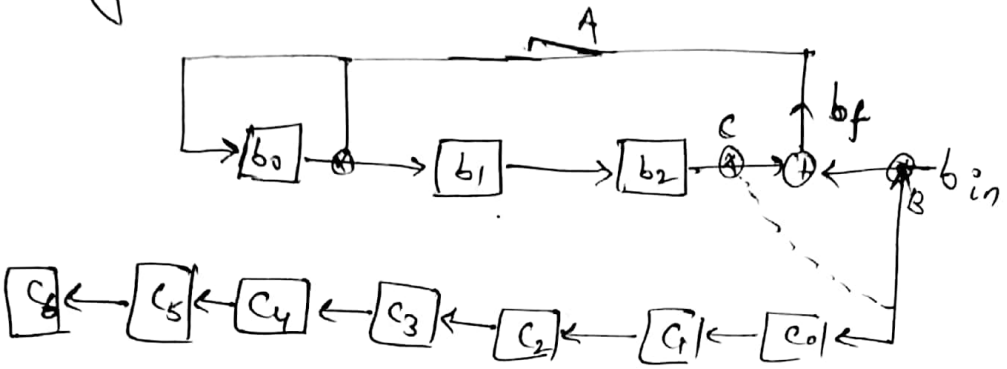
LFSR Based Cyclic Codes

k } computation
$n-k$ }

$n-k$ → shifting.

x^{n-k}. ← lower order

High order :



Eg. $i(x) = x^3 + x^2 + 1 = 1101$

b_{in}	b_f / 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	
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 $x^{n-k} i(x)$			open switch A and connect to C.						
	0	1	0	0	1	0	1	1	0	0	–
	0	0	1	0	0	1	0	1	1	0	–
	0	0	0	1	0	0	1	0	1	1	–
				codeword.							

$c = 1101001$

$b_f = b_0 + b_{in}$
$b_2 = b_1$
$b_1 = b_0 + b_f$
$b_0 = b_f$
~~$c_0 = b_{in}$~~
$c_6 = c_5$
$c_5 = c_4$
$c_4 = c_3$
$c_3 = c_2$
$c_2 = c_1$
$c_1 = c_0$
$c_0 = b_{in} / b_2$

Decoding in cyclic codes

$v(x)$

App1 $r(x) = \cancel{v(x)}$ $R_{g(x)}$

if $r(x) = 0$ then valid codeword

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

$s(x) = R_{g(x)}\ c(x) + e(x) = R_{g(x)}\ e(x)$

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

1	
x	
x^2	
x^3	
x^4	1000
x^5	
x^6	

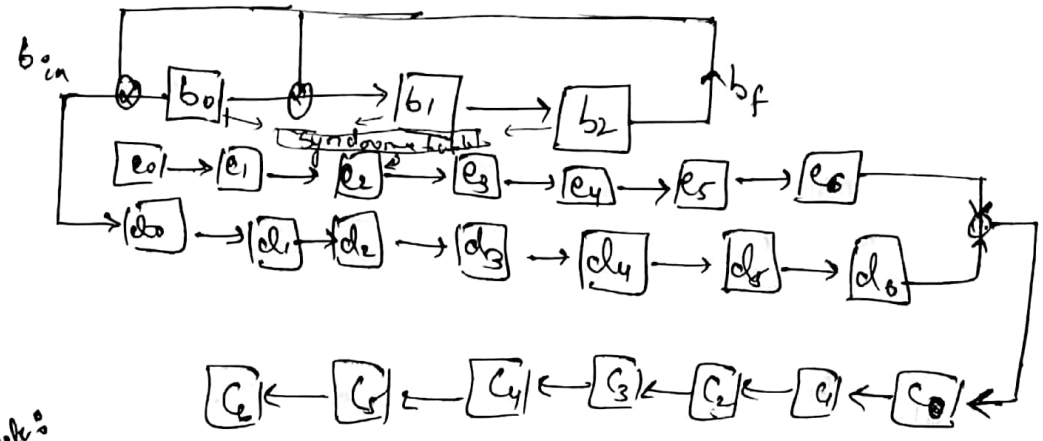
error is in 5th position ←

↓ Syndrome ↓ error

eg. (7,4)

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

App1



Drawback:

In main memory syndrome table is present.

So it is not a good approach.

This circuit is of above theory.

App2 ~~AGA-6 meggitt~~

No syndrome table in main memory

$s(x) = R_{g(x)}\, v(x)$

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

if $e'(x) = x\,e(x)$ ← cyclic shifting

then $s'(x) = R_{g(x)}\, x\, s(x)$

if ~~$s''(x)$~~

$e''(x) = x^2 e(x)$

then $s''(x) = R_{g(x)}\, x\, s'(x) = R_{g(x)}\, x^2 s(x)$

∴ cyclic shifting of a syndrome gives another syndrome.

eg. $g(x) = x^3 + x + 1$ $\qquad v(x) = x^4$

$s(x) = x^2 + x$

$s'(x) = x^2 + x + 1 = \dfrac{x^6 + x^2}{x^3 + x + 1}$

Meggitt Decoder

$s(x) = R_{g(x)}\, e(x)$

eg. (7, 4)

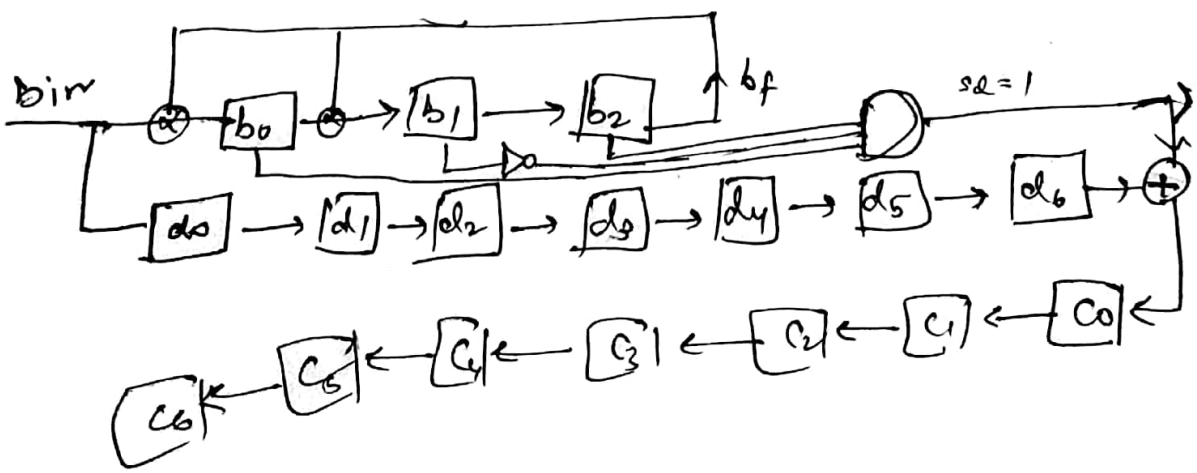
$g(x) = x^3 + x + 1$

$e(x) = x^6 + x^4 + x + 1$

$v(x) = x^6 + x^4 + x^3 + x + 1$

$e(x) = x^6$

initially $s(x) = R_{g(x)}\, e(x) = x^2 + 1$



real syndrome is that when sd = 1

when sd = 0 then just shift until sd = 1

$b_f = b_2$

$b_2 = b_1$

$b_1 = b_0 + b_f$

$b_0 = b_{in} + b_f$

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

1011011

b_{in}	b_0	b_1	b_2	b_f	d_0	d_1	d_2	d_3	d_4	d_5	d_6	sd	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	0	1	1	1	0	1	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
1	1	0	0	0	1	0	1	1	0	1	0	-	0	0	0	0	0	0	0
1	1	1	0	0	1	1	0	1	1	0	1	-	0	0	0	0	0	0	0
-	0	1	1	0	0	1	1	0	1	1	0	0	1	0	0	0	0	0	0
-	1	1	1	1	0	0	1	1	0	1	1	0	0	1	0	0	0	0	0
-	1	0	1	1	1	0	0	1	1	0	1	1	0	0	1	0	0	0	0
-																			
-																			
-																			
-																			

High order decoding

$e(x) = x^6$

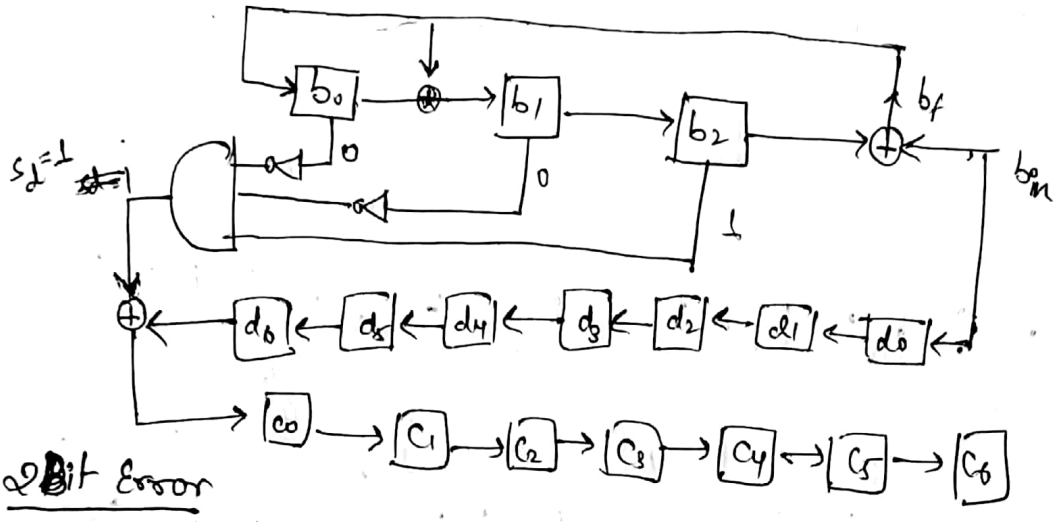
LO: $S(x) = x^2 + 1$

HO: $S(x) = R_{g(x)} x^3 \cdot x^6$

$= x^2$

$R_{g(x)} U(x) = R_{g(x)} x^{n-k} U(x)$

b_0	b_1	b_2
0	0	1



2 Bit Error

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

(15, 7)

15 bit ⇒ single bit error pattern

105 bits ⇒ Double bits " "

~~15 bits are sufficient for~~

x^{14} is sufficient to correct any kind of single bit error (15 bit)

possible 2 bit error

000000000011 → cyclic shift → 000000000110

000000000101 → 000000001100

⋮

100000000001

Same so only consider 1

110000000000

100000000001

Among above there will be only 1 error whose $d = 1$.
Here we use multiple AND Gate.

codes
- → Source code.
- ⇒ Product code
- → Block code
- → Linear code
- → cyclic code.
- → BCH, RS
- → Convolution code ⇒ memory based

BCH ⇒ g(x) is user defined. ⇒ Binary BCH code.
cyclic code but with more freedom
RS ⇒ Non binary BCH code.

Galois field

Group: $(a, b, \circ)$, for set
1) $a \circ b \Rightarrow$ closure
2) $a \circ b = b \circ a \Rightarrow$ commutative
3) $a \circ e = a \Rightarrow$ identity
4) $a \circ a' = e \Rightarrow$ inverse
5) $a \circ (b \circ c) = (a \circ b) \circ c \Rightarrow$ associative

Ring: $(a, b, \circ, \Delta)$
~~A~~ ~~a, Δ satisfy~~
1) one operator satisfy all grp property & other operator satisfy first 3 properties

~~xx~~

Field: $(a, b, \circ, \Delta)$
1) $(a, b, \circ)$ ~~satisfy~~ (a, b, Δ) satisfy all 5 grp property

Galios field / Finite field

Prime field

→ if p is prime no. then has p elements then field elements = {0, 1, 2 -- p-1}
→ satisfy field element
→ GF(7) = {0, 1 -- 6}
GF(2) = {0, 1}
• computer science focus on GF(2)

Extension field.

→ extension = p^n i.e. total no. of elements = p^n if p → prime no.
→ GF(2^3) = 8 elements in the field

Field elements are obtained from primitive polynomial

Primitive Polynomial

irreducible polynomial : behave like prime no.
eg. x^3+x+1 (we can not factor the polynomial)

steps
→ find irreducial polynomial
→ check if it satisfy properties of primitive poly.
→ find imaginary roots
$x^2 = 1 \quad x = -1 \quad x = i$
→ find field elements

for GF(p^n)
factor $(x^{p^n-1}+1)$ then basic polynomial is selected. as irreducible polynomial

GF(2^3) = factor of x^7+1
$x = 1$ is its factor ⇒ mod 2 add.
$(x+1)$ is a factor.

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

$x+1$ will not be the another factor because $7 \% 2 = 1$

$$x^6+x^5+x^3+x^2+x+1 = (ax^2+bx+c)(dx^4+ex^3+fx^2+gx+h)$$

multiply then find a, b, c, d.

but this has no solution

$x^6+x^5+x^4+x^3+x^2+x+1 = (ax^3+bx^2+cx+d)(ex^3+fx^2+gx+h)$

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

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

$(x+1)$ – irreducible pol of deg 1

(x^3+x+1) – deg 3

(x^3+x^2+1) – deg 3

} check primitive property

x^3+x+1 follows primitive properties

$GF(p^n)$ has field elements in term of polynomial

$a_1x^n + a_2x^{n-1} + a_3x^{n-2} + \dots$ a_n

$a_i \in GF(p)$

$GF(2^3)$ = has a set of elements because of (x^3+x+1) & (x^3+x^2+1)

both are same with diff. orientation

Primitive poly. has primitive grps & primitive grp can derive all primitive elements of grp

x is a primitive element when x^n became equal to x

eg $\{0,1,2,3,4,5,6\}$

let $x=2$

$x^2 = 4 \% 7 = 4$

$x^3 = 8 \% 7 = 1$

$x^4 = 2$

$\Rightarrow$ so order = 3.

eg $x=3$ $x^7=3=x$

$x^2 = 2$

$x^3 = 6$

$x^4 = 4$

$x^5 = 5$

$x^6 = 1$

} can be able to find all elements of set, order of. so 3 is primitive element

⇒ $x^n + x + 1$ is one of the irreducible polynomial

If any poly of deg n then it wont divide 'polynomial' of $x^{2^n-1}+1$

it does not divide any other polynomial of degree less than $2^n - 1$

x^3+1 is divisible by $S(4)$,
x^6+1 is not $S(4)$
x^5+1 $S(4)$
x^4+1 $S(4)$
x^3+1 $S(4)$
x^2+1 $S(4)$
S

eg. $P_1(x) = x^4 + x + 1$
$P_2(x) = x^4 + x^3 + x^2 + x + 1$ } irreducible.

$x^{15}+1 \;\%\; P_1(x) == 0$ smaller are not divisible

$x^{15}+1 \;\%\; P_2(x) == 0$ $x^5+1 \;\%\; P_2(x) == 0$ but other are not divisible

So $P_2(x)$ is primitive poly.

The primitive polynomial have primitive roots — root belong to irreducible

if α is a root then $P(\alpha) = 0$

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

$GF(2^4) = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4 \ldots \alpha^{13}, \alpha^{14}, \alpha^{15}\}$

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

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

$\alpha^4 = \alpha + 1$
$\alpha^5 = \alpha^2 + \alpha$
$\alpha^6 = \alpha^3 + \alpha^2$
$\alpha^7 = \alpha^4 + \alpha^3 = \alpha^3 + \alpha + 1$
$\alpha^8 = \alpha^2 + 1$
$\alpha^9 = \alpha^3 + \alpha$

$\alpha^{10} = \alpha^2 + \alpha + 1$
$\alpha^{11} = \alpha^3 + \alpha^2 + \alpha$
$\alpha^{12} = \alpha^3 + \alpha^2 + \alpha + 1$
$\alpha^{13} = \alpha^3 + \alpha^2 + 1$
$\alpha^{14} = \alpha^3 + 1$
$\alpha^{15} = 1$

repeat

same mistake

If a poly. is having elements then called primitive poly.

$\alpha \rightarrow$ primitive elem.

So $\alpha^4 + \alpha + 1 = 0$ is primitive poly

eg. $p(x) = x^4 + x^3 + x^2 + x + 1$

$p(\alpha) \quad \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0$

order $\Rightarrow$ when the elem. will start repeating

$\alpha^1 =$

$\alpha^2 =$

$\alpha^3 =$

$\alpha^4 = \alpha^3 + \alpha^2 + \alpha + 1$

$\alpha^5 = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = 1$

} order is 5 but should be 15

So $p(x)$ is not a primitive poly

This is a approach to show if poly is primit poly ∈ for small one.

eg. $p(x) = x^3 + x + 1$

$GF(2^3) = 0, 1, \alpha, \alpha^2, \alpha^3 = \alpha + 1, \alpha^4 = \quad, \alpha^5 = \ldots$

eg. $(x^7 + 1) = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1)$

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

$\alpha^3 + \alpha^2 + 1 = 0$

$0 \rightarrow 000$

$1 \rightarrow 001$

$\alpha \rightarrow 010$

$\alpha^2 \rightarrow 100$

$\alpha^3 = \alpha^2 + 1 \rightarrow 101$

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

$\alpha^5 = \alpha + 1$

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

$\alpha^7 = \alpha^3 + \alpha^2 = 1$

if $\alpha^{2^r - 1}$ is not 1 then we have done some thing wrong

$x^3 + x + 1$ & $x^3 + x^2 + 1$ are producing same elements but in diff order

eg $\sqrt{\alpha}$ in $GF(2^3)$

$\sqrt{\alpha} \cdot 1 = \sqrt{\alpha} \cdot \alpha^7 = \alpha^4$

eg. $\frac{1}{\alpha}$ in GF(2^4)

$\frac{1}{\alpha} \cdot 1 = \frac{1}{\alpha} \cdot \alpha^{15} = \alpha^{14}$ $\qquad \frac{1}{\alpha} = \alpha^{-1}$

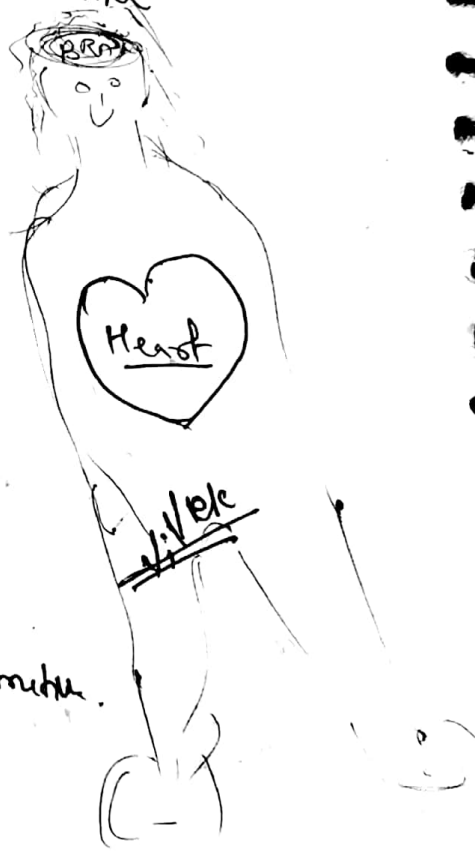
eg. $(\alpha + \alpha^2)(\alpha^3 + \alpha) = \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2$ ← put values & simplify.

$=$

eg. $\sqrt{\alpha^4 \cdot \alpha^5 + \sqrt{\alpha}} = \sqrt{\alpha^9 + \sqrt{\alpha^8}} = \sqrt{\alpha^2 + \alpha^4} = \sqrt{\alpha^2 + \alpha^2 + \alpha}$

$= \sqrt{\alpha} = \alpha^4$

Question Type: determine whether is a irreducible / primitive



eg. $P(x) = x^2 + x + 1$

$x^{2^2 - 1} + 1 = x^3 + 1$

$\frac{x^3 + 1}{x^2 + x + 1} = x + 1$

$P(x)$ is primitive

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

α

$\alpha^2 = \alpha + 1$

$\alpha^3 = \alpha^2 + \alpha = 1$ } order = 3. So $P(x)$ is primitive.

Question Type: Determine inverse of matrix over GF

eg. $A = \begin{vmatrix} 1 & \alpha^4 & \alpha^3 \\ \alpha^2 & 0 & \alpha \\ \alpha^4 & \alpha & \alpha^5 \end{vmatrix}$ over GF(2)

BCH Codes

Minimum Polynomial: A polynomial M is min. polynomial if $m(\alpha) = 0$ and if p is any non zero polyno. with $p(\alpha) = 0$ then degree of $m \leq \deg(p)$

$x+iy$

$z = a+ib$ is one of the root then other root is $(a-ib) = z'$

- $(x-z)(x-z')$
  $= (x-a-ib)(x-a+ib)$
  $= (x-a)^2 + b^2 = x^2 + a^2 - 2xa + b^2$ (real)

$z = a+ib \quad z' = a+i3b$.

- $(x-z)(x-z') =$ (imaginary)

So if conjugate root exist then only lie in real space

if α is root then conjugate occur in $\alpha, \alpha^2, \alpha^4, \alpha^8, \ldots \alpha^{2^l} = ?$

eg. GF(2^3) $x^3 + x + 1$

$\alpha^3 + \alpha + 1 = 0$

0
1
α
α^2
$\alpha^3 = \alpha + 1$
$\alpha^4 = \alpha^2 + \alpha$
$\alpha^5 = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1$
$\alpha^6 = \alpha^2 + 1$

for conjugate of $\alpha^3 \Rightarrow \beta = \alpha^3$
$\beta^2 = \alpha^6$
$\beta^4 = \alpha^{12} = \alpha^5$
$\beta^8 = \alpha^{24} = \alpha^3$
$\beta^{16} = \alpha^2$
$\beta^{32} = \alpha^4$

$\alpha^3, \alpha^5, \alpha^6$ are conjugate

- $(x+\alpha^3)(x+\alpha^5)$
  $= x^2 + x(\alpha^3 + \alpha^5) + \alpha^8$
  $= x^3 + \alpha^2 x + \alpha$

$(x+\alpha^3)(x+\alpha^5)(x+\alpha^6)$
$= (x^2 + \alpha^2 x + \alpha)(x + \alpha^6)$
$= x^3 + x^2(\alpha^6 + \alpha^2) + x(\alpha^8 + \alpha) + \alpha^7$
$= x^3 + x^2 + 1$

$x^3 + x + 1$ is min poly w.r.to $\alpha^6, \alpha^3, \alpha^5$

if $\beta = \alpha$, $\beta^2 = \alpha^2$, $\beta^4 = \alpha^4$, $\beta^8 = \alpha^{16} = \alpha$

conjugate of $\alpha = \alpha, \alpha^2, \alpha^4$

$(x+\alpha)(x+\alpha^2)(x+\alpha^4)$ = real

so $x^3 + x + 1$ is min poly for $\alpha, \alpha^2, \alpha^4$

BCH code.

A t error correcting cyclic code with generator polynomial is BCH code if and only if $g(x)$ is the least degree poly. over $GF(2)$ while β, $\beta^2, \beta^3, \beta^4 \dots \beta^{2t}$ are roots over $GF(2^m)$ and the length of the BCH code will be $n = 2^m - 1$

eg. $t = 2$

$g(x)$ has root $\beta, \beta^2, \beta^3, \beta^4$

↳ are field elements of $GF(2^m)$

So $n = 2^m - 1$

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

$c(\beta) = 0 \quad g(\beta) = 0$

$c(\beta^2) = 0 \quad g(\beta^2) = 0$

eg. $GF(2^4)$ $\quad x^4 + x + 1$

$\alpha^4 + \alpha + 1$

0	$\alpha^9 = \alpha^3 + \alpha$
1	$\alpha^{10} = \alpha^2 + \alpha + 1$
α^1	$\alpha^{11} = \alpha^3 + \alpha^2 + \alpha$
α^3	$\alpha^{12} = \alpha^3 + \alpha^2 + \alpha + 1$
$\alpha^4 = \alpha + 1$	$\alpha^{13} = \alpha^3 + \alpha^2 + 1$
$\alpha^5 = \alpha^2 + \alpha$	$\alpha^{14} = \alpha^3 + 1$
$\alpha^6 = \alpha^3 + \alpha^2$	$\alpha^{15} = 1$
$\alpha^7 = \alpha^3 + \alpha + 1$	
$\alpha^8 = \alpha^2 + 1$	

eg $t = 2$

elements = $\alpha, \alpha^2, \alpha^3, \alpha^4$

these are roots of $g(x)$

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

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

$= [x^2 + (\alpha + \alpha^2)x + \alpha^3][x^2 + (\alpha^3 + \alpha^4)x + \alpha^7]$

$= x^4 + x^3[\alpha^3 + \alpha^4 + \alpha + \alpha^2] + x^2[\alpha^7 + \alpha^4 + \alpha^5 + \alpha^6] + x[\alpha^6 + \alpha^7 + \alpha^8 + \alpha^9] + \alpha^{10}$

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

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

→ not in valid space. So not a solution.

So in $g(x)$ replace α by min poly of α & do same for all.

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

$= m_1(\alpha)\, m_2(\alpha^2)\, m_3(\alpha^3)\, m_4(\alpha^4)$

$= LCM[m_1(\alpha)\, m_2(\alpha^2)\, m_3(\alpha^3)\, m_4(\alpha^4)]$

min poly. below to valid space.

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

$m_2(\alpha^2) = m_1(\alpha) = x^4 + x + 1$

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

$m_4(\alpha^4) = m_1(\alpha)$

substitute in $g(x)$

$m_3(\alpha^3) = x^4 + x^3 + x^2 + 1$

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

$= m_1(\alpha) \times m_3(\alpha^3)$

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

$= x^8 + x^7 + x^6 + x^4 + 1$ ← using this codeword can be calculated

$n = 2^4 - 1$

$n = 15$ Block length.

$k = 15 - 8 = 7$

can correct 2 bit of error.

g(x) is min poly.
g(x) is cyclic code
min ham dis(g(x)) = 5

$2t + 1 \leq 5$

$t = 2$