Cyclic Codes

$5\ 4\ 3\ 2\ 1\ 0$
$1\ 0\ 1\ 1\ 1\ 0 \rightarrow x^5 + x^3 + x^2 + x$

cyclic operation on valid codeword gives valid codeword.

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

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

for decoding $R_{g(x)}\, c(x) = 0$

↓

Residual.

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

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

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

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

where the co-efficient

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

rest are 0 or 1

$g_0(x)$ is an unique polynomial from which all the codeword polynomial can be generated.

Theorem: 1.

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

code : (n,k)

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

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

let there exists a

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

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

Proof using contradiction.

$g'(x) = g'_{n-k}x^{n-k} + \ldots g'_1 x + g'_0$ — ②, let there is another polynomial g' with min degree $n-k$.

also $g_{n-k} = g'_{n-k} = 1$

$$g(x) + g'(x) = \underbrace{(1 \oplus 1)}_{0} x^{n-k} + \ldots + (g_0 \oplus g'_0)$$

modulo 2

$$= \left(g_{n-k-1} + g'_{n-k-1}\right) x^{n-k-1} + \ldots$$

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: $c_{n-1}c_{n-2}c_{n-3} \ldots c_2 c_1 c_0$

$\Rightarrow c_{n-2}c_{n-3} \ldots c_1 c_0 c_{n-1}$ (all left/right rotation are valid)

Code (6,3) $= x^5 + x^3 + x^2 + 1 = C(x)$

$= 101101 \xrightarrow{\text{left rotation}} 011011$

$R_{x^6+1}(xC(x)) = x^6 + x^4 + x^3 + x$

$= 1011010 \rightarrow$ new code length 7

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

$$\underline{x^6 + 1}$$

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

$(0\,1\,1\,0\,1\,1)$ 6 length.

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

Theorem: 2

Let $g(x) = x^r + g_{r-1}x^{r-1} + \cdots g_1 x + g_0$.

$\Rightarrow g_0 = 1$.

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

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

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

$= x(g'(x))$

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.

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

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 codeword $v(x)$ not perfectly divisible by $g(x)$

$v(x) = a(x)g(x) + r(x)$, $r(x) \neq 0$

$v(x)$: valid code word

$a(x)g(x)$: valid code word $C_1(x)$

$r(x) = C(x) + v(x)$

$r(x) = C_2(x)$ thus addition of 2 valid code word is also valid!

$r(x)$ is valid.

also degree $r(x)$ < degree of $g(x)$ (as per division rule.)

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

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

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

Thus contradiction.

→ $g(x)$ is a factor of x^n+1

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

$\therefore x^n g(x) = 1.(x^n+1) + g_n'(x)$

$x^n+1 = x^n.g(x) + g_n'(x)$

Residual = cyclic code

$g_n'(x) = a(x).g(x)$ Theorem 3.

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

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

(7,4) cyclic coder :

$n=7$

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

modulo 2 division
$1+1=0$

↓ further factorize

$\times \to \deg(1)\times\deg(5)$ → $x+1$ is not a factor ($\deg(1\times 5)$ not prime)
$\deg(2)\times\deg(4)$
$\deg(3)\times\deg(3)$

$\therefore x^6+x^5+\dots x+1 = (a_1x^2+a_2x+a_3)(b_1x^4+b_2x^3+b_3x^2+b_4x+b_5)$

↓ this does not have a solution for this equation

$\therefore x^6+x^5\dots+x+1 = (a_4x^3+a_2x^2+a_3x+a_4)(b_4x^3+b_2x^2+b_3x+b_4)$
$= (x^3+x+1)(x^3+x^2+1)$

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

Behave like primes. this cannot be further factored..

$g(x) = x^{n-k} + g_{n-k-1}x^{n-k-1} + \dots + g_1x+1$

$n=7, k=4$

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

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

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

For (7,3)

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

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

Example:

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

1) Find number cyclic codes with (15, 11)

Ans: $n=15$ $n-k=4$.
$k=11$

$\therefore g(x)$ 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)

$n-k=8$.

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

Encoding of Cyclic codes:

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

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

and if $i(x) = 1010$ (x^3+x)

$\therefore c(x) = (x^3+x)(x^3+x+1)$

$= x^6 + x^2 + 2x^4 + x^3 + x$ (mod 2)

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

$1010 \longrightarrow = 1001110$

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

Systematic codeword:

(7,4) → 1010 xxx
fill the parity.

To do this shifting.

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

$x^{7-4} \cdot (x^3+x) = x^3 \cdot (x^3+x) = x^6+x^4 = 1010\,000$ (parity unknown.)

Now this polynomial is not divisible by $g(x)$ but cyclic code should be.

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

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

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

x^3

x^3+x+1

$x+1$

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

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

$c(x)$

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

1010 011
parity.

{Modulo 2 +, - same Galloisfield.}

thus.

1010 → 1010 011
i c
codeword in systematic form.

Algorithm: Encoding of Cyclic codes:

I/p : $i(x)$

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

step 2 : $r(x) = R_{g(x)}\left(x^{n-k} \cdot i(x)\right)$

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

Decoding of Cyclic codes:

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

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

If some error. $v(x) = c(x) + e(x)$ $v(x)$ = received code word

$e(x)$ = error polynomial

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

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

$R_{g(x)}\, c(x)$: divisible, $= 0$

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

Linear

1) $C = i \cdot G$

2) $GH^T = 0$

3) $vH^T = 0$

cyclic

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

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

- $h(x)$ = parity check polynomial.

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

$\Rightarrow$ $v(x)$ = valid

Proof:

$v(x) \cdot h(x) = i(x)\, g(x)\, h(x)$

$= i(x)(x^n+1)$

$\therefore R_{x^n+1}\, v(x)\, h(x) = 0$

$\boxed{R_{g(x)}\, v(x) = 0}$

→ Linear codes are subset of block codes.

→ Cyclic codes are subset of linear code.

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

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

$$G = \begin{bmatrix} g_r & g_{r-1} & g_{r-2} & \cdots & g_1 & g_0 & 0 & 0 \cdots \\ 0 & g_r & g_{r-1} & \cdots & g_1 & g_0 & 0 & \cdots \\ 0 & 0 & \ddots & & & & & \\ \vdots & & & & & & & \\ 0 & 0 & 0 & \cdots & & & & \end{bmatrix}_{k \times n}$$

(R-1 zeros.)

Example: $(7,4)$ $g(x) = x^3 + x + 1$ (coefficients $g_3\, g_2\, g_1\, g_0 = 1\ 0\ 1\ 1$)

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}_{(k \times n)} = k \times n$$

$$h(x) = \frac{x^n+1}{g(x)} = \frac{x^7+1}{x^3+x+1}$$

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

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

$x^5 + x^4 + 1$

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

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

$= x^4 + x^2 + x + 1$

$= h_4 x^4 + h_3 x^3 + h_2 x^2 + h_1 x + h_0\, 1$

$h_4\ h_3\ h_2\ h_1\ h_0$

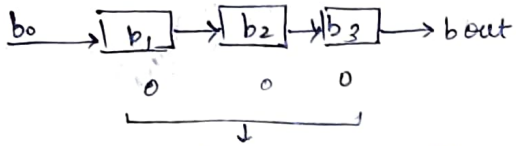
$\therefore \quad 1\ 0\ 1\ 1\ 1$

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

$$= \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$

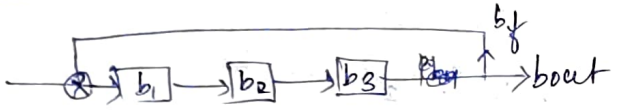
LFSR

Forward LFSR:



$b_{out} = b_3$
$b_3 = b_2$
$b_2 = b_1$
$b_1 = b_0$.

Feedback LFSR:



$b_{out} = b_3$
$b_3 = b_2$
$b_2 = b_1$
$b_1 = b_0 \oplus b_f$

Encoding and decoding in systematic form:

as, $r(x) = R_{g(x)}\, x^{n-k}\, i(x)$

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

Example:

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

Here $\frac{v(x)}{g(x)}$ = not then

$r(x)$ of the form $a_0 + a_1 x + a_2 x^2$

3 coefficient values.

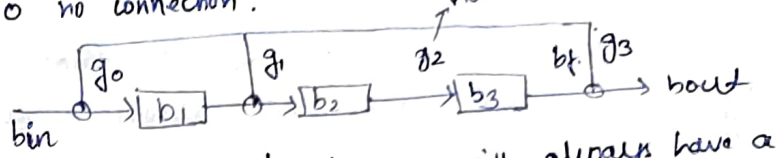
∴ needed 3 shift registers.

first, represent $g(x)$ as $= g_3 x^3 + g_2 x^2 + g_1 x + g_0$.

$1 \quad 0 \quad 1 \quad 1$

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_{x-1} will always have a connection, as $g_0 = g_{x-1} = 1$.

Here, $b_{out} = b_f = b_3$.

$b_3 = b_2$

$b_2 = b_1 + b_f$

$b_1 = b_0 + b_f$

(b0 or bin same)

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

$1\ 0\ 1 \quad 1\ 0\ 1_2$

MSB LSB.

	bin	b_1	b_2	b_3	b_f	bout	
Initial:	—	0	0	0	0	—	
MSB→ 1	1	1	0	0	0	0	q_4
0	0	0	1	0	0	0	q_3
1	1	1	0	1	0	0	q_2
1	1	0	0	0	1	1	q_1
0	0	0	0	0	0	0	q_0
LSB 1	1	1	0	0	0	0	

$q(x)$

$r(x)$

$r_0 \quad r_1 \quad r_2$

fill the table using above rules.

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

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

In LFSR,

$$r(x) = R_{g(x)}\, x^{n-k}\, i(x).$$

Here first multiplication of x^{n-k}. $i(x)$ and then division with $g(x)$ 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	bout
–	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

required $r(x) = R_{g(x)}\, x^{n-k}\, i(x)$

$x+1$

← Here we get $R_{g(x)}\, i(x)$ but we want $R_{g(x)}\, x^{n-k}\, i(x)$ ∴ continue it another $n-k$ times. $n-k = 3$. without any input.

compare with old process. multiply then divide.

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

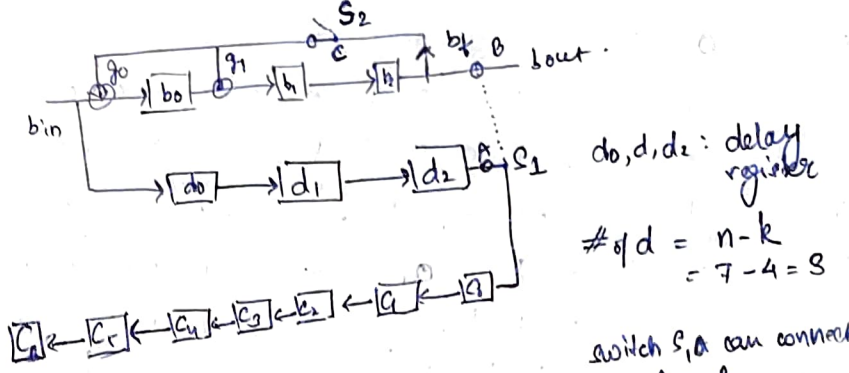
$x+1$

Encoding using LFSR:

(7,4)

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

$g_3\ g_2\ g_1\ g_0$



d_0, d_1, d_2 : delay registers

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

switch S_1 can connect at A or B. S_2 and one switch at C.

$b_f = bout = b_2$

$b_2 = b_1$

$b_1 = b_0 + b_f$

$b_0 = bin + b_f$

$c_6 = c_5$

$c_5 = c_4$

$c_3 = c_2$

⋮

$c_0 = d_2$ (Till 7 shift operation) $n=7$

$d_2 = d_1$

$d_1 = d_0$.

$d_0 = bin$

** Initially S_1 connected at A and S_2 connected.

After 7 shifts S_1 connected at B and S_2 disconnected

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

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

systematic codeword:

$R_{g(x)}(x^5+x^3) = x^2$

$c(x) = x^5+x^3+x^2$ ← old method

Now using LFSR :-

Example: $g(x) = x^3 + x + 1$ ~~x^2+1~~

$i(x) = x^3 + x^2 + 1$ → 1101

1 = no input = 0

bout

	bin	b_0	b_1	b_2	b_f	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

info. | vacant

Now switch S_1 connected to B. and switch S_2 disconnected. ⇒ $c_0 = b_2$

Now just b_i content shifted to c_i, (Di no use)

need 3 more shifts to shift info to actual position.

8	–	0	1	0	–	–	–	0	1	0	1	1	0	0
9	–	0	0	1	–	–	–	1	0	0	1	0	1	1
10	–	0	0	0	–	–	–	1	0	0	1	0	1	1

codeword.

To cross check:

make sure $b_i = 0$

code = ~~1101001~~

1101 001

Verify using old method:

$R_{g(x)}\, x^n\, i(x) \Rightarrow R_{g(x)}\, x^3 (x^3 + x^2 + 1)$

$x^3 + x + 1 \;)\; x^6 + x^5 + x^3 \;(\; x^3 + x^2 + x + 1$

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

$x^5 + x^4$

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

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

$x^4 + x^2 + x$

$x^3 + x$

$x^3 + x + 1$

1

same

$R_{g(x)}\, x^n\, i(x) = 1$

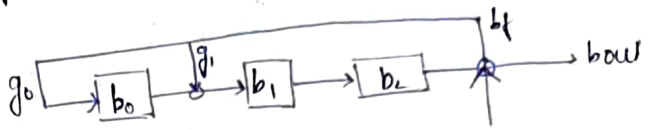
$\therefore c(x) = x^3 \cdot i(x) + 1$

$= x^6 + x^5 + x^3 + 1$

$= 1101001$

Higher Order LFSR:

Objective: Reduce number of shifts.



Here,

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

$b_2 = b_1$

$b_1 = b_0 + b_f$

$b_0 = b_f$

High order means:

bin given at max (b_i)

Example: (7,4)

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

let $i(x) = x^3 + x^2 + 1 \Rightarrow 1101$

bin	b_0	b_1	b_2	b_f	bout
–	0	0	0	0	0
1	1	1	0	1	1
1	1	1	0	1	1
0	1	0	0	1	1
1	1	0	0	1	1

b_i content. $= R_{g(x)}\, x^{n-k}\, i(x)$.

We need only 4 shifts (7 shifts in low order LFSR) ~~to~~ last method

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

High order LFSR → k shifts

Low " " → n shifts

LFSR based cyclic codes:

(n,k)

① $x^{n-k}\, i(x)$

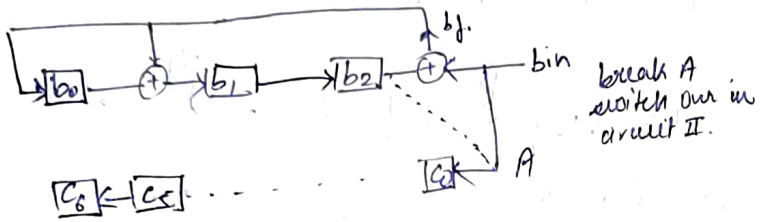
② $R_{g(x)}\, x^{n-k}\, i(x)$

③ $x^{n-k} \cdot i(x) + R_{g(x)}\, x^{n-k}\, i(x)$

↑ Systematic codeword.

Encoding using higher Order LFSR:

→ (7,4) $g(x) = x^3 + x + 1$



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

(1 1 0 1)

bin	b_0	b_1	b_2	c_0	c_1	c_2	c_3	c_4	c_5	c_6	b_j
–	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.
↳ answer 3 shift needed.

$c_6 = c_5$
$c_5 = c_4$
⋮
$c_0 = bin / b_2$
(based on switch A)

$b_j = b_2 \oplus bin$
$b_2 = b_1$
$b_1 = b_0 \oplus b_j$

c register content after total n steps.

c_0	c_1	. . .	c_6
1	0	0	1 0 1 1

∴ systematic code word = 1 1 0 1 0 0 1.

∴ Encoding needed only n shifts in total

∴ (In lower order we have $2n-k$ shifts)

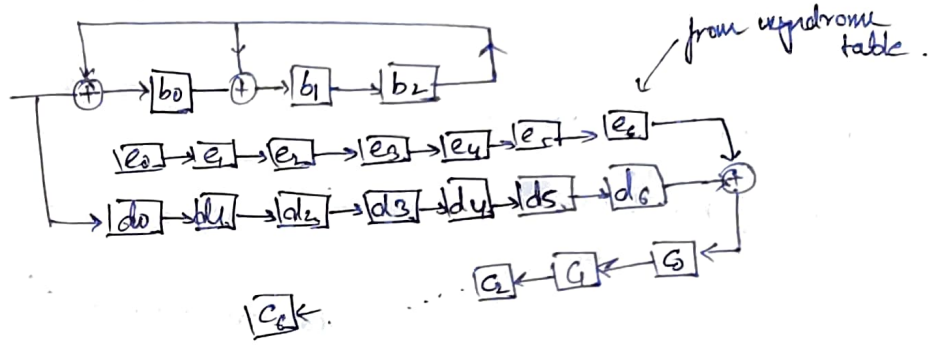
Decoding using LFSR.

v(x)

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

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

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



Limitation:
Need to store syndrome table in memory

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

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

$e'(x) = x\, e(x)$ cyclic shifting of e(x)

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

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

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

Meggitt Decoder

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

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

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

(7,4)

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

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

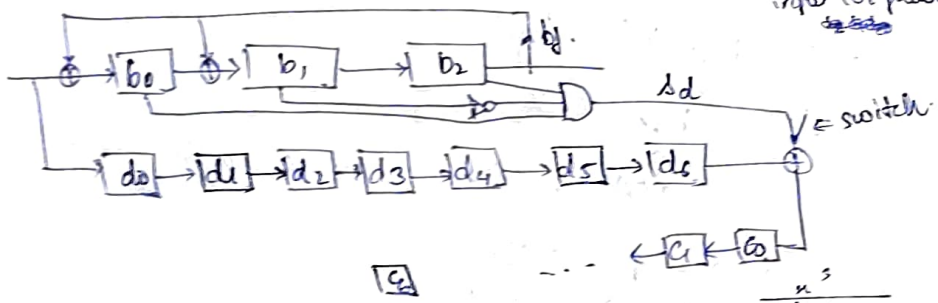
$v(x) = x^6 + x^5 + x^3 + x + 1$

single bit error.

1 bit error, if $e(x) = x^6$ (initial error pattern x^{n-1})

$s(x) = R_{g(x)}\, x^6 = x^2 + 1$

$s_d = 1$ when input 101 pattern



$$x^3 + x + 1 \;\overline{)\; x^6 + x^4 + x^3 + x^2 \;(\; x^3}$$
$$x^6 + x^4 + x^3$$
$$\overline{x^2 + 1}$$

syndrome of $v(x)$

$S(x) = R_{g(x)}\, v(x) = x^2 + 1$

$b_f = b_2$

$b_2 = b_1$

$b_1 = b_0 + b_f$

$b_0 = bin + b_f$

$v(x) = 1011011$

bin	b_0	b_1	b_2	b_f	d_0	d_1	d_2	d_3	d_4	d_5	d_6	s_d	C_0	C_1	C_2	C_3	C_4	C_5	C_6
–	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
1	1	0	1	0	1	0	1	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	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
→ another 7 times																			
–	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	0	0	0	1	1	0	1	0	1	0	1	0	0	0	0
–													1	0	1	0	1	0	0

s_d value = 7

1 0 1 0 1 0 0 0

↳ value flipped

Higher Order decoding:

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

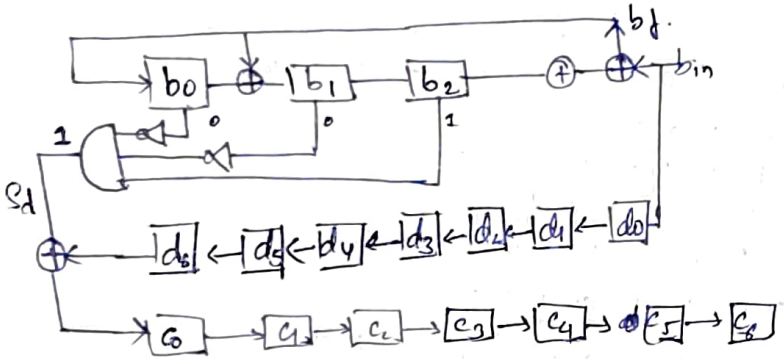
Example $e(x) = x^6$ (7,4)

Lower order $S(x) = x^2 + 1$

Higher order $e(x) = R_{x^3+x+1}\, x^3 (v(x)) = R_{g(x)}\, x^3 \cdot x^6 = x^2$

$\Rightarrow$ syndrome is unique.

Higher order circuit:



2 bit errors:-

→ (15,7) cyclic code.

Correction of 2 bit error.

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

15 single bit error pattern ⟵ can be corrected using x^{14} syndromes

105 double " " " $(15c_2)$

15 patterns:

000000000000011 ← 2 bit consecutive error.
000000000000101 ← 2 bit error with 1 interval
⋮
100000000000001

cyclic shift of consecutive error.

000000000000110
⋮
110000000000000

Also circular shift of
100000000000001
is same as
000000000000011

similarly,
2 circular shift of
010000000000001
is same as
000000000000101

∴ out of 15 only 7 patterns are needed.

~~Galois Field~~ Galois field.

Ring. Field.

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 = $\{0, 1, 2 \ldots, p-1\}$

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

Extension

No. of elements (p^n), p is prime

Steps:

1. Irreducible polynomial : A prime polynomial. (cannot be factored)
   eg: $x^3 + x + 1$
2. Primitive polynomial : have primitive roots and roots can derive all elements of field.
3. Imaginary roots
4. Field elements

For $GF(p^r)$ → take polynomial $x^{p^r - 1} + 1$
Factors of above are irreducible polynomial for given GF.

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

modulo 2

$(x+1)\overline{)x^7+1}\,(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
$x^7 + x^6$
$x^6 + 1$
$x^6 + x^5$
$x^5 + 1$
$x^5 + x^4$
$x^4 + 1$
$x^4 + x^3$
$x^3 + 1$
$x^3 + x^2$
$x^2 + 1$
$x^2 + x$
$x + 1$
$x + 1$
0

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

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

$x+1$ is not a factor

$\therefore$ sub factor 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 $3*3$. $= (ax^3+bx^2+cx+d)(ex^3+fx^2+gx+h)$

multiple and compare.

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

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

$x+1$: IR of degree 1.

x^3+x+1 : IR of " 3

x^3+x^2+1 : " " " 3

Field element of GF is represented as a polynomial.

$GF(p^r)$

$a_1x^r + a_2x^{r-1} + a_3x^{r-2} \ldots + a_r$

where $a_i \in GF(p)$

$GF(2^3)$ ⊢ x^3+x+1, x^3+x^2+1

$GF(2^4)$ ⊢ x^4+x+1

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

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

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

$x = 3$

$x^2 = 2$

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

$x^4 = 4$ $\quad x^6 = 1$

$x^5 = 5$ $\quad x^7 = (3^7 \bmod 7) = 3$

Thus 3 is primitive element.

Primitive polynomial:

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

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

$r = 3$.

$R_{g(x)}\, x^7+1 = 0$, $R_{g(x)}\, x^6+1 \neq 0$, $R_{g(x)}\, x^5+1 \neq 0$, $R_{g(x)}\, x^4+1 \neq 0$.

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

Eg: $p_1(x) = x^4+x+1$

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

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

$\therefore p_1(x)$ is irreducible and primitive polynomial.

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

Method 2

* Note: Modulo 2 operation.

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

let α be the imaginary root.

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

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

$\alpha^4 = \alpha+1$

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

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

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

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

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

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

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

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

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

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

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

when we take $\beta = \alpha$ then β^2

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

$\beta^{16} = \alpha$.

thus α is primitive element.

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

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

$\alpha^4+\alpha^3+\alpha^2+\alpha+1 = 0$.

$\Rightarrow \alpha, \alpha^2, \alpha^3$

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

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

thus not a primitive element

If $p(x)$

Then $p(x)$ not a primitive polynomial.

Eg: $x^3+x+1 = p(x) \Rightarrow \alpha^3+\alpha+1 = 0$.

$GF(2^3)$

field elements

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

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

thus α is primitive element of order 7.

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

→ Representing elements in form of polynomial.

$a\alpha^2+b\alpha+c$

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

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

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

Q) Find α^{-1} in $GF(2^4)$

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

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

Ans) $\alpha^4+\alpha^2+\alpha^5+\alpha^3$ = substitute from given elements table or generate from given primitive polynomial

Q) Given α is primitive element of $GF(2^3)$

Find $\sqrt{\alpha^4+\alpha^5+\sqrt{\alpha}}$

$= \sqrt{\alpha^7+\sqrt{\alpha^8}} = \sqrt{\alpha^2+\alpha^4}$ $(\alpha^2 = \alpha+1)$.

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

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

$\alpha^2 = \alpha+1$

α

$\alpha^2 = \alpha+1$ ∴ primitive polynomial.

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

$= 1$

Q) $A = \begin{bmatrix} 1 & \alpha^4 & \alpha^3 \\ \alpha^2 & 0 & \alpha \\ \alpha^4 & \alpha & \alpha^7 \end{bmatrix}$ over $GF(2^4)$

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.

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

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

$\alpha \quad \alpha^2 \quad \alpha^4 \quad \alpha^8 \quad \ldots \quad \alpha^{2^t}$

$\beta = \alpha^3$
$\beta^2 = \alpha^6$
$\beta^4 = \alpha^{12}$
$\beta^8 = \alpha^{24} = \alpha^3$

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

$\alpha^8(\alpha^3+\alpha+1)$

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

$(x+\alpha^3)(x+\alpha^5)(x+\alpha^6)$
$= x^3+(\alpha^3+\alpha^5+\alpha^6)x^2+(\alpha^8+\alpha^{11}+\alpha^7)x+\alpha^{14}$
$= x^3+x^2+1$

conjugates $(\alpha, \alpha^2, \alpha^4)$

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

↓
minimal polynomial of $\alpha, \alpha^2, \alpha^4$.

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 GF(2) where $\beta, \beta^2, \beta^3 \ldots \beta^{2t}$ are roots over GF(2^m) and length of block code will be $n=2^m-1$.

$t=2$
$\beta, \beta^2, \beta^3, \beta^4 \rightarrow$ roots of $g(x)$ + roots of $c(x)$

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

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

Field Elements:

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

$t=2 \quad \alpha \quad \alpha^2 \quad \alpha^3 \quad \alpha^4$

$g(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)$
$= [x^2+(\alpha^3+\alpha)x+\alpha^3][x^2+(\alpha^3+\alpha+1)x+\alpha^7]$
$= (x^2+\alpha^5 x+\alpha^3)(x^2+\alpha^7 x+\alpha^7)$
$= x^4+x^3(\alpha^3+\alpha^2+1)+x^2(\alpha^3+\alpha^2)+x(\alpha^3+\alpha^{10})$
$\quad +\alpha^{10}$

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

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

↓ imaginary but $g(x) \in R$

∴ replace $(x+\alpha)$ with minimal polynomial of α.

↓ $\in R$

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

$m_1(\alpha) = (x+\alpha)(x+\alpha^4)(x+\alpha^8)(x+\alpha^2) = x^4+x+1$

$m_2(\alpha^2) = m_1(\alpha)$

$m_3(\alpha^3) = (x+\alpha^3)(x+\alpha^6)(x+\alpha^9)(x+\alpha^{12}) = x^4+x^3+x^2+1$

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

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

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

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

Block length $= 2^4-1 = 15$

$n-k = 8$

$k = 7$

(15,7) cyclic code

(2 bit error correction)

BCH

Codes Decoding:

$C(x) = i(x)\, g(x)$ ← code word with no error.

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

$C(\alpha) = 0$

$C(\alpha^2) = 0$ $\qquad C(\alpha^i) = 0$

$\vdots$

$C(\alpha^{2t}) = 0$

If some error:

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

$e(x) = x^{\mu_1} + x^{\mu_2} + \ldots x^{\mu_k}$ ⇒ error at μ_i position.

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

$S_1 = v(\alpha) = e(\alpha) = \alpha^{\mu_1} + \alpha^{\mu_2} + \ldots \alpha^{\mu_k}$

$S_1 = v(\alpha)$

$S_2 = v(\alpha^2) = \alpha^{2\mu_1} + \alpha^{2\mu_2} + \ldots \alpha^{2\mu_k}$

(if all $2t$ syndrome $= 0$ ⇒ no error)

$\vdots$

$S_{2t} = v(\alpha^{2t}) = \alpha^{2t\mu_1} + \alpha^{2t\mu_2} \ldots \alpha^{2t\mu_k}$

Let $\alpha^{\mu_i} = X_i$

$\therefore S_1 = X_1 + X_2 \ldots + X_k$ (To solve this $k \le t$)

$S_2 = X_1^2 + X_2^2 \ldots + X_k^2$

$\vdots$

$S_{2t} = X_1^{2t} + X_2^{2t} \ldots X_k^{2t}$

In galois Galios field $(a+b)^2 = a^2 + b^2 + \underbrace{(ab+ab)}_{=0}$

$= a^2 + b^2$

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

thus. $S_1^2 = S_2$

$S_2^2 = S_4$

$S_3^2 = S_6$

$\Rightarrow \boxed{S_{2i} = S_i^2}$

Example:
(7,4) in GF(2^3)
$c(x) = x^5+x^2+x+1$, $e(x) = x^5$

$\Rightarrow v(x) = x^2+x+1$

~~the~~ here $t = 1$.
$\therefore$ roots α, α^2.
$S_1 = v(\alpha) = \alpha^2+\alpha+1$
$S_3 = v(\alpha^3) = \alpha^4+\alpha^2+1$, $S_3 = S_1^2$ $\therefore$ no need of 2nd eqn.

$S_1 = \alpha^2+\alpha+1 = \alpha^5$
$x^\mu = \alpha^5$, $\mu = 5$ then error $= x^5$
$c(x) = v(x) + e^x = x^2+x+1+x^5 =$ given $c(x)$.

Example: $t = 2$
$\alpha, \alpha^2, \alpha^3, \alpha^4$

$S_1 = X_1+X_2$ $\quad S_2 = S_1^2$ $\quad X_1 = x^{\mu_1}$
$S_3 = X_1^3+X_2^3$ $\quad S_4 = S_2^2$ $\quad X_2 = x^{\mu_2}$
solve 2 eqn to get μ_1, μ_2

$(X_1+X_2)^3 = (X_1+X_2)^2(X_1+X_2)$
$S_1^3 = (X_1^2+X_2^2)(X_1+X_2)$
$= X_1^3 + X_1^2X_2 + X_2^2X_1 + X_2^3$
$= X_1^3 + X_2^3 + X_1X_2(X_1+X_2)$
$S_1^3 = S_3 + X_1X_2(S_1)$ | $S_1 = X_1+X_2$, $X_2 = S_1+X_1$
$S_1^3 = S_3 + (S_1+X_1)S_1X_1$

$S_1^3 + S_1^2 + S_3$ ~~terms~~

$(X_1^2 + S_1X_1)S_1 + S_3 + S_1^3 = 0$

$$X_1^2 + S_1X_1 + \frac{S_3+S_1^3}{S_1} = 0$$ ← same eqn w.r.t X_2 also

generalise $\Rightarrow$ $$f(X) = X^2 + S_1X + \frac{S_3+S_1^3}{S_1} = 0$$ ← X_1, X_2 are roots of this eqn.

To solve this eqn use chien search
i.e put elements one by one and check whether its 0 or not. If 0, element is a root.

Example:
(15,7) BCH in GF(2^4)
$v(x) = x^8+x^{10}+x^8+x^7+x^6+x^3$

$S_1 = \alpha^{11}+\alpha^{10}+\alpha^8+\alpha^7+\alpha^6+\alpha^3$
$S_3 = \alpha^{33}+\alpha^{30}+\alpha^{24}+\alpha^{21}+\alpha^{18}+\alpha^9$

$S_1 = (\alpha^3+\alpha^2+\alpha) + (\alpha^2+\alpha+1) + (\alpha^2+1) + (\alpha^3+\alpha+1) + (\alpha^3+\alpha^2) + \alpha^3$.
$= 4\alpha^3 + 4\alpha^2 + 3\alpha + 3 = \alpha+1 = \alpha^4$

$S_3 = \alpha^3 + 1 + \alpha^2 = \alpha^{13}$

$\frac{S_3+S_1^3}{S_1} = \frac{\alpha^{13}+\alpha^{12}}{\alpha^4} = \frac{\alpha^{13}(1+\alpha^{-1})}{\alpha^4} = \frac{\alpha^{15}}{\alpha^3} = \alpha^{12}$

$f(X) = X^2 + \alpha^4X + \alpha^{12}$
$f(1) = 1+\alpha^4+\alpha^{12} = \alpha^3+\alpha^2+1 = \alpha^{13} \neq 0$
$f(\alpha) = \alpha^2+\alpha^5+\alpha^{12} = \alpha^{13} \neq 0$.
$f(\alpha^2) = \alpha^4+\alpha^6+\alpha^{12} = 0$
$\Rightarrow X_1 = \alpha^2$

this is called chien search ⇐

also $X_1+X_2 = S_1$
$\alpha^2+X_2 = \alpha^4$
$X_2 = \alpha^4+\alpha^2 = \alpha^2+\alpha+1 = \alpha^{10}$.

$\therefore X_1 = \alpha^2$, $X_2 = \alpha^{10}$

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

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

When more than 2 bits of error:

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

$$x^2 + \sigma_1 x + \sigma_2 = 0 \quad , \sigma_1 = S_1 \, , \; \sigma_2 = \frac{S_1^3 + S_3}{S_1}$$

↓
2 bit.

for t bit error:

$$\sigma_0 x^t + \sigma_1 x^{t-1} + \sigma_2 x^{t-2} + \cdots \sigma_t = 0 \quad = f(x) \qquad — (1)$$

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

let roots $= \beta_1, \beta_2 \cdots \beta_t$ of $y\left(\frac{1}{x}\right)$

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

$$\therefore \quad y(x) = (1 + x\beta_1)(1 + x\beta_2) \cdots (1 + x\beta_t) \qquad — (2)$$

multiply (2) and compare with (1).

$\sigma_0 = 1$

$\sigma_1 = x_1 + x_2 \cdots + x_t$ $\qquad x_i = \beta_i$

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

$\vdots$

$\sigma_t = x_1 x_2 \cdots x_t$

$S_1 = \sigma_1$

$S_2 = \sigma_1 S_1 + 2\sigma_2 \quad = \sigma_1 S_1 + 0 \qquad (2\sigma_2 = 0)$

$S_3 = \sigma_1 S_2 + \sigma_2 S_1 + 3\sigma_3$

$\vdots$

$S_t = \sigma_1 S_{t-1} + \sigma_2 S_{t-2} \cdots t\sigma_t$

$$\begin{bmatrix} S_1 \\ S_2 \\ S_3 \\ \vdots \\ S_t \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ S_1 & 2 & 0 & 0 & \cdots & 0 \\ S_2 & S_1 & 3 & 0 & \cdots & 0 \\ S_3 & S_2 & S_1 & 4 & \cdots & 0 \\ \vdots & & & & & \\ S_{t-1} & S_{t-2} & & & S_1 \; t \end{bmatrix} \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_t \end{bmatrix}$$

$$\begin{bmatrix} S_{t+1} \\ S_{t+2} \\ \vdots \\ S_{2t} \end{bmatrix} = \begin{bmatrix} S_t & S_{t-1} & S_{t-2} & \cdots & S_2 \; S_1 \\ S_{t+1} & S_t & S_{t-1} & \cdots & S_3 \; S_2 \\ & & & & \\ S_{2t-1} & S_{2t-2} & & & S_{t+1} \; S_t \end{bmatrix} \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_t \end{bmatrix}$$

$$\begin{bmatrix} S_1 \\ S_3 \\ S_5 \\ \vdots \\ S_{2t-1} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ S_2 & S_1 & 1 & 0 & \cdots & 0 \\ S_4 & S_3 & S_2 & & & \\ & & & & & \\ S_{2t-2} & S_{2t-3} & & & S_{t-1} \end{bmatrix} \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_t \end{bmatrix}$$

mod. $(3 \% 2 = 1)$

2 bit error:

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

$S_1 = \sigma_1$

$S_3 = S_2\sigma_1 + S_1\sigma_2$

$= S_1^2 S_1 + S_1\sigma_2$

$S_3 = S_1^3 + S_1\sigma_2$

$\therefore \sigma_2 = \dfrac{S_1^3 + S_3}{S_1}$ (2 bit).

3 bit error:-

$\sigma(x) = \underset{\sigma_0}{1} + \sigma_1 x + \sigma_2 x^2 + \sigma_3 x^3$

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

$S_1 = \sigma_1$

$S_3 = S_2\sigma_1 + S_1\sigma_2 + \sigma_3$

$S_5 = S_4\sigma_1 + S_3\sigma_2 + S_2\sigma_3$

$S_2 = S_1^2$

$S_4 = S_2^2$

$S_3 = S_1^3 + S_1\sigma_2 + \sigma_3$

$S_5 = S_1^5 + S_3\sigma_2 + S_1^2\sigma_3$

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

Easy to solve.

take $\sigma_1 = \alpha^3$

$\sigma_2 = \alpha^6$

$\sigma_3 = \alpha^8$

$\sigma(x) = 1 + \alpha^3 x + \alpha^6 x^2 + \alpha^8 x^3$.

using chien search

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

$x_2 = \alpha^j$

then $e(x) = \dfrac{1}{\alpha^i} + \dfrac{1}{\alpha^j} + \dfrac{1}{\alpha^k}$

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

PGZ Algo

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

$\underline{S} = M\sigma$

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

Steps in PGZ Algo:

1. Calculate the error syndrome $S_1, S_2 \ldots S_{2t}$ 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 $\sigma(x)$
7. Take reciprocal of roots
8. Basis of new roots find $e(x)$
9. $c(x) = v(x) + e(x)$

PGZ Algorithm

$$\begin{bmatrix} S_{2t+1} \\ S_{2t+2} \\ \vdots \\ S_{2t} \end{bmatrix} = \begin{bmatrix} S_1 & S_2 & S_3 & \cdots & S_{t-1} & S_t \\ S_2 & S_3 & S_4 & \cdots & & \\ \vdots & & & & & \\ S_t & S_{t+1} & \cdots & I & \cdots & S_{2t-1} \end{bmatrix} \begin{bmatrix} v_t \\ v_{t-1} \\ \vdots \\ v_1 \end{bmatrix}$$

i.e. $S = MV$

if $|M| \neq 0$ then $\boxed{V = M^{-1}S}$

$v(x)$ obtained ✓ brute force

i) Calculate error syndrome $S_1 S_2 \cdots S_{2t}$ from $r(x)$
ii) Assume max. errors $t = t$;
iii) Construct M
iv) Find $|M|$ & check if it is 0
v) If $|M| = 0$, then $t = t-1$ & GOTO iii)
vi) Compute $V = M^{-1}S$
vii) Determine roots of $v(x)$ — $v(x)$ = ungiven
viii) Take reciprocal of roots
ix) Form error polynomial

~~Find Determine roots~~ GF(2^4) (15, 5) $\alpha^{15} = 1$

$t = 3$

$v(x) = x^8 + x^5 + x^4 + x + 1$

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

$S_2 = r(\alpha^2) = \alpha^{16} + \alpha^{10} + \alpha^8 + \alpha^4 + 1$

$S_3 = \alpha^{11}$

$S_4 = \alpha^2$

$S_5 = 0$

$S_6 = \alpha^7$

$$M = \begin{bmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{bmatrix}$$ find $|M|$

$$M = \begin{vmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & 0 \end{vmatrix} = S_3(S_2 S_4 - S_3^2) - S_4(S_1 S_4 - S_2 S_3)$$

$$= S_2 S_3 S_4 - S_3^3 - S_1 S_4^2 + S_2 S_3 S_4$$

$$= S_3^3 + S_1 S_4^2$$

$$= \alpha^{33} + (\alpha^8 + \alpha^5 + \alpha^3 + \alpha + 1)(\alpha^{16})$$

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

$$= \alpha^3 + \alpha^9 + \alpha^6 + \alpha^3 + \alpha^2 + \alpha$$

$$= \alpha^9 + \alpha^6 + \alpha^2 + \alpha$$

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

$$= 0$$

Reduce dimension $(t=2)$

$$M = \begin{bmatrix} S_1 & S_2 \\ S_2 & S_3 \end{bmatrix} = S_1 S_3 - S_2^2$$

$$M^{-1} = \begin{bmatrix} \alpha^8 & \alpha \\ \alpha & \alpha^{14} \end{bmatrix}$$

$$\begin{bmatrix} S_{t+1} \\ S_{t+2} \\ \vdots \\ S_{2t} \end{bmatrix} = M\nabla \qquad \nabla = M^{-1}S = \begin{bmatrix} \alpha^8 & \alpha \\ \alpha & \alpha^{14} \end{bmatrix} \begin{bmatrix} \alpha^{11} \\ \alpha^8 \end{bmatrix}$$

$$= \begin{bmatrix} \alpha^{19} + \alpha^9 \\ \alpha^{12} + \alpha^{22} \end{bmatrix}$$

$$= \begin{bmatrix} \alpha^4 + \alpha^9 \\ \alpha^{12} + \alpha^7 \end{bmatrix}$$

$$= \begin{bmatrix} \alpha + 1 + \alpha^3 + \alpha \\ \alpha^3 + \alpha^3 + \alpha + 1 + \alpha^3 + \alpha + 1 \end{bmatrix} = \begin{bmatrix} \alpha^3 + 1 \\ \alpha^2 \end{bmatrix}$$

$$\therefore \nabla = \begin{bmatrix} \alpha^{14} \\ \alpha^2 \end{bmatrix}$$

$$\nabla(x) = 1 + \nabla_1 x + \nabla_2 x^2 = 1 + \alpha^{14} x + \alpha^2 x^2$$

$\nabla(1) \neq 0$

$\nabla(\alpha) = 1 + \alpha^{15} + \alpha^4 \neq 0$

$\nabla(\alpha^5) = 0 \qquad \nabla(\alpha^{11}) = 0 \quad \therefore$ roots are $\alpha^5 : \alpha^{11}$

reciprocal $\alpha^{10} \quad \alpha^4$

$e(x) = x^{10} + x^4$

$\therefore c(x) = \nabla(x) + e(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$

Reed Soloman Codes:

t error

$\alpha^1 \alpha^2 \dots \alpha^{2t}$ → roots of $g(x)$

BCH constraint → $g(x) \in IR$

but here no constraint — can be imaginary

$$g(x) = (x+\alpha)(x+\alpha^2)\dots(x+\alpha^{2t})$$

$t=1$ α, α^2 → roots $\therefore g(x) = (x+\alpha)(x+\alpha^2)$

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

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

$\alpha^3 = \alpha + 1$

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

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

Decoding

co-efficient $\neq 1$ find location & magnitude

① Detect error location ② Find magnitude of error

$$e(x) = \alpha_i^{?} x^{i} + \alpha_j^{?} x^{j}$$

RS $e(x) = Y_{p_1} x^{p_1} + Y_{p_2} x^{p_2} + \dots + Y_{p_\mu} x^{p_\mu}$

μ: correctable error

BCH $e(x) = x^{p_1} + x^{p_2} + \dots + x^{p_\mu}$ only location — all real co-efficients

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

$S_1 = r(x) = c(x) + e(x) = e(x)$

$S_2 = e(\alpha^2)$

$S_3 = e(\alpha^3)$ $\quad S_i = e(\alpha^i)$

Let $Y_{p_i} = Y_i$ & $x^{p_i} = X_i$

$S_1 = Y_1 X_1 + Y_2 X_2 + \dots + Y_\mu X_\mu$

$S_2 = Y_1 X_1^2 + Y_2 X_2^2 + \dots + Y_\mu X_\mu^2$

$S_3 = Y_1 X_1^3 + Y_2 X_2^3 + \dots + Y_\mu X_\mu^3$

$\vdots$

$S_{2t} = Y_1 X_1^{2t} + Y_2 X_2^{2t} + \dots + Y_\mu X_\mu^{2t}$

$$X = \begin{bmatrix} X_1 & X_2 & X_3 & \cdots & X_\mu \\ X_1^2 & X_2^2 & X_3^2 & \cdots & X_\mu^2 \\ \vdots & & & & \\ X_1^{2t} & X_2^{2t} & \cdots & & X_\mu^{2t} \end{bmatrix} \qquad Y = \begin{bmatrix} Y_1 \\ Y_2 \\ Y_3 \\ \vdots \\ Y_\mu \end{bmatrix}$$

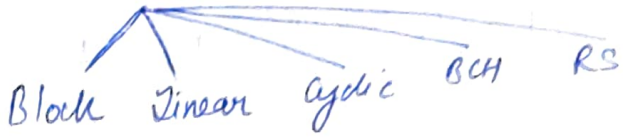
$$S = XY$$

$$Y = X^{-1}S$$

PGZ to find X

then find Y

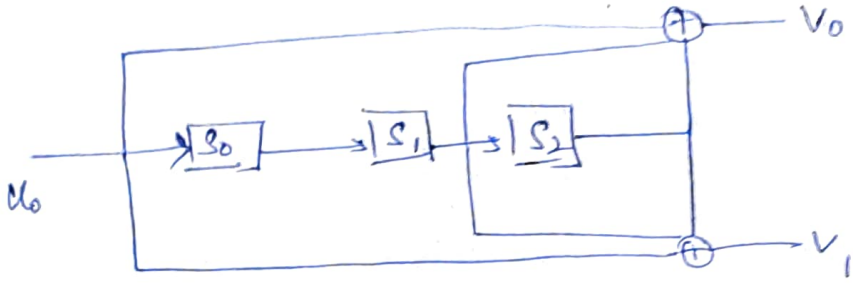
Convolutional Codes (n, k)

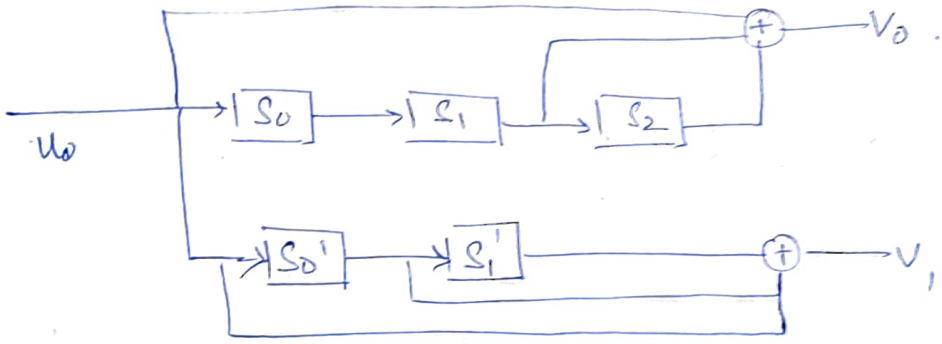


Memory based Coding: (n, k, m)

k bits of information mapped to n bits of ~~information~~ code along with m bits of previous information

(2, 1, 3)





$U_0 \longrightarrow V_0$ 3 memory order

$U_0 \longrightarrow V_1$ 2 " "

when multiple, take max (3, 2) = 3

$\therefore$ (2, 1, 3) code.

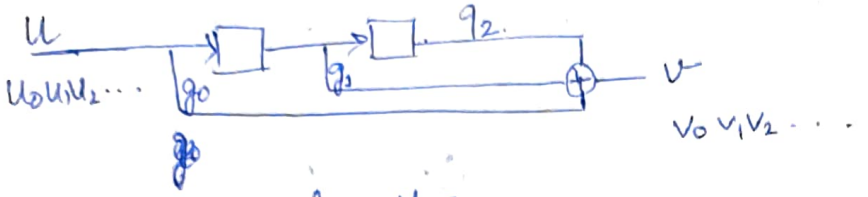
$u_0 = (1011101)$

$v = (v_0^{(s)} v_1^{(s)})$

$= (v_0^{(0)} v_1^{(0)} v_0^{(1)} v_1^{(1)} v_0^{(2)} v_1^{(2)} \ldots)$

For one input u_i we get v_0^i & v_1^i

$(1, 1, 2)$



g_0

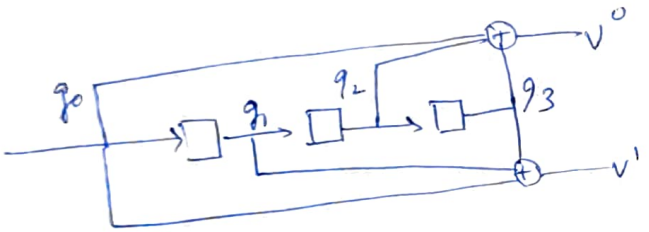
$v_0 = u_0 g_0$.

$v_1 = u_1 g_0 + u_0 g_1$

$v_2 = u_2 g_0 + u_1 g_1 + u_0 g_2$

$v_3 = u_3 g_0 + u_2 g_1 + u_1 g_2$

$$v_i = \sum_{j=0}^{2} u_{i-j} g_j \qquad (m = 2)$$



$u \rightarrow v^0$

g_0	g_1	g_2	g_3
1	0	1	1

input 1

$v_0 = 1$

input 0 1

$v_0 = 0+0 = 0$

$u \rightarrow v^1$

g_0	g_1	g_2	g_3
1	1	0	1

← initial g values

1

$v_0^1 = 1$.

0 1

v^1 0+1 = 1

	1st	2nd	3rd
input :	1	0	1
	11	01	01

Polynomial based encoding:

g_1 is delayed by 1 bit
g_2 " " " 2 bit
g_3 " " " 3 bit

g_0	g_1	g_2	g_3
1	0	1	1

$g(D) = 1 + D^2 + D^3$

$u = u_0 u_1 u_2 \ldots$

$v_0 = u_0 g_0$

$v_1 = u_1 g_0 + u_0 g_1$

$v_2 = u_2 g_0 + u_1 g_1 + u_0 g_2$

$u = 1011$

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

$i(D) \cdot g(D)$

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

$= 1 + D^4 + D^6 \quad = (1000101)$

$u_0 u_1 u_2 u_3$

If $u = 1011$

$v_0 = 1 \cdot 1 = 1$

$v_1 = 0 \cdot 1 + 1 \cdot 0 = 0$

$v_2 = 1 \cdot 1 + 0 \cdot 0 + 1 \cdot 1 = 0$

$v_3 = 0$

1000

$v_0 v_1 v_2 v_3$

This process is continued until the contents of shift register become empty.

Then continue with null input.

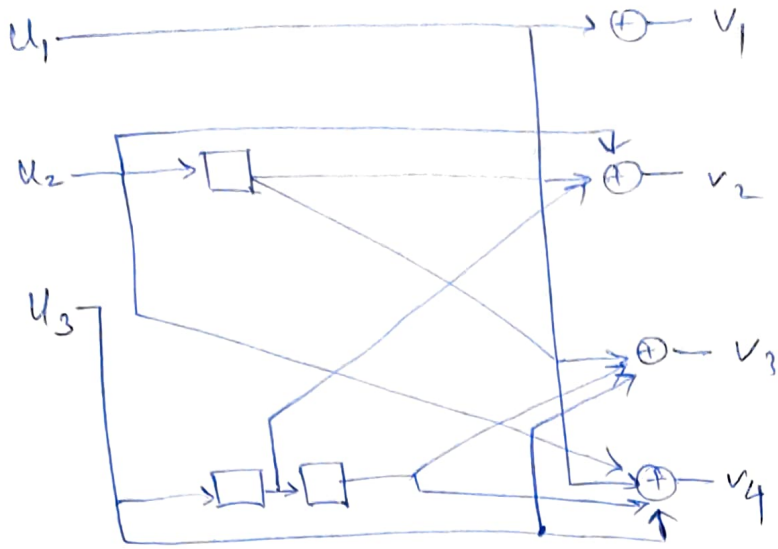
Another 3 bit

$u_4 u_5 u_6$

0 0 0

$v_4 = 1, \quad v_5 = 0, \quad v_6 = 1$

$\therefore$ (1000101)



(4, 3, 2)

110, 011, 101
u_0 u_1 u_2

g^{ij} = input i to output j

$g^{11} = 100$ $g^{12} = 100$ $g^{13} = 100$ $g^{14} = 100$
$g^{21} = 000$ $g^{22} = 110$ $g^{23} = 010$ $g^{24} = 100$
$g^{31} = 000$ $g^{32} = 010$ $g^{33} = 101$ $g^{34} = 101$

$$G = \begin{bmatrix} G_{00} G_1 G_2 & & & \\ 0\ G_{00}\ G_1\ G_2 & & & \\ 0\ 0\ G_{00}\ G_1\ G_2 & & & \end{bmatrix}$$

G_{00} = 1st bit of every g^{ij}

$$= \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

G_{01} = 2nd bit of every g^{ij}.

$$= \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

G_{02} = 3rd bit of every g^{ij}

$$= \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

$$G = \begin{bmatrix} 1111 & 0000 & 0000 & 0 \\ 0101 & 0110 & 0000 & 0 \\ 0011 & 0100 & 0011 & \\ 0000 & 1111 & 0000\ 0000 & \\ 0000 & 0101 & 0110\ 0000 & \\ 0000 & 0011 & 0100\ 0011 & \\ 0 & 0 & G_{00}\ G_1\ G_2 & \end{bmatrix}$$

U.G

$v_0 = u_0 G_{00} = 1010$

$v_1 = u_1 G_{00} + u_0 G_1 = 0110 + 0110$
$= 0000$

Now using polynomial

$g^{11} = 1 \quad g^{12} = 1 \quad g^{13} = 1 \quad g^{14} = 1$

$g^{21} = 0 \quad g^{22} = 1+D \quad g^{23} = D \quad g^{24} = 1$

$g^{31} = 0 \quad g^{32} = D \quad g^{33} = 1+D^2 \quad g^{34} = 1+D^2$

$$v^j(D) = \sum_{i=1} u^i(D) \otimes g^{ij}(D)$$

$v^1(D) = (1+D^2)\cdot 1 + (1+D)\cdot 0 + (D+D^2)\cdot 0 = 1+D^2$

$v^2(D) = D^2 + D^3$

$v^3(D) = 1 + D^2 + D^3 + D^4$

$v^4(D) = D^3 + D^4$

$$v(D) = v^1(D^4) + D v^2(D^4) + D^2 v^3(D^4) + D^3 v^4(D^4)$$

$$= 1 + D^8 + D(D^8 + D^{12}) + D^2(1 + D^8 + D^{12} + D^{16}) + D^3(D^{12} + D^{16})$$