Properties of cyclic codes.

Cyclic codes are a subset of LBC which satisfy the following properties,

(1) Property of Linearity (same as LBC)

If $C = \{c_1, c_2, \ldots c_n\}$,

then $c_i \oplus c_j = c_k \in C$.

(2) Cyclic property

Shifting any codeword in C by one or more bits to left or right will result in another codeword which belongs to C.

e.g $S = \{0000, 0101, 1010, 1111\}$

(1) Linearity

$$\begin{array}{lll} 0000 & 0101 & 1010 \\ \oplus\ 0101 & \oplus\ 1010 & \oplus\ 1111 \quad \text{---etc.} \\ \hline 0101 & 1111 & 0101 \end{array}$$

This property is satisfied.

(2) Cyclic Property.

$(0101)_{1/8} \Rightarrow 1010 \rightarrow 0101 \rightarrow \ldots$

$(1111) \rightarrow 1111 \rightarrow 1111 \rightarrow \ldots$

$0000 \rightarrow 0000 \rightarrow 0000 \rightarrow \ldots$

This property is also satisfied.

$\therefore$ S is a cyclic code.

$G = [I | P]$

How do we calculate the generator matrix given a generator ~~of~~ polynomial.

1st row : $\text{Rem}\left[\frac{x^{n-1}}{g(x)}\right]$

2nd row : $\text{Rem}\left[\frac{x^{n-2}}{g(x)}\right]$

3rd row $\text{Rem}\left[\frac{x^{n-3}}{g(x)}\right]$

$\vdots$

k^{th} row

$\text{Rem}\left[\frac{x^{n-k-1}}{g(x)}\right]$

for a (7,4) cyclic code,

eg If $g(x) = x^3 + x + 1$, calculate the generator matrix.

$n = 7, \quad k = 4$

$$G = [I_k \mid P] = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & - & - & - \\ 0 & 1 & 0 & 0 & - & - & - \\ 0 & 0 & 1 & 0 & - & - & - \\ 0 & 0 & 0 & 1 & - & - & - \end{array}\right]$$

↑ ?

1st row $\quad \dfrac{x^{7-1}}{g(x)} = \dfrac{x^6}{x^3+x+1}$

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

$$\oplus\; x^6 + x^4 + x^3$$

$$x^4 + x^3$$

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

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

$$x^3 \quad + x + 1$$

$$x^2 + 1 = [1\ 0\ 1]$$

2^{nd} row $= \dfrac{x^{7-2}}{x^3+x+1}$

$$x^3+x+1 \overline{)\, x^5} \quad x^2+1$$

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

$$x^3+x^2$$

$$x^3+x+1$$

$$x^2+x+1 = [1\ 1\ 1]$$

3^{rd} row $= \dfrac{x^{7-3}}{x^3+x+1}$

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

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

$$x^2+x = [1\ 1\ 0]$$

4^{th} row $= \dfrac{x^{7-4}}{x^3+x+1}$

$$x^3+x+1 \overline{)\, x^3} \quad 1$$

$$x^3+x+1$$

$$x+1 = [0\ 1\ 1]$$

$$\therefore G = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right]$$

Generator matrix for a systematic cyclic code.

- In a systematic cyclic code, the first k ~~digits~~ bits = message bits
  last n-k bits = parity bits.
- For a systematic code the codeword polynomial $c(x)$ corresponding to the data polynomial $d(x)$ is given by

$$c(x) = x^{n-k} d(x) + p(x)$$

where

$$p(x) = \text{remainder}\left(\frac{x^{n-k} d(x)}{g(x)}\right)$$

eg. Given a data vector $d(x) = 1010$

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

$x^{n-k} d(x) = x^3(x^3 + x) = x^6 + x^4$

$$\begin{array}{r} x^3 + x^2 + 1 \\ x^3 + x^2 + 1 \;\overline{)\; x^6 + x^4} \\ x^6 + x^5 + x^3 \\ \hline x^5 + x^4 + x^3 \\ x^5 + x^4 + x^2 \\ \hline x^3 + x^2 \\ x^3 + x^2 + 1 \\ \hline 1 \end{array}$$

$P(x) = 1$

$\therefore c(x) = x^3 d(x) + p(x)$

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

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

Similarly

$d(x)$	$c(x)$	
1000	x^6+x^2+x	= [1000 110]
0100	x^5+x+1	= [0100 011]
0010	x^4+x^2+x+1	[0010 111]
0001	x^3+x^2+1	[0001 101]

$$G = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right]$$

Now $c = d \cdot G$

Using this equation it is easy to find the remaining codewords.

data	code
1111	1111111
1110	1110010
1101	1101000
1100	1100101
1011	1011100
1010	1010001
1001	1001011
1000	1000110
0111	0111001
0110	0110100
0101	0101110
0100	0100011
0011	0011010
0010	0010111
0001	0001101
0000	0000000

Cyclic Codes for Non Systematic Codeword.

$$C(x) = m(x)\, g(x)$$

e.g.: $g(x) = 1 + x^2 + x^3$.

$m(x) = 1010 = x^3 + x$.

$$C(x) = m(x)\, g(x)$$
$$= (x^3 + x)(1 + x^2 + x^3)$$
$$= x^3 + x^5 + x^6 + x + x^3 + x^4.$$
$$= x^6 + x^5 + x^4 + x$$
$$= [1\ 1\ 1\ 0\ 0\ 1\ 0]$$

Cyclic Codes - Syndrome Calculation

e.g. For a given (7, 4) code the generator polynomial is

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

The received sequence is

$R = 100100$

Find if the received sequence is valid.

$S(x)$ = syndrome $= \text{Rem}\left[\frac{R(x)}{g(x)}\right]$

$R = 1001000$

$R(x) = x^6 + x^3$

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

$$
\begin{array}{r}
x^3 + x \\
x^3 + x + 1 \;\overline{)}\; x^6 + x^3 \\
\underline{x^6 + x^4 + x^3} \\
x^4 \\
\underline{x^4 + x^2 + x} \\
x^2 + x
\end{array}
$$

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

Syndrome is not zero

∴ Received sequence contains errors.

Error patterns for Correction of Identified errors:-

Error Patterns.	Error Polynomial.	Syndrome Polynomial.	Syndrome.
1000000	x^6	x^2+1	101
0100000	x^5	x^2+x+1	111
0010000	x^4	x^2+x	110
0001000	x^3	$x+1$	011
0000100	x^2	x^2	100
0000010	x	x	010
0000001	1	1	001

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

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

$$\frac{x^6+x^4+x^3}{x^4+x^3}$$

$$\frac{x^4+x^2+x}{x^3+x^2+x}$$

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

$S(x) = x^2+x$ which corresponds to

$e(x) = x^4$

$$C(x) = R(x) + e(x)$$
$$= (x^6 + x^3) + x^4$$
$$= x^6 + x^4 + x^3$$
$$= 1011000$$

↑
error bit