

Properties of cyclic codes.

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

(1) Property of linearity (same as LBC)

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

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

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

This property is satisfied.

(2) Cyclic Property

$$(0101) \rightarrow 1010 \rightarrow 0101 \rightarrow \dots$$

$$(1111) \rightarrow 1111 \rightarrow 1111 \rightarrow \dots$$

$$0000 \rightarrow 0000 \rightarrow 0000 \rightarrow \dots$$

This property is also satisfied.

$\therefore S$ is a cyclic code.

$$G = [I | P]$$

How do we calculate the generator matrix given a generator polynomial?

1st row : Rem $\left[\begin{array}{c} x^{n-1} \\ \hline g(x) \end{array} \right]$

2nd row : Rem $\left[\begin{array}{c} x^{n-2} \\ \hline g(x) \end{array} \right]$

3rd row : Rem $\left[\begin{array}{c} x^{n-3} \\ \hline g(x) \end{array} \right]$

kth row

Rem $\left[\begin{array}{c} x^{n-k+1} \\ \hline g(x) \end{array} \right]$

for a (7,4) cyclic code,

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

$$n = 7, K = 4$$

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

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

$$\begin{array}{r} x^3 + x + 1 \\ \hline x^3 + x + 1) x^6 \\ \oplus x^6 + x^4 + x^3 \\ \hline x^4 + x^3 \\ \oplus x^4 + x^2 + x \\ \hline x^3 + x^2 + x \\ \oplus x^3 + x + 1 \\ \hline x^2 + 1 \end{array} = [1 \ 0 \ 1]$$

$$\begin{bmatrix} 1 & 1 & 0 \end{bmatrix} = \frac{1}{1+x+\epsilon^2 x}$$

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

$$\begin{array}{r} x^2 + 1 \\ \hline x^3 + x + 1) x^5 \\ - x^5 - x^3 - x^2 \\ \hline x^3 + x^2 \\ - x^3 - x - 1 \\ \hline x^2 + x + 1 \end{array}$$

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

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

$$\begin{array}{r} x \\ \hline x^3 + x + 1) x^4 \\ - x^4 - x^2 - x \\ \hline x^2 + x \end{array}$$

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

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

$$\begin{array}{r} 1 \\ \hline x^3 + x + 1) x^3 \\ - x^3 - x - 1 \\ \hline x + 1 \end{array} = [0 \ 1 \ 1]$$

Transpose of column columns

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

base has no unique unique set

set of prime sets being given

Set up a (a) binary pair where

$a_1 \oplus a_2 \oplus a_3 \oplus a_4 = 0$

(a) $b^x \oplus c^x$ which is $a_1 \oplus a_2$

and (c) $b^x \oplus d^x$ which is $a_3 \oplus a_4$

and (d) $c^x \oplus d^x$ which is $a_1 \oplus a_4$

and (e) $b^x \oplus c^x \oplus d^x$ which is $a_1 \oplus a_2 \oplus a_3 \oplus a_4$

$b^x + c^x + d^x = (a_1 + a_2 + a_3 + a_4)$

$b^x + c^x + d^x = (a_1 + a_2 + a_3 + a_4)$

$b^x + c^x + d^x = (a_1 + a_2 + a_3 + a_4)$

$b^x + c^x + d^x = (a_1 + a_2 + a_3 + a_4)$

$b^x + c^x + d^x = (a_1 + a_2 + a_3 + a_4)$

$b^x + c^x + d^x = (a_1 + a_2 + a_3 + a_4)$

$b^x + c^x + d^x = (a_1 + a_2 + a_3 + a_4)$

$b^x + c^x + d^x = (a_1 + a_2 + a_3 + a_4)$

$b^x + c^x + d^x = (a_1 + a_2 + a_3 + a_4)$

$b^x + c^x + d^x = (a_1 + a_2 + a_3 + a_4)$

$b^x + c^x + d^x = (a_1 + a_2 + a_3 + a_4)$

$b^x + c^x + d^x = (a_1 + a_2 + a_3 + a_4)$

$b^x + c^x + d^x = (a_1 + a_2 + a_3 + a_4)$

$b^x + c^x + d^x = (a_1 + a_2 + a_3 + a_4)$

$b^x + c^x + d^x = (a_1 + a_2 + a_3 + a_4)$

$b^x + c^x + d^x = (a_1 + a_2 + a_3 + a_4)$

$b^x + c^x + d^x = (a_1 + a_2 + a_3 + a_4)$

$b^x + c^x + d^x = (a_1 + a_2 + a_3 + a_4)$

Generator matrix for a systematic cyclic code.

- In a systematic cyclic code, the first k digits = 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

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

e.g.

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

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

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

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

$$p(x) = 1$$

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

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

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

Similarly

$$d(x) = c(x)$$

$$1000 \quad | \quad x^6 + x^2 + x = [1000110]$$

$$0100 \quad | \quad x^5 + x + 1 = [0100011]$$

$$0010 \quad | \quad x^4 + x^2 + x + 1 = [0010111]$$

$$0001 \quad | \quad x^3 + x^2 + 1 = [0001101]$$

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

$$\text{Now } c = d \cdot G$$

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

Hamming code for 8 bits

data	Code
1111	1111111 = (x) 56
1110	1110010
1101	+ 1101000
1100	1100101
1011	1011100 = (x) 32
1010	1010001
1001	1001011
1000	1000110
0111	= 0111001
0110	0110100
0101	+ 0101110
0100	0100011
0011	0011010
0010	0010111
0001	0001101
0000	0000000

Hamming code for 8 bits

Wieso ist die Abstand 3 mit genau
einem bit fehler detektierbar?

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.

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

$$R = 1001000$$

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

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

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

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

Syndrome is not zero

\therefore Received sequence ~~is~~ contains errors.

Error patterns for Correction of Identified errors:-

$$P(x) + (S(x))$$

Errors patterns.	Error Polynomial	$S(x) + \text{Syndrome}$	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

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

$S(x) = x^2 + x$ which corresponds to
 $e(x) = x^4$

Goppa Codes - Syndrome Calculation

$$C(x) = R(x) + e(x)$$

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

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

$$= 1011000$$

↑
1st error bit

1st error bit

$$011 \quad x + \epsilon x \quad 011 \quad x \quad 000100$$

$$100 \quad \text{in syndrome} \quad 100 \quad x^2 + \epsilon x^2 \quad 000100$$

$$001 \quad \epsilon x \quad x^2 + \epsilon x^2 \quad 001000$$

$$010 \quad \epsilon x^2 \quad x^2 + \epsilon x^2 \quad 000000$$

$$100 \quad x^6 + x^3 \quad 1 \quad 1 \quad 100000$$

$$101 \quad x^4 + \epsilon x^4 \quad 1 \quad 1 \quad 100000$$

$$100 \quad x^6 + x^3 \quad 1 \quad 1 \quad 100000$$

$$101 \quad x^4 + \epsilon x^4 \quad 1 \quad 1 \quad 100000$$

$$100 \quad x^6 + x^3 \quad 1 \quad 1 \quad 100000$$

$$101 \quad x^4 + \epsilon x^4 \quad 1 \quad 1 \quad 100000$$

$$100 \quad x^6 + x^3 \quad 1 \quad 1 \quad 100000$$

$$101 \quad x^4 + \epsilon x^4 \quad 1 \quad 1 \quad 100000$$

$$100 \quad x^6 + x^3 \quad 1 \quad 1 \quad 100000$$

$$101 \quad x^4 + \epsilon x^4 \quad 1 \quad 1 \quad 100000$$

$$100 \quad x^6 + x^3 \quad 1 \quad 1 \quad 100000$$

$$101 \quad x^4 + \epsilon x^4 \quad 1 \quad 1 \quad 100000$$

$$100 \quad x^6 + x^3 \quad 1 \quad 1 \quad 100000$$

$$101 \quad x^4 + \epsilon x^4 \quad 1 \quad 1 \quad 100000$$

$$100 \quad x^6 + x^3 \quad 1 \quad 1 \quad 100000$$

$$101 \quad x^4 + \epsilon x^4 \quad 1 \quad 1 \quad 100000$$