Cyclic Codes

$C \rightarrow$ Code (Codebook)

$\bar{c} \rightarrow$ codeword (n-tuples)

$\bar{c} = (c_{n-1}\ c_{n-2} \ldots c_0)$

A cyclic leftward shift of $\bar{c}$ is $\bar{c}'$

$\bar{c}' = (c_{n-2}\ c_{n-3} \ldots c_0\ c_{n-1})$

A cyclic leftward shift of $\bar{c}'$ is $\bar{c}''$

$\bar{c}'' = (c_{n-3} \ldots c_0\ c_{n-1}\ c_{n-2})$

- A cyclic code is a linear code that has the property that a cyclic shift on any of its codewords produces another codeword. The cyclic shift may be leftward or rightward by any number of places.

Ex° $C = \{000, 110, 101, 011\}$

C is a cyclic code

$101 \rightarrow 110$

Ex° $C = \{0000000, 1011100, 0101110, 0010111, 1110010, 0111001, 1001011, 1100101\}$

C is a cyclic code.

i.e, $\bar{c} = (1001011) \in C$ any right or leftward shifted $\bar{c}$ is also $\in C$

Polynomials

An n-bit word $(a_{n-1}\ a_{n-2}\ \dots\ a_0)$ can be represented by the polynomial

$$p(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_2x^2 + a_1x + a_0$$

Ex:

$$0110010 \rightarrow p_1(x) = 0x^6 + 1x^5 + 1x^4 + 0x^3 + 0x^2 + 1x + 0x^0$$
$$= x^5 + x^4 + x$$

$$001011 \rightarrow p_2(x) = x^3 + x + 1$$

$p_1(x)$ has degree 5
$p_2(x)$ has degree 3

Polynomials can be added, multiplied & divided

$$p(x) = p_1(x)\,p_2(x) \quad , \quad p(x) = p_1(x) + p_2(x)$$

$$p(x) = p_1(x) / p_2(x)$$

Exercise:- Divide $x^{12} + x^7 + x^4 + x^3 + 1$ by $x^3 + x^2 + 1$

Ex:

$$p_1(x) = x^5 + x^3 + x^2 + 1 \qquad p_2(x) = x^2 + 1$$

Divide $p_1(x)$ by $p_2(x)$

Sln:

$$\begin{array}{r|l} x^3+1 & x^2+1 \\ \hline x^5+x^3+x^2+1 & \\ -x^5+x^2 & \\ \hline x^3+1 & \\ -x^3+1 & \\ \hline 0\ \ 0 & \end{array}$$

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

(77)

Notation:

$$r(x) = R_{p(x)}(p_1(x)) \longrightarrow$$ remainder polynomial when $p_1(x)$ is divided by $p(x)$

A cyclic shift of an n-bit word can be represented in terms of polynomials

$$p(x) = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

$$p'(x) = a_{n-2}x^{n-2} + \cdots + a_0 x + a_{n-1}$$

$$p'(x) = R_{x^n+1}(x\,p(x))$$

$p'(x)$ is given by the remainder of $xp(x)$ when divided by x^n+1

Ex:

101100 leftward shift $\longrightarrow x^5+x^3+x^2 = p(x)$

$011001 \longrightarrow x^4+x^3+x^0 = p'(x)$

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

$$p'(x) = x^4 + x^3 + x^0 = R_{x^6+1}(x^6+x^4+x^3)$$

($x^6+x^4+x^3$) $\rightarrow xp(x)$

Remark:

$$p(x) = R_{x^n+1}(p_1(x))$$

$\downarrow$ degree does not exceed $n-1$

Generator Polynomials

For an (n,k) binary cyclic code, the generator polynomial has the form

$$g(x) = g_{n-k}x^{n-k} + g_{n-k-1}x^{n-k-1} + \cdots g_2x^2 + g_1x + g_0$$

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

- The product of $g(x)$ with every polynomial of degree $k-1$ or less generates all the codeword polynomials of an (n,k) cyclic code
- The generator polynomial $g(x)$ is the smallest degree codeword polynomial of a cyclic code and no other codeword polynomial have degree less than or equal to $n-k$. Note that the degree of $g(x)$ is equal to the number of parity check bits of the code.

Encoding Cyclic Codes

bits → word

$\bar{d} = (d_{k-1}\ d_{k-2} \cdots d_0)$ → data bits (dataword)

$g(x)$ → generator polynomial

$d(x)$ → polynomial for dataword

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

$c(x)$ → codeword polynomial

Ex:

(7,4) Hamming code

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

$\bar{d} = (0\,1\,0\,1)$

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

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

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

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

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

$\bar{c} = (0\,1\,0\,0\,1\,1\,1)$ → codeword

This is non-systematic encoding

Systematic Encoding

$\bar{d} = (d_{k-1} \ldots d_1 d_0) \rightarrow d(x) = d_{k-1}x^{k-1} + \ldots + d_1 x + d_0$

$x^{n-k} d(x) = d_{k-1}x^{n-1} + \ldots + d_1 x^{n-k+1} + d_0 x^{n-k}$

↓ corresponds to

$(d_{k-1} \ldots d_0\ \underbrace{0 \ldots 0}_{n-k \text{ zeros}})$

Now divide $x^{n-k} d(x)$ by $g(x)$ to obtain a quotient and remainder

$$x^{n-k} d(x) = q(x) g(x) + r(x)$$

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

By the degree of $r(x)$ it corresponds to the code sequence

$$(0 \cdots 0\ r_{n-k-1} \cdots r_1 r_0) \rightarrow r(x)$$

Now form

$$x^{n-k} d(x) - r(x) = q(x) g(x)$$

Since the left-hand side is a multiple of $g(x)$, it must be a codeword.

$$(d_{k-1} \cdots d_1 d_0 - r_{n-k-1} \cdots - r_1 r_0)$$

↑ codeword in systematic form

In summary (Systematic encoding)

① Multiply $d(x)$ by x^{n-k}

② $r(x) = R_{g(x)}\left(d(x) x^{n-k}\right)$ $\quad d(x) x^{n-k} = q(x) g(x) + r(x)$

③ Add $r(x)$ to $d(x) x^{n-k}$ to get Codeword in systematic form.

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

81

Ex° $d=(0101) \rightarrow d(x)=x^2+1$

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

↓ generator polynomial

systematically encode data polynomial $d(x)$.

S/n°2

① $k=4,\ n=7$

$$d(x)x^{n-k} = (x^2+1)\,x^3$$
$$= x^5+x^3$$

②

$$r(x) = R_{g(x)}\left(d(x)x^{n-k}\right)$$
$$= R_{x^3+x+1}\left(x^5+x^3\right)$$

$$\frac{x^5+x^3}{x^3+x+1} \rightarrow r(x)=x^2 \quad q(x)=x^2$$

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

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

↓

$$c=(\underbrace{0101}_{d}\underbrace{100}_{p})_{1\times 7}$$

Decoding Cyclic Codes

$r(x)$ → received word polynomial

$g(x)$ → generator polynomial

The syndrome polynomial of $r(x)$ is defined as

$$s(x) = R_{g(x)}[r(x)]$$

For a codeword polynomial $c(x)$

$$s(x) = R_{g(x)}[c(x)]$$

$$= 0$$

If $r(x)$ represents a codeword polynomial containing errors then

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

$$s(x) = R_{g(x)}[r(x)]$$

$$= R_{g(x)}[c(x) + e(x)]$$

$$= R_{g(x)}[c(x)] + R_{g(x)}[e(x)]$$

$$= 0$$

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

(8)

Consider a codeword polynomial $c(x)$ incurring an error polynomial $e(x)$ such that the input to the decoder is $r(x)$. The syndrome polynomial is determined using $s(x) = R_{g(x)}[r(x)]$

and the error polynomial denoted by $\hat{e}(x)$ corresponding to $s(x)$ is read from the syndrome table. Adding $\hat{e}(x)$ to $r(x)$ gives

$$\hat{c}(x) = r(x) + \hat{e}(x)$$

the estimated codeword polynomial for $c(x)$.

Ex°: Generator polynomial for (7,4) code is $g(x) = x^3 + x + 1$

Syndrome table for the (7,4) code

e	e(x)	s(x)
0000000	0	0
0000001	1	1
0000010	x	x
0000100	x^2	x^2
0001000	x^3	$x+1$
0010000	x^4	x^2+x
0100000	x^5	x^2+x+1
1000000	x^6	x^2+1

Factors of x^n+1

We now ask whether any polynomial can be used to generate a cyclic code, and if not, then what characteristics must a polynomial have such that it can generate a cyclic code.

Answer is:

A polynomial $g(x)$ with degree r generates an (n,k) cyclic code, where $k=n-r$, if $g(x)$ divides x^n+1.

If $g(x)$ divides x^n+1

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

If x^n+1 is factored as

$$x^n+1=f_1(x)\,f_2(x)\cdots f_m(x)$$

then $g(x)$ can be chosen as any product of $f_i(x)$ $i=1\ldots m$

Ex: If $x^3+1=(x+1)(x^3+x^2+1)(x^3+x+1)$

then $g(x)$ can be chosen as

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

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

Ex^o Given that $x^9+1=(x+1)(x^2+x+1)(x^6+x^3+1)$

Determine the cyclic codes with blocklength 9.

i.e, $(9,k)$

n fixed, k may change

Degree of $g(x)$ is $n-k$

If $g(x)$ is chosen of $g(x)=x+1$ then $k=8 \to (9,8)$

" " " " " $g(x)=x^2+x+1$ then $k=7 \to (9,7)$

" " " " " $g(x)=x^6+x^3+1$ then $k=3 \to (9,3)$

" " " " " $g(x)=(x+1)(x^2+x+1)$ then $k=6 \to (9,6)$

" " " " " $g(x)=(x+1)(x^6+x^3+1)$ then $k=2 \to (9,2)$

" " " " " $g(x)=(x^2+x+1)(x^6+x^3+1)$ then $k=1 \to (9,8)$

Parity check polynomial's

Given the generator polynomial $g(x)$

parity check polynomial is found from

$$g(x)h(x)=x^n+1$$

where $h(x)$ is the parity check polynomial

The parity check polynomial can be written as

$$h(x)=h_k x^k+h_{k-1}x^{k-1}+\cdots+h_2x^2+h_1x^1+h_0=1$$

Ex: (7,4) code with generator polynomial

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

parity-check polynomial is found of

$$h(x) = \frac{x^7+1}{x^3+x+1} \longrightarrow h(x) = x^4 + x^2 + x + 1$$

Consider encoding $d(x)$

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

$$c(x)\, h(x) = d(x)\, \underbrace{g(x)\, h(x)}_{x^n+1}$$

$$R_{x^n+1}\left[c(x)\, h(x)\right] = 0$$

$$s(x) = R_{g(x)}\left[r(x)\right] \qquad r(x) = c(x) + e(x)$$

$\Leftrightarrow$ $r(x)$ is divided by $g(x)$ and remainder is taken

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

division of $r(x)$ by $g(x)$ equals to multiplication of $r(x)$ by $h(x)$ and then taking its division by x^n+1

Thus syndrome polynomial can also be computed as

$$S(x) = R_{x^n+1}[r(x)h(x)]$$

Comparison between Linear Codes & Cyclic Codes

Linear Codes	Cyclic Codes
$C = dG$	$c(x) = d(x)g(x)$
$GH^T = 0$	$R_{x^n+1}[g(x)h(x)] = 0$
$cH^T = 0$	$R_{x^n+1}[c(x)h(x)] = 0$
$S = rH^T$	$S(x) = R_{x^n+1}[r(x)h(x)]$
	or $S(x) = R_{g(x)}[r(x)]$

Dual Cyclic Codes

The parity-check polynomial of a code C can be used to generate another code referred to as the dual code of C. This is achieved first defining the reciprocal polynomial $h^*(x)$ of $h(x)$ as

$h^*(x) = x^r h(1/x)$ where r is the degree of $h(x)$. The generator polynomial of the dual code is $g(x) = h^*(x)$

Ex: The generator polynomial of (7,4) code is $g(x) = x^3 + x + 1$

The parity-check polynomial is

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

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

The generator polynomial of the dual code is

$$g(x) = x^n h\left(\frac{1}{x}\right)$$

$$= x^4\left(\frac{1}{x^4} + \frac{1}{x^2} + \frac{1}{x} + 1\right)$$

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

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